Electronic version
http://www.tsouanas.org/fmcbook/

WORK IN PROGRESS

Matemática Fundacional

para Computação

Thanos Tsouanas
Universidade Federal do Rio Grande do Norte

2025-10-15
924 minutes past midnight,
Rio Grande do Norte, Brasil

Instituto Metrópole Digital
Universidade Federal do Rio Grande do Norte

Please report errors by email or via the book's github page:
thanos@tsouanas.org
https://github.com/tsouanas/fmcbook/issues

Escrito em português ~~do Brasil~~ do Θάνος.

Typeset in TEX with the ΘάTEX package;
built with the XΗTEX engine.

CONTEÚDO CURTO

Preface **17**

1. Introduções **19**

2. Demonstrações **52**

3. Os inteiros **67**

4. Recursão; indução **153**

5. Combinatória enumerativa **205**

6. Os reais **222**

7. Tipos **275**

8. Coleções **284**

9. Funções **337**

10. Relações **432**

11. Teoria dos grupos **474**

12. Estruturas algébricas **555**

13. O paraíso de Cantor **572**

14. Posets; reticulados **604**

15. Teoria das categorias **616**

16. Teoria dos conjuntos **618**

17. Espaços métricos **664**

18. Topologia **669**

19. Teoria dos tipos **680**

20. Lambdas e combinadores **681**

21. Semântica denotacional **683**

22. Teasers **684**

A. Demonstrações completas **689**

Onde tu prometes estudar estas demonstrações apenas depois de ter tentado escrever tuas próprias, baseadas nos esboços que tem no texto.

B. Dícas **704**

Onde tu prometes consultar as dicas apenas depois de ter tentado resolver a atividade sem elas.

C. Resoluções **758**

Onde tu prometes estudar as resoluções apenas depois de ter consultado todas as dicas disponíveis no appêndice anterior.

Referências **885**
Glossário de símbolos **897**
Índice de pessoas **907**
Índice geral **909**

CONTEÚDO DETALHADO

Preface 17

Como ler este texto 17
Sobre o leitor 17

1. Introduções 19

§1. Proposições vs. objetos 19
§2. Igualdade vs. equivalência 20
§3. Type erros 22
§4. Definições 22
§5. Intensão vs. extensão 27
§6. Variáveis 29
§7. Tipos de números 36
§8. Números, numerais, dígitos 37
§9. Conjuntos, funções, relações 38
§10. Teoremas e seus amigos 40
§11. Demonstrações 41
§12. Axiomas e noções primitivas 42
§13. Expressões de aritmética 43
§14. Expressões aritméticas: sintaxe vs. semântica 43
§15. Linguagem vs. metalinguagem 45
§16. Abreviações e açúcar sintáctico 46
§17. Árvores de derivação 47
§18. Mais erros 48
§19. Nível coração e palavras de rua 50
Leitura complementar 51

2. Demonstrações 52

§20. Demonstrações, jogos, programas 52
§21. Atacando a estrutura lógica duma proposição 56
§22. Igualdade 57
§23. Real-life exemplos: divisibilidade 57
§24. Conjunção 58
§25. Implicação 58
§26. Existencial 59
§27. Disjunção 60
§28. Negação 60
§29. Universal 60
§30. Exemplos e contraexemplos 60
§31. Equivalência lógica 61
Intervalo de problemas 61
§32. Ex falso quodlibet 61
§33. Feitiço: LEM 61
§34. Feitiço: RAA 63
§35. Feitiço: Contrapositivo 63
§36. Feitiço: NNE 63

§37. Feitiço: Disjunção como implicação ... 63
§38. Provas de unicidade ... 63
§39. Mais jargão e gírias ... 63
§40. Erros comuns e falácias ... 64
§41. Deu errado; e agora? ... 66
Problemas ... 66
Leitura complementar ... 66

3. Os inteiros ... **67**

§42. Primeiros passos ... 67
§43. Divisibilidade ... 74
§44. Conjuntos fechados sob operações ... 76
§45. Ordem e positividade ... 79
§46. Mínima e máxima ... 84
§47. Valor absoluto ... 85
§48. Indemonstrabilidade e metateoremas ... 87
Intervalo de problemas ... 88
§49. Wishlist ... 88
§50. O princípio da boa ordem ... 89
§51. Induções ... 90
§52. Somatórios e produtórios iterativos ... 92
§53. Binomial e seus coeficientes ... 96
§54. O lemma da divisão de Euclides ... 98
§55. Expansão e sistemas posicionais ... 98
§56. Quando uma base não é suficiente ... 100
Intervalo de problemas ... 102
§57. Mais sobre conjuntos fechados sob subtração ... 105
§58. Invertíveis, units, sócios ... 106
§59. Desenhando ordens ... 107
§60. Melhor divisor comum ... 108
§61. O algoritmo de Euclides ... 111
§62. Fatoração ... 115
§63. Irredutíveis, primos ... 118
§64. O teorema fundamental da aritmética ... 121
§65. Valuações ... 123
§66. Conjecturas ... 124
Intervalo de problemas ... 125
§67. A idéia da relação de congruência ... 126
§68. Duas definições quase equivalentes ... 126
§69. Aritmética modular ... 129
§70. Inversos e cancelamentos ... 130
§71. Exponenciação ... 133
§72. Resolvendo umas congruências ... 134
§73. O teorema chinês do resto ... 134
§74. Critéria de divisibilidade ... 139
Intervalo de problemas ... 140
§75. Umas idéias de Fermat ... 141
§76. Primalidade ... 143
§77. Geração de primos ... 144
§78. Sistemas de resíduos ... 146
§79. Euler entra ... 147
Intervalo de problemas ... 149

§80. Criptografia ... 150
§81. Assinaturas digitais ... 151
§82. Funções hash ... 151
Problemas ... 151
Leitura complementar ... 151

4. Recursão; indução ... **153**

§83. Os Nats ... 153
§84. Pouco de setup ... 157
§85. Definindo funções recursivamente ... 158
§86. Demonstrando propriedades de naturais sem indução ... 161
§87. Indução ... 164
§88. Demonstrando propriedades de naturais com indução ... 167
§89. Por que aceitar o princípio da indução? ... 173
§90. Ordem nos naturais ... 174
Intervalo de problemas ... 175
§91. Abusando tipos e seus habitantes ... 177
§92. Os Bools ... 177
§93. Internalização de conceitos ... 177
§94. O Unit ... 178
§95. O Empty ... 179
§96. O ListNat ... 179
§97. Princípio da indução estrutural ... 180
Intervalo de problemas ... 180
§98. Listas ... 180
§99. Destrutores ... 181
§100. Dois lados da mesma moeda ... 182
§101. Umas funções de ordem superior ... 183
§102. Polimorfísmo ... 186
§103. Somatórios e produtórios ... 186
Intervalo de problemas ... 186
§104. Tipos de Maybe ... 187
§105. Tipos de Either ... 187
§106. Produtos, somas, etc. ... 187
Intervalo de problemas ... 187
§107. Functors ... 188
§108. Árvores ... 191
§109. Ordenando ... 193
§110. Um toque de complexidade ... 193
§111. Eficiênia via indução ... 195
§112. Eficiênia via álgebra ... 197
§113. Folding ... 197
Problemas ... 197
§114. A notação BNF ... 197
Problemas ... 200
§115. Uma linguagem de numerais binários ... 201
§116. Tipos de expressões ... 201
§117. Uma pequena linguagem de programação ... 202
§118. Indução em tal coisa ... 202
Intervalo de problemas ... 203
Problemas ... 204
Leitura complementar ... 204

5. Combinatória enumerativa 205

§119. Princípios de contagem 205
§120. Permutações e combinações 206
§121. Permutações cíclicas 208
§122. Juntos ou separados 209
§123. Permutações de objetos não todos distintos 209
§124. Número de subconjuntos 211
§125. O triângulo de Pascal 212
§126. Contando recursivamente 214
§127. Soluções de equações em inteiros 215
§128. Combinações com repetições 215
§129. O princípio da inclusão–exclusão 215
§130. Probabilidade elementar 216
§131. Desarranjos 216
§132. O princípio da casa dos pombos 216
§133. Funções geradoras e relações de recorrência 216
Problemas 216
Notas históricas 221
Leitura complementar 221

6. Os reais 222

§134. Construindo os racionais 222
§135. De volta pra Grécia antiga: racionais e irracionais 222
§136. A reta real 223
§137. Primeiros passos 223
§138. Subconjuntos notáveis e inaceitáveis 228
§139. Ordem e positividade 229
§140. Valor absoluto 232
§141. Conjuntos de reais 233
§142. Mínima e máxima 235
§143. Seqüências 236
§144. Uniões e interseções 239
§145. Operações e relações entre seqüências 240
§146. Os reais naturais 241
§147. Sobre modelos 242
Intervalo de problemas 243
§148. Infimum e supremum 243
§149. Epsilons 246
§150. Distância 247
§151. Limites 250
§152. Limites e a estrutura atual 256
§153. Seqüências autoconvergentes 259
Intervalo de problemas 262
§154. Completude 262
§155. MCT, NIP, CCC, B–W 264
§156. Propriedades arquimedeanas 266
§157. Raizes 267
§158. Densidades 268
§159. Cardinalidades infinitas 268
§160. Representação geométrica 269
Intervalo de problemas 269
§161. Liminf e limsup 270

§162. Séries ... 270
Intervalo de problemas ... 271
§163. Funções reais ... 272
§164. Convergência pointwise (ponto a ponto) ... 273
Intervalo de problemas ... 273
§165. Os complexos ... 274
§166. Os surreais ... 274
Problemas ... 274
Leitura complementar ... 274

7. Tipos ... **275**

§167. Tipos produto ... 275
§168. Tipos soma ... 277
§169. O tipo Unit ... 279
§170. O tipo Empty ... 280
§171. Tipos função ... 280
§172. Implementações de tipos ... 281
§173. Tipos têm lógica ... 282
§174. Aritmética de tipos ... 282

8. Coleções ... **284**

§175. Conceito, notação, igualdade ... 284
§176. Intensão vs. extensão ... 289
§177. Relações entre conjuntos e como defini-las ... 290
§178. Vazio, universal, singletons ... 291
§179. Oito proposições simples ... 293
§180. Mais set builder ... 295
§181. Operações entre conjuntos e como defini-las ... 296
§182. Demonstrando igualdades e inclusões ... 301
§183. Cardinalidade ... 303
§184. Powerset ... 303
§185. União grande; intersecção grande ... 304
Intervalo de problemas ... 307
§186. Tuplas ... 309
§187. Produto cartesiano ... 312
§188. Implementação de tipo: triplas ... 313
§189. n-tuplas ... 316
§190. Seqüências ... 320
§191. Multisets ... 324
Intervalo de problemas ... 324
§192. Famílias indexadas ... 325
§193. Conjuntos indexados vs. famílias indexadas ... 328
§194. Disjuntos dois-a-dois ... 329
§195. Coberturas e partições ... 329
§196. Traduzindo de e para a linguagem de conjuntos ... 330
§197. Produto cartesiano generalizado ... 330
§198. Conjuntos estruturados ... 333
Problemas ... 334
Leitura complementar ... 336

9. Funções ... **337**

§199. Conceito, notação, igualdade ... 337

§200. Diagramas internos e externos 344
§201. Jecções: injecções, sobrejecções, bijecções 346
§202. Como definir e como não definir funções 349
§203. (Co)domínios vazios 354
§204. Expressões com buracos 355
§205. Um toque de lambda 356
§206. Aplicação parcial 363
§207. Funções de ordem superior 364
§208. Currificação 370
§209. Novas implementações: seqüências e famílias 374
Intervalo de problemas 375
§210. Composição 375
§211. Funções de graça 379
§212. Funções inversas 384
§213. Imagens, preimagens 386
§214. Definições estilo point-free (tácito) 392
Intervalo de problemas 394
§215. Leis de composição 397
§216. Diagramas comutativos 401
§217. Produtos e demais construções 403
§218. Coproduto; união disjunta 406
Intervalo de problemas 409
§219. Funções parciais 409
§220. Fixpoints 410
§221. Definições recursivas 411
Intervalo de problemas 418
§222. Uma viagem épica 419
§223. Retracções e secções 425
§224. Duma resolução para um problema para uma teoria 426
§225. Pouco de cats—um primeiro toque de categorias 427
Problemas 431
Leitura complementar 431

10. Relações 432

§226. Conceito, notação, igualdade 432
§227. Definindo relações 436
§228. Diagramas internos 437
§229. Construções e operações em relações 438
§230. Propriedades de relações 443
§231. Fechos 447
§232. Bottom-up vs. top-down 454
§233. Relações de ordem 456
§234. Relações de equivalência 457
Intervalo de problemas 460
§235. Partições 463
§236. Conjunto quociente 463
§237. Relações recursivas 469
§238. Programação lógica 470
§239. Relações de ordem superior 470
§240. Pouco de cats—categorias e relações 470
Problemas 470
Leitura complementar 473

11. Teoria dos grupos 474

Notas históricas 474
§241. Permutações 475
§242. O que é um grupo? 478
§243. Exemplos e nãœxemplos 482
§244. Primeiras conseqüências 485
§245. Tabelas Cayley 492
§246. Potências e ordens 495
§247. Escolhendo as leis 499
§248. Conjugação de grupo 501
Intervalo de problemas 502
§249. Subgrupos 503
§250. Geradores 508
§251. Um desvio: bottom-up e top-down 513
Intervalo de problemas 515
§252. Congruências e coclasses 516
§253. O teorema de Lagrange 524
§254. Teoria dos números revisitada 527
§255. O grupo quociente 528
§256. Subgrupos normais 537
Intervalo de problemas 539
§257. Simetrias 540
§258. Morfismos 545
§259. Kernel, Image 548
§260. Pouco de cats—categorias e grupos 550
Problemas 552
Leitura complementar 553

12. Estruturas algébricas 555

§261. Semigrupos 555
§262. Monóides 555
§263. Anéis 558
§264. Anéis booleanos 562
§265. Domínios de integridade 563
§266. Corpos 564
§267. Ações 565
§268. Modules 565
§269. Espaços vetoriais 565
§270. Teoria de Galois 566
§271. Reticulados 566
§272. Estruturas não puramente algébricas 568
Problemas 570
Leitura complementar 571

13. O paraíso de Cantor 572

Um pouco de contexto histórico 572
§273. O que é contar e comparar quantidades? 573
§274. Equinumerosidade 574
§275. O que é cardinalidade? 576
§276. Finitos e infinitos; contáveis e incontáveis; jogos para imortais 576
§277. O primeiro argumento diagonal de Cantor 579
Intervalo para hackear 583

§278. O segundo argumento diagonal de Cantor . . . 584
§279. O conjunto de Cantor . . . 586
§280. Umas aplicações importantes da teoria de Cantor . . . 586
Intervalo de problemas: Cantor vs. Reais . . . 588
§281. Procurando bijecções . . . 588
§282. O teorema Cantor–Schröder–Bernstein . . . 589
§283. Procurando injecções . . . 590
§284. Codificações . . . 590
§285. O teorema de Cantor e suas conseqüências . . . 591
§286. As menores infinidades . . . 594
§287. Duas grandes hipoteses . . . 595
§288. Os números transfinitos . . . 595
§289. Um toque de teoria da medida . . . 596
§290. Conseqüências em computabilidade e definabilidade . . . 596
§291. Problemas no paraíso de Cantor: o paradoxo de Russell . . . 598
§292. As soluções de Russell e de Zermelo . . . 599
Problemas . . . 600
Leitura complementar . . . 603

14. Posets; reticulados **604**

§293. Conceito, notação, propriedades . . . 604
§294. Posets de graça: operações e construções . . . 607
§295. Dualidade . . . 610
§296. Mapeamentos . . . 610
§297. Direções . . . 611
§298. Reticulados como posets . . . 611
§299. Reticulados como estruturas algébricas . . . 611
§300. Reticulados completos . . . 612
§301. Fixpoints . . . 612
§302. Elementos irredutíveis . . . 614
§303. Álgebras booleanas . . . 614
§304. Álgebras Heyting . . . 614
§305. Pouco de cats—categorias e posets . . . 614
§306. Teoria de domínios . . . 614
Problemas . . . 614
Leitura complementar . . . 615

15. Teoria das categorias **616**

§307. O que é uma categoria? . . . 616
§308. Exemplos e nãœxemplos . . . 616
§309. Primeiras definições . . . 616
Problemas . . . 616
Leitura complementar . . . 616

16. Teoria dos conjuntos **618**

§310. O princípio da puridade . . . 618
§311. Traduções de e para a FOL de conjuntos . . . 619
§312. Classes vs. Conjuntos (I) . . . 621
§313. Os primeiros axiomas de Zermelo . . . 622
§314. Árvores de construção . . . 628
§315. Fundações de matemática . . . 629
§316. Construindo as tuplas . . . 630

§317. Construindo a união disjunta ... 633
§318. Construindo as relações ... 634
§319. Construindo as funções ... 636
§320. Construindo mais tipos familiares ... 638
§321. Os cardinais ... 638
§322. Classes vs. Conjuntos (II) ... 639
Intervalo de problemas ... 639
§323. O axioma da infinidade ... 641
§324. Construindo os números naturais ... 643
§325. Teoremas de recursão ... 646
§326. Conseqüências de indução e recursão ... 647
§327. Construindo mais números ... 649
Intervalo de problemas ... 652
§328. Mais axiomas (ZF) ... 653
§329. Wosets ... 655
§330. Indução transfinita ... 656
§331. Recursão transfinita ... 656
§332. Os ordinais ... 656
§333. Axiomas de escolha (ZFC) ... 656
§334. Conseqüências desejáveis e controversiais ... 658
§335. Escolhas mais fracas ... 658
§336. Outras axiomatizações ... 658
§337. Um outro ponto de vista ... 658
§338. Outras teorias de conjuntos ... 661
§339. Outras fundações ... 662
Problemas ... 662
Leitura complementar ... 663

17. Espaços métricos ... 664

§340. Distáncias ... 664
§341. Exemplos e nãœxemplos ... 666
§342. Conjuntos abertos e fechados ... 666
§343. Continuidade ... 667
§344. Completude ... 667
§345. Compacidade ... 668
§346. Pouco de cats—categorias e espaços métricos ... 668
Problemas ... 668
Leitura complementar ... 668

18. Topologia ... 669

§347. O que é uma topologia ... 669
§348. Especificações equivalentes ... 669
§349. Uns espaços topológicos ... 671
§350. Noções topológicas ... 671
§351. Continuidade ... 673
§352. Bases ... 674
§353. Construções ... 675
§354. Compacidade ... 676
§355. Conexidade ... 677
§356. Separações ... 677
§357. Convergências ... 678
§358. Pouco de cats—categorias e espaços topológicos ... 679

Problemas 679
Leitura complementar 679

19. Teoria dos tipos 680

Problemas 680
Leitura complementar 680

20. Lambdas e combinadores 681

§359. O λ-calculus não-tipado 681
§360. Representando matemática fielmente 681
§361. Programmando 681
§362. Recursão e fixpoints 681
§363. Programação funcional revisitada 681
§364. Lógica de combinadores 681
Leitura complementar 682
Problemas 682
Leitura complementar 682

21. Semântica denotacional 683

Problemas 683
Leitura complementar 683

22. Teasers 684

§365. Lógica linear 684
§366. Teoria das demonstrações 684
§367. Lógica matemática 684
§368. Teoria da computabilidade 684
§369. Complexidade computacional 685
Leitura complementar 685

A. Demonstrações completas 689

B. Dícas 704

Dícas #1 704
Dícas #2 728
Dícas #3 742
Dícas #4 749
Dícas #5 752
Dícas #6 754
Dícas #7 755
Dícas #8 756
Dícas #9 756
Dícas #10 756

C. Resoluções 758

Referências 885

Glossário de símbolos 897

Índice de pessoas 907

Preface

Como ler este texto

Fight it. Nas palavras do grande Paul Halmos:

> *«Don't just read it; fight it! Ask your own questions, look for your own examples, discover your own proofs. Is the hypothesis necessary? Is the converse true? What happens in the classical special case? What about the degenerate cases? Where does the proof use the hypothesis?»*

Cada demonstração de teorema é marcada com um '∎', conhecido como *Halmos (tombstone)*.[1] Para te motivar a tentar demonstrar os teoremas antes de estudar suas demonstrações, muitas vezes eu apresento apenas um esboço da demonstração, cujo fim eu marco com um '□'. Nesses casos, as demonstrações completas aparecem no apêndice. Eu marco com '►' os itens do texto que precisam ser resolvidos.

Cuidado! Nunca leia matemática passivamente! Umas das demonstrações e definições têm falhas e/ou erros (nesses casos o '∎' torna-se '↯'). Os problemas e exercícios pedem para identificar os erros.

Spoiler alerts. Em certos pontos aparecem "spoiler alerts". Isso acontece quando eu tenho acabado de perguntar algo, ou preciso tomar uma decisão, etc., e seria bom para o leitor pensar sozinho como ele continuaria desse ponto, antes de virar a página e ler o resto.

Dicas e resoluções. Para muitos dos exercícios e problemas eu tenho dicas para te ajudar a chegar numa resolução. Tente resolver sem procurar dicas. Se não conseguir, procure uma primeira dica no apêndice "Dicas #1", e volte a tentar. Se ainda parece difícil, procure segunda dica no "Dicas #2", etc., etc. Finalmente, quando não tem mais dicas para te ajudar, no apêndice tem resoluções completas. Quando tem dicas, no fim do enunciado aparecem numerinhos em parenteses e cada um deles é um link que te leva para a dica correspondente. Não tenho link para a resolução: a idéia é dificultar a vida de quem quer desistir facilmente e procurar logo a resolução.

Sobre o leitor

Prerequisitos. Nada demais: o texto é bastante "self-contained". Supostamente o leitor sente confortável com as propriedades básicas de aritmética, manipulações algébricas, convenções e notação relevante. Idealmente experiência com programação ajudaria entender muitos exemplos e metáforas que uso para explicar uns conceitos matemáticos,

[1] A idéia é que conseguimos matar nosso alvo com nossa demonstração, e logo mostramos (com orgulho) o seu túmulo!

mas quem não programou nunca na vida ainda consegue acompanhar. Se esse é o teu caso, sugiro começar a aprender ambas as artes de *demonstrar* e de *programar* em paralelo, até chegar na conclusão que não se trata de duas artes mesmo, mas sim da mesma, só com roupas diferentes.

CAPÍTULO 1

INTRODUÇÕES

Sim, plural: neste capítulo intoduzo todas as noções e idéias básicas com a profundidade mínima—e logo com umas mentiras também, e logo com uns erros—para começar aprofundar nos próximos capítulos. Se encontrar alguma notação, algum termo, símbolo, processo, etc., que tu não reconhece, continue lendo; o importante é entender bem as idéias básicas. E os detalhes? Depois.

§1. Proposições vs. objetos

Olhando para matemática de longe, podemos enxergar dois tipos principais: *proposições* e *objetos* (também *indivíduos*).[2] O primeiro e mais elementar desafio do meu leitor seria entender essas duas noções, no ponto que nunca confundiria uma por outra.

- **EXEMPLO 1.1 (Objetos).**
Uns exemplos de frases que denotam objetos:
  (1) Brasil
  (2) a mãe do Bart
  (3) $(1+1)^3$
  (4) Évariste Galois
  (5) 8
  (6) Matemática

  Não faz sentido supor nenhuma delas, nem duvidar, nem tentar demonstrar, nem nada disso. Não têm verbo! Imagine alguém dizer:

  «Eu acho que $(1+1)^3$.»

  Tu acha que $(1+1)^3$ o quê?!

- **EXEMPLO 1.2 (Proposições).**
Uns exemplos de frases que denotam proposições:
  (1) Brasil é um país na Europa.
  (2) A mãe do Bart fala português.
  (3) $(1+1)^3 = 3^2 - 1$
  (4) Galois morreu baleado.
  (5) $8 \leq 12$

[2] Para o leitor que já sabe o que é um *sintagma nominal* em lingüística, as expressões que denotam objetos são exatamente os sintagmas nominais.

(6) Matemática estuda cavalos.

Cada uma dessas frases, tem um verbo, e afirma algo completo. Não importa a veracidade dessas proposições, o importante aqui é entender que essas frases realmente são proposições. Faz sentido afirmá-las, questioná-las, demonstrá-la, refutá-las, etc.

! **1.3. Aviso (Expressões que denotam proposições).** Umas expressões matemáticas que normalmente denotam proposições podem assumir um papel diferente dependendo do contexto. Por exemplo, ‘ $x = y$ ’ normalmente denota a proposição “x é igual ao y”; mas se o contexto já tem seu verbo principal, o papel da ‘ $x = y$ ’ pode mudar:

«Por outro lado, _____ é primo e logo . . . »

Aqui, pelo contexto, precisamos algo que denota um objeto: não faria sentido afirmar que uma proposição é primo. Nesse caso a expressão ‘ $x = y$ ’ pode ser lida como qualquer uma das:

$x = y$: “x, que é igual a y,”
$x = y$: “x é igual ao y, e y”.

Assim, a frase

«Por outro lado, $2^n + 1 = 5$ é primo e logo . . . »,

pode ser lida, respectivamente, como qualquer uma das:

«Por outro lado, $2^n + 1$, que é igual a 5, é primo e logo . . . »
«Por outro lado, $2^n + 1$ é igual a 5, e 5 é primo e logo . . . ».

A mesma coisa vale sobre outras notações que vamos encontrar depois: ‘ $x \in A$ ’, ‘ $A \subseteq B$ ’, ‘ $f : A \to B$ ’, etc.

§2. Igualdade vs. equivalência

1.4. Igual ou equivalente?. Usamos os símbolos ‘ $=$ ’ e ‘ $\iff$ ’ para afirmar uma relação especifica entre as coisas que aparecem nos dois lados deles. Só que os *tipos* de coisas são diferentes para cada símbolo. O ‘ $=$ ’ fica entre *objetos*, o ‘ $\iff$ ’ entre *proposições*.

Usamos ‘ $=$ ’ para dizer que os objetos nos seus lados são *iguais*, ou seja, as coisas escritas nos seus dois lados, denotam o mesmo objeto. Por exemplo ‘$1 + 5$’ denota um número e ‘3’ também denota um número, e escrevendo

$$1 + 5 = 3$$

estamos afirmando—erroneamente nesse caso—que as duas expressões denotam o mesmo número. Se tivesse escrito ‘$1 + 5 = 3 + 3$’ teria sido uma afirmação correta. Pronunciamos o ‘$A = B$’ como «A é igual ao B».

Usamos ‘ $\iff$ ’ para dizer que as proposições nos seus lados são *logicamente equivalentes*, ou seja, são ambas verdadeiras ou ambas falsas. Escrevemos então

$$p \text{ é primo e } p > 2 \iff p \text{ é um primo ímpar}$$

e nesse caso essa é uma afirmação correta. Note que não sabemos dizer qual é o caso aqui: são ambas verdadeiras, ou ambas falsas? Não sabemos qual número é denotado pela variável p, mesmo assim as afirmações são equivalentes. Pronunciamos o '$A \iff B$' como «A é equivalente a B» ou «A se e somente se B», usando a abreviação *sse* para a frase «se e somente se».

Entendemos o '$\implies$' como uma abreviação de «implica» e o '$\impliedby$' como uma abreviação de «é implicado por». Podemos ler as expressões seguintes assim também:

$$A \implies B: \quad \text{«se } A \text{ então } B\text{»} \qquad A \iff B: \quad \text{«}A \text{ se e somente se } B\text{»}.$$

▸ **EXERCÍCIO x1.1.**
Já que '$\iff$' corresponde à frase «se e somente se», faz sentido pensar que uma das setinhas envolvidas ('$\implies$' e '$\impliedby$') corresponde na frase «se» e a outra na «somente se». Qual é qual? (x1.1H0)

▸ **EXERCÍCIO x1.2.**
Mesma pergunta, agora lendo o '$\iff$' como «é suficiente e necessário para». Uma direção corresponde ao «suficiente» outra ao «necessário». Qual é qual? (x1.2H0)

1.5. Lógicas de relevância. Note que seguindo nossa interpretação de implicação e equivalência nos permite corretamente afirmar implicações e equivalências entre proposições que não tem nada a ver uma com outra. Por exemplo, seria correto afirmar:

- $0 = 1$ se e somente se existe número natural maior que todos os outros.
- $1 + 1 = 2 \iff$ Creta é uma ilha grega.
- Se Brasil é um país na Europa, então 4 é um número par.
- Se 4 é um número par, então Grécia é um país na Europa.

Felizmente, afirmações desse tipo raramente aparecem em matemática. Lógicas que tomam cuidado para proibir implicações entre proposições irrelevantes são chamadas *lógicas de relevância* (por motivos óbvios) mas não vamos estudá-las aqui.

1.6. Observação (Subjuntivo). Considere a frase

$$\text{«}n \text{ é par se e somente se existir inteiro } k \text{ tal que } n = 2k\text{»}.$$

Usar o *subjuntivo* «existir» aqui não faz muito sentido: não se trata de algo que futuramente pode acontecer ou não. Ou existe (hoje, ontem, sempre) tal inteiro k ou não existe; daí seria melhor escrever usando o verbo no "modo normal":[3]

$$\text{«}n \text{ é par se e somente se existe inteiro } k \text{ tal que } n = 2k\text{»}.$$

Mas há um ponto de vista filosófico (que tá bem alinhado com a lógica constructiva que analisaremos logo) onde esse subjuntivo faz até sentido numa maneira que pode aparecer meio engraçada: *até o momento que um ser humano vai chegar e mostrar pra mim um tal inteiro k, eu não vou considerar nada sobre a paridade do n.* Se alguém me perguntar *«n é par ou n não é par?»*, eu, sendo intuicionista, vou simplesmente responder: *«Eu não sei.»*. Entretanto, o matemático clássico responderia *«Sim.»*.

[3] também conhecido como *presente do indicativo*

§3. Type erros

1.7. O que é?. Um *type error* ocorre quando usamos uma expressão cujo tipo é incompatível com o tipo esperado pelo contexto. Esse tipo de erro é muito comum quando começamos aprender matemática e infelizmente é completamente destruidor: com um type error nosso texto *nem compila*, nem chega a dizer algo para ter chances de ser avaliado para sua corretude. Um texto com type errors não chega a ter significado nenhum. Chamamos de *mal-tipada* uma expressão que contem type errors.

1.8. O type error mais grave. Claramente o type error mais gritante seria confundir objeto com proposição ou vice versa, pois como discutimos (§1) são os grupos mais distantes.

• **EXEMPLO 1.9.**
Todas as frases seguintes têm o type error mais grave: confusão entre proposição e objeto:

(1) $(x+y)^2 \iff x^2+2xy+y^2$.
(2) $x(a-(b+c)) = xa - x(b+c) \implies xa - xb - xc$.
(3) Concluimos que $(A \subseteq B) = (B \subseteq A)$.
(4) Suponha n. Vamos demonstrar que $n+1$.

(1) Temos uma suposta equivalência entre dois objetos. O '$\iff$' tava esperando ver (receber) proposições nos seus lados, mas recebeu objetos. (2) No lado esquerdo da implicação temos uma proposição, (isso tá OK), mas no seu lado direito aparece um objeto. Não faz sentido implicar um objeto:

- Se chover amanhã, então Maria.
- ... então Maria o quê?!

(3) Aqui aparece igualdade entre duas proposições em vez de objetos. (4) Como assim supor um objeto? E como assim demonstrar um objeto? Supomos proposições, e demonstramos suposições. O que significa supor Alex? O que significa demonstrar o 5?

▸ **EXERCÍCIO x1.3.**
Mude cada uma das frases do Exemplo 1.9 para resolver o type error. Não se preocupe com a *veracidade*. (x1.3H0)

1.10. Refinando mais. Podemos subdividir os objetos em tipos também, por exemplo: números, pessoas, conjuntos de pessoas, palavras, cidades, funções, programas, etc. Sobre proposições, vamos fazer algo parecido no Capítulo 2: conjunções, disjunções, implicações, negações, etc.

§4. Definições

Tanto em matemática quanto fora de matemática, para facilitar nosso pensamento e a comunicação com outras pessoas introduzimos novos termos, e novas notações de certos conceitos, assim evitando a necessidade de descrever em todo detalhe a mesma idéia repetidamente.

1.11. De mente para papel. O processo de definir algo começa na nossa cabeça, onde identificamos—ou pelo menos, achamos que identificamos—um conceito que consideramos interessante e que merece seu próprio nome, sua própria notação, etc. Depois disso começa o processo de *traduzir* nossa idéia, do mundo mental para uma linguagem, freqüentemente sendo uma linguagem natural pouco enriquecida com notação, termos, convenções, etc., para atender as necessidades de matemática. Também precisamos de *escolher um nome bonito* para nossa definição, uma notação conveniente e útil.

1.12. Definição vs. proposição. Para enfatizar que estamos definindo algo, e não afirmando uma equivalência ou uma igualdade, decoramos o símbolo correspondente por um '$\overset{\text{def}}{}$': usamos '$A \overset{\text{def}}{\iff} B$' para *definir a proposição* A para significar a mesma coisa com a proposição B; usamos '$A \overset{\text{def}}{=} B$' para *definir o objeto* A como um novo nome do objeto B. Olhe nisso:

$$\underbrace{\overbrace{A}^{(\text{prop})} \overset{\text{def}}{\iff} \overbrace{B}^{\text{prop}}}_{\text{definição}} \qquad\qquad \underbrace{\overbrace{A}^{\text{prop}} \iff \overbrace{B}^{\text{prop}}}_{\text{afirmação}}.$$

Na '$A \overset{\text{def}}{\iff} B$' estamos *definindo algo:* a expressão A, que vai acabar tendo o significado da proposição B, logo apos dessa definição. Ou seja, na esquerda do '$\overset{\text{def}}{\iff}$' temos uma *futura-proposição*, na sua direita temos uma proposição mesmo. Na '$A \iff B$', estamos *afirmando algo:* que as proposições A, B são equivalentes. Necessariamente então ambas já têm significados conhecidos. Similarmente sobre as

$$\underbrace{\overbrace{A}^{(\text{obj})} \overset{\text{def}}{=} \overbrace{B}^{\text{obj}}}_{\text{definição}} \qquad\qquad \underbrace{\overbrace{A}^{\text{obj}} = \overbrace{B}^{\text{obj}}}_{\text{afirmação}}:$$

a primeira é uma definição, a segunda a afirmação que A, B são iguais.

• **EXEMPLO 1.13.**
Qual a diferença entre as duas expressões?:

$$n \text{ é ímpar} \overset{\text{def}}{\iff} n = 2k+1 \text{ para algum inteiro } k$$
$$n \text{ é ímpar} \iff n = 2k+1 \text{ para algum inteiro } k.$$

Resolução. A primeira linha *é uma definição.* Estamos *definindo* o que significa «ser ímpar», dizendo como traduzir a afirmação «n é ímpar» para uma outra afirmação que supostamente entendemos. A segunda linha *é uma afirmação*: afirma que as duas proposições nos seus lados são equivalentes. Ou seja, é algo que pode ser demonstrado ou refutado. E para usar o '$\iff$' com certeza seus dois lados precisam ser proposições bem-definidas.

1.14. Observação (Convenções). Essa ênfase com o '$\overset{\text{def}}{}$' não é obrigatória, e muitas vezes o contexto é suficiente para deixar claro que se trata de definição e não de afirmação. Note que por convenção a coisa sendo definida vai no lado esquerdo do símbolo que decoramos com esse '$\overset{\text{def}}{}$' e a sua definição fica no lado direito. Então mesmo que nos símbolos '$=$' e '$\iff$' podemos trocar seus lados, nos '$\overset{\text{def}}{=}$' e '$\overset{\text{def}}{\iff}$' não!

1.15. Exemplos e nãœxemplos. Talvez já temos vários *exemplos* de objetos que satisfazem nossa definição, ou nem sabemos se existem tais objetos! Observe então que para definir algo não é necessário—e com certeza nem suficiente!—mostrar exemplos de objetos. Mesmo assim, quando escrevemos um texto matemático e queremos ajudar nosso leitor confirmar seu entendimento da nossa definição, podemos dar uns exemplos e/ou uns *nãœxemplos* (ou seja, objetos que *não* satisfazem nossa definição). Mas é importante entender que a natureza deles nunca é essencial para a definição, e que *eles não fazem parte da definição*. É apenas uma ferramenta pedagógica.

• **EXEMPLO 1.16.**
As afirmações seguintes são todas corretas:

- 41 é um exemplo de: número ímpar[4]
- 18 é um exemplo de: múltiplo de 3
- 16 é um nãœxemplo de: múltiplo de 3
- 16 é um nãœxemplo de: número ímpar

Mas não contam como definição do que significa ser ímpar, ou ser múltiplo de 3.

! **1.17. Cuidado (nãœxemplo vs. contraexemplo).** Não confunda as palavras «nãœxemplo» e «contraexemplo». Um *nãœxemplo* é algo que *não* satisfaz uma definição, que não tem uma propriedade, etc. Por outro lado, quando usamos o termo *contraexemplo*? Apenas quando estamos tentando *refutar* uma afirmação da forma «todos os tais x têm tal propriedade». Qualquer tal objeto x que não possui essa propriedade conta como contraexemplo dessa afirmação. Isso vai ficar mais claro na Secção §30 do Capítulo 2 (onde estudamos demonstrações).

Dando uma definição de algum termo, notação, etc., precisamos deixar claro o que exatamente eles denotam. Considere como exemplo a noção de *primos gêmeos* que aparece em teoria dos números:

• **EXEMPLO 1.18.**
Considere a definição:

$$\text{«Dois números } p, q \text{ são } \textit{primos gêmeos} \text{ sse } p, q \text{ são primos e } |p-q| = 2.\text{»}$$

Dados então dois números a, b, sabemos o que a afirmação "a, b são primos gêmeos" significa:

$$a, b \text{ são primos e } |a-b| = 2.$$

1.19. Contexto. Para definir qualquer coisa precisamos primeiramente deixar claro o *contexto*. No Exemplo 1.18 o contexto é:

$$\begin{aligned} p &: \text{número} \\ q &: \text{número.} \end{aligned}$$

Porém, se a definição fosse «dois números primos p, q são *primos gêmeos* sse $|p-q| = 2$» o contexto seria pouco diferente:

$$\begin{aligned} p &: \text{número primo} \\ q &: \text{número primo.} \end{aligned}$$

[4] sim, acabei de usar a palavra exemplo para dar um exemplo para ajudar entender o que significa exemplo

1.20. O que é tijolo?. No meu primeiro semestre como professor no Brasil, em algum momento—não lembro porquê—um aluno na sua explicação usou a palavra "tijolo". O problema é, que eu nunca tinha encontrado essa palavra antes; então perguntei ao meu aluno:

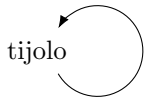
«O que é tijolo?»

Neste momento o aluno sentiu um desafio: como você explica o que é um tijolo para um gringo?[5] Ele precisou dar uma *definição* dessa palavra. A resposta dele foi

«Tijolo é tijolo, ué!»

. . . E isso não me ajudou muito.

1.21. Definições circulares. A resposta do aluno acima é um exemplo duma *definição circular*.



Tenho então uma questão pra ti:

«O que é um conjunto?»

Uma resposta razoável neste momento seria a seguinte:

«Um conjunto é uma colecção de objetos.»

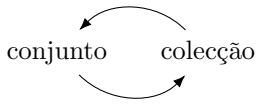
E, se eu sei o que significa «colecção» eu vou entender o que é um conjunto e vou ficar feliz; mas caso contrário, eu vou perguntar:

«E o que é uma colecção?»

Provavelmente aquele aluno que me ensinou o que é "tijolo" ia responder:

«Uma colecção é um conjunto de objetos.»

Aqui o problema é o mesmo com o "tijolo", só que um tiquinho menos óbvio, pois o cíclo aqui pelo menos tem duas setinhas:



Pensando numa forma computacional, entendemos essa definição como um programa cuja execução caiu num *loop infinito*. Como ele nunca termina, nos nunca sabemos se um objeto satisfaz ou não essa definição.

1.22. Teaser (Definições recursivas). Alguém pode pensar que o problema com as definições circulares é que a palavra que estamos definindo apareceu na sua própria definição. Isso *não* é o caso! Numa *definição recursiva* a palavra que queremos definir parece aparacer dentro da sua própria definição, e mesmo assim, não estamos caindo num loop infinito, e realmente conseguimos definir o que queremos. Mas bora deixar esse assunto para depois, quando com pouco mais experiência vamos trabalhar com recursão.

[5] O aluno não falava inglês—nem grego!—e logo a gente não tinha uma linguagem "fallback" para usá-la e tirar minha dúvida.

1.23. Erros em definições. Pode ser que para algum erro uma suposta definição acaba não definindo nada pois seu texto não conseguiu descrever nenhum conceito. Ou, pode ser que acabou definindo algo mesmo, só que esse algo não é o que queríamos definir!

• **EXEMPLO 1.24 (definição errada que nem compila).**
Considere a definição seguinte:

> Definição. Seja n um inteiro. Chamamos o n de *par* se e somente se $n = 2k$.

Essa definição *nem compila*. Por quê?
RESOLUÇÃO. O compilador reclamaria com a mensagem

> Usou 'k' mas 'k' não está declarado aqui.

Para esclarecer mais a situação, vamos testar a afirmação «6 é par». Abrindo a definição temos que «6 é par» significa «$6 = 2k$». Ou seja, basta verificar se realmente $6 \stackrel{?}{=} 2k$. Mas nessa afirmação está sendo referido um objeto 'k' que nunca foi declarado (nem definido). *Quem é esse k?* Ninguém sabe. Não faz sentido então afirmar nada que envolve 'k'.

• **EXEMPLO 1.25 (definição errada que compila).**
Considere a definição seguinte:

> Definição. Seja n um inteiro. Chamamos o n de *par* se e somente se $n = 2k$ para qualquer inteiro k.

Essa definição "compila". Mas o conceito que foi definido não é o que o seu escritor tinha no coração dele.

▸ **EXERCÍCIO x1.4.**
Por quê? Qual o problema com a definição do Exemplo 1.25? Como podemos consertar? (x1.4H0)

1.26. O que é "bem-definido"?. Essa frase deixa muita gente confusa em matemática. Realmente fica estranho pedir para teu leitor demonstrar, por exemplo, que um tal símbolo, notação, função, não foi bem-definida. Como assim? Se não foi bem-definida, como que estamos usando sua notação então? A idéia nesse caso seria explicar exatamente o porquê que o compilador reclamaria na sua definição. Em geral, o erro fica na falta de determinicidade: *fingimos* que determinamos um certo objeto que nomeamos numa certa forma, mas na verdade deixamos muita liberdade (ambigüidade) no nosso leitor, pois vários objetos satisfazem essa condição, então nossa descripção *não determinou* um objeto. No outro extremo, pode ser que nenhum objeto satisfaz a condição, então é como se a gente tentou dar nome para algo que nem existe.

1.27. A importância das definições. Superficialmente alguém pode pensar que "não existe definição errada". Ficando no pé da letra seria difícil convencer esse alguém que ele não tem razão. Mas muitas vezes dar as definições "certas" é o que te permite demonstrar um teorema difícil que seria inatacável sem elas. Uma definição deve ser escrita na maneira mais simples possível para entender e usar. E deve capturar um conceito interessante. Tendo as definições corretas, raciocinamos melhor, e conseguimos formular nosso pensamento numa forma curta e entendível. Com prática, vamos conseguir identificar quando faria sentido definir um termo novo, dar uma definição elegante e correta, e escolher um nome bom, e se for útil uma notação conveniente também.

1.28. Comparação com programação. Enquanto programando, para muitos programadores a parte mais desafiadora (e divertida) é *inventar os nomes corretos*[6] para partes dos seus programas. Em muitas linguagens existe um *entry point* para teu programa, onde a execução começa. Por exemplo, em C isso seria o corpo da função `main`. Seria bizarro (no mínimo) tentar escrever um programa inteiro apenas usando os primitivos da C dentro dessa função `main`. Felizmente as linguagens oferecem ferramentas de abstracção para o programador—umas bem mais que outras—e assim começamos definindo nossos próprios conceitos: funções, variáveis, constantes, tipos, etc.

§5. Intensão vs. extensão

1.29. Muitas vezes é útil diferenciar entre a intensão e a extensão de expressões que denotam tanto objetos quanto proposições. Considere a frase *a mãe de Thanos*, que denota a minha mãe mesmo, *Styliani*. Agora vamos supor para esse exemplo que minha mãe é *a reitora da UFRN*. Temos três expressões que denotam o mesmo objeto: mainha. Alguém diria que

$$\textit{a mãe de Thanos} \;=\; \textit{a reitora da UFRN} \;=\; \textit{Styliani}.$$

Realmente a *extensão* dessas três frase é a mesma. Mas a *intensão* é diferente: é uma coisa ser a mãe de Thanos, outra coisa ser a reitora da UFRN, e outra coisa ser a Styliani. Para enfatizar que não faz sentido tratar as três frases como *iguais*, considere as frases seguintes:

> «Eu não sabia que a mãe de Thanos é a reitora da UFRN.»
> «A mãe de Thanos é Styliani, mas não sei quem é a reitora da UFRN.»

Agora, supondo que realmente são iguais essas frases, tente trocar uma por outra e tu vai descobrir que o significado muda bastante; uns exemplos:

> «Eu não sabia que Styliani é a mãe de Thanos.»
> «Eu não sabia que a mãe de Thanos é a mãe de Thanos.»
> «A reitora da UFRN é Styliani, mas não sei quem é a mãe de Thanos.»

As extensões são iguais pois todas essas frases denotam o mesmo objeto, mas as intensões não. Nesse exemplo usei um objeto (Styliani) para explicar a diferença entre igualdade intensional e extensional. A mesma idéia aplica se entre *equivalência* intensional e extensional. Considere a equivalência entre as proposições que cada uma afirma algo sobre um número x:

$$x \text{ é primo e par} \iff \text{uma molécula de água tem } x \text{ átomos de hidrogênio} \iff x = 2$$

Sim, as proposições são equivalentes extensionalmente: ambas são verdadeiras ou ambas são falsas. Mas a intensão de cada proposição é bem diferente. Considere dado um número x. Para decidir se a primeira é verdadeira precisamos saber o que significa número primo, o que significa número par, e também saber responder sobre nosso x se satisfaz ambas essas definições. Para a segunda, precisamos saber pouca coisa de química: H_2O é a molécula da água. Finalmente para a terceira não precisamos nenhum conhecimento (além de reconhecer a constante '2' como um nome do número dois), pois afirma diretamente que x é o número 2.

---

[6] Ou até *descobrir os nomes escondidos*, dependendo do caso e do ponto de vista, para enfatizar!

D1.30. Notação. Em matemática os símbolos '$=$' e '$\iff$' são usados na maneira extensional: '$A = B$' significa que A e B denotam o mesmo objeto; '$A \iff B$' significa que as proposições A, B são logicamente equivalentes. Para diferenciar entre intensional e extensional, adicionamos mais uma linha nos símbolos correspondentes: usamos '$\equiv$' para igualdade intensional e '$\iff$' para equivalência intensional.

1.31. Observação (Definição e intensão). A partir duma definição

$$A \overset{\text{def}}{\iff} B$$

as expressões A e B não são apenas extensionalmente (logicamente) equivalentes, mas intensionalmente também: definimos o A para ter o próprio significado (intensão) de B. Então depois da definição acima claro que temos

$$A \iff B$$

mas, ainda mais, temos

$$A \iff B.$$

Parece então que em vez de '$\overset{\text{def}}{\iff}$' deveriamos decorar o '$\iff$' com o '$_{\text{def}}$' mas não precisamos fazer isso pois já o fato que é uma definição implica que as expressões nos dois lados vão ter até a mesma intensão![7] Mesma coisa sobre o '$\overset{\text{def}}{=}$'.

1.32. Conselho (Compare os algoritmos). Uma dica para decidir se os dois lados são intensionalmente iguais ou equivalentes é *comparar os algoritmos* em vez dos seus resultados. Olhe para cada lado e considere o algoritmo que alguém precisaria executar para achar seu valor (se é objeto) ou para verificar sua veracidade (se é proposição). Se os algoritmos são os mesmos, temos igualdade (ou equivalência) intensional. Se os seus resultados são os mesmos, temos igualdade (ou equivalência) extensional.

▸ **EXERCÍCIO x1.5.**
Verdadeiro ou falso?:

(i) se $A \equiv B$ então $A = B$;
(ii) se $A \iff B$ então $A \iff B$.

Observe que para cada uma dessas afirmações fazer sentido os A, B denotam objetos na primeira, mas proposições na segunda. (x1.5H0)

▸ **EXERCÍCIO x1.6.**
Para cada um par de expressões escolha a melhor opção dos:

$$\iff, \quad \iff, \quad \equiv, \quad =.$$

Observe que as versões intensionais são mais fortes que as extensionais, então quando aplica a versão intensional, precisa escolhé-la.

(1) $\begin{cases} 2 \cdot 3 \\ 6 \end{cases}$
(2) $\begin{cases} 2 \cdot 3 \\ 3 \cdot 2 \end{cases}$

[7] Assim não vamos precisar de escrever '$\overset{\text{def}}{\iff}$'.

(3) $\begin{cases} x \text{ ama } y \\ y \text{ é amado por } x \end{cases}$

(4) $\begin{cases} n \text{ é par} \\ \text{existe } k \in \mathbb{Z} \text{ tal que } n = 2k \end{cases}$

(5) $\begin{cases} \text{Matheus mora na capital do RN} \\ \text{Matheus mora na maior cidade do RN} \end{cases}$

(6) $\begin{cases} \text{a capital da Grécia} \\ \text{Aténas} \end{cases}$

(7) $\begin{cases} \text{o vocalista da banda Sarcófago é professor da UFMG} \\ \text{Wagner Moura é professor da maior universidade de MG} \end{cases}$

(8) $\begin{cases} \text{Aristoteles foi professor de Alexandre o Grande} \\ \text{Aristoteles ensinou Alexandre o Grande} \end{cases}$

(9) $\begin{cases} \text{A terra é plana} \\ \text{A lua é feita de queijo} \end{cases}$

(10) $\begin{cases} x^2 + y^2 \leq 0 \\ x = y = 0 \end{cases}$

(11) $\begin{cases} x^2 + y^2 \leq 0 \\ 0 \geq x \cdot x + y \cdot y \end{cases}$

(12) $\begin{cases} (x^2 + y^2)^2 \\ (x \cdot x + y^2)(x^2 + y \cdot y) \end{cases}$

(x1.6 H 0)

§6. Variáveis

Vamos usar e estudar variáveis demais. Por enquanto precisas só entender o básico. Esta secção, é esse básico.

1.33. De pronomes para variáveis. Considere as proposições:

(i) «Existe número tal que ele é múltiplo de todos os números.»
(ii) «Para todo país, existe cidade tal que ela fica perto da fronteira dele.»
(iii) «Para toda pessoa, existe pessoa tal que ela a ama.»

aqui usamos os pronomes 'ele', 'ela', 'a', para referir a algum objeto que foi "introduzido" a partir dos «existe» e «para todo». Na segunda frase graças à coincidência que temos em português onde a palavra 'país' é masculina, e a 'cidade' feminina, não existe confusão: 'ele' refere ao país, e 'ela' refere à cidade.[8] Porém, na última frase não é claro a que as palavras 'ela' e 'a' referem. Usando variáveis escrevemos as primeiras duas assim:

(i) «Existe número n tal que n é múltiplo de todos os números.»
(ii) «Para todo país p, existe cidade c tal que c fica perto da fronteira de p.»

Agora olhe na terceira frase. Temos duas razoáveis maneiras de interpretá-la, dependendo de a que cada pronome refere:

$(\text{iii})_1$ «Para toda pessoa x, existe pessoa y tal que x ama y.»
$(\text{iii})_2$ «Para toda pessoa x, existe pessoa y tal que y ama x.»

[8] Já em grego não temos essa coincidência para nos ajudar nessa frase pois ambos os substantivos são femininos; e em inglês ambos são neutros e seriam referidos pelo mesmo pronome: *it*.

Observe que os significiados são bem diferentes:

(iii)$_1$ «Toda pessoa ama.»
(iii)$_2$ «Toda pessoa é amada.»

Ou seja, a frase (iii) não tem um significado bem determinado e sendo ambígua não podemos usá-la.

1.34. Ocorrência de variável. Numa frase que envolve variáveis é muito importante poder separar (e falar sobre) cada *ocorrência* (ou *instância*) de variável na frase. Na frase seguinte por exemplo, temos 4 ocorrências da variável p e 2 da variável q.

$$\text{«}\underline{p}_1 \text{ é primo e para todo primo } \underline{p}_2 \text{ tal que } \underline{p}_3 \text{ divide } \underline{q}_1\text{, } \underline{p}^2_4 \text{ divide } \underline{q}_2\text{»}$$

Sublinhei e rotulei todas. Mesmo sem isso, alguém poderia falar da «terceira ocorrência da variável p» e entenderiamos qual seria.

▸ **EXERCÍCIO x1.7 (typecheck warmup).**
Considere as expressões:

(a) $(x+y)^2 = x^2 + 2xy$;
(b) a mãe de p;
(c) $2^n + 1$;
(d) p é irmão de q;
(e) a capital do país p;
(f) a mora em Atenas.

Para cada uma decida se ela denota objeto ou proposição. (x1.7H0)

1.35. Variáveis livres e ligadas. Cada uma das expressões da Exercício x1.7 refere a pelo menos uma coisa por meio de variáveis, e logo seu significado é dependente (dessas variáveis). Essas *ocorrências de variáveis* chamamos de *livres*. Sobre as expressões que denotam proposições: não sabemos o que cada uma afirma sem saber quais são os objetos denotados por essas variáveis; similarmente sobre as expressões que denotam objetos: não sabemos qual objeto é denotado sem saber quais são os objetos denotados por essas variáveis. Agora considere as expressões:

(1) existe $k \in \mathbb{Z}$ tal que $13 = 2k + 1$;
(2) existem números x, y tais que $(x+y)^2 = x^2 + 2xy$;
(3) aquela função que dada um número x retorna o $x + 1$;
(4) o conjunto de todos livros b tais que existe palavra w no b com tantas letras quantas as letras do título de b;
(5) para toda pessoa p, a pessoa q não gosta de p.

Aqui as ocorrências das variáveis são todas *ligadas*, exceto na última frase onde ambas as ocorrências da variável p são ligadas, mas (a única ocorrência de) q é livre.[9]

1.36. Oxe! Como assim a 'w' do Nota 1.35 é ligada? Ligada com quê? A 'w' do «existe w» tem papel de *ligador de variável* (1.46) aconteceu que o escopo desse ligador não teve nenhuma 'w' livre para ser ligada com o 'w' do «existe w». Isso não torna a 'w' do «existe w» livre; apenas uma ligada que... acabou não ligando com nada. Pense no codigo seguinte:

```
1  for i in 0..10 {
```

[9] Na literatura aparece como sinônimo de variável ligada o termo *dummy* (boba) também.

```
2       println!(''Boo!'');
3   }
```

o `i` não é livre. Acabou nao conseguindo ligar ninguém mas mesmo assim, com certeza livre não tá. Em certos casos vale a pena distinguïr as ocorrências não-livres entre ligadores e ligadas, mas aqui chamamos todas elas de simplesmente ligadas.

1.37. Observação. Quando não existe possibilidade de confundir, falamos apenas de «variável» em vez de «tal ocorrência de variável». Assim, mesmo que ser livre ou ligada não é uma propriedade de variáveis mas de instâncias de variáveis, nos permitimos o abuso de usar frases como «x é ligada», etc. Acabei de fazer isso no 1.36.

1.38. Observação (Ligações implícitas). Linguisticamente falando a ligação existe sim; só que não foi feita usando variáveis em forma explícita. Foi deixada implicita. Aqui o que foi escondido: «existe palavra w no livro b tal que w tem tantas letras quantas letras tem o título do b».

Precisamos entender *muito bem* essa idéia de variáveis ligadas e livres, mas antes de continuar com isso...

▸ **EXERCÍCIO x1.8.**
Para cada uma das cinco expressões do 1.35: objeto ou proposição? (x1.8H0)

1.39. Conselho. Para saber se uma variável 'x' aparece livre numa expressão, tente enunciar uma frase com o mesmo significado da expressão sem pronunciar «x». Se conseguir, a variável é ligada. Por exemplo, a frase (5) do 1.35 afirma que «q não gosta de ninguém».

▸ **EXERCÍCIO x1.9.**
Enuncie cada uma das (1)–(4) do 1.35 sem pronunciar nenhuma das variáveis ligadas que aparecem. (x1.9H0)

▸ **EXERCÍCIO x1.10.**
Mesma coisa sobre as frases seguintes:

(1) existem pessoas p, q tais que p ama q e q ama p;
(2) existe pessoa p tal que p ama q e q ama p;
(3) $x + y = z$;
(4) existe número x tal que $x + y = z$;
(5) existem números x, z tais que $x + y = z$;
(6) para todo número y, existe número x tal que $x + y = z$;
(7) para quaisquer números y, z, existe número x tal que $x + y = z$.

(x1.10H0)

Vamos ver agora a mesma idéia no contexto de programação:

- **EXEMPLO 1.40.**
  Considere o código seguinte:

```
1  i = 10 * w;
2  for (int i = 0; i < f(w); i++) {
3      w = w + i;
4  }
```

  A `i` da primeira linha é livre, e nas suas outras ocorrências ligada; a `w` é livre em todo canto.

! **1.41. Cuidado.** Numa frase, a mesma variável pode ter ocorrências livres e ligadas também! Olha por exemplo a frase do Nota 1.34. A primeira ocorrência da p é livre, mas todas as outras são ligadas!

1.42. Atribuição e substituição. Quando queremos *substituir* uma variável por um outro termo, ou *atribuir* um valor a uma variável, para evitar o uso do símbolo da igualdade ‘$=$’ e escrever frases como «para $n = 1$ temos...» usamos o símbolo ‘$:=$’: «para $n := 1$ temos...». A idéia é que a expressão na esquerda é para assumir o valor determinado pela direita. Escrevemos, por exemplo:

- A proposição (5) do 1.35 com $q :=$ Larry é a proposição que a Larry não gosta de ninguém.
- *Usando* a (5) do 1.35 para $p :=$ Amanda *inferimos* que a pessoa q não gosta de Amanda.

Naturalmente, usamos o ‘$=:$’ nas raras vezes que queremos inverter os papeis da esquerda e da direita. Caso que a variável que estamos substituindo é uma variavel proposicional (ou seja, serve para denotar proposições e não objetos) podemos usar os ‘$:\iff$’ e ‘$\iff:$’.

1.43. Renomeamento. Considere o texto seguinte:

$$\text{«Existe número } x \text{ tal que } x^2 = k.\text{»}$$

A variável ‘x’ *sendo ligada* pode ser renomeada por outra, por exemplo, a ‘n’, sem mudar o significado da proposição:

$$\text{«Existe número } n \text{ tal que } n^2 = k.\text{»}$$

Porém, não podemos renomear a ‘k’, pois ela é livre, e logo o significado da proposição mudaria, pois em vez de ser uma afirmação sobre um certo objeto k, viraria uma afirmação sobre outra coisa. O processo de (re)nomear variáveis tem certos perigos, então precisamos tomar cuidado. Vamos analisar:

1.44. Capturamento e sombreamento de variável. Leia o texto seguinte:

> «Seja p a maior potência de 2 que divide o x.
> Qualquer número que divide p, também divide x.»

Aqui conseguimos evitar o uso de variável na segunda linha para referir nesse número que divide o p. Realmente ficou sem ambigüidade o texto, então realmente não necessitamos. Mas se quisermos usar, podemos usar qualquer uma? Não sempre! Precisamos tomar cuidado. Vamos tentar usar uma *variável fresca*, ou seja, uma variável que não temos usado ainda:

> «Seja p a maior potência de 2 que divide o x.
> Para todo número d, se d divide p, então d divide x.»

Primeiramente confirme que *nada mudou no significado* do texto. Usamos a variável 'd' para referir ao divisor arbitrário de p. Essa (usar uma variável fresca) seria a melhor e mais segura escolha aqui. Mas, o que acontece se usar, por exemplo, a 'x'? Vamos ver:

> «Seja p a maior potência de 2 que divide o x.
> Para todo número x, se x divide p, então x divide x.»

Acabou de acontecer sombreamento e capturamento. Para explicar vou pintar as variáveis no texto anterior onde usamos 'd':

> «Seja p a maior potência de 2 que divide o x.
> Para todo número d, se d divide p, então d divide x.»

e no novo, onde usamos a 'x':

> «Seja p a maior potência de 2 que divide o x.
> Para todo número x, se x divide p, então x divide x.»

A partir da frase «Para todo número x», o x da linha anterior não tem mais como ser referido até o fim desse escopo, nesse caso até o ponto final da linha. Aconteceu *sombreamento* (*shadowing*) da variável x nesse escopo. Dizemos também que a variável x da segunda linha da versão anterior, foi *capturada* pela frase «Para todo número x», ou seja, virou azul.

- **EXEMPLO 1.45.**
Para os programadores, aqui um exemplo de código e uma análise relevante:

```
1  int a;
2  int i;
3
4  a = 8;
5  i = 4;
6
7  int foo(int x, int a)
8  {
9      if (x < a) {
10         return x + i;
11     } else {
12         for (i = 0; i < x; i++) {
13             a = a + i;
14         }
15     }
16     return a + i;
17 }
```

Nas linhas 12–14 aconteceu sombreamento da `i` que foi declarada na linha 2, por causa do `for`. Esse `for` capturou a `i` que aparece na linha 13. Ainda mais, a variável `a` declarada na linha 1 foi sombreada no escopo ta função `foo` pois escolhemos usar o mesmo nome para segunda parámetro da função `foo`, e logo qualquer ocorrências de `a` no corpo da `foo` refere ao segundo argumento da função, e não à `a` da linha 1. Assim, dentro do corpo da função não temos mais como referir à `a`.

1.46. Ligadores de variáveis e suas ligações. Já encontramos dois *ligadores (binders) de variáveis*: «existe __ tal que . . . » e «para todo __, . . . ». Tem muito mais que esses dois, e provavelmente o leitor já encontrou vários em matemática, programação, ou na vida mesmo (Exercício x1.12). Para entender melhor que onde aparecem variáveis ligadas não está sendo afirmado algo sobre certos objetos denotados por essas variáveis, podemos desenhar explicitamente as ligações. É melhor pensar que uma proposição *é* sua forma com ligações, assim a desvinculando das escolhas de nome de variáveis insignificantes que seu escritor favoreceu. Espero que isso fique mais claro depois do exemplo seguinte:

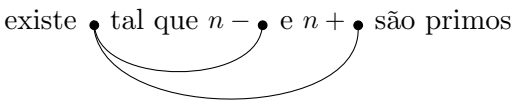
• **EXEMPLO 1.47.**
Considere a proposição

(1) $$n - d \text{ e } n + d \text{ são primos.}$$

Sem sequer saber o que significa ser um número primo, sabemos que essa proposição afirma que dois números (o $n - d$ e o $n + d$) possuem essa propriedade (misteriosa de ser primo). Aparecem as variáveis 'n' e 'd', e em todas as suas ocorrências são livres. Ou seja, a proposição (1) pode ser vista como uma afirmação sobre dois números n e d. Podemos *quantificiar* uma ou ambas delas, por um dos quantificadores que discutimos:

(2) $$\text{existe } d \text{ tal que } n - d \text{ e } n + d \text{ são primos.}$$

Aqui todas as ocorrências da 'd' são ligadas (com o ligador «existe d tal que . . . »). Ou seja, a proposição (2) afirma algo sobre um certo número n. Ela não fala nada sobre d. Podemos pronunciá-la sem dizer «d»: *«Existe numero que tanto subtraindo ele de n, quanto somando ele com n, resulta em números primos.»*. Mas não sem dizer «n». Podemos desenhar as ligações da (2) para esclarecer:



Voltando na (1) podemos quantificar a outra variável:

(3) $$\text{existe } n \text{ tal que } n - d \text{ e } n + d \text{ são primos.}$$

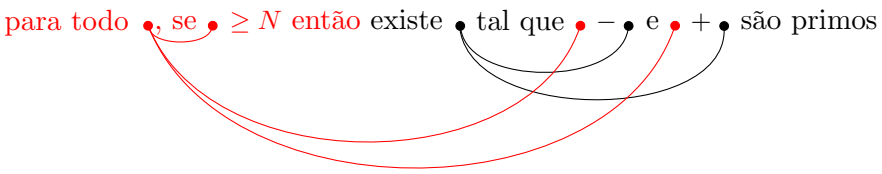
Agora d é livre e n ligada, ou seja (3) afirma algo sobre um certo número d, e nada sobre nenhum n. Podemos pronunciá-la sem dizer «n»: *«Existe numero que tanto subtraindo d dele, quanto somando d nele, resulta em números primos.»*. Mas não sem dizer «d». Deixo os desenhos de ligações pra ti (Exercício x1.11). Observe que os significados das (2) e (3) são bem diferentes:

- Na (2) o n é fixo (podemos pensar o n como o centro da nossa busca) e ficamos estendendo mais e mais os dedos (com distâncias iguais do centro) até encontrar (se encontrar) uma certa distância d tal que (novamente) ambos os nossos dedos apontam para primos.
- Na (3) o d é fixo (podemos pensar o d como distância) e procuramos n com essa propriedade. Parece que fixamos nossos dedos numa distância $2d$ (d pela esquerda e d pela direita) e procuramos achar se existe n no meio tal que ambos os nossos dedos apontam para primos.

Agora, volte na (2) e considere a proposição

(4) $$\text{para todo } n, \text{ se } n \geq N \text{ então existe } d \text{ tal que } n - d \text{ e } n + d \text{ são primos.}$$

que obtemos botando esse «para todo n, se $n \geq N$ então» na frente da (2). Aconteceu o seguinte:



Essa então é uma afirmação sobre um certo número N. Quantificando 'N' também, podemos chegar na:

(5) existe N tal que para todo n, se $n \geq N$ então existe d tal que $n - d$ e $n + d$ são primos

Te deixo desenhar suas ligações (Exercício x1.11).

▸ **EXERCÍCIO x1.11.**
Desenhe as ligações da (3) e (5) do Exemplo 1.47. (x1.11 H 0)

▸ **EXERCÍCIO x1.12.**
Já encontramos dois ligadores «existe __ tal que . . . » e «para todo __, . . . ». Dê mais exemplos de ligadores que tu conhece: de matemática, de programação, de vida. . . (x1.12 H 0)

▸ **EXERCÍCIO x1.13.**
Na (3) do Exemplo 1.47 podemos renomear a variável. . . :

(i) 'n' por 'm'? (ii) 'n' por 'd'? (iii) 'd' por 'x'?

(x1.13 H 0)

▸ **EXERCÍCIO x1.14.**
E na (5). . . :

(i) 'N' por 'n'? (iii) 'n' por 'N'? (v) 'd' por 'n'?
(ii) 'N' por 'd'? (iv) 'n' por 'd'? (vi) 'd' por 'N'?

Cuidado! (x1.14 H 0)

! **1.48. Cuidado.** Em matemática—por incrível que pareça—uma variável não. . . varia! Ela denota um objeto especifico e pronto, não pode mudar depois duns minutos para denotar algo diferente, nem mudar no mesmo escopo da mesma expressão como acontece por exemplo com o que chamamos de "variáveis" em programação imperativa. Encontrando então a expressão '$f(x) + x$', não tem como as duas ocorrências de 'x' denotar objetos diferentes.

1.49. Antes de fechar nossa discussão sobre variáveis tenho uma última coisa para expôr. Considere as frases:

(1) todo inteiro x divide ele mesmo;
(2) existe número n tal que ele é primo e par;
(3) qualquer conjunto A é determinado por seus membros;
(4) não existe país P tal que a pessoa p não viajou para esse país;
(5) existe pessoa p tal que para todo filme f na lista F, p assistiu tal filme.

E agora...

? **Q1.50. Questão.** Qual o problema com elas?

!! SPOILER ALERT !!

! **1.51. Cuidado (variáveis inúteis).** Cada uma dessas frases usa pelo menos uma variável ligada numa maneira completamente inútil: a frase introduz uma variável para denotar algo, mas nunca usa essa variável mesmo para referir a esse algo! Acaba usando pronomes. *Nunca introduza uma variável se não pretende usá-la mesmo!* Aqui as mesmas frases, essa vez sem as variáveis inúteis:

(1) todo inteiro divide ele mesmo;
(2) existe número (tal que ele é) primo e par;
(3) qualquer conjunto é determinado por seus membros;
(4) não existe país tal que a pessoa p não viajou para esse país;
(5) existe pessoa p, tal que p assistiu todos os filmes da lista F.

Observe que na última frase podemos nos livrar da variável 'p' também já que é ligadas.[10] Mas pelo menos ela foi usada (referenciada) sim, e aqui o objetivo era jogar fora as variáveis que não foram usadas.

§7. Tipos de números

Vamos encontrar e estudar vários tipos de números: naturais (Capítulo 4), inteiros (Capítulo 3), racionais (Secção §270), reais (Capítulo 6), ... Além disso, nos capítulos 13 e 16 vamos identificar certos reais que são ainda mais selvagens do que os irracionais: os transcendentais; e uns números transfinitos: os cardinais e os ordinais.

[10] Assim: «alguém assistiu todos os filmes que estão na lista F».

1.52. De e para os reais. Uma abordagem é começar considerando como conhecida ou dada a noção dos números reais, freqüentemente identificados com os pontos duma linha reta que extende infinitamente para ambas as direcções; um ponto dela chamamos de 0, botamos na sua direita mais um ponto chamado de 1, e pensamos que a distancia entre esses pontos é medida pelo número real 1 mesmo; na outra direção temos o -1, etc., etc., e o leitor provavelmente já ouviu dessa estoria muitas vezes na vida.[11] Nada disso faz sentido formalmente falando, mas não estamos falando formalmente neste momento, e com certeza essa imagem geométrica ajuda demais em elaborar uma intuição sobre os reais.

Então: *começando com a reta dos reais* como dada, podemos procurar e definir um subconjunto dela para representar os racionais, um subconjunto deles para os inteiros e um deles para os naturais. Naturalmente definimos primeiramente os naturais, depois adicionamos para cada ponto o seu oposto chegando assim nos inteiros, e depois formamos todas as fracções m/n para quaisquer inteiros m, n com $n \neq 0$ e pronto, temos o racionais também.

Podemos trabalhar também no sentido contrário (Capítulo 16): *começar com os naturais*, usá-los para *construir* os inteiros, usá-los para construir os racionais, e usá-los para construir os reais, etc. Nesse contexto, 'construir' significa definir.

§8. Números, numerais, dígitos

1.53. Aceitamos *por enquanto* como dado o conceito dos números que usamos para contar, que costumamos denotar por

$$0, 1, 2, 3, \ldots, 247, 248, 249, \ldots$$

Usando então apenas um *alfabeto* composto de dez símbolos

$$0\ \ 1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8\ \ 9$$

e seguindo as regras bem-conhecidas do sistema decimal conseguimos denotar qualquer um dos números, mesmo que tem uma infinidade deles!

Chamamos esses símbolos de *dígitos* ou *algarismos*. Para *representar os números*, usamos palavras (ou *strings*) que formamos justapondo esses dígitos; essas palavras chamamos de *numerais do sistema posicional decimal*. Sem contexto, lendo o '10' já temos uma ambigüidade: é o numeral $\underline{10}$ ou o número dez? Para apreciar essa diferença ainda mais, note que o numeral $\underline{10}$, pode representar outro número em outro contexto. Por exemplo, no sistema binário, o numeral $\underline{10}$ representa o número dois. E a ambigüidade pode ser ainda maior lendo "1": é o numeral $\underline{1}$; o número um; ou o dígito 1? Quando o contexto é suficiente para entender, não precisamos mudar a fonte como acabei de fazer aqui, nem escrever explicitamente o que é. Note que existem numerais bem diferentes para denotar esses números: o numeral (romano) XII e o numeral (grego) ιβ denotam o mesmo número, que em português chamamos de *doze*.

Temos então umas pequenas linguagens que nos permitem descrever *números*. Não fatos sobre números. Nem cálculos com números. Números. Quais números? Todos os números *naturais* (veja §7), cuja totalidade simbolizamos com $\mathbb{N}$ e deixamos seu estudo para o Capítulo 4.

[11] Caso contrário vamos voltar a discutir isso numa maneira melhor bem depois, nos capítulos 6 e 16.

§9. Conjuntos, funções, relações

Rascunhamos aqui três tipos importantíssimos, só para ter uma idéia do que se trata, pois vamos precisá-los desde já! Mas cada um deles tem seu próprio capítulo dedicado ao seu estudo: estudamos conjuntos no Capítulo 8, funções no 9, e relações no 10. Agora, bora rascunhar!

1.54. Conjuntos. Um *conjunto* é uma colecção de objetos que já conhecemos. Denotamos um conjunto escrevendo seus membros entre "chaves", separados por vírgulas, por exemplo

$$\{1, 2, 3\}$$

denota o conjunto cujos membros são os números 1, 2, e 3. Conjuntos não têm seus membros numa certa ordem; e também não faz sentido perguntar quantas vezes um objeto pertence àlgum conjunto:

$$\{1, 2, 3\} = \{3, 1, 2\} = \{1, 1, 3, 2, 2, 1\}\,.$$

Dizemos que dois conjuntos são iguais sse eles possuem exatamente os mesmos membros. Vamos também usar a notação

$$\{\, x \mid x \text{ é um múltiplo de } 3 \,\}$$

para descrever o conjunto de todos os múltiplos de 3 e—parabéns para nos—acabamos de definir um conjunto infinito numa maneira tão curta e simples! A gente lê o conjunto acima assim:

«o conjunto de todos os x, tais que x é um múltiplo de 3».

Costumamos usar letras maiúsculas para denotar conjuntos, mas não ficamos obsecados demais com essa costume. Usamos a notação $x \in A$, para afirmar que x é um dos membros do conjunto A, e escrevemos $A \subseteq B$ para afirmar que cada membro de A é um membro de B (nesse caso dizemos que A é um *subconjunto de* B). Por exemplo, o conjunto de todos os brasileiros é um subconjunto do conjunto de todos os humanos. Usamos variações da notação em cima como por exemplo

$$\{\, p : \mathsf{Int} \mid p \text{ e } p+2 \text{ são números primos} \,\}$$

denotando o conjunto de todos os inteiros p tais que p é primo e $p+2$ também.

Temos tudo que precisamos para começar até chegar no Capítulo 8 onde estudamos mesmo conjuntos e outros tipos de "containers", notavelmente tuplas:

1.55. Tuplas. Quando temos uns objetos botados numa certa ordem, temos uma *tupla*. Denotamos a tupla dos objetos $x_1, \ldots, x_n$ assim:

$$\langle x_1, \ldots, x_n \rangle \qquad \text{ou} \qquad (x_1, \ldots, x_n)\,.$$

Observe que temos

$$\langle 1, 2, 3 \rangle \neq \langle 1, 3, 2 \rangle$$

pois *consideramos duas tuplas iguais sse elas concordam em cada posição.*

1.56. Funções. *Funções* são objetos que dados objetos *retornam* objetos. É comum usar as letras f, g, h, etc. para denotar funções, mas, novamente isso não é uma regra inquebrável. Escrevemos

$$f : A \to B$$

para dizer que f é uma função que dada qualquer objeto de tipo A, retorna algum objeto de tipo B. Dado qualquer $x : A$, escrevemos '$f\,x$' ou $f(x)$ para o *valor* ou *saida* da f no x, e chamamos x de *argumento* ou *entrada* da f. Observe que $f\,x : B$. O objeto $f\,x$ é determinado pelo $x : A$, ou seja, para qualquer $x \in A$, *exatamente um* objeto é denotado por $f\,x$. Por exemplo, $\mathit{mother}(x)$ pode denotar a mãe duma pessoa x. Aqui entendemos que

$$\mathit{mother} : \mathsf{Person} \to \mathsf{Person}$$

onde Person é o tipo cujos habitantes são todas as pessoas. Por outro lado, seria errado pensar que

$$\mathit{sister} : \mathsf{Person} \to \mathsf{Person}$$

também é uma função, pois para certos $x : \mathsf{Person}$ o $\mathit{sister}(x)$ não seria determinado!

▸ **EXERCÍCIO x1.15.**
Quais são esses $x \in P$ tais que $\mathit{sister}(x)$ não é determinado? Cuidado: tem mais que uma categoria de x's "problemáticos"! (x1.15 H 0)

1.57. Aridade. Uma função pode precisar mais que um argumento: a adição por exemplo precisa dois números para retornar seu valor. A quantidade de argumentos que uma função f precisa é chamada *aridade* da f. Não são apenas funções que têm aridade, relações também têm:

1.58. Relações. Funções dadas objetos viram objetos. *Relações* dadas objetos viram proposições. Por exemplo

«____ é a mãe de ____»

é uma relação de aridade 2, mas

«Stella é a mãe de ____»
«____ é a mãe de Thanos»

são relações de aridade 1. Para relações de qualquer aridade emprestamos a notação de funções e escrevemos, por exemplo

$$\begin{aligned} \mathrm{MotherOf}(x, y) &: \quad \text{«}x \text{ é a mãe de } y\text{»} \\ \mathrm{StellaIsMotherOf}(x) &: \quad \text{«Stella é a mãe de } x\text{»} \\ \mathrm{MotherOfThanos}(x) &: \quad \text{«}x \text{ é a mãe de Thanos».} \end{aligned}$$

D1.59. Notação (infix, prefix, postfix, mixfix). Especialmente para funções e relações de aridade 2 usamos também notação *infix* em vez de *prefix*, ou seja, escrevemos o símbolo da função ou relação *entre* os seus argumentos em vez de *antes*. Como exemplo considere as $(+)$, $(=)$, $(\leq)$, etc.:

em vez de escrever:	$+(1,2)$	$=(1+1,2)$	$\leq(0,+(x,y))$
escrevemos:	$1+2$	$1+1=2$	$0 \leq x+y$.

Às vezes também usamos notação *postfix*: exemplo padrão aqui seria a função fatorial que denotamos por um simples '!' postfixo, escrevendo, por exemplo, $3!$ em vez de $!(3)$. Quando escrevemos partes da notação do operador e os argumentos intercalados falamos de notação *mixfix*, por exemplo: `if__then__else__`.

! **1.60. Aviso (Convenção notacional).** Para enfatizar a diferença entre funções e relações, tentarei denotar funções com nomes que começam com letra minúscula, e relações com maiúscula: usarei '$mother(x)$' para *o objeto* (aqui pessoa) «mãe de x», e '$\mathrm{Mother}(x)$' para *a proposição* «x é uma mãe». Novamente, essa também é uma convenção que vou seguir, um costume, e não uma regra inquebrável.

§10. Teoremas e seus amigos

1.61. Teorema. Chamamos de *teorema* uma proposição que já foi demonstrada por alguém. Então: que tipo de coisa é um teorema? É uma proposição. E ainda mais, sabemos que essa proposição é verdadeira, pois já possui uma demonstração. Uma proposição P que não conseguimos demonstrar ainda, talvez um belo dia alguém vai demonstrar e assim vamos falar do teorema P, ou pode ser que alguém refute, e logo sabemos que não se-trata dum teorema. Mas por enquanto, não sabemos se P é um teorema ou não.

1.62. Lemma, teorema, corolário. Matematicamente falando então não existe diferença essencial entre lemma e teorema, nem entre teorema e corolário; mas cuidado no seu uso pois nosso objetivo em matemática é *comunicar*, e chamando um teorema de lemma ou de corolário comunica algo diferente. Pense que estamos tentando demonstrar uma proposição que consideramos importante, e provavelmente não vai ser muito simples demonstrá-la. Chamamos de *lemma* um teorema que demonstramos para usar em demonstrar nosso teorema. E assim que demonstrar nosso teorema, talvez para divulgá-lo e falar da importância dele, consideramos várias proposições que são conseqüências (fáceis) do nosso teorema principal. Esses são os *corolários* dele.

1.63. Conjectura. Uma proposição interessante que alguém afirmou e tentou demonstrar sem conseguir, é uma *conjectura*. Em qualquer momento pode ser que alguém consiga demonstrar: nesse caso a proposição vai ganhar o direito de ser chamada um teorema. Similarmente, pode ser que alguém consegue refutar: nesse caso a proposição é mais uma conjectura, pois já sabemos a resposta (negativa) sobre sua veracidade. Já no Capítulo 3 (Os inteiros) vamos conhecer umas conjecturas que têm atrapalhado—ou, entretido—matemáticos por séculos. O que talvez pareça estranho—e eu espero pelo menos um pouco incrível para meu leitor—é que existe mais uma possibilidade para "resolver" uma tal *questão em aberto*: pode ser que alguém *demonstre que não tem como*

demonstrá-la nem como refutá-la! Mas é cedo demais para analisar mais isso; paciência; durante esse texto vamos ver vários tais exemplos dessa situação e acabar entendendo bem a situação.

§11. Demonstrações

1.64. O que é?. Vamos começar com a idéia que uma *demonstração* é uma argumentação ao favor duma proposição, convincente e sem erros, escrita como um pedaço de texto, entendível para uma pessoa que entende as noções matemáticas envolvidas.

1.65. Linguagem de demonstração. Normalmente a linguagem que usamos para escrever demonstrações é uma linguagem natural, como grego, português, inglês, etc., *enriquecida* saudavelmente por símbolos e notações matemáticas. Além disso, entendemos essa linguagem como uma coisa mutável (especialmente aumentável), algo que aproveitamos introduzindo novas notações, noções, convenções, etc. Infelizmente, especialmente quando começamos estudar e *fazer* matemática, não é uma idéia boa ter de lidar com umas ambigüidades que as linguagens naturais carregam. Vamos elaborar uma *linguagem de demonstração*, bastante "seca"—e sem a expressividade nem a beleza que uma linguagem natural oferece—e tratá-la como se fosse uma *linguagem de programação:* vamos diferenciar entre linhas de código e comentários, e identificar certas palavras-chaves, explicar seus efeitos, como, por que, e quando podemos usar. Exatamente como na linguagem C, por exemplo, temos as palavras `while`, `return`, `float`, `switch`, `else`, etc., cada uma com seu uso correto, sua sintaxe, sua semântica, etc. A idéia é que uma demonstração escrita em linguagem natural, corresponde "por trás" num texto feito por "linhas de código" escritas nessa linguagem de demonstração. Demonstrações escritas na linguagem de demonstração acabam sendo cansativas de ler, sem graça: pode parecer que foi um robô escreveu. Essa seria uma linguagem *low-level* para demonstrar teoremas. Um dos nossos objetivos aqui é aprender como ler e escrever numa linguagem *high-level*, natural e humana mesmo, mas entendendo em qualquer momento as linhas de código "compiláveis" por trás. Elaboramos isso no Capítulo 2 (Demonstrações), onde estabelecemos nosso sistema de demonstrações e sua linguagem low-level. No Capítulo 3 (Os inteiros) botamos isso na prática e começamos aumentar o nível gradualmente; no Capítulo 4 (Recursão; indução) aprofundamos nas idéias de recursão e indução e enriquecemos nossa linguagem; no Capítulo 6 (Os reais) continuamos aumentando o nível, chegando a escrever numa forma *mid-level* ou até um tiquinho mais alta.

1.66. Programando vs. demonstrando. Em muitos sentidos *demonstrar* e *programar* são atividades parecidas—tanto que podemos até identificá-las![12] Além disso vou fazer muitas metáforas usando noções de programação. Caso que o leitor não tem nenhum contato com programação, deveria começar (aprender) programar em paralelo—com certeza, mas o que deveria ter dito aqui foi que o leitor sem experiência de programação vai perder apenas certos exemplos, metáforas, e referências, e nada essencial. Esses exemplos são aqui para ajudar o programador, não para prejudicar o não-programador. No final das contas, o não-programador já se-prejudica sozinho na vida, pela falta de. . . "progranoção"!

[12] Isso não é um modo de falar, nem um exagero, mas infelizmente vou ter que pedir para bastante paciência no teu lado, pois vamos demorar até chegar a entender essa idéia.

1.67. Teses vs. hipoteses. «Tese» vem da grega *θέσις* e similarmente «hipótese» da palavra *ὑπόθεσις*. *Tese* significa *posição*, e nesse sentido também *opinião*. Tu tens uma tese sobre um assunto, e queres argumentar para defendê-la. O prefixo «ὑπο-» (hipo-) denota uma idéia de *embaixo de*. O equivalente prefixo latino (e usado em português) é o «sub-». *Hipoteses* então são *su(b)posições*, ou seja, afirmações "embaixo" da tese: as proposições de quais a tese depende.

§12. Axiomas e noções primitivas

1.68. Uma criança "chata". Imagine tentando convencer uma criança sobre alguma proposição P:

- P.
- por que P?
- P pois Q.
- E por que Q?
- Q pois R.
- E por que R?

Quem conversou com uma criança sabe que não tem como ganhar nesse jogo. Não tem como justificar tudo: esse dialogo continuando nessa forma nunca vai terminar. A idéia é que nosso "oponente" ou "inimigo" (nesse exemplo a criança) vai continuar duvidando qualquer uma das novas proposições que usamos em nossa argumentação, *até finalmente chegar em algo que concorda aceitar*. Talvez no exemplo da criança chegando numa afirmação do tipo «comer sorvete é bom» faria o dialogo terminar:

- ... pois comer sorvete é bom.
- Ah sim, faz sentido.

1.69. Um exemplo: geometria euclideana. Euclides na Grécia antiga elaborou, investigou, e estabeleceu o que chamamos de *geometria euclideana*. Uma das mais importantes idéias que temos desde então é a percepção que precisamos deixar claro quais são nossos axiomas, e trabalhar para elaborar nossa teoria, investigando suas conseqüências: os teoremas. Similarmente, separamos as noções primitivas que aceitamos sem definir formalmente, e as usando continuamos em aumentar mais e mais nosso vocabulário. As noções primitivas da geometria euclideana são os *pontos* e as *linhas* (retas). E também a relação entre pontos e linhas seguinte:

«o ponto ____ pertence à linha ____».

Não definimos o que significa ser um ponto; nem ser uma linha; nem o que significa que um ponto pertence àlguma linha. De fato, Euclides tentou dar uma intuição, uma descripção informal sobre suas noções primitivas em vez de escrever algo do tipo

> Essas aqui são noções primitivas, não me perguntem o que significam; aceitem.

A partir dessas noções primitivas, podemos *definir* conceitos interessantes. Por exemplo, em vez de adicionar como primitiva a noção de linhas parallelas, podemos realmente definir o que significa ser parallela, numa maneira que a criança chata do exemplo acima um belo momento cairia apenas em noções primitivas e não teria como continuar com seus «e o que é...?».

► **EXERCÍCIO x1.16.**
Defina o que significa *ser parallelas*. (x1.16H0)

§13. Expressões de aritmética

1.70. Expressões sintácticas e sua semântica. Aprendendo aritmética queremos expressar números numa maneira mais interessante do que simplesmente usar os próprios nomes deles: '$2+5$', por exemplo, é uma *expressão de aritmética*. Podemos pensar que essas expressões acabam denotando números: a expressão '$2+5$' denota *o número 7*. Alternativamente podemos usá-las para denotar os próprios cálculos: a expressão '$2+5$' denota *o cálculo de somar o 2 com o 5*. E nesta paragrafo estou usando o '$2+5$' para referir à propria expressão sintáctica mesmo. Mas em todos essas interpretações as expressões de aritmética denotam objetos (números ou cálculos ou até elas mesmo) e ainda não temos como expressar *afirmações* sobre eles.

1.71. Semântica denotacional. As expressões fazem parte da *sintaxe* duma linguagem (aqui, duma linguagem de aritmética). Uma *semântica* atribui um significado para esses objetos sintácticos. Já encontramos três exemplos acima: uma interpretou a expressão como número, outra como cálculo, outra (trivial) como um string mesmo. Vamos voltar a esse assunto várias vezes, uma das mais interessantes sendo quando analisaremos essas idéias no contexto de linguagens de programação (Capítulo 21).

§14. Expressões aritméticas: sintaxe vs. semântica

1.72. Precedência. Considere agora a expressão

$$1+5\cdot 2$$

que envolve os numerais 1, 5, e 2, e os símbolos de funções $(+)$ (adição) e $(\cdot)$ (multiplicação). O que ela representa? A multiplicação de $1+5$ com 2, ou a adição de 1 com $5\cdot 2$? A segunda opção, graças a uma convenção que temos—e que você provavelmente já encontrou na vida. Digamos que a $(\cdot)$ "pega mais forte" do que a $(+)$, então precisamos "aplicá-la" primeiro. Mais formalmente, a $(\cdot)$ tem uma *precedência* mais alta que a da $(+)$. Quando não temos convenções como essa, usamos parenteses para tirar a ambigüidade e deixar claro como parsear uma expressão. Então temos

$$(1+5)\cdot 2 \neq 1+5\cdot 2 = 1+(5\cdot 2).$$

1.73. Associatividade sintáctica. E a expressão

$$1 + 5 + 2$$

representa o quê? Não seja tentado dizer «tanto faz», pois mesmo que as duas razoáveis interpretações

$$(1 + 5) + 2 \qquad \text{e} \qquad 1 + (5 + 2)$$

denotam valores iguais, elas expressam algo diferente:

$$\begin{aligned} (1 + 5) + 2 :&\quad \text{adicione o } 1 + 5 \text{ com o } 2; \\ 1 + (5 + 2) :&\quad \text{adicione o } 1 \text{ com o } 5 + 2. \end{aligned}$$

Ou seja: a intensão é diferente, Então...

$$(1 + 5) + 2 \stackrel{?}{=} 1 + (5 + 2)$$

Como *expressões* (a *sintaxe*) são diferentes; como *intensões* também; como *valores* (a *semântica*) são iguais, pois denotam o mesmo objeto: o número oito. Como já discutimos (§5) em matemática ligamos sobre as denotações das expressões, e logo escrevemos igualdades como

$$(1 + 5) + 2 = 6 + 2 = 8 = 1 + 7 = 1 + (5 + 2).$$

Lembre que o símbolo '$=$' em geral denota *igualdade semântica*: $A = B$ significa que os dois lados, A e B, denotam o mesmo objeto. Querendo representar *igualdade sintáctica*, às vezes usamos outros símbolos. Vamos usar o '$\equiv$' agora, de modo que:

$$\begin{aligned} 1 + 2 = 3 \qquad &\text{mas} \qquad 1 + 2 \not\equiv 3; \\ (1 + 5) + 2 = 1 + (5 + 2) \qquad &\text{mas} \qquad (1 + 5) + 2 \not\equiv 1 + (5 + 2); \quad \text{etc.} \end{aligned}$$

Voltando à expressão '$1 + 5 + 2$', precisamos *declarar uma associatividade esquerda ou direita*. Vamos concordar que '$a + b + c$' representa a expressão '$((a + b) + c)$', ou seja, atribuimos à $(+)$ uma *associatividade esquerda*. Mas $(+)$ não é uma operação associativa? Sim, e isso implica que *como valores*,

$$((a + b) + c) = (a + (b + c)).$$

Essa associatividade é uma propriedade matemática (algébrica) da operação $(+)$. Umas operações binárias possuem essa propriedade e as chamamos de *associativas* (e.g. adição, multiplicação) e outras não (e.g. exponenciação). Por outro lado, a associatividade que *declaramos* acima não é uma propriedade da operação, não é uma proposição para demonstrar ou refutar ou nada disso. É sim uma definição sintáctica, e logo chamamos de *associatividade sintáctica*. Sem essa convenção '$a + b + c$' não representaria nenhuma expressão de aritmética!

▸ **EXERCÍCIO x1.17.**
Sejam a, b, c números naturais. Usando '$=$' para igualdade semântica e '$\equiv$' para igualdade sintáctica, decida para cada uma das afirmações seguintes se é verdadeira ou falsa:

(i) $a + b + c \equiv a + (b + c)$
(ii) $a + b + c \equiv (a + b) + c$
(iii) $a + b + c = a + (b + c)$
(iv) $a + b + c = (a + b) + c$
(v) $2 \cdot 0 + 3 = 0 + 3$

(vi) $2 \cdot 0 + 3 \equiv 0 + 3$
(vii) $(2 \cdot 0) + 3 + 0 = 1 + 1 + 1$
(viii) $2 \cdot 0 + 3 \equiv 1 + 1 + 1$
(ix) $2 \cdot 0 + 3 \equiv 2 \cdot (0 + 3)$
(x) $2 \cdot 0 + 3 = 2 \cdot (0 + 3)$
(xi) $2 \cdot 0 + 3 \equiv (2 \cdot 0) + 3$
(xii) $1 + 2 \equiv 2 + 1$

(x1.17H0)

▸ **EXERCÍCIO x1.18.**
Verdadeiro ou falso?:

$$A \equiv B \implies A = B$$

(x1.18H0)

§15. Linguagem vs. metalinguagem

1.74. (Meta)linguagem. Já encontramos o conceito de linguagem como um objeto de estudo. Logo vamos estudar bem mais linguagens, de lógica matemática, estudar linguagens de programação, etc. É preciso entender que enquanto estudando uma linguagem, esse próprio estudo acontece também usando uma (outra) linguagem. Aqui usamos por exemplo português,[13] demonstrando propriedades, dando definições, afirmando relações, etc., de outras linguagens que estudamos, como da aritmética, de lógica matemática, de programação, etc. Para enfatizar essa diferença e para tirar certas ambigüidades, chamamos *linguagem-objeto* a linguagem que estudamos, e *metalinguagem* a linguagem que usamos para falar sobre a linguagem-objeto. Note que todos os símbolos '$\iff$', '$\implies$', e '$\impliedby$' fazem parte da *metalinguagem*, e não é para confundir com os '$\leftrightarrow$', '$\to$', e '$\leftarrow$' que geralmente usamos como símbolos de certas *linguagens formais* de lógica.

1.75. (Meta)variável. Imagine que você trabalha como programador e teu chefe lhe pediu fazer uma mudança no código de todos os teus programas escritos na linguagem de programação C. Ele disse: «Em todo programa teu Π, substitua cada variável α de tipo τ que aparece no código fonte por α`_of_`τ.» «Por exemplo,» ele continuou abrindo o programa no seu editor, «essa variável aqui `i` que é de tipo `int`, precisa ser renomeada para `i_of_int`; e essa `count` também para `count_of_int`; e essa `mean` de tipo `float`, para `mean_of_float`, etc.».

Nesse pedido—obviamente sem noção, algo muito comum em pedidos de chefes de programadores—aparecem duas "espécies" de variáveis diferentes: as Π, α, e τ são variáveis de uma espécie; as `i`, `i_of_int`, `count`, `count_of_int`, `mean`, e `mean_of_float` de outra. Chamamos as Π, α, e τ de *metavariáveis*, pois elas pertencem à metalinguagem, e não à linguagem-objeto, que nesse exemplo é a linguagem de programação C. Observe que a metavariável Π denota programas escritas na linguagem-objeto (C) a metavariável α denota variáveis de C, e a metavariável τ denota tipos da C.

[13] quase

§16. Abreviações e açúcar sintáctico

▸ **EXERCÍCIO x1.19.**
Tente gerar a expressão

$$(1+5)\cdot 2$$

usando a Gramática Γ4.103. (x1.19H0)

1.76. Abreviações. Seguindo nossa Gramática Γ4.103, cada vez que escrevemos um operador binário começamos e terminamos com '(' e ')' respectivamente. Logo, '1 + 2' nem é uma expressão gerada por essa gramática! Mas como é tedioso botar as parenteses mais externas, temos a convenção de omiti-las. Logo, consideramos a '1 + 2' como uma *abreviação* da expressão aritmética '(1+2)'. Então qual é o primeiro caráter da '1+2'? É sim o '(', pois consideramos o 1+2 apenas como um nome que usamos na metalinguagem para denotar a expressão aritmética '(1 + 2)', que pertence à linguagem-objeto.

! **1.77. Cuidado.** Não se iluda com a palavra "abreviação" que usamos aqui: uma expressão pode ser mais curta do que uma das suas abreviações! Nosso motivo não é preguiça de escrever; mas sim ajudar nossos olhos humanos a parsear.

1.78. Açúcar sintáctico. Querendo enriquecer uma linguagem com um novo conceito, uma nova operação, etc., parece que precisamos aumentar sua sintaxe para adicionar certos símbolos e formas para corresponder nessas novas idéias. Mas isso não é sempre necessário. Por exemplo, suponha que trabalhamos com a linguagem da Gramática Γ4.104, e queremos usá-la com sua interpretação canônica, onde suas expressões aritméticas geradas denotam realmente as operações que conhecemos desde pequenos. Agora, queremos adicionar uma operação unária S, escrita na forma prefixa, onde a idéia é que Sn denota o sucessor de n (o próximo inteiro):

$$Sn \overset{\text{sug}}{\equiv} n+1$$

Nesse caso, em vez de realmente alterar a sintaxe da nossa linguagem, podemos definir como *açúcar sintáctico* o uso de S tal que, para qualquer expressão aritmética α, o $S\alpha$ denota a expressão $(\alpha+1)$. Por exemplo, $S4$ é apenas uma abreviação para o $(4+1)$, e $SS4$ só pode denotar o $((4+1)+1)$.[14] Açúcar sintáctico é muito usado em linguagens de programação, para agradar os programadores (que ganham assim um mecanismo "doce" para usar nos seus programas) sem mexer e complicar a linguagem de verdade. Para um exemplo mais perto da vida real, imagine que numa linguagem orientada a objetos, certos objetos escutem às mensagens '`.set(`i`,`v`)`' e '`.get(`i`)`' a idéia sendo que utilizamos a primeira método para atribuir o valor v à posição i e a segunda para solicitar em tal posição. Mas ninguém merece escrever isso, e logo introduzimos:

$$\begin{aligned} a\texttt{[}i\texttt{]} \texttt{ = } v &\overset{\text{sug}}{\equiv} a\texttt{.set(}i\texttt{,}v\texttt{)} \\ a\texttt{[}i\texttt{]} &\overset{\text{sug}}{\equiv} a\texttt{.get(}i\texttt{)} \end{aligned}$$

Observe que esse açúcar não é um simples *search and replace* do padrão 'a`[`i`]`', pois seu sentido muda dependendo de se aparece no lado esquerdo duma atribuição (primeira linha) ou não (segunda linha).

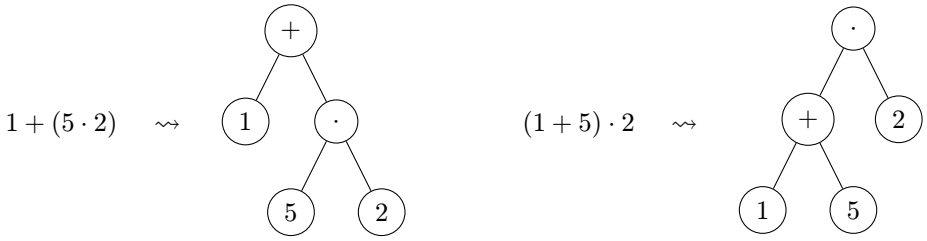
[14] Percebeu que esse α aqui é uma metavariável?

▸ **EXERCÍCIO x1.20.**
Mostre como um `while` loop pode ser implementado como açúcar sintáctico numa linguagem que tem `for` loops mas não `while` loops, e vice versa. (x1.20 H 1 2)

▸ **EXERCÍCIO x1.21.**
Mostre como um `for` loop no estilo da linguagem C pode ser implementado sem usar nenhum dos loops disponíveis em C (for, while, do-while). (x1.21 H 1)

§17. Árvores de derivação

1.79. Parsing. Lendo uma expressão "linear" como a '$1 + 5 \cdot 2$' nós a *parseamos* para revelar sua estrutura, freqüentemente representada numa forma bidimensional, como uma *árvore sintáctica*. Temos então as árvores:



Não vamos usar mais este tipo de árvore sintáctica nessas notas.

1.80. Árvores de derivação. Em vez, vamos usar *árvores de derivação* como essas:

$$\dfrac{1 \qquad \dfrac{5 \qquad 2}{(5 \cdot 2)}\,(\cdot)}{1 + (5 \cdot 2)}\,(+) \qquad\qquad \dfrac{\dfrac{1 \qquad 5}{(1 + 5)}\,(+) \qquad 2}{(1 + 5) \cdot 2}\,(\cdot)$$

Sendo esse nosso primeiro contato com árvores sintácticas, vou explicar em detalhe como as escrevemos. Começamos então com a expressão (linear) que queremos parsear:

$$(1 + 5) \cdot 2.$$

Graças à sua parêntese, o "operador principal" (o mais "externo") é o $(\cdot)$. Isso quer dizer que, no final das contas, essa expressão representa uma multiplicação de duas coisas. Exatamente por isso, reduzimos essa expressão em duas novas, escrevendo uma linha em cima dela, onde temos agora dois lugares para botar essas duas coisas. No lado da linha, escrevemos sua "justificativa"

$$\dfrac{\square \qquad \square}{(1 + 5) \cdot 2}\,\cdot$$

e nos dois buracos que aparecem botamos as expressões que estão nos lados desse $(\cdot)$:

$$\dfrac{(1 + 5) \qquad 2}{(1 + 5) \cdot 2}\,(\cdot)$$

Agora '2' já é uma expressão *atômica* (ou seja, inquebrável), mas a '$(1+5)$' não é; então repetimos o mesmo processo nela:

$$\dfrac{\dfrac{1 \qquad 5}{(1+5)}\,{+} \qquad 2}{(1+5)\cdot 2}\,(\cdot)$$

Chegamos finalmente na árvore

$$\dfrac{\dfrac{1 \qquad 5}{(1+5)}\,(+) \qquad 2}{(1+5)\cdot 2}\,(\cdot)$$

que mostra como a expressão aritmética '$(1+5)\cdot 2$' que é a *raiz* (ou *root*) dessa árvore é composta por os numerais 1, 5, e 2 que são as suas *folhas* (ou *leaves*).

? **Q1.81. Questão.** Mas, como assim "de derivação"? O que derivamos?

!! SPOILER ALERT !!

Resposta. Podemos visualizar a árvore acima como uma derivação (demonstração!) da afirmação «'$(1+5)\cdot 2$' é uma expressão de aritmética» que podemos simbolizar assim:

$$(1+5)\cdot 2 : \mathsf{ArExp}.$$

Cada node da árvore (incluindo sua raiz e suas folhas) são afirmações, mesmo se a parte de afirmar fica invisível (implícita). Aqui todas as nodes têm a mesma parte invisível. Aqui a mesma árvore com nada invisível:

$$\dfrac{\dfrac{1 : \mathsf{ArExp} \qquad 5 : \mathsf{ArExp}}{(1+5) : \mathsf{ArExp}}\,(+) \qquad 2 : \mathsf{ArExp}}{(1+5)\cdot 2 : \mathsf{ArExp}}\,(\cdot)$$

§18. Mais erros

1.82. De lógica. Uma argumentação errada envolve concluir algo que não segue necessariamente pelas premissas usadas: talvez usamos incorretamente uma hipótese, talvez reduzimos incorretamente nosso alvo para outro, ... Assim, não conseguimos convencer uma pessoa que sabe pensar sobre a validade da nossa tese. Em termos de programação, nosso programa (i.e., nossa demostração) *não compilou!* Durante esse texto vamos encontrar e discutir várias *falácias*, ou seja, erros comuns em argumentação, mas não

vamos focar agora em criar e discutir uma lista de falácias aqui. Logo no Capítulo 2 estudaremos qual é a maneira correta de raciocinar e demontrar proposições e também discutimos umas falácias comuns (§40). Mas só pra te dar uma idéia desde já, vamos ver um exemplo duma argumentação.

• **EXEMPLO 1.83.**
Considere a inferência seguinte, que quer convencer alguém sobre a tese que uma certa árvore é uma oliveira.

> «Oliveiras têm azeitonas.
> Essa árvore tem azeitonas.
> Portanto, essa árvore é uma oliveira.»

Aqui a partir das hipoteses nas duas primeiras linhas, inferimos a tese (terceira).

? **Q1.84. Questão.** Tá tudo OK com essa inferência?

!! SPOILER ALERT !!

Resposta. Não, a inferência tá erradíssima, mesmo que sua conclusão—por sorte!—acontece que é válida: o processo de inferi-la, não foi! Compare com:

> «Jogadores de basquetes são fortes.
> Esse homem é forte.
> Portanto, esse homem é jogador de basquete.»

Observe que a estrutura da inferência é exatamente *a mesma* com a anterior. Não parecida; mesma! Outra maneira: substitua a palavra 'árvore' pela palavra 'pizza' na argumentação original.

1.85. De matemática. Usando propriedades inválidas, erros em cálculos, etc. Não tem muita coisa para discutir sobre esse tipo de erro: ficar acordado ajuda evitá-los.

1.86. De semântica. Isso acontece quando o que escrevemos realmente significa algo, mas não o que temos na nossa cabeça. É quando um programador escreveu seu cógido e ele compilou "com sucesso", mas o programa que foi criado não faz o que ele queria. Isso acontece muito dando definições como discutimos na Secção §4.

1.87. De ética e de estética. *Meio* brincando, quero analisar mais dois tipos de erros. *Erro ético* é uma escolha de nome ou notação desonesta, que ajuda o leitor—ou até o escritor—errar. *Erro de aestética* seria uma escolha de nome ou notação que quebra um padrão ou uma convenção estabelecida; algo que introduz uma complexidade desnecessária. Um bom programador dedica grande parte do seu tempo na escolha de nomes para suas variáveis, suas funções, etc. Um nome bom deve ajudar em pensar, carregar

informação correta sem ficar pesado ou cansativo para usar, etc. Com prática tu deves desenvolver um bom gosto nisso!

- **EXEMPLO 1.88.**
Considere a frase:

> «Para quaisquer $a, x, y \in \mathbb{Z}$ se a divide x e x divide y então a divide y.»

A escolha de nomes dessas variáveis não faz sentido nenhum. Queremos três nomes para os três inteiros que estão na mesma situação, moram no mesmo bairro, são parentes da mesma família. Não faz sentido quebrar a norma alfabética pegando um nome do bairro dos $a, b, c, \ldots$ e outros dois do bairro dos $x, y, z, \ldots$. Outra:

> «Seja n um número real e seja x o menor natural tal que $n \leq x$.»

Aqui temos um natural e um real e escolhemos a letra 'n' para o real. Bizarro.

§19. Nível coração e palavras de rua

TODO terminar

O maior objetivo deste texto é te ajudar elaborar teu entendimento de matemática nos dois níveis. Não faz sentido pensar que esses dois lados estão combatendo um o outro. Eles se ajudam e se completam, e estão dando à matemática sua elegância e beleza característica.

1.89. Dois níveis de entendimento.
TODO Escrever

1.90. Nível coração.
TODO Escrever

1.91. Conselho (palavras de rua). Vamos dizer que acabamos de definir um objeto. Então crie um apelido legal para esse objeto. Sinta-se à vontade virar de melhor amigo até um bully. Quais são as propriedades que ele tem? O que *característico* sabemos dele? É um conjunto? Então... se fosse um time, qual seria o nome dele? Se fosse uma banda, uma empresa, um vilarejo? E esses membros que já temos mencionado nele, como traduzem na nossa metáfora? É uma função? Talvez algo que termina em -or(a)? É uma relação? Então invente uma gíria significativa para a "situação" descrita por ela. Use tua imaginação, teu humor, inspira-se de coisas que tu conhece bem e que tu gosta. Quando puder, tente fazer isso em mais que uma maneira: no teu bairro então o tal objeto ganhou esse apelido; quais outros apelidos tu acha que ele tem em outros bairros? *Cada apelido, cada gíria, é mais uma ferramenta valiosa para pensar; não subestime esse processo!* E muitas vezes, uma metáfora boa num contexto, que nos ajudou pensar e chegar numa idéia linda, pode acabar nos limitando em outro, ou, até pior, nos ajudar errar, nos levar para caminhos inúteis, etc.

1.92. Lado mecânico. Aí chega o outro lado do entendimento que não vai nos permitir ser enganados e levados por esses caminhos errados. E, alem disso, nos momentos que nossas metáforas não nos ajudam, ou que simplesmente não temos nenhuma maneira "de rua" para descrever e pensar, ele pode nos dar o apóio para andar uns passos no jogo, seguindo agora nossa intuição elaborada jogando o jogo e conhecendo suas regras.

1.93. Conselho (jogo formal). No Capítulo 2 estudamos os principais conectivos de lógica que mais usamos em matemática. Lá enfatiso o ponto que matemática pode ser vista como um jogo formal, com suas regras e seu objetivo: o jogador joga escrevendo demonstrações e definições, seguindo as regras do jogo. Como tu vai ver, temos até um tabuleiro (de Dados/Alvos) e cada "movimento" no jogo é uma linha, que altera o estado desse tabuleiro. Quando tu tá tentando escrever ou entender uma demonstração, *fique atualizando esse tabuleiro no teu rascunho, com cada linha escrita ou lida!*

D1.94. Notação. Para enfatizar que estou. . . "caindo", "subindo", ou "entrando" ao nível coração, decoro os símbolos correspondentes com um ♡. Aqui uns exemplos imaginários para ilustrar:

$$r \overset{\heartsuit}{=} \text{o árbitro;} \qquad f(x) \rightsquigarrow g(x) \overset{\heartsuit}{\Longrightarrow} x \text{ é triste;}$$

$$G \overset{\heartsuit}{=} \text{os goleiros;} \qquad u < v \overset{\heartsuit}{\Longleftrightarrow} u \text{ observa } v;$$

$$g(T) \overset{\heartsuit}{=} \text{o goleiro do } T; \qquad r = g(A) \overset{\heartsuit}{\Longleftrightarrow} \text{o árbitro é o goleiro do } A;$$

$$N(x) \overset{\heartsuit}{=} \text{o bairro do } x; \qquad N(x) = N(y) \overset{\heartsuit}{\Longleftrightarrow} x, y \text{ são vizinhos.}$$

Leitura complementar

Matemática elementar: **[Sim03]** (para uma revisão rápida); **[Lan98]** (para uma (re)visão com mais detalhes).

Sobre geometria euclideana: **[Euc02]**, **[CG67]**; **[Har10]**.

Mais sobre falácias: **[Wik20]**.

Sobre linguagens: **[Cur12:** Cap. 2**]**.

CAPÍTULO 2

DEMONSTRAÇÕES

TODO terminar e arrumar

Neste capítulo estudamos varios tipos diferentes de proposições, e para cada uma discutimos qual é a maneira correta de usá-la para inferir algo novo, e também o que conta como argumentação válida para demonstrá-la. Para cada proposição precisamos saber:

- como atacá-la;
- como usá-la.

Aqui *atacar* significa *progressar em demonstrar*, e nesse contexto *matar um teorema* é sinónimo de *demonstrar um teorema*.[15] (Lembra do túmulo '∎' de Halmos?) A partir dessas "regras principais" e talvez outros princípios de lógica podemos derivar mais maneiras de usar ou de demonstrar proposições. Para realmente aprender como demonstrar teoremas, existe apenas um caminho: *demonstrando*. E vamos fazer isso no resto desse texto mesmo. Nosso objectivo aqui *não é* estudar profundamente estratégias de demonstração num contexto abstrato, mas apenas introduzir umas idéias e estabelecer uma terminologia e metodologia para nos ajudar demonstrar teoremas e falar sobre demonstrações. Durante esse capítulo vamos desenvolver uma *linguagem de demonstração* e usá-la como um "backend", uma low-level linguagem em qual as nossas demonstrações escritas numa linguagem mais humana "compilam".

TODO diss truth tables

§20. Demonstrações, jogos, programas

2.1. Existem várias maneiras de usar jogos para estudar demonstrações. Num dos mais comuns, é selecionada uma afirmação e dois jogadores estão jogando um *contra* o outro: um acredita na afirmação e está tentando demonstrá-la; o outro não, e está tentando refutá-la. Muitas variações disso existem e correspondem principalmente em alterações da "lógica por trás".

2.2. Mas aqui vamos usar terminologia de jogos numa maneira diferente, onde o jogo é jogado só por você mesmo, como um jogo de Solitaire ou de Minesweeper.[16] Tu estás jogando com um ou mais alvos, onde cada alvo é uma afirmação matemática que tu estás querendo matá-la (demonstrar). Para conseguir isso, tu tens na tua disposição: certas

[15] Vamos pegar emprestada muita da terminologia de *jogos* e de *programação* para nos ajudar comunicar certas idéias.

[16] Podes visualizar esses jogos como jogos de 2 jogadores onde teu oponente só joga uma vez (e joga primeiro) escolhendo a ordem das cartas no caso de Solitaire ou onde botar as minas no caso de Minesweeper. Após disso, quem joga é apenas você.

armas: os seus dados (hipoteses), definições, teoremas, etc., e finalmente *a própria lógica*, que é representada aqui por *as próprias regras do jogo*. O jogo é feito numa maneira que se não roubar (ou seja, se seguir as regras), então tua demonstração realmente estabelece a veracidade dos teus alvos.

2.3. Cadê o compilador?. Um dos maiores problemas em nossos primeiros contatos com matemática *de verdade*, é "roubar sem querer". Em programação, o compilador assume bastante um papel de regulador que não nos permite roubar. O desafio em matemática é que, escrevendo uma demonstração, estamos assumindo o papel tanto do programador quanto do compilador. No início isso pode aparecer uma carga muito pesada, mas praticando acaba sendo algo natural. No mesmo sentido, o programador iniciante "briga" com o compilador o tempo todo, e com mais experiência ele assume (conscientemente ou não) cada vez mais um papel de compilador mental também, e acaba brigando cada vez menos com o compilador da sua máquina.

2.4. O jogo e seu tabuleiro (REPL). Podemos pensar que o jogo acontece em duas partes. A primeira parte é a «Demonstração»: É aqui que o jogador (você) joga, onde cada movimento é escrever uma frase mais nessa parte. Chamamos essa parte também de *proof script*. A segunda parte é a tabela de Dados/Alvos. O enunciado do teorema que queres demonstrar cria o contexto da prova, ou seja, ele está deixando claro quais são os *dados*, e qual (ou quais) os *alvos*. Com cada movimento—ou seja, frase escrita na parte «Demonstração»)—a tabela dos Dados/Alvos muda para refletir a situação atual do jogo: o *estado* (ou *state*). Novos dados podem ser adicionados, uns alvos podem ser matados, outros nascidos. O jogo termina quando não tem mais nenhum alvo vivo.

As partes do jogo e seu tabuleiro parecem assim então:

Demonstração	**Dados**	**Alvos**

- **EXEMPLO 2.5.**
Nesse exemplo encontramos uma demonstração dum teorema sobre inteiros. Neste momento apenas siga essa demonstração, movimento-por-movimento, para entender a idéia desse jogo e nada mais. A afirmação que queremos demonstrar é a seguinte:

«Todos os quadrados de ímpares são ímpares.»

Primeiramente precisas entender bem a forma do teu alvo:

$$(\forall n : \mathsf{Int})\big[\, n \text{ ímpar} \implies n^2 \text{ ímpar} \,\big]$$

Bora começar jogar então!

Demonstração	**Dados**	**Alvos**
		$(\forall n : \mathsf{Int})\big[\, n \text{ ímpar} \implies n^2 \text{ ímpar} \,\big]$

Começamos com nossa primeira linha:

	Demonstração	**Dados**	**Alvos**
1	Seja x inteiro.	$x : \mathsf{Int}$	~~$(\forall n : \mathsf{Int})\big[\, n \text{ ímpar} \implies n^2 \text{ ímpar} \,\big]$~~ x ímpar $\implies x^2$ ímpar

	Demonstração	**Dados**	**Alvos**
1	Seja x inteiro.	$x : \mathsf{Int}$	~~x ímpar $\Longrightarrow$ x^2 ímpar~~
2	Suponha x ímpar.	x ímpar	x^2 ímpar

Neste momento, olhamos para o tabuleiro de Dados/Alvos e anotamos, como rascunho, o significado dumas dessas afirmações.

	Demonstração	**Dados**	**Alvos**
1	Seja x inteiro.	$x : \mathsf{Int}$	x^2 ímpar
2	Suponha x ímpar.	x ímpar	$\Updownarrow$
		$\Updownarrow$	$(\exists a : \mathsf{Int})[\, x^2 = 2a + 1 \,]$
		$(\exists k : \mathsf{Int})[\, x = 2k + 1 \,]$	

Poderiamos escrever uma *linha de comentário* na nossa demonstração, mas por enquanto quero mostrar apenas as *linhas de código* mesmo.

	Demonstração	**Dados**	**Alvos**
1	Seja x inteiro.	$x : \mathsf{Int}$	x^2 ímpar
2	Suponha x ímpar.	x ímpar	$\Updownarrow$
3	Seja $k : \mathsf{Int}$ tal que $x = 2k + 1$.	$k : \mathsf{Int}$	$(\exists a : \mathsf{Int})[\, x^2 = 2a + 1 \,]$
		$x = 2k + 1$	

	Demonstração	**Dados**	**Alvos**
1	Seja x inteiro.	$x : \mathsf{Int}$	x^2 ímpar
2	Suponha x ímpar.	x ímpar	$\Updownarrow$
3	Seja $k : \mathsf{Int}$ tal que $x = 2k + 1$.	$k : \mathsf{Int}$	$(\exists a : \mathsf{Int})[\, x^2 = 2a + 1 \,]$
4	Calculamos:	$x = 2k + 1$	
	$x^2 = (2k + 1)^2$	$x^2 = 2(2k^2 + 2k) + 1$	
	$\quad = 4k^2 + 4k + 1$		
	$\quad = 2(2k^2 + 2k) + 1$		

	Demonstração	**Dados**	**Alvos**
1	Seja x inteiro.	$x : \mathsf{Int}$	~~x^2 ímpar~~
2	Suponha x ímpar.	x ímpar	$\Updownarrow$
3	Seja $k : \mathsf{Int}$ tal que $x = 2k + 1$.	$k : \mathsf{Int}$	$(\exists a : \mathsf{Int})[\, x^2 = 2a + 1 \,]$
4	Calculamos:	$x = 2k + 1$	
	$x^2 = (2k + 1)^2$	$x^2 = 2(2k^2 + 2k) + 1$	
	$\quad = 4k^2 + 4k + 1$	x^2 ímpar	
	$\quad = 2(2k^2 + 2k) + 1$		
5	Usando o inteiro $2k^2 + 2k$, temos que x^2 é ímpar. ∎		

Matamos todos os alvos—só tinha um—então podemos concluir que o que queríamos demonstrar, foi demonstrado (ou seja: é um teorema mesmo).

2.6. Observação. O texto que a demonstração acabou sendo talvez pouco *feio*. Parece escrito por um robô que não entende nada (mas mesmo assim é eficaz). Não costumamos escrever demonstrações nesse jeito. Em vez disso, um texto "real e humano" que corresponde nessa demonstração seria algo do tipo:

> Seja x inteiro ímpar, e logo seja $k \in \mathbb{Z}$ tal que $x = 2k + 1$. Preciso mostrar que x^2 é ímpar também. Calculamos:
>
> $$x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$
>
> Como $2k^2 + 2k \in \mathbb{Z}$, logo x^2 é ímpar.

Mesmo assim, é importante entender o "backend" e esse lado *dinâmico* duma demonstração, em termos da tabela "Dados/Alvo(s)" e das mudanças que estão acontecendo nela. Então quando tu vai escrever tuas próprias demonstrações, pelo menos no início, podes aproveitar um rascunho para fazer teu *bookkeeping*, escrevendo e apagando coisas nele com cada frase que escreveu na tua prova. Com mais experiência, esse processo vai virar automático e subconsciente.

2.7. REPL. Muitas linguagens de programação hoje em dia têm *REPL:* Read–Eval–Print Loop. Começou em LISP e é exatamente o que ele promete. Um programa que: (1) lê expressões (em geral escritas pelo usuário); (2) calcula para achar o valor da expressão; (3) imprime o valor (4) loop para o (1). Executando o programa `python` por exemplo, abrimos uma sessão com o REPL da linguagem Python, e brincamos com o sistema. Abrindo o REPL certas coisas já estão definidas e carregadas na memória, e muitas vezes abrimos já especificando um *script*, um arquivo que contem linhas de código e que já defina várias coisas na nossa linguagem. Podemos pensar que uma demonstração é parecida com uma sessão num REPL, onde o script carregado é o enunciado da demonstração, e cada linha que escrevemos na demonstração corresponde numa linha que o programador escreveria no REPL. Uma diferença é que o demonstrador precisa assumir o papel de tanto do escritor quanto do sistema, não vai ver nada impresso, e nenhum cálculo vai ser feito *para* ele; tudo *por* ele mesmo. Consideramos então que os cálculos utilizados fazem parte da demonstração, e precisamos justificar cada passo deles. *Obviamente* certos passos deixamos sem justificativa se as consideramos óbvias, mas vejá também o Nota 2.30.

2.8. Linha de código vs. comentário. Vamos continuar pouco ainda mais essa metáfora relacionada a programação. Lendo um texto de demonstração certas partes valem como linhas de código e outras como comentários. *Linhas de código* tem efeito no tabuleiro do jogo: mudam algo nos alvos ou nos dados. *Comentários* servem o mesmo propósito em programação: ajudar o leitor (humano) do nosso código entender nossa idéia e seguir nossos passos; não fazem parte da demonstração; não oferecem nenhum progresso. Com prática—e dependendo de quem é o teu alvo (leitor)—tu vai ganhar uma noção de onde botar um comentário, quão detalhado deveria ser, etc.[17]

2.9. Keywords. Cada linguagem de programação tem seus *reserved keywords* que, quando usados corretamente formam expressões e outras construções da linguagem para finalmente virar um programa. Por exemplo uns keywords de C seriam os `if`, `while`,

[17] Cuidado pois existe um máu hábito de decorar programas com comentários demais, e o mesmo problema pode acontecer com demonstrações. Tanto em programação quanto em demonstração a dica é a mesma sobre escrever comentários: *escreva um comentário apenas se sua falta deixaria o leitor confuso.* Seja lacônico.

`int`, `void`, `switch`, etc. Observe que tem várias categorias sintacticamente corretas: expressões, comandos, literais, etc., e a gramática da linguagem não nos permite trocar uma frase duma categoria para uma frase de outra. Uma frase da categoria *declaração de variável*, por exemplo, precisa começar com uma frase da categoria *tipo* (por exemplo '`int`' seguida por uma frase da categoria *variável* (por exemplo '`x1`') e terminar com o '`;`'. Assim foi formada a declaração

```
int x1;
```

Lembra que falei que demonstrar e programar é a mesma coisa? Bem; em demonstrações, é a mesma coisa! Temos as categorias de frases, os keywords, e as regras que precisamos seguir para escrever frases bem formadas, e também as regras de lógica que precisamos respeitar, se é pra nosso código "compilar" e servir o seu propósito. Exemplos de keywords são *"seja"*, *"ou"*, *"suponha"*, *"tal que"*, etc.

§21. Atacando a estrutura lógica duma proposição

Enquanto nosso alvo não é atômico, podemos atacá-lo numa maneira direta, "batendo na lógica" mesmo. Similarmente, tendo dados não atômicos podemos usá-los na nossa demonstração considerando a estrutura lógica deles.

▸ **EXERCÍCIO x2.1.**
Até agora encontramos como usar os $\exists, \wedge$ e como atacar os $\forall, \exists, \to$. Para cada um dos conectivos que ainda não achamos como usar ou atacar, pense em: o que tu podes escrever na tua demonstração; o que efeito tem nos dados; e o que nos alvos.

	Usar	**Atacar**
$\forall x\, \varphi(x)$	?	«Seja u.» Novos dados: u Novo alvo: $\varphi(u)$
$\exists x\, \varphi(x)$	«Seja u tal que $\varphi(u)$.» Novos dados: u, $\varphi(u)$ Efeito nos alvos: –	«Demonstrarei $\varphi(u)$.» (eu escolho o u) Efeito nos dados: – Novo alvo: $\varphi(u)$
$\varphi \wedge \psi$	– Novos dados: φ, ψ Efeito nos alvos: –	?
$\varphi \vee \psi$	?	?
$\varphi \to \psi$	?	«Suponha φ.» Novo dado: φ Novo alvo: ψ
$\neg\varphi$	?	?

(x2.1 H 0)

§22. Igualdade

2.10. Leis da igualdade. *Aceitamos como parte da nossa lógica que a igualdade é: reflexiva, simétrica, e transitiva:*

$$\frac{}{\alpha = \alpha}\ \textsc{Refl} \qquad \frac{\alpha = \beta}{\beta = \alpha}\ \textsc{Sym} \qquad \frac{\alpha = \beta \qquad \beta = \gamma}{\alpha = \gamma}\ \textsc{Trans}$$

Além disso, aceitamos a lei de substituição: em qualquer fórmula ou qualquer termo podemos substituir um subtermo por um igual sem mudar o significado da fórmula ou termo.

2.11. O que eu ganhei?. Ganhando como dado o $\alpha = \beta$, tu agora podes substituir α por β e vice versa em qualquer contexto que eles aparecem!

2.12. Como atacar?. Simples: pega um lado, e calcule até chegar no outro! Às vezes fica difícil enxergar um caminho direto de α pra β; nesse caso tente pegar um lado até chegar num ponto γ; depois pega o outro lado e se conseguir chegar no mesmo ponto γ, teu alvo já era!

§23. Real-life exemplos: divisibilidade

Para brincar com algo da "vida real", vamos definir a relação de *dividir* entre números e demonstrar vários teoremas relacionados.

TODO espalhar os teoreminhas no capítulo todo e botar mais

Definição. Sejam $a, b \in \mathbb{Z}$. Digamos que *o a divide o b* (ou *o b é divisível por a*), sse $b = ak$ para algum $k \in \mathbb{Z}$. Nesse caso, escrevemos $a \mid b$. Em símbolos:

$$a \mid b \iff^{\text{def}} (\exists k \in \mathbb{Z})[\, b = ak \,].$$

Os *divisores* do a são todos os inteiros d tais que $d \mid a$. Naturalmente, usamos a notação $a \nmid b$ quando a não divide b.

• **EXEMPLO 2.13.**
$3 \mid 12$, porque $12 = 3 \cdot 4$ e $4 \in \mathbb{Z}$, mas $8 \nmid 12$, porque, nenhum inteiro u satisfaz $12 = 8u$. ↯

▸ **EXERCÍCIO x2.2.**
Qual o problema no Exemplo 2.13? (x2.2H0)

2.14. Proposição. *Sejam $a, b, m \in \mathbb{Z}$. Se $a \mid m$ e $b \mid m$, então $ab \mid m$.*

▸ DEMONSTRAÇÃO ERRADA. Como $a \mid m$, pela definição de $(\mid)$, existe $u \in \mathbb{Z}$ tal que $a = mu$. Similarmente, como $b \mid m$, existe $v \in \mathbb{Z}$ tal que $b = mv$. Multiplicando as duas equações por partes, temos

$$ab = (mu)(mv) = m(umv),$$

e como $umv \in \mathbb{Z}$, $ab \mid m$. ↯

▸ **EXERCÍCIO x2.3.**
Ache o erro na demonstração acima e *demonstre* que a proposição é falsa! (x2.3H12)

A falsa Proposição 2.14 tem uma "versão correta" que encontramos depois (Corolário 3.134).

▸ **EXERCÍCIO x2.4.**
Sejam $a, b, c \in \mathbb{Z}$. Demonstre ou refute cada uma das afirmações:

$$\begin{array}{ll}
\text{(i)} & a \mid b+c \implies a \mid b \ \&\ a \mid c \\
\text{(ii)} & a \mid b+c \ \&\ a \mid b-c \implies a \mid b \\
\text{(iii)} & a \mid b+c \ \&\ a \mid b+2c \implies a \mid b \\
\text{(iv)} & a \mid b+c \ \&\ a \mid 2b+2c \implies a \mid b \\
\text{(v)} & a \mid b+c \ \&\ a \mid 2b+3c \implies a \mid 3b+2c\,.
\end{array}$$

(x2.4H0)

§24. Conjunção

2.15. Entender.
TODO Escrever

2.16. O que eu ganhei?. Escrevendo como regras—agora temos duas—de inferência

$$\frac{\varphi \wedge \psi}{\varphi} \qquad \frac{\varphi \wedge \psi}{\psi}$$

Na prática, podes pensar que tendo como dado o $\varphi \wedge \psi$ tu ganha os dados φ e ψ.

2.17. Como eu ataco?. Para convencer alguém que $\varphi \wedge \psi$, precisamos convencê-lo que φ, e também convencê-lo que ψ. Ou seja, o alvo $\varphi \wedge \psi$ é reduzível em dois alvos: o φ e o ψ.

$$\frac{\varphi \qquad \psi}{\varphi \wedge \psi}$$

§25. Implicação

Controversial.

2.18. Entender. Pensando no que uma implicação realmente é, vamos visualizá-la como uma premissa:

«Prometo que B com a condição A.»

E o que é prometido caso que a condição A não for verdadeira? *Nada!* É importante entender essa parte, e talvez essa piada conhecida ajuda:

> Um filho tá gritando e seu pai vire e fala pra ele: *"se tu continuar gritando, eu vou bater em ti!"* O filho, com medo, imediatemente fica calado, e logo após seu pai bate nele.

A pergunta para pensar é: *o pai mentiu?* Em matemática entendemos a implicação numa forma que não culpa esse pai de mentiroso.[18] Entendemos a implicação

«se $__A__$ então $__B__$»

como uma promessa. Aqui o pai não prometeu nada no caso que seu filho parasse de gritar! Nesse exemplo bobo então, a afirmação do pai é verdadeira *trivialmente* como a gente fala: ou seja, como não aconteceu a *premissa*, não tem como culpá-lo de mentiroso, e logo a implicação inteira é verdadeira.

2.19. O que eu ganhei?. Tenho nos meus dados a implicação $\varphi \to \psi$. O que eu posso fazer agora, que não podia fazer antes? Considerando só essa proposição, nada demais! Sozinha parece inútil: pensando numa metáfora de jogo com cartas, para jogar essa carta e ganhar algo, preciso ter mais uma carta: sua *premissa* φ. Jogando ambas juntas, ganhamos a ψ. Podemos pensar então numa implicação $\varphi \to \psi$ como uma fabrica do dado ψ, só que para *funcionar*, ela precisa da proposição φ. Escrevendo como regra de inferência,

$$\frac{\varphi \to \psi \qquad \varphi}{\psi}$$

O nome dessa regra é *modus ponens*.

2.20. Como eu ataco?. Para convencer teu inimigo sobre a veracidade duma implicação $\varphi \implies \psi$ tu tens o direito de mandá-lo *aceitar* a premissa φ. No final das contas, ele tá duvidando a proposição ψ, *dado a proposição* φ. Ou seja, para atacar uma implicação $\varphi \to \psi$ escrevemos

> Suponha φ.

Assim ganhamos nos nossos dados o φ e nosso alvo é ψ.

§26. Existencial

[18] relaxe que tu podes culpar o pai para outras coisas se quiser

§27. Disjunção

2.21. Entender. A disjunção $\varphi \vee \psi$ representa uma informação ambígua, estritamente mais fraca que qualquer uma das φ, ψ: $\varphi \vee \psi$ é a proposição que pelo menos uma das φ, ψ é válida.

2.22. Silogismo disjuntivo.

TODO Escrever

§28. Negação

TODO Botando negações pra dentro

TODO Negando fórmulas atômicas

§29. Universal

2.23. Por vacuidade.

TODO Escrever

TODO arbitrário vs. aleatório

§30. Exemplos e contraexemplos

TODO elaborar e referir ao Cuidado 1.17

- **EXEMPLO 2.24.**
As afirmações seguintes são corretas:

(i) 21 é um contraexemplo para a: todos os múltiplos de 3 são pares;
(ii) 18 é um contraexemplo para a: todos os múltiplos de 3 são ímpares;
(iii) 18 é um contraexemplo para a: nenhum múltiplo de 3 é par;
(iv) 18 não é um contraexemplo para a: todos os ímpares são multiplos de 3;
(v) 18 não é um contraexemplo para a: todos os ímpares são múltiplos de 7;
(vi) 21 não é um contraexemplo para a: todos os ímpares são múltiplos de 3.

Vamos ver curtamente a razão de cada uma das últimas três: nas (iv) e (v) o 18 nem é ímpar então não tem chances de ser contraexemplo de qualquer afirmação que todos os ímpares fazem algo; na (vi) o 21 é ímpar mas ele *tem sim* a propriedade descrita, e logo também não é um *contra*exemplo.[19]

[19] Para misturar nossa conversa com a discussão sobre exemplos e nãœxemplos (1.15): acabei de listar aqui, em ordem: três exemplos de contraexemplos e três nãœxemplos de contraexemplos.

§31. Equivalência lógica

Intervalo de problemas

▸ **PROBLEMA Π2.1.**
Sejam $a, b \in \mathbb{Z}_{\geq 0}$. Digamos que *o a explode o b*, sse $b = a^n$ para algum $n \in ?$. Nesse caso, escrevemos $a \parallel b$. Dependendo do qual conjunto botamos no ? chegamos numa definição diferente:

$$a \parallel b \overset{\text{def}}{\iff} \begin{cases} (\exists n \in \mathbb{Z})[\, b = a^n \,] & \text{(Definição D1)} \\ (\exists n \in \mathbb{Z}_{\geq 0})[\, b = a^n \,] & \text{(Definição D2)} \\ (\exists n \in \mathbb{Z}_{>0})[\, b = a^n \,]. & \text{(Definição D3)} \end{cases}$$

Proposição P1: para quaisquer $a, b, c \in \mathbb{Z}_{\geq 0}$, se $a \parallel b$ e $b \parallel c$ então $a \parallel c$.
Proposição P2: para quaisquer $a, b \in \mathbb{Z}_{\geq 0}$, se $a \parallel b$ então $a \mid b$.
Proposição P3: para quaisquer $a, b, c \in \mathbb{Z}_{\geq 0}$, se $a \mid b$ e $b \parallel c$ então $a \mid c$.

Como cada proposição depende da definição de «explode» temos em total 9 proposições. Para cada uma delas, demonstre ou refute. (Π2.1 H 0)

§32. Ex falso quodlibet

2.25. Em qualquer momento durante uma demonstração, o estado é a tabela de Dados/Alvos, e nosso objetivo é mostrar que se os dados são todos verdadeiros, então os alvos também devem ser. Mas o que acontece se dentro dos nossos dados temos uma *inconsistência*, ou seja, nosso estado descreve uma situação impossível. Nesse caso, ganhamos trivialmente o jogo, pois conseguimos mostrar a impossibilidade dos dados acontecerem, então não temos nada mais pra fazer: matamos assim qualquer alvo pois garantimos que a premissa (que os dados são verdadeiros) é falsa. Na pratica isso significa que se em qualquer momento numa demonstração conseguimos como dado uma contradição ($\bot$), já podemos parar vitoriosamente: *explodimos o mundo inteiro, e logo nosso alvo morreu também.* Como regra, temos

$$\frac{\bot}{\varphi}$$

para qualquer φ.

§33. Feitiço: LEM

Suponha que está tentando demonstrar uma afirmação. Para matar esse monstro, em qualquer momento da tua prova, você pode separar em casos, e mostrar como matá-lo em cada um deles. Quando decidir atacar nessa maneira precisa tomar certos cuidados.

2.26. Nossos novos alvos. O alvo tá sendo clonado igualzíssimo para cada um dos casos.

2.27. Observação. Mas, peraí. A gente quer matar um monstro G. Depois desse passo de separar em, sei lá, 4 casos, agora nosso objectivo é matar 4 cópias desse monstro, uma em cada caso. Se fosse cada um desses novos monstros pelo menos um pouquinho mais fraco, o motivo de separar em casos faria sentido. Mas, como eu acabei de dizer, em cada caso temos que matar um clone de G. Não uma versão diferente de G. O mesmo G!

? **Q2.28. Questão.** Por que separar em casos então e multiplicar nossos alvos?

!! SPOILER ALERT !!

Resposta. Não é que teus novos alvos são mais fracos—pois eles não são—mas é você mesmo que fica mais forte em cada um deles. Em cada caso, ganhas mais uma arma: o dado que o próprio caso te oferece para matar esse mesmo alvo.

2.29. Não deixar nenhum caso por fora. Uma maneira de ter certeza que não esqueceu nada, é escolher uma propriedade A e separar nos dois casos complementares: A ou não A. Para um exemplo de como errar, suponha que queremos demonstrar que para todo inteiro n, o $n(n-1)$ é um múltiplo de 3. Consideramos dois casos:

- Caso $n = 3k$ para algum $k \in \mathbb{Z}$.
- Caso $n = 3k + 1$ para algum $k \in \mathbb{Z}$.

Em cada um deles, é fácil demonstrar que realmente $n(n-1)$ é um múltiplo de 3. Mas claramente temos um erro aqui, pois, como um contraexemplo tome o inteiro 5 e calcule: $5(5-1) = 20$, e com certeza 20 não é um múltiplo de 3. O problema é que em nossa separação em casos a gente não considerou todas as possibilidades! Esquecemos um terceiro caso:

> Caso contrário.

Como aprenderemos no Capítulo 3, a única possibilidade que deixamos, esse "caso contrário" é equivalente ao:

> Caso $n = 3k + 2$ para algum $k \in \mathbb{Z}$.

Uma separação em casos correta então seria considerar todos os:

- Caso $n = 3k$ para algum $k \in \mathbb{Z}$.
- Caso $n = 3k + 1$ para algum $k \in \mathbb{Z}$.
- Caso $n = 3k + 2$ para algum $k \in \mathbb{Z}$.

E com essa separação, felizmente, não podemos demonstrar essa afirmação errada, pois no terceiro caso, não temos como matar nosso alvo!

§34. Feitiço: RAA

§35. Feitiço: Contrapositivo

§36. Feitiço: NNE

§37. Feitiço: Disjunção como implicação

§38. Provas de unicidade

§39. Mais jargão e gírias

2.30. Óbvio, trivial, imediato: é mesmo?. Muitas vezes matemáticos costumamos deixar certos passos sem justificativas, ou até enfatizamos escrevendo palavras como «trivial», «imediato», «óbvio», «fácil». Muitas vezes essas palavras são usadas como sinônimos, mas seus significados não são exatamente iguais. *Trivial* é algo que não necessita pensar em nada, e é só fazer o trabalho de corno óbvio para terminar.[20] Note bem que isso significa que o escritor já sabe bem claramente *qual* é esse trabalho e com certeza *é capaz de fazê-lo até seu fim* caso que ele for desafiado. *Óbvio* e *fácil* são palávras notórias entre matemáticos, como também a frase «exercício para o leitor». Normalmente significa que os passos e/ou suas justificativas para uma parte da demonstração devem ser óbvios (quais exatamente são) para o leitor. O uso honesto de ambas é muito conveniente, mas infelizmente elas podem ser usadas também para criar uma *demonstração por intimidação*, a idéia sendo que o leitor não vai assumir que não consegue ver o passo "fácil" em questão, e logo vai aceitar a demonstração. *Nunca faça isso! Imediato* usamos dentro dum caso ou parte duma demonstração cujo alvo é *intensionalmente equivalente* a um dos dados, ou quando não falta nada para verificar.[21] Não fique obcecado com essas "definições" ou "instruções" sobre o uso dessas palavras; como falei: muitas vezes são usadas sinonimamente. Com experiência elaborarás uma noção melhor de quando e como usá-las.

[20] A palavra *trivial* também é usada para demonstrações de implicações cuja premissa é falsa, algo que vamos discutir na Secção §25.

[21] A palavra *imediato* também é usada para demonstrações por vacuidade.

§40. Erros comuns e falácias

2.31. Prova por repetição da definição. Imagine que uma pessoa tá querendo demonstrar que 3 divide 12 e considere a argumentação seguinte:

> «O 3 divide o 12 pois existe inteiro k tal que $3k = 12$.»

Para apreciar quão inútil seria isso, imagine um advogado defendendo um cara suspeito

> «Meu cliente é inocente, porque ele não matou a vítima.»

Ninguém deveria considerar essa frase como um argumento convincente e válido da inocência do acusado. Nesse contexto, «x é inocente» *significa* «x não matou a vítima». É *exatamente a mesma afirmação*, expressada com outras palavras. Ou seja, traduzindo o argumento do advogado, percebemos que o que ele falou mesmo foi:

> «Meu cliente não matou a vítima, porque ele não matou a vítima.»

ou

> «Meu cliente é inocente, porque ele é inocente.»

dependendo de qual direção da tradução escolhemos aplicar. Esse advogado não deveria ter muito sucesso no seu futuro assim![22]

2.32. Esquecer um dos ramos. Lembre-se o modus ponens:

$$\frac{\varphi \implies \psi \qquad \varphi}{\psi}\ \text{M.P.}$$

Que nos permite inferir a proposição ψ, pelas *duas* proposições

(1) $\varphi \implies \psi$;
(2) φ.

É comum esquecer sobre uma das duas e mesmo assim tentar inferir (a partir da outra) a mesma conclusão ψ. Estudando matemática é mais freqüente esquecer a φ; na vida real qualquer uma das duas pode acabar sendo "esquecida".

2.33. Refutação do antecedente.

TODO Escrever

2.34. Seja e demonstre vs. demonstre que todos.

TODO Escrever

[22] Infelizmente muitas pessoas caem por esse tipo de argumento na vida real, onde políticos, pastores, e advogados como o não-tão-fictício do meu exemplo, "argumentam" em maneiras erradas para convencer seus ouvidores (que não estudaram matemática).

2.35. Se vs. como. Considere as frases seguintes:

«Se $__A__$, $__B__$.»
«Como $__A__$, $__B__$.»

Observe que, em português, cada uma delas tem uma palavra implícita logo após da virgula:

«Se $__A__$, ($____$) $__B__$.»
«Como $__A__$, ($____$) $__B__$.»

Quais são? Na primeira frase a palavra implícita é a "então", e na segunda a "logo":

«Se $__A__$, (então) $__B__$.»
«Como $__A__$, (logo) $__B__$.»

Numa lida superficial as duas frases podem aparecer parecidas. Mas são bem, bem diferentes!

▸ **EXERCÍCIO x2.5.**
Qual é a diferença entre as duas frases? (x2.5H0)

! **2.36. Aviso (Declare apenas variáveis).** Não podemos "sejar" algo que envolve um termo. Não faz sentido escrever

> Seja $x + y$ natural.

por exemplo. Novamente: depois dum "seja" segue uma variável, inclusive fresca para evitar sombreamento (1.44). Voltando no exemplo da soma, não faria sentido escrever:

> Sejam x, y naturais. Seja $x + y$ a soma dos x e y.

Não! Já definimos a operação binária $(+)$ entre naturais, então não podemos "sejar" a expressão '$x + y$'. Quando "sejamos" algo como um membro arbitrário dum conjunto usamos apenas uma variável! Nem constantes, nem termos que envolvem operações. Imagine alguém escrevendo: «seja $3 \in \mathbb{Z}$», ou «seja $x^2 \in \mathbb{R}$». Não! A operação $-^2$ já é definida, e logo para qualquer real r o real r^2 já é definido! Para dar um exemplo para quem programou em linguagem similar à C. Tu escreverias essas declarações?

```
1  int 28;
2  float 1.2;
3  int x + 8;
4  int x * y;
```

Espero que não!

TODO complete and provide math and life examples

2.37. Mãe de todos.

TODO mother of all vs everybody has a mom

2.38. Seja vs. suponha. Vamos analisar pouco as duas frases que as vezes geram uns mal-entendidos: «Seja ...» e «Suponha ...». Vamos começar com umas perguntas:

TODO Terminar

2.39. Seja vs. existe.

TODO Escrever

§41. Deu errado; e agora?

TODO Erro na demonstração não é suficiente para dizer que o teorema é errado

TODO Conseqüência de teorema errado não é suficiente para concluir que a conseqüência é errada também

Problemas

▸ **PROBLEMA Π2.2.**
Sem saber qual afirmação é denotada por $\varphi(x,y)$, demonstre as equivalências:

$$(\forall x)(\forall y)[\,\varphi(x,y)\,] \iff (\forall y)(\forall x)[\,\varphi(x,y)\,]; \qquad (\exists x)(\exists y)[\,\varphi(x,y)\,] \iff (\exists y)(\exists x)[\,\varphi(x,y)\,].$$

(Π2.2 H 0)

▸ **PROBLEMA Π2.3.**
Sem saber qual afirmação é denotada por $\varphi(x,y)$, demonstre *uma* das duas direções da equivalência

$$(\forall x)(\exists y)[\,\varphi(x,y)\,] \overset{?}{\iff} (\exists y)(\forall x)[\,\varphi(x,y)\,].$$

Podes demonstrar ou refutar a outra? (Π2.3 H 0)

▸ **PROBLEMA Π2.4.**
Precisamos mesmo aceitar como axiomas todas as leis no Leis da igualdade 2.10? (Π2.4 H 12)

Leitura complementar

[**Niv05**]. [**Vel06**: Cap. 3].

CAPÍTULO 3

OS INTEIROS

Neste capítulo estudamos os inteiros e sua teoria: inicialmente demonstraremos as propriedades mais básicas, que talvez parecem quase infantis. Logo depois, neste capítulo ainda, encontramos e demonstramos os primeiros teoremas realmente lindos e interessantes. Além disso, andamos aqui nossos primeiros passos na *teoria dos números inteiros*. Terminamos com umas aplicações dessa teoria na área de criptografia; algo que deixaria muitos matemáticos do passado surpresos (e talvez frustrados): como uma coisa tão *pura* acaba sendo aplicada em algo tão... aplicado![23]

§42. Primeiros passos

3.1. Os (números) inteiros tu provavelmente já conheceu:

$$\ldots, \quad -3, \quad -2, \quad -1, \quad 0, \quad 1, \quad 2, \quad 3, \quad \ldots$$

Talvez tu não questiona sua existência—qualquer coisa que isso pode significar—e talvez não questiona nem suas propriedades que aprendeu enquanto criança.

Aqui não vamos *definir* então *o que é* um inteiro; o que significa ser um (número) inteiro.[24]

Em vez disso, vamos responder em outra pergunta: *como comportam os inteiros?* Os inteiros não são assim uns bichinhos soltos sem alma; eles chegam junto com uma *estrutura* feita por constantes (uns "destacados" inteiros, vamos dizer), umas operações, e ainda mais.

Sobre suas operações binárias (adição e multiplicação) provavelmente já foi ensinado que ambas são associativas, possuem identidades—talvez chamaram isso de elemento neutro?—, ambas são comutativas, o $-x$ é o oposto de x—o que isso significa mesmo?—, a multiplicação distribua-se sobre a adição, etc. etc.![25] Além dessas *operações*, nos inteiros temos uma *relação de ordem* cujas propriedades também devem ser conhecidas. Sabes, por exemplo, que para qualquer inteiro x temos $x^2 \geq 0$, e que para quisquer inteiros x, y tais que $x \leq y$, temos $-y \leq -x$, e muitas mais coisas.

Caso que tudo isso pareceu estranho pra ti, especialmente a questão sobre o que aceitar e o que não, está num caminho bom! Neste capítulo separamos exatamente o que vamos aceitar (axiomas e noções primitivas), e o que vamos demonstrar (teoremas) e definir (noções definidas). Eu não vou supor conhecimento sobre outras operações, e sugiro esquecê-lo desde já, pois pode acabar te confundindo. Tradicionalmente denotamos o conjunto dos inteiros por $\mathbb{Z}$.[26] Neste capítulo trabalharemos inteiramente no mundo

[23] Oi, G. H. Hardy!

[24] Caso que isso pareceu óbvio pra ti, segure tua reação até o Capítulo 16 onde vamos fazer exatamente isso: construir (definir) mesmo os inteiros!

[25] acabei assumindo que tu conheces certas palavras também (associativa, comutativa, etc.) mas isso não é essencial: se tu encontrou alguma palavra desconhecida (ou esquecida), se preocupe não; continue e vamos introduzir tudo diretinho daqui a pouco.

[26] *Zahl* em alemão significa número.

dos inteiros, e logo entendemos que os quantificadores $(\forall, \exists)$ *quantificam sobre os inteiros* exceto se explicitamente especificar algo diferente.

! 3.2. Aviso (Uma palavrinha). Considere as duas definições:

(i) Denotamos por A o conjunto cujos membros são todos inteiros.
(ii) Denotamos por B o conjunto cujos membros são todos os inteiros.

Vamos ver como uma palavrinha (aqui o *os*) pode fazer tanta diferença. A primeira não defina nada. O problema é que há mais que um conjunto que goza dessa popriedade: o conjunto $\{2, 5\}$ é mesmo um conjunto cujos membros são todos inteiros: ele só tem dois membros, e ambos são inteiros. Do $\{3, 4, 8\}$, também todos os membros são inteiros. Por isso, o uso do artigo definido *o* nesta frase é *plenamente errado*. Não podemos usá-lo sem garantir unicidade, e aqui é algo que não temos como garantir. Por outro lado, a segunda realmente defina um conjunto: o conjunto de todos os inteiros, que denotamos por $\mathbb{Z}$.

S3.3. Especificação (Os inteiros (1/5)). Usamos Int para denotar um tipo cujos membros chamamos de (números) inteiros e onde temos:

$$\begin{aligned} 0 &: \mathsf{Int} \\ 1 &: \mathsf{Int} \\ (+) &: \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int} \\ (-) &: \mathsf{Int} \to \mathsf{Int} \\ (\cdot) &: \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int}. \end{aligned}$$

Estipulamos as proposições seguintes como axiomas:

(ZA-Ass)	$(\forall a, b, c)[\, a + (b + c) = (a + b) + c \,]$
(ZA-IdR)	$(\forall a)[\, a + 0 = a \,]$
(ZA-InvR)	$(\forall a)[\, a + (-a) = 0 \,]$
(ZA-Com)	$(\forall a, b)[\, a + b = b + a \,]$
(ZM-Ass)	$(\forall a, b, c)[\, a \cdot (b \cdot c) = (a \cdot b) \cdot c \,]$
(ZM-IdR)	$(\forall a)[\, a \cdot 1 = a \,]$
(ZM-Com)	$(\forall a, b)[\, a \cdot b = b \cdot a \,]$
(Z-DistR)	$(\forall d, a, b)[\, (a + b) \cdot d = (a \cdot d) + (b \cdot d) \,].$

3.4. Associatividades sintácticas. Temos operações binárias nas nossas mãos que escrevemos com notações *infixas*: escrevemos $x + y$ para denotar a aplicação da $(+)$ nos argumentos x, y, em vez de optar para notação *prefixa* escrevendo $(+)(x, y)$ ou $+(x, y)$. Sem atribuir uma *associatividade sintáctica* para esses símbolos, expressões como as

$$a + b + c + d + e \qquad\qquad a \cdot (1 + a) \cdot b \cdot c$$

não significam nada! Dá pra entender que a primeira é pra ser uma soma (dos 5 termos a, b, c, d, e) e a segunda um produto (dos 4 termos $a, 1 + a, b, c$), mas tanto a $(+)$ quanto a

$(\cdot)$ são operações binárias e logo não podem *funcionar* nesse jeito. Escolhemos atribuir associatividade sintáctica à direita para ambas: dizemos que elas *associam à direita*. Assim, as expressões acima agora são apenas abreviações das

$$a + (b + (c + (d + e))) \qquad\qquad a \cdot ((1 + a) \cdot (b \cdot c)).$$

3.5. Precedência sintáctica. Queremos fazer mais um acordo sintáctico que vai nos permitir escrever expressões onde as duas operações parecem "em níveis iguais" como se estivessem brigando sobre quem vai receber o que como argumento. Considere as expressões:

$$a \cdot b + c \qquad\qquad a \cdot b + c \cdot d \cdot e + a.$$

Agora nem sabemos se elas denotam somatórios ou produtórios: A primeira é a soma dos 2 termos $a \cdot b, c$ ou o produto dos termos $a, b + c$? E a segunda é a soma dos 3 termos $a \cdot b, c \cdot d \cdot e, a$ ou o produto dos 4 termos $a, b + c, d, e + a$? Resolvemos atribuir à $(\cdot)$ uma precedência mais alta, dizendo que ela *pega mais forte* do que a $(+)$.[27] Assim, as expressões acima denotam somatórios e não produtórios:

$$(a \cdot b) + c \qquad\qquad (a \cdot b) + (c \cdot d \cdot e) + a.$$

3.6. Mais uma convenção sintáctica. Quando não tiver ambiguïdade, denotamos a aplicação da operação $(\cdot)$ silenciosamente, por *justaposição:* escrevemos ab para denotar o produto $a \cdot b$. Assim,

$$ab(c + da)bce \equiv a \cdot b \cdot (c + d \cdot a) \cdot b \cdot c \cdot e.$$

▸ **EXERCÍCIO x3.1.**
Para cada axioma que parece favorecendo o lado direito, sua versão esquerda é um teorema: o 0 é uma $(+)$-identidade-L; o 1 é uma $(\cdot)$-identidade-L; para todo a o $-a$ é um $(+)$-inverso-L de a; e a $(\cdot)$ distribui-se sobre a $(+)$ pela esquerda também:

(ZA-IdL)	$(\forall a)[\, 0 + a = a \,]$
(ZA-InvL)	$(\forall a)[\, (-a) + a = 0 \,]$
(ZM-IdL)	$(\forall a)[\, 1 \cdot a = a \,]$
(Z-DistL)	$(\forall d, a, b)[\, d \cdot (a + b) = (d \cdot a) + (d \cdot b) \,].$

(x3.1 H 1)

[27] A idéia aqui é imaginar as operações numa expressão como a $a+b\cdot c$ como ímãs atraindo os argumentos, e pela nossa atribuição o ímã $(\cdot)$ é mais forte e logo ele "ganha" tal briga e a expressão denota o $a + (b \cdot c)$. Mais num outro sentido, quem ganhou a batalha final foi a $(+)$: a expressão inteira acabou denotando um somatório e não um produtório.

3.7. Açúcar sintáctico: subtração. Será que esquecemos de adicionar nas operações primitivas a subtração? Não: introduzimos açúcar sintáctico para denotar a aplicação da operação *binária*

$$(-) \;:\; \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int}$$

de subtração definindo

$$a - b \stackrel{\text{def}}{=} a + (-b).$$

Observe que o símbolo $-$ tá sendo *sobrecarregado* mas o contexto sempre deixará claro qual das

$$(-) \;:\; \mathsf{Int} \to \mathsf{Int} \qquad\qquad (-) \;:\; \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int}$$

está sendo usada.

3.8. Açúcar sintáctico: numerais e potências. Introduzimos imediatamente as definições seguintes:

$2 \;:\; \mathsf{Int}$	$3 \;:\; \mathsf{Int}$	$4 \;:\; \mathsf{Int}$	$\cdots$
$2 \stackrel{\text{def}}{=} 1 + 1$	$3 \stackrel{\text{def}}{=} 2 + 1$	$4 \stackrel{\text{def}}{=} 3 + 1$	$\cdots$

Considerando que temos acesso aos números naturais definimos para qualquer inteiros x os símbolos

$x^0 \;:\; \mathsf{Int}$	$x^1 \;:\; \mathsf{Int}$	$x^2 \;:\; \mathsf{Int}$	$\cdots$
$x^0 \stackrel{\text{def}}{=} 1$	$x^1 \stackrel{\text{def}}{=} x \cdot x^0$	$x^2 \stackrel{\text{def}}{=} x \cdot x^1$	$\cdots$

! 3.9. Aviso (Três pontinhos). Nenhuma dessas definições pode ser aceita formalmente na sua inteiridade: parece que eu acabei de escrever uma linha infinita, introduzindo assim uma infinidade de novos símbolos. Mas calma: aceite por enquanto que cada nome desses que tu já conhece corresponde no que tu realmente entende, e logo vamos justificar *em maneira finita* o sistema posicional de numerais que conhecemos desde criança, justificando sim toda essa infinidade de nomes para os inteiros, e todas as potências (naturais) de qualquer inteiro x também.

▸ **EXERCÍCIO x3.2.**
Demonstre as leis de "passar termo por outro lado":

$$\begin{aligned}(\forall a, b, c)[\, a + b = c \iff a = c - b \,]\\ (\forall a, b, c)[\, a + b = c \iff b = c - a \,]\\ (\forall a, b)[\, a = b \iff a - b = 0 \,].\end{aligned}$$

▸ **EXERCÍCIO x3.3.**
Seja $\heartsuit$ uma operação binária. Demonstre que para quaisquer a, b, x,

$$a = b \implies a \heartsuit x = b \heartsuit x;$$
$$a = b \implies x \heartsuit a = x \heartsuit b.$$

Observe que isso tem como casos especiais que podemos somar (ou multiplicar) o mesmo inteiro nos dois lados duma equação (pelo mesmo lado), já que a operação binária $\heartsuit$ aqui é uma operação arbitrária. (x3.3H0)

▸ **EXERCÍCIO x3.4.**
Podemos "desfazer" a mesma operação nos dois lados?:

$$a \heartsuit x = b \heartsuit x \overset{?}{\implies} a = b.$$

(x3.4H0)

Θ3.10. Teorema.

(ZA-CanR) $(\forall a, b, c)[\, a + c = b + c \implies a = b\,]$;
(ZA-CanL) $(\forall a, b, c)[\, c + a = c + b \implies a = b\,]$.

Demonstração. Essa é tua: Exercício x3.5. ∎

▸ **EXERCÍCIO x3.5.**
Demonstre o Teorema Θ3.10. Cuidado: terminando uma, não faz sentido a outra ocupar um espaço parecido no teu texto! (x3.5H1)

▸ **EXERCÍCIO x3.6.**
Enuncie e refute a proposição correspondente para a multiplicação. (x3.6H0)

Θ3.11. Unicidade da (+)-identidade. *Existe único u tal que para todo x, $u + x = x = x + u$.*

Demonstração. Preciso demonstrar duas coisas.
Existência: existe pelo menos uma identidade aditiva. Essa parte é imediata pois já conhecemos uma (+)-identidade: o 0, pelas (ZA-IdR) e (ZA-IdL), que afirmam exatamente isso.
Unicidade: existe no máximo uma unicidade aditiva. Basta demonstrar que qualquer u que é uma (+)-identidade, necessariamente é o próprio 0:

$$(\forall u)[\, u \text{ é uma (+)-identidade} \implies u = 0\,].$$

Seja u uma (+)-identidade. Calculamos:

$$\begin{aligned} u &= u + 0 && \text{(pois 0 é uma (+)-identidade-R)} \\ &= 0. && \text{(pois } u \text{ é uma (+)-identidade-L)} \end{aligned}$$

∎

Θ3.12. Unicidade da $(\cdot)$-identidade. *Existe único u tal que para todo x, $ux = x = xu$.*

Demonstração. Essa também é tua: Exercício x3.7. ∎

▸ **EXERCÍCIO x3.7.**
Demonstre o Unicidade da $(\cdot)$-identidade Θ3.12. (x3.7H1)

Θ3.13. Unicidade dos inversos aditivos. *Para todo x, existe único x' tal que $x' + x = 0 = x + x'$.*

Demonstração. Seja x inteiro.
Existência: existe pelo menos um $(+)$-inverso de x. Imediato pois $-x$ é um $(+)$-inverso de x (pelas (ZA-InvR) e (ZA-InvL)).
Unicidade: existe no máximo um $(+)$-inverso de x. Seja x' um $(+)$-inverso de x. Ou seja, $x + x' = 0$ (usando apenas o fato que x' é um inverso direito). Como $-x$ também é um inverso direito, temos $x + (-x) = 0$. Preciso demonstrar que $x' = -x$. Calculamos:

$$\begin{aligned} x + x' &= 0 && (x' \text{ é um inverso direito de } x) \\ &= x + (-x) && (-x \text{ é um inverso direito de } x) \end{aligned}$$

Como $x + x' = x + (-x)$, logo $x' = -x$ (pela (ZA-CanL) com $c, a, b := x, x', -x$). ∎

O próximo lemmazão deixa muitos teoremas como corolários triviais.

Λ3.14. Unicidade de resoluções. *Para quaisquer a, b, existe único x tal que $a + x = b$ e existe único y tal que $y + a = b$.*

Demonstração. Teu também! (Exercício x3.8) ∎

▸ **EXERCÍCIO x3.8.**
Demonstre o Unicidade de resoluções Λ3.14. (x3.8H123)

▸ **EXERCÍCIO x3.9.**
Demonstre as unicidades anteriores (Θ3.11, Θ3.13) como corolários do Unicidade de resoluções Λ3.14. (x3.9H0)

Θ3.15. Teorema (Negação é involutiva). *Para todo x, $-(-x) = x$.*

Demonstração. Temos $x + (-x) = 0$ (1) (pela (ZA-InvR) com $a := x$). Também temos $(-(-x)) + (-x) = 0$ (pela (ZA-InvL) com $a := -x$). Logo $x = -(-x)$ (pela Unicidade de resoluções Λ3.14 com $a, b := (-x), 0$). ∎

▸ **EXERCÍCIO x3.10.**
Para todo a, $(-1)a = -a$. (x3.10H0)

▸ **EXERCÍCIO x3.11.**
Para quaisquer a, b, $(-a)b = -(ab) = a(-b)$. (x3.11H0)

▸ **EXERCÍCIO x3.12.**
Para quaisquer a, b, $(-a)(-b) = ab$. (x3.12H0)

▸ **EXERCÍCIO x3.13.**
Para quaisquer a, b, temos $-(a-b) = b-a$ e $-(a+b) = -a-b$. (x3.13H0)

!! SPOILER ALERT !!

3.16. Três candidatos. Três sugestões razoáveis nesse ponto seriam as seguintes:

(Z-AnnR) $(\forall a)[\, a \cdot 0 = 0\,]$
(Z-MCanR) $(\forall c, a, b)[\, c \neq 0 \;\&\; ac = bc \implies a = b\,]$
(Z-NZD) $(\forall a, b)[\, ab = 0 \implies a = 0 \text{ ou } b = 0\,]$.

O primeiro afirma que o 0 é um *anulador*; o segundo é a *lei de cancelamento multiplicativo pela direita*; o terceiro afirma que não há *zerodivisores* (no mundo dos inteiros). Com certeza todas devem ser satisfeitos pelo nosso sistema de inteiros; então que tal adicioná-las como axiomas?

3.17. Não tão rápido assim (1). Primeiramente precisamos ver se conseguimos *demonstrar* essas proposições, as ganhando assim como teoremas. Tente agora demonstrar cada uma delas e não desista fácil! Consegues alguma?

!! SPOILER ALERT !!

▸ **EXERCÍCIO x3.14.**
Demonstre que 0 é um $(\cdot)$-anulador:

(Z-AnnL) $(\forall a)[\, 0 \cdot a = 0\,]$
(Z-AnnR) $(\forall a)[\, a \cdot 0 = 0\,]$.

(x3.14H0)

3.18. Dois candidatos. Os (Z-MCanR) e (Z-NZD) são de fato *indemonstráveis* pelos axiomas que temos até agora. Por enquanto—e apenas por enquanto!—aceite isso, pois

realmente é um fato, e responda na próxima pergunta: *então já que são indemonstráveis, bora adicioná-los como axiomas?* O que achas?

!! SPOILER ALERT !!

3.19. Não tão rápido assim (2). Mesmo que realmente nenhuma das duas é demonstrável pelos axiomas atuais, não faz sentido adicioná-las simultaneamente: talvez uma das duas já é forte o suficiente para permitir demonstrar a outra. Neste caso, acontece que ambas são igualmente fortes: escolhendo qualquer uma das duas para adicionar nos nossos axiomas, podemos inferir a outra como teorema! Qual das duas vamos escolher então? Felizmente essa escolha não vai fazer nenhuma diferença matemática para nossos objetivos aqui. Mesmo assim, que seja apenas por motivos burocráticos e administrativos, precisamos fazer uma escolha—talvez jogando uma moeda no ar—então vamo lá:

S3.20. Especificação (Os inteiros (2/5)). Estipulamos mais um axioma:

(Z-NZD) $\qquad (\forall a, b)[\, ab = 0 \implies a = 0 \text{ ou } b = 0\,]$

Imediatamente demonstramos a outra proposição como teorema antes de esquecer:

Θ3.21. Teorema (A lei de cancelamento multiplicativo). *Temos:*

(Z-MCanR) $\qquad (\forall c, a, b)[\, c \neq 0 \;\&\; ac = bc \implies a = b\,].$

(Z-MCanL) $\qquad (\forall c, a, b)[\, c \neq 0 \;\&\; ca = cb \implies a = b\,].$

Demonstrarás agora. Exercício x3.15. ∎

▸ **EXERCÍCIO x3.15.**
Demonstre a lei de cancelamento multiplicativo. (x3.15H1)

§43. Divisibilidade

No Capítulo 2 já encontramos a relação de «divide» que realmente é a mais interessante relação para os inteiros. Será que vamos aumentar então a estrutura dos inteiros para incluí-la como *noção primitiva* com

$$(|) \;:\; \mathsf{Int} \times \mathsf{Int} \to \mathsf{Prop}?$$

Não! A noção de «divide» podemos realmente *definir* em termos do que temos até agora e logo não vamos adicioná-la como primitiva.

D3.22. Definição (Divisibilidade). Sejam $a, b \in \mathbb{Z}$. Digamos que *o a divide o b* (ou *o b é divisível por a*), sse $b = ak$ para algum $k \in \mathbb{Z}$. Nesse caso, escrevemos $a \mid b$. Em símbolos:

$$a \mid b \iff^{\text{def}} (\exists k \in \mathbb{Z})[\, b = ak \,].$$

Os *divisores* do a são todos os inteiros d tais que $d \mid a$. Naturalmente, usamos a notação $a \nmid b$ quando a não divide b.

Θ3.23. Teorema (Divide é uma preordem). *Para quaisquer inteiros a, b, c,*

$$\begin{array}{ll} a \mid a & \text{reflexividade} \\ a \mid b \;\&\; b \mid c \implies a \mid c. & \text{transitividade} \end{array}$$

Demonstrarás agora mesmo. Exercício x3.16. ∎

▸ **EXERCÍCIO x3.16.**
Demonstre o Teorema Θ3.23. (x3.16 H 0)

Θ3.24. Teorema (bottom). $(\forall a)[\, 1 \mid a \,]$.

Demonstrarás agora mesmo. Exercício x3.17. ∎

▸ **EXERCÍCIO x3.17.**
Demonstre o Teorema Θ3.24. (x3.17 H 0)

Θ3.25. Teorema (top). $(\forall a)[\, a \mid 0 \,]$.

Demonstração. Essa também é tua Exercício x3.18. ∎

▸ **EXERCÍCIO x3.18.**
Demonstre o Teorema Θ3.25. (x3.18 H 0)

Λ3.26. Lema (combinações lineares).

(i) $d \mid a \implies (\forall x)[\, d \mid ax \,]$;
(ii) $d \mid a \;\&\; d \mid b \implies d \mid a + b$;
(iii) $d \mid a \;\&\; d \mid b \implies (\forall x, y)[\, d \mid ax + by \,]$.

Demonstração. Todas tuas: Exercício x3.19. ∎

▸ **EXERCÍCIO x3.19.**
Demonstre todas as propriedades da Lema Λ3.26, com duas estratégias diferentes: (A) demonstre as duas primeiras, e mostre como ganhar a terceira como corolário delas; (B) demonstre a terceira, e mostre como ganhar as duas primeiras como corolário ela. (x3.19 H 0)

▸ **EXERCÍCIO x3.20 (sign-blind).**
Para quaisquer a, b, se $a \mid b$, então $-a \mid b$, $a \mid -b$, e (logo) $-a \mid -b$. (x3.20 H 0)

▸ **EXERCÍCIO x3.21.**
Sejam a, b, c inteiros com $c \neq 0$. Demonstre: $a \mid b \iff ca \mid cb$. Alguma das duas direções continua válida sem a hipótese $c \neq 0$? (x3.21 H 0)

§44. Conjuntos fechados sob operações

D3.27. Definição ((+)-fechado). Seja A um conjunto de inteiros. (Escrevemos: $A : \mathsf{Set\ Int.}$) Dizemos que A é *fechado sob adição* sse a soma de quaisquer $a, b \in A$ pertence ao A:

$$(\forall a, b \in A)[\, a + b \in A \,].$$

Também chamamos o A de (+)-*fechado*.

3.28. Observação. Dessugarizando a forma que escrevi a proposição acima obtemos

$$(\forall a, b \in A)[\, a + b \in A \,] \iff (\forall a, b : \mathsf{Int})[\, a, b \in A \implies a + b \in A \,].$$

A definição pode ser generalizada para qualquer operação n-ária (i.e., de aridade n— veja Nota 1.57).

▸ **EXERCÍCIO x3.22.**
Escreva a definição generalizada de «ser fechado sob uma operação binária», a deixando bem escrita. Cuidado: cada definição precisa começar estabelecendo primeiramente o contexto necessário para o conceito que queremos definir ser afirmável. (x3.22 H 1 2)

3.29. Proposição. *O conjunto*

$$3\mathbb{Z} \stackrel{\text{def}}{=} \{\, 3x \mid x \in \mathbb{Z} \,\}$$

é (+)*-fechado.*

Demonstração. Sejam a, b inteiros tais que $a, b \in 3\mathbb{Z}$. Vou demonstrar que $a + b \in 3\mathbb{Z}$. Vamos traduzir esses dois dados que temos sobre os a, b e nosso alvo também, já que todos envolvem a idéia de *pertencer ao* $3\mathbb{Z}$*:*

$$\begin{aligned} a \in \{\, 3x \mid x \in \mathbb{Z} \,\} &\iff (\exists x \in \mathbb{Z})[\, a = 3x \,]; \\ b \in \{\, 3x \mid x \in \mathbb{Z} \,\} &\iff (\exists x \in \mathbb{Z})[\, b = 3x \,]; \\ a + b \in \{\, 3x \mid x \in \mathbb{Z} \,\} &\iff (\exists x \in \mathbb{Z})[\, a + b = 3x \,]. \end{aligned}$$

Logo sejam $u, v \in \mathbb{Z}$ inteiros tais que $a = 3u$ (1) e $b = 3v$ (2). Precisamos escrever o $a + b$ na forma $3x$ para algum inteiro x. Calculamos:

$$\begin{aligned} a + b &= 3u + b && \text{(pela (1))} \\ &= 3u + 3v && \text{(pela (2))} \\ &= 3(u + v). && \text{(pela (Z-DistL))} \end{aligned}$$

Logo $a + b \in 3\mathbb{Z}$. ∎

3.30. Conselho («Pela escolha de»). Na demonstração da Proposição 3.29 precisamos citar os dados $a = 3u$ e $b = 3v$, e logo acabamos os rotulando, usando os rótulos (1) e (2), assim citando «pela (1)» e «pela (2)» no cálculo. Podemos evitar todo esse trabalho burocrático e conseguir citar *cada um desses dois dados* sem sequer rotulá-los. Como? A justificativa «pela escolha de...» serve exatamente pra isso. O cálculo acima fica assim:

$$\begin{aligned} a+b &= 3u+b && \text{(pela escolha de } u\text{)} \\ &= 3u+3v && \text{(pela escolha de } v\text{)} \\ &= 3(u+v). && \text{(pela (Z-DistL))} \end{aligned}$$

Mas o que exatamente significa esse *pela escolha de*? O seguinte: *Caro leitor, vá lá no momento que tal objeto foi declarado nesta demonstração, e olha que ele foi escolhido para satisfazer algo. É exatamente esse algo que estou citando aqui.*

• **NÃOEXEMPLO 3.31.**
O conjunto de todos os inteiros ímpares não é (+)-fechado (por quê?). Nem o conjunto de todos os inteiros não nulos (diferentes de 0) (por quê?). Nem o conjunto de todos os inteiros cujos numerais no sistema decimal não termina em '1' (por quê?).

▸ **EXERCÍCIO x3.23.**
Por quê? Por quê? Por quê? (x3.23H1)

▸ **EXERCÍCIO x3.24.**
O $\mathbb{Z}$ e o $\emptyset$ são fechados sob: adição, negação, subtração, multiplicação. O $\mathbb{Z}$ porque não tem como sair (já que é o universo inteiro); o $\emptyset$ porque não tem como entrar (e pra sair, precisa primeiro entrar). Verifique. (x3.24H0)

▸ **EXERCÍCIO x3.25.**
Generalize a noção de «ser fechado sob uma operação binária» ainda mais: considerando uma operação n-ária, de qualquer aridade $n \geq 1$. (x3.25H0)

▸ **EXERCÍCIO x3.26.**
Enuncie e demonstre uma versão mais geral dos dois extremos do Exercício x3.24. (x3.26H0)

3.32. Proposição. *Seja m inteiro. O conjunto*

$$m\mathbb{Z} \stackrel{\text{def}}{=} \{\, mx \mid x \in \mathbb{Z} \,\}$$

é fechado sob: adição (+), negação (−), subtração (−), multiplicação (·).

Demonstração. Adição. Basta substituir todos os '3' por 'm' na demonstração da Proposição 3.29, já que a única informação sobre o 3 que precisamos naquela demonstração foi que 3 é um inteiro.
Multiplicação. Sejam $a, b \in m\mathbb{Z}$ e logo seja u tal que $a = mu$. Calculamos:

$$\begin{aligned} ab &= (mu)b && \text{(pela escolha de } u\text{)} \\ &= m(ub) && \text{(pelo (ZM-Ass))} \\ &\in m\mathbb{Z}. \end{aligned}$$

NEGAÇÃO. Deixo pra ti (Exercício x3.27).
SUBTRAÇÃO. Isso é corolário fácil das duas anteriores pela maneira que definimos subtração. Vamos seguir os detalhes mesmo assim. Sejam a, b inteiros tais que $a \in m\mathbb{Z}$ (1), $b \in m\mathbb{Z}$ (2). Como $m\mathbb{Z}$ é fechado sob negação, temos $-b \in m\mathbb{Z}$ (3). Agora pelas (1) e (2) temos o desejado $a - b \in m\mathbb{Z}$, já que $m\mathbb{Z}$ é $(+)$-fechado. ∎

▸ **EXERCÍCIO x3.27.**
Demonstre que $m\mathbb{Z}$ é fechado sob a negação $(-)$. (x3.27 H 0)

▸ **EXERCÍCIO x3.28.**
Quais dos conjuntos abaixo são fechados sob quais das operações $(+), (-), (-), (\cdot)$?[28]

$$\begin{aligned} I &= \mathbb{Z}_{\neq 0} & A &= \{0, 4, 6, 10, 12, 16, 18, 22, 24, \dots\} \\ U &= \{0\} & B &= \{1, 2, 4, 8, 16, \dots\} \\ W &= \{0, 1\} & C &= \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} \\ T &= \{-1, 0, 1\} & D &= \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}. \end{aligned}$$

Antes de tudo, defina os conjuntos A, B, C, D sem usar '…', usando a notação set-builder. (x3.28 H 0)

? **Q3.33. Questão.** Por que nos limitar no caso $n > 1$ e não considerar o $n = 0$ também? O que significaria fechado sob uma operação nulária—aliás, faz sentido falar de operações nulárias?

!! SPOILER ALERT !!

3.34. Operações nulárias. Uma operação binária (de aridade 2) recebe 2 inteiros e retorna um inteiro. Uma operação unária precisa 1 inteiro para retornar um inteiro. Uma operação nulária (de aridade 0) então deve ser algo que recebendo… 0 inteiros, já retorna um inteiro. Podemos identificar isso com as constantes. Nesse sentido, afirmar que A é fechado sob 0 significa simplesmente que $0 \in A$, e similarmente sobre o 1.

▸ **EXERCÍCIO x3.29.**
Demonstre que se um conjunto F é fechado sob a *operação binária de subtração* $(-)$ então F deve ser $(+)$-fechado também, e mostre que o reciproco não é necessariamente verdadeiro. (x3.29 H 0)

? **Q3.35. Questão.** Demonstramos que o conjunto

$$m\mathbb{Z} \stackrel{\text{def}}{=} \{\, mx \mid x \in \mathbb{Z} \,\}$$

[28] Não finja que tu não entendeu o porquê que o $(-)$ foi repetido alí.

de todos os múltiplos de m é fechado sob adição e subtração. Será que podemos dizer algo sobre a direção contrária? Sabendo que um conjunto de inteiros F é fechado por adição e subtração, será que podemos inferir que existe um certo inteiro m tal que $F = m\mathbb{Z}$? Tente dar sua própria resposta nisso desde já; pois logo a gente voltar a resolver mesmo essa questão (com o Lema Λ3.92).

§45. Ordem e positividade

3.36. Algo está faltando (1). Mesmo que temos demonstrado tanta coisa importante sobre os inteiros, ainda falta um componente crucial que também faz parte da estrutura deles: a ordem ($<$), ou seja a noção de comparar dois inteiros e ver se um é menor que o outro ou não.

Parece então razoável aumentar a estrutura para

$$(\mathbb{Z}\,;\,0,1,+,-,\cdot,<)$$

com

$$(<) : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Prop}.$$

Isso apenas declara que tipo de coisa é esse ($<$): é uma relação binária nos inteiros. Não confunda isso com uma definição do que significa mesmo $x < y$.

3.37. Algo está faltando (2). Uma outra idéia seria aumentar a estrutura dos inteiros para incluir um *subconjunto* Pos de $\mathbb{Z}$: o subconjunto dos inteiros positivos. Em vez de complicar a tipagem considerando o Pos como um conjunto de inteiros mesmo, o declarando como

$$\mathrm{Pos} : \mathsf{Set}(\mathsf{Int}),$$

vamos considerar o Pos com a tipagem seguinte:

$$\mathrm{Pos} : \mathsf{Int} \to \mathsf{Prop}.$$

Ou seja, Pos não é, literalmente, o *conjunto* dos inteiros positivos; Pos é o *predicado* (unário) «__ é positivo». Escrevemos, de acordo com a tipagem,

$$\mathrm{Pos}\ x \qquad \text{ou} \qquad \mathrm{Pos}(x)$$

para significar «x é positivo». Mas observe que isso *não define* o Pos, pois não temos definido mesmo o que significa «ser positivo». Aqui estamos apenas falando como pronunciar a afirmação Pos x.

3.38. Bora adicionar?. Ambas as idéias parecem razoáveis, então talvez faria sentido adicionar ambas mesmo como partes primitivas nos inteiros, assim:

$$(\mathbb{Z}\,;\,0,1,+,-,\cdot,<,\mathrm{Pos})$$

com

$$(<) : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Prop} \qquad\qquad \mathrm{Pos} : \mathsf{Int} \to \mathsf{Prop}.$$

Mas realmente não precisamos ambas. Tendo uma (qualquer uma das duas), a outra é definível, em tal forma que seus axiomas correspondentes são demonstráveis como teoremas. Mesmo assim, precisamos escolher qual vai ser a primitiva; e aqui escolhemos a Pos.

S3.39. Especificação (Os inteiros (3/5)). Aumentamos a estrutura dos inteiros adicionando um predicado unário:

$$(\mathbb{Z}\,;\,0,1,+,-,\cdot,\mathrm{Pos})$$

com

$$\mathrm{Pos} : \mathsf{Int} \to \mathsf{Prop}.$$

Introduzimos logo como açúcar sintáctico um *abuso notacional* que nos permite tratar o predicado Pos *como se fosse* conjunto:

$$x \in \mathrm{Pos} \iff^{\mathsf{abu}} \mathrm{Pos}\ x.$$

Estipulamos os axiomas seguintes sobre os inteiros positivos:

(ZP-ACl)	$(\forall a, b \in \mathrm{Pos})[\, a + b \in \mathrm{Pos}\,]$	(Pos é $(+)$-fechado)
(ZP-MCl)	$(\forall a, b \in \mathrm{Pos})[\, a \cdot b \in \mathrm{Pos}\,]$	(Pos é $(\cdot)$-fechado)
(ZP-Tri)	$(\forall a)[\,\text{e.u.d.: } a \in \mathrm{Pos};\ a = 0;\ -a \in \mathrm{Pos}\,].$	

onde «e.u.d.» significa *exatamente uma das*.

D3.40. Definição (Negatividade). Seja x inteiro. Dizemos que x é *negativo* sse $-x$ é positivo. Introduzimos também a notação

$$\mathrm{Neg} : \mathsf{Int} \to \mathsf{Prop}$$

com o mesmo abuso notacional que nos permite tratá-la como se fosse conjunto.

D3.41. Definição (ordens). Tendo escolhido como primitiva a noção de positividade, queremos introduzir como açúcar sintáctico as notações usuais de ordem para poder escrever $x < y$, $x \geq y$, etc. Como podemos definir o que significa $x < y$?

Sejam x, y inteiros. Definimos as relações

$$(<), (\leq), (>), (\geq) : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Prop}$$

pelas

$$x < y \iff^{\mathsf{def}} y - x \text{ é positivo} \qquad x \leq y \iff^{\mathsf{def}} x < y \text{ ou } x = y$$
$$x > y \iff^{\mathsf{def}} y < x \qquad x \geq y \iff^{\mathsf{def}} y \leq x$$

3.42. Conjuntos ordenados. Relações binárias como a $(<)$ e a $(\leq)$ que definimos aqui são chamadas relações de ordem: a $(<)$ é uma ordem estrita, a $(\leq)$ não. Um conjunto cujos membros podemos comparar com uma relação de ordem destacada é chamado conjunto ordenado e mais pra frente vamos dedicar capítulos inteiros para seu estudo numa maneira abstrata. Por enquanto precisamos só trabalhar com o conjunto de inteiros, e com certeza sabemos como comparar inteiros: tanto com a $(<)$, quanto com a $(\leq)$.

▸ **EXERCÍCIO x3.30.**
Demonstre que para todo inteiro x, x é negativo sse $x < 0$. (x3.30 H 0)

Θ3.43. Teorema. *A relação* $(<)$ *goza das propriedades seguintes:*

(ZO-Trans) $(\forall a,b,c)[\,a<b \;\&\; b<c \implies a<c\,]$
(ZO-Tri) $(\forall a,b)[\,\text{exatamente uma das: } a<b;\ a=b;\ a>b\,]$
(ZO-A) $(\forall a,b,c)[\,a<b \implies a+c<b+c\,]$
(ZO-M) $(\forall a,b,c)[\,a<b \;\&\; c>0 \implies ac<bc\,]$.

Demonstração. Parte (ZO-Trans). Sejam a,b,c inteiros. Suponha $a<b$ e $b<c$, ou seja, $b-a\in\text{Pos}$ (1) e $c-b\in\text{Pos}$ (2). Preciso demonstrar $a<c$, ou seja, $c-a\in\text{Pos}$. Como Pos é $(+)$-fechado, pelas (1) e (2) temos $(b-a)+(c-b)\in\text{Pos}$. Basta então estabelecer que $(b-a)+(c-b)=c-a$. Calculamos:

$$\begin{aligned}
(b-a)+(c-b) &\equiv (b+(-a))+(c+(-b)) \\
&= (c+(-b))+(b+(-a)) && ((+)\text{-com. com } a,b := (b+(-a)),(c+(-b))) \\
&= ((c+(-b))+b)+(-a) && ((+)\text{-ass. com } a,b,c := (c+(-b)),b,-a) \\
&= (c+((-b)+b))+(-a) && ((+)\text{-ass. com } a,b,c := c,-b,b) \\
&= (c+0)+(-a) && (\text{(ZA-InvL) com } a := b) \\
&= c+(-a) && (\text{(ZA-IdR) com } a := c) \\
&\equiv c-a.
\end{aligned}$$

Parte (ZO-Tri). No Exercício x3.34
Parte (ZO-A). Sejam a,b,c inteiros. Suponha $a<b$, ou seja $b-a\in\text{Pos}$. Preciso demonstrar $a+c<b+c$, ou seja, $(b+c)-(a+c)\in\text{Pos}$. Calculamos:

$$\begin{aligned}
(b+c)-(a+c) &\equiv (b+c)+(-(a+c)) \\
&= (b+c)+(-1)(a+c) \\
&= (b+c)+((-1)a+(-1)c) \\
&= (b+c)+((-a)+(-c)) \\
&= (b+c)+((-c)+(-a)) \\
&= ((b+c)+(-c))+(-a) \\
&= (b+(c+(-c)))+(-a) \\
&= (b+0)+(-a) \\
&= b+(-a) \\
&\equiv b-a.
\end{aligned}$$

Parte (ZO-M). Sejam a,b,c inteiros. Suponha $a<b$ e $c>0$. Ou seja, $b-a\in\text{Pos}$ (1) e $c\in\text{Pos}$ (2). Vou demonstrar $ac<bc$, ou seja, $bc-ac\in\text{Pos}$. Mas $bc-ac=(b-a)c$ (por quê?) e realmente $(b-a)c\in\text{Pos}$ pelas (1) e (2), pois Pos é $(\cdot)$-fechado. ∎

▸ **EXERCÍCIO x3.31.**
Justifique cada linha do cálculo da demonstração de (ZO-A). (x3.31 H 0)

▸ **EXERCÍCIO x3.32.**
Tem algo feio nas primeiras 4 linhas desse cálculo aí. O quê? (x3.32 H 1)

▸ **EXERCÍCIO x3.33.**
Escreva o cálculo que não escrevi na demonstração de (ZO-M), justificando cada um dos seus passos. (x3.33 H 0)

▸ **EXERCÍCIO x3.34.**
Demonstre a parte (ZO-Tri) do Teorema Θ3.43. (x3.34 H 1 2)

Θ3.44. Teorema. *A relação $(<)$ é uma ordem estrita, ou seja, ela é transitiva, irreflexiva, e assimétrica:*

$$\begin{aligned}
(\forall a,b,c)[\,a<b \;\&\; b<c \implies a<c\,] &\qquad \text{transitiva}\\
(\forall a)[\,a \not< a\,] &\qquad \text{irreflexiva}\\
(\forall a,b)[\,a<b \implies b \not< a\,]. &\qquad \text{assimétrica}
\end{aligned}$$

Ainda mais, ela é conectada ou estritamente total:

$$(\forall a,b)[\,a\neq b \implies a<b \text{ ou } b<a\,] \qquad \text{conectada}$$

e portanto ela é uma ordem estrita total.

Demonstração. A transitividade já demonstramos no Teorema Θ3.43. O resto é o Exercício x3.35: ∎

▸ **EXERCÍCIO x3.35.**
A relação $(<)$ é *irreflexiva*, *assimétrica*, e *conectada*. (x3.35 H 0)

Θ3.45. Teorema. *A relação $(\leq)$ goza das propriedades seguintes:*

$$\begin{aligned}
(\forall a)[\,a\leq a\,] &\qquad \text{reflexividade}\\
(\forall a,b)[\,a\leq b \;\&\; b\leq a \implies a=b\,] &\qquad \text{antissimetria}\\
(\forall a,b,c)[\,a\leq b \;\&\; b\leq c \implies a\leq c\,] &\qquad \text{transitividade}
\end{aligned}$$

e por isso chamamos de ordem. Ainda mais ela goza da

$$(\forall a,b)[\,a\leq b \text{ ou } b\leq a\,] \qquad \text{totalidade}$$

e logo ela é ainda mais: uma ordem total.

Demonstrarás agora mesmo. É o Exercício x3.36. ∎

▸ **EXERCÍCIO x3.36.**
Demonstre que $(\leq)$ é uma ordem total (Teorema Θ3.45). (x3.36 H 0)

▸ **EXERCÍCIO x3.37.**
Sejam c, a, b inteiros. Se $c > 0$, então $ac < bc$ implica $a < b$. (x3.37 H 0)

▸ **EXERCÍCIO x3.38.**
Para quaisquer inteiros a, b, u, v, se $a < b$ e $u < v$, então $a + u < b + v$. (x3.38 H 0)

▸ **EXERCÍCIO x3.39.**
Sejam a, b, u, v inteiros. Demonstre, refute, ou mostre independente: se $a < b$ e $u < v$, então $au < bv$. (x3.39 H 0)

Λ3.46. Lema. *Para todo $a \neq 0$, a^2 é positivo.*

Demonstração. Seja a inteiro tal que $a \neq 0$. Vou demonstrar que a^2 é positivo. Separamos em casos: a positivo; $a = 0$; $-a$ positivo, onde o segundo caso é eliminado pela hipótese. Caso a positivo. Imediato pelo (ZP-MCl) (com $a, b := a$) pois $a^2 = a \cdot a$. Caso $-a$ positivo. Novamente pelo (ZP-MCl) (essa vez com $a, b := -a$) pois $a^2 = (-a)(-a)$. ∎

3.47. Proposição. *1 é positivo.*

Demonstração. Isso é um corolário imediato do Lema Λ3.46 pois $1 = 1^2$. ↯ ∎

? **Q3.48. Questão.** Qual o erro na demonstração acima?

!! SPOILER ALERT !!

Resposta. A demonstração aplica a

$$(\forall a)\big[\, a \neq 0 \implies a^2 \text{ é positivo} \,\big]$$

(o Lema Λ3.46) no inteiro 1, fingindo que isso fornece a proposição que 1^2 é positivo. Mas, olhando bem, o Λ3.46 aplicado no 1 fornece na verdade *a implicação*

$$1 \neq 0 \implies 1^2 \text{ é positivo}$$

então para conseguir mesmo seu lado direito (que é o que precisamos aqui), devemos conseguir seu lado esquerdo, $1 \neq 0$, que é algo que não temos demonstrado. Com certeza desejamos que $0 \neq 1$ para nossos inteiros, então ou precisamos demonstrá-lo para ganhar como teorema, ou estipulá-lo como axioma.

? **Q3.49. Questão.** Como podemos demonstrar $0 \neq 1$? Tente, antes de continuar para ver a resposta!

!! SPOILER ALERT !!

Resposta. Eu espero que tu deu pelo menos um esforço mental tentando demonstrar $0 \neq 1$. E eu sei que tu não conseguiu.[29] De fato, é algo que precisamos aceitar aqui como axioma:

S3.50. Especificação (Os inteiros (4/5)). Estipulamos o

(Z-NZero) $0 \neq 1$

como axioma para os inteiros.

Agora consertamos a demonstração do Teorema Θ3.51 e conseguimos finalmente o $1 > 0$:

Θ3.51. Teorema. *1 é positivo.*

Demonstração. Isso é um corolário imediato do Lema Λ3.46 pois $1 \neq 0$ e $1 = 1^2$. ∎

▸ **EXERCÍCIO x3.40.**
Demonstre que a equação $x^2 + 1 = 0$ não possui resolução no incógnito x. (x3.40 H 0)

§46. Mínima e máxima

D3.52. Definição. Definimos as operações binárias de mínimo e máximo:

$$\min_2 : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int} \qquad \max_2 : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int}$$

$$\min_2(x,y) \stackrel{\text{def}}{=} \begin{cases} x, & \text{caso } x \leq y; \\ y, & \text{caso } x > y; \end{cases} \qquad \max_2(x,y) \stackrel{\text{def}}{=} \begin{cases} y, & \text{caso } x \leq y; \\ x, & \text{caso } x > y. \end{cases}$$

Em notação infixa usamos os símbolos $(\wedge)$ e $(\vee)$, respectivamente.

▸ **EXERCÍCIO x3.41.**
Para cada uma das propriedades algébricas que temos destacado até agora investigue quais são satisfeitas pelos $(\wedge)$ e $(\vee)$. Não esqueça investigar possíveis distributividades. (x3.41 H 0)

D3.53. Notação. Sejam A um conjunto de inteiros e x um inteiro. Abusando a notação escrevemos $x \leq A$ e $A \leq x$:

$$x \leq A \stackrel{\text{abu}}{\iff} (\forall a \in A)[\, x \leq a \,] \qquad A \leq x \stackrel{\text{abu}}{\iff} (\forall a \in A)[\, a \leq x \,].$$

D3.54. Definição (mínimo, máximo). Seja A um conjunto de inteiros. Um membro $m \in A$ é chamado de *(membro) mínimo do* A sse para todo $a \in A$, $m \leq a$. Escrevemos

$$m = \min A \stackrel{\text{def}}{\iff} m \in A \ \ \& \ \ m \leq A.$$

Note que necessariamente um mínimo dum conjunto A, se existe, pertence ao A. Similarmente definimos a noção de *(membro) máximo* (Exercício x3.44).

[29] Caso que tu achas que conseguiu, tu acabou de ganhar um exercício bônus: ache o erro na tua demonstração!

! 3.55. Aviso (abuso notacional). Escrevendo ‘ $m = \min A$ ’ dá para confundir e pensar que se trata de uma igualdade. Na verdade é apenas uma conjunção disfarçada, vestindo roupas notacionais de (=).

Para justificar a definição do símbolo $\min A$, *devemos* demonstrar o seguinte:

▸ **EXERCÍCIO x3.42 (Unicidade de mínimo).**
Um conjunto de inteiros não pode ter mais que um mínimo. (x3.42 H 1 2)

▸ **EXERCÍCIO x3.43.**
Tecnicamente expressões como ‘ $\min A = \min B$ ’ e ‘ $\max A < \min B$ ’ também não foram definidas. Mesmo assim, é útil ter essas notações significando algo. Defina ambas atribuindo a elas seus significados desejados. (x3.43 H 0)

! 3.56. Cuidado. Definimos o predicado

$$_ = \min _ : \mathsf{Int} \times \mathsf{Set\ Int} \to \mathsf{Prop}$$

assim podendo escrever coisas como ‘ $1 = \min A$ ’; mas a expressão ‘ $\min A$ ’ sozinha não foi definida.

▸ **EXERCÍCIO x3.44 (E o máximo?).**
Defina o que significa *(membro) máximo* dum conjunto de inteiros A, e demonstre o que deves demonstrar junto com tua definição. (x3.44 H 0)

▸ **EXERCÍCIO x3.45 (de min pra max).**
Seja $A \subseteq \mathbb{Z}$. Definimos o conjunto $-A$ de todos os opostos de A assim:

$$-A \stackrel{\text{def}}{=} \{\, -a \mid a \in A \,\},$$

ou seja, $-A$ é o conjunto de todos os $-a$, tais que $a \in A$. Demonstre que se A possui mínimo, então $-A$ possui máximo e

$$\min A = -\max(-A)$$

e, dualmente, se A possui máximo, então $-A$ possui mínimo e

$$\max A = -\min(-A).$$

(x3.45 H 0)

§47. Valor absoluto

D3.57. Definição (valor absoluto). Introduzimos o operador unário

$$|_| : \mathsf{Int} \to \mathsf{Int}$$

definido por casos assim:

$$|x| \stackrel{\text{def}}{=} \begin{cases} x, & \text{se } x \geq 0; \\ -x, & \text{se } x < 0. \end{cases}$$

Chamamos o $|x|$ de *valor absoluto de* x.[30]

▸ **EXERCÍCIO x3.46.**
Para todo x inteiro, $|x| \geq 0$. (x3.46 H 0)

▸ **EXERCÍCIO x3.47.**
Para todo x inteiro, $|x| = 0 \iff x = 0$. (x3.47 H 0)

▸ **EXERCÍCIO x3.48 (idempotência).**
Para todo x inteiro, $||x|| = |x|$. (x3.48 H 1)

▸ **EXERCÍCIO x3.49.**
Para todo x inteiro, $|-x| = |x|$. (x3.49 H 1)

▸ **EXERCÍCIO x3.50.**
Demonstre: $(\forall a, u)[\, |a| \leq |u| \iff -|u| \leq a \leq |u|\,]$. (x3.50 H 0)

▸ **EXERCÍCIO x3.51.**
Demonstre: $(\forall a)[\, -|a| \leq a \leq |a|\,]$. (x3.51 H 0)

Θ3.58. Teorema. *Para quaisquer a, b inteiros,*

$$|a+b| \leq |a| + |b|\,.$$

Demonstração. Sejam a, b inteiros. Logo (x3.52)

$$-|a| \leq a \leq |a|$$
$$-|b| \leq b \leq |b|\,.$$

Logo (x3.52) $-|a| - |b| \leq a + b \leq |a| + |b|$.
Logo (x3.52) $-(|a| + |b|) \leq a + b \leq |a| + |b|$.
Logo (x3.52) $|a+b| \leq |a| + |b|$. ∎

▸ **EXERCÍCIO x3.52.**
Justifique em detalhe cada «logo» da demonstração do Teorema Θ3.58. (x3.52 H 0)

▸ **EXERCÍCIO x3.53.**
Sejam a, b inteiros. Demonstre: $|a| = |b| \implies a = b$ ou $a = -b$. (x3.53 H 0)

▸ **EXERCÍCIO x3.54.**
Sejam a, b inteiros. Demonstre: $||a| - |b|| \leq |a - b| \leq |a| + |b|$. (x3.54 H 0)

[30] O $|x|$ é conhecido em português como *módulo de* x, mas vamos falar tanto a palavra "módulo" que acho melhor usar o "valor absoluto" do *absolute value* para este uso.

▸ **EXERCÍCIO x3.55 (multiplicatividade).**
$(\forall a, b)[\,|ab| = |a|\,|b|\,]$. (x3.55 H 0)

§48. Indemonstrabilidade e metateoremas

3.59. Por que desistimos de demonstrá-la?. Se a gente tentar demonstrar uma proposição a partir duns axiomas e não conseguir produzir uma demonstração correta, podemos concluir que tal proposição é indemonstrável? Não necessariamente. Nosso insucesso não garanta que não vai chegar daqui uns dias um matemático que vai pensar em algo que nós não conseguimos pensar ainda. Enquanto demonstrar ou refutar uma proposição, se trata duma *questão aberta*. Mesmo assim, em certos casos podemos sim demonstrar que ninguém nunca vai conseguir nem demonstrar nem refutar uma certa proposição.

Considere como exemplo a proposição $0 \neq 1$. Podemos realmente *demonstrar* a *indemonstrabilidade da proposição* $0 \neq 1$ *a partir dos axiomas anteriores*. Isso se trata na verdade duma *metademonstração*, já que é uma demonstração sobre demonstrações sobre inteiros. Efetivamente podemos demonstrar a (meta)proposição: *não existe demonstração de* $0 \neq 1$ *a partir dos axiomas anteriores*. Podemos também demonstrar a *irrefutabilidade da* $0 \neq 1$ *a partir dos mesmos axiomas*, ou seja, a indemonstrabilidade da sua negação. Essas duas informações juntas fazem tal proposição ser *independente* dos axiomas anteriores: os axiomas não determinam sua vericidade, ou seja tanto a $0 \neq 1$ quanto a sua negação são *compatíveis* com os axiomas que trabalhávamos no momento.

Talvez numa primeira lida isso parece muito louco. Como demonstrar que algo é indemonstrável? Na verdade a idéia é bem simples: basta fazer duas coisas: (i) Construir um mundo onde todos os axiomas são válidos (precisamos verificar isso), e onde nossa proposição também é. (Isso significa que nossa proposição é *compatível* com tais axiomas.) (ii) Construir um mundo onde todos os axiomas são válidos e onde nossa proposição não é. (Isso significa que a negação da nossa proposição também é compatível com tais axiomas.) Se alguém chegar alegando que conseguiu demonstrar tal demonstração, sabemos que sua suposta demonstração seria errada pois a usando poderiamos inferir que a proposição deveria ser válida no mundo do (ii), que é impossível. Similarmente, se alguém afirmar que conseguiu refutar a mesma proposição, com certeza não conseguiu, pois tal suposta refutação geraria uma contradição graças ao mundo do (i). Concluimos então que ninguém pode nem demonstrar nem refutar tal proposição a partir dos axiomas.

3.60. A indemonstrabilidade de $0 \neq 1$**.** Mas o que mesmo significa *construir um mundo para o* $(\mathbb{Z}\,;0,1,+,-,\cdot,\mathrm{Pos})$*?* Simplesmente interpretar cada um dos seus componentes, em forma compatível com sua tipágem. E se todos os axiomas da especificação são válidos quando os interpretamos nesse mundo, o chamamos de *modelo* (ou *implementação*) da especificação.[31] Para nosso exemplo precisamos decidir: qual colecção de objetos vai servir o papel de $\mathbb{Z}$; qual objeto deles vai ser o 0; qual objeto deles vai ser o 1; quais vão ser as operações $+,-,\cdot$; e qual vai ser o predicado Pos (quais dos nossos "inteiros" vão ser chamados de "positivos").

Agora se a gente construir um mundo de

$$(\mathbb{Z}\,;0,1,+,-,\cdot,\mathrm{Pos})$$

31

onde todos os axiomas até agora são válidos, mas onde $0 \neq 1$ não é, seria uma garantia que não há tal demonstração e logo não faz sentido continuar pensando em achar uma, e portanto vamos adicioná-la como axioma, já que é algo fundamental para os inteiros que queremos axiomatizar aqui.

Eu deixo esse papel de construir tal mundo para ti (Problema Π3.5).

Intervalo de problemas

▸ **PROBLEMA Π3.1 (NZD vs. MCan).**
No texto escolhi adicionar como axioma a lei de não zerodivisores (Z-NZD) e demonstramos como teorema a lei de $(\cdot)$-cancelamento. Demonstre que o caminho contrário também é possivel, estabelecendo assim a equivalência das duas proposições a partir dos axiomas anteriores. (Π3.1 H 0)

▸ **PROBLEMA Π3.2 (Ordem como primitiva).**
Aqui escolhemos tratar a noção Pos de positividade como primitiva, e definimos a ordem $(<)$ em termos de Pos. Faça tudo que precisa para mostrar que o outro caminho é equivalente. (Π3.2 H 1)

▸ **PROBLEMA Π3.3 (A indemonstrabilidade da não trivialidade dos inteiros).**
Mostre que não tem como demonstrar $0 \neq 1$ pelos axiomas da Especificação S3.39 (Os inteiros (3/5)). (Π3.3 H 0)

▸ **PROBLEMA Π3.4 (A indemonstrabilidade da não zerodivisores dos inteiros).**
Mostre que não tem como demonstrar a (Z-NZD) pelos axiomas da Especificação S3.3 (Os inteiros (1/5)). (Π3.4 H 0)

▸ **PROBLEMA Π3.5.**
Retire o $0 \neq 1$ dos axiomas, e no seu lugar adicione a proposição superficialmente mais fraca:

(Z-NTriv) $\qquad (\exists u, v)[\, u \neq v \,]$

Demonstre $0 \neq 1$. (Π3.5 H 0)

§49. Wishlist

Estamos quase lá. Falta adicionar um axioma na nossa especificação para finalmente encerrar a sua elaboração e começar desfrutar teoremas da teoria dos inteiros. Mas vamos tentar fazer um *wishlist* do que desejamos conseguir. Queremos:

(1) (diversas versões de) indução;
(2) que os conjuntos de inteiros que são inferiormente cotados são *bem ordenados*;

(3) divisão (de Euclides);
(4) sistemas posicionais de numerais;
(5) mdc, mmc, e algoritmos para achá-los;
(6) teorema binomial;
(7) fatoração e teorema fundamental da aritmética;
(8) infinidade de primos (irredutíveis);

Assim que conseguir tudo isso continuaremos para elaborar aritmética modular e umas das suas aplicações, incluindo criptografia e assinaturas digitais.

§50. O princípio da boa ordem

D3.61. Definição (conjunto bem ordenado). Seja W um conjunto de inteiros. Chamamos o W de *bem ordenado* sse qualquer subconjunto habitado de W possui mínimo. Em símbolos:

$$W \text{ é bem ordenado} \overset{\text{def}}{\iff} (\forall H \subseteq W)[\, H \text{ habitado} \implies H \text{ possui mínimo}\,].$$

S3.62. Especificação (Os inteiros (5/5)). Estipulamos o princípio da boa ordem como último axioma:

(Z-WOP) O conjunto dos inteiros positivos é bem ordenado.

Θ3.63. Teorema. *Não existe inteiro k tal que $0 < k < 1$.*

Demonstração. Suponha que existe inteiro k tal que $0 < k < 1$. Preciso chegar numa contradição. Pela hipótese, o conjunto $C = \{\, c \in \mathbb{Z} \mid 0 < c < 1 \,\}$ de todos os tais inteiros é habitado (pelo menos pelo k). Logo, pelo PBO, seja $m = \min C$ o menor membro de C. Ou seja, sobre o m sabemos que: (a) $0 < m < 1$; (b) para todo $c \in C$, $m \leq c$. Eu vou achar um outro membro de C que é ainda menor que o m, assim contradizendo a escolha de m. Esse membro é o m^2. Basta demonstrar que: (i) $m^2 \in C$; (ii) $m^2 < m$. Como $0 < m < 1$ (pela (a)), logo multiplicando tudo por m temos $0m < mm < 1m$, ou seja, $0 < m^2 < m$, que já nos dá o (ii). Mas $m < 1$ e logo $0 < m^2 < m < 1$. Como $0 < m^2 < 1$, consegui o (i): $m^2 \in C$. Chegamos assim numa contradição, pois m foi escolhido para ser o menor membro de C. ∎

3.64. Corolário. *Para todo inteiro u, não existe inteiro k tal que $u < k < u + 1$.*

Demonstração. Tu demonstrarás isso agora no Exercício x3.56. ∎

▸ **EXERCÍCIO x3.56.**
Demonstre o Corolário 3.64. (x3.56 H 1 2)

3.65. Observação. Vamos supor que temos um conjunto de inteiros A e, ainda mais, sabemos que ele tem pelo menos um membro positivo. A PBO não parece aplicável no A já que ele pode possuir membros não positivos, assim não sendo um subconjunto do Pos. Mesmo assim, seu subconjunto

$$A_{>0} \stackrel{\text{def}}{=} \{\, a \in A \mid a \text{ positivo} \,\}$$

é feito totalmente por positivos e é habitado, e logo podemos sim usar o PBO para solicitar o menor membro de $A_{>0}$, ou seja, podemos solicitar *o menor membro positivo* de A.

▸ **EXERCÍCIO x3.57 (PBO shiftado).**
Sejam ℓ inteiro e A um conjunto de inteiros. Demonstre que se A possui membro $a \geq \ell$, então o $\{\, a \in A \mid \ell \leq a \,\}$ possui mínimo. (x3.57H0)

3.66. Observação (Conjuntos como predicados). Já encontramos a idéia de identificar objetos do tipo $\mathsf{Set}(\mathsf{Int})$ (conjuntos de inteiros) por predicados unários nos intéiros (objetos do tipo $\mathsf{Int} \to \mathsf{Prop}$). Aplicamos a mesma idéia aqui, no sentido contrário para olhar no princípio da boa ordem (até shiftado) numa versão formulada com predicados:

▸ **EXERCÍCIO x3.58 (PBO shiftado, predicate form).**
Sejam $\varphi : \mathsf{Int} \to \mathsf{Prop}$ e $\ell : \mathsf{Int}$ tais que para algum $x \geq \ell$, $\varphi(x)$. Logo existe um inteiro m tal que: (i) $\varphi(m)$; (ii) $m \geq \ell$; (iii) $(\forall x < \ell)[\, \neg\varphi(x) \,]$. (x3.58H0)

? **Q3.67. Questão.** Tu acha que deveriamos adicionar mais proposições como axiomas na nossa especificação? Cuidado: em geral, não queremos axiomas desnecessários: se podemos demonstrar algo a partir dos axiomas já estipulados, não faz sentido estipulá-lo como axioma também!

§51. Induções

Θ3.68. Teorema (Indução (set form)). *Para qualquer conjunto de inteiros P, se $1 \in P$ e P é (+1)-fechado,*[32] *então* Pos $\subseteq P$*, ou seja, todos os inteiros positivos pertencem ao P.*

▸ Esboço. Caso contrário, existeriam "contraexemplos", ou seja, inteiros positivos que não pertencem ao P. Aplicamos a PBO para escolher m como o menor deles e olhamos para o inteiro anterior que deve ser positivo e, ainda mais, menor que m, e logo pertence ao P, algo que obrigaria m também pertencer. □ (Θ3.68P)

3.69. Como usar. As versões de indução que demonstramos aqui são enunciadas em termos dum conjunto P que, satisfazendo certas condições, concluímos que deve possuir como membros todos os objetos do nosso interesse.

Na sua versão original, os objetos do nosso interesse são os inteiros positivos, e as condições que o P precisa satisfazer são:

$$1 \in P \qquad\qquad (\forall x)[\, x \in P \implies x+1 \in P \,]$$

[32] P é (+1)-fechado $\iff$ para todo $x \in P$, $x+1 \in P$

Lembre que quando a gente queria introduzir a noção dos inteiros positivos na nossa especificação, em vez de introduzí-la como conjunto, optamos para considerar como *predicado unário*. (Se não lembra: Nota 3.38.) Ainda mais, introduzimos logo apos açúcar sintáctico que nos permitiu identificar as duas abordagens, escrevendo $x \in \mathrm{Pos}$ e $\mathrm{Pos}\ x$ sinonimamente.

Vamos aproveitar essa equivalência entre os dois conceitos só que na direção contrária agora. Vamos visualizar o conjunto P dos objetos do nosso interesse como o predicado de «ser interessado», e escrever $P\ x$ em vez de $x \in P$, ou, voltando para o uso das metavariáveis gregas, $\varphi(x)$. Visto assim, isso é uma ferramenta para demonstrar proposições da forma

$$(\forall x \in \mathbb{Z}_{>0})[\,\varphi(x)\,]$$

onde φ é uma propriedade que inteiros podem ter ou não, ou seja:

$$\varphi : \mathsf{Int} \to \mathsf{Prop}.$$

Para demonstrar então que todos os *inteiros positivos* gozam da propriedade φ, basta demonstrar:

$$\varphi(1) \qquad\qquad (\forall x \geq 1)[\,\varphi(x) \implies \varphi(x+1)\,].$$

Θ3.70. Teorema (Indução (predicate form)). *Seja φ qualquer predicado unário afirmável sobre inteiros, ou seja, $\varphi : \mathsf{Int} \to \mathsf{Prop}$. Suponha que:*

(1) $\varphi(1)$*;*
(2) $(\forall x)[\,\varphi(x) \implies \varphi(x+1)\,]$.

Logo para todo inteiro positivo p, $\varphi(p)$.

JÁ DEMONSTRADO. Basta só traduzir as afirmações sobre conjuntos da demonstração do Θ3.68 para as correspondentes sobre predicados: $x \in P$ por $\varphi(x)$, etc. ∎

▸ **EXERCÍCIO x3.59.**
Demonstre o Teorema Θ3.63 usando indução. (x3.59H1234)

3.71. Corolário (Indução shiftada). *Para qualquer conjunto de inteiros P, se $\ell \in P$ e P é $(+1)$-fechado, então todos os inteiros x tais que $x \geq \ell$ pertencem ao P.*

▸ ESBOÇO. Aplicamos o princípio da indução no conjunto

$$P - \ell \stackrel{\mathsf{def}}{=} \{\, p - \ell \mid p \in P \,\}$$

de todos os membros de P "shiftados" por $-\ell$. □

A versão seguinte, conhecida como "indução forte" não merece seu apelido. A demonstramos como teorema e logo não se trata de algo mais forte mesmo. Mesmo assim, é muito mais natural e conveniente em certos casos e logo faz sentido a destacar.

3.72. Corolário (Indução forte). *Seja P conjunto de inteiros. Suponha*

$$(\forall x)(\forall 0 < i < x)[\, i \in P\,] \implies x \in P.$$

Logo todos os inteiros positivos pertencem ao P.[33]

DEMONSTRAÇÃO. Suponha que há inteiros positivos que não pertencem ao P. Seja m o menor deles (PBO). Logo, para todo positivo $i < m$, $i \in P$. Logo $m \in P$, e chegamos numa contradição. ∎

3.73. Regra de inferência. Graças ao Teorema Θ3.70 podemos enriquecer nosso sistema de demonstrações com a regra de inferência seguinte:

$$\frac{\varphi(1) \qquad (\forall k)[\,\varphi(k) \implies \varphi(k+1)\,]}{(\forall x > 1)[\,\varphi(x)\,]}\ \textsc{Ind}_{\varphi}$$

Essa corresponde à versão original; adaptá-la para as outras versões, é pra ti.

▸ **EXERCÍCIO x3.60.**
Escreva como regras de inferência as variações de indução que encontramos (shifted e forte). (x3.60 H 0)

§52. Somatórios e produtórios iterativos

3.74. Sejam s, t inteiros e $\tau(i)$ uma expressão em qual ocorre possivelmente a variável i. Queremos definir a notação $\sum_{i=s}^{t} \tau(i)$ para denotar a soma de todos os inteiros denotados pelos termos $\tau(s), \ldots, \tau(t)$, e similarmente a $\prod_{i=s}^{t} \tau(i)$ para denotar o seu produto:

$$\sum_{i=s}^{t} \tau(i) = \tau(s) + \cdots + \tau(t) \qquad\qquad \prod_{i=s}^{t} \tau(i) = \tau(s) \cdot \cdots \cdot \tau(t).$$

Caso $s > t$ não temos nenhum termo para operar, e logo se trata de somatório vazio e de produtório vazio respectivamente; e precisamos pensar qual seria o valor correto para cada um desses casos:

$$\sum_{i=s}^{t} \tau(i) = ? \qquad\qquad \prod_{i=s}^{t} \tau(i) = ?$$

Caso $s \leq t$ existem duas maneiras óbvias para definir cada um deles, ambas recursivas:

$$\sum_{i=s}^{t} \tau(i) \stackrel{\text{def}}{=} \begin{cases} \left(\sum_{i=s}^{t-1} \tau(i)\right) + \tau(t) \\ \ldots \text{ou} \ldots \\ \tau(s) + \sum_{i=s+1}^{t} \tau(i) \end{cases} \qquad \prod_{i=s}^{t} \tau(i) \stackrel{\text{def}}{=} \begin{cases} \left(\prod_{i=s}^{t-1} \tau(i)\right) \cdot \tau(t) \\ \ldots \text{ou} \ldots \\ \tau(s) \cdot \prod_{i=s+1}^{t} \tau(i). \end{cases}$$

[33] O quantificador no '$(\forall 0 < i < x)$' quantifica o i. Ou seja, essa parte no que escrevi acima, *desaçucarizando*, fica assim: $(\forall i)[\, 0 < i < x \implies i \in P\,]$.

D3.75. Definição (Somatório iterativo). Sejam s,t inteiros e $\tau(i)$ uma expressão em qual ocorre possivelmente a variável i. Definimos recursivamente:

$$\sum_{i=s}^{t} \tau(i) \stackrel{\text{def}}{=} \begin{cases} \left(\sum_{i=s}^{t-1} \tau(i)\right) + \tau(t), & \text{caso } s \leq t; \\ 0, & \text{caso } s > t. \end{cases}$$

▸ **EXERCÍCIO x3.61.**
Verifique que $\sum_{i=1}^{4} i = 10$, mostrando todos os passos do cálculo. (x3.61 H 0)

▸ **EXERCÍCIO x3.62.**
Demonstre que a definição alternativa

$$\sum_{i=s}^{t} \tau(i) \stackrel{\text{def}}{=} \begin{cases} \tau(s) + \sum_{i=s+1}^{t} \tau(i), & \text{caso } s \leq t; \\ 0, & \text{caso } s > t; \end{cases}$$

é equivalente à Definição D3.75. (x3.62 H 0)

▸ **EXERCÍCIO x3.63.**
Verifique que $\sum_{i=1}^{4} i = 10$, essa vez aplicando pelo menos uma vez a Definição D3.75 e pelo menos uma vez a propriedade do Exercício x3.62, novamente mostrando todos os passos do cálculo. (x3.63 H 0)

▸ **EXERCÍCIO x3.64.**
Já sabemos que não há diferença extensional entre as duas maneiras de definir somatórios. Há diferença intensional? (x3.64 H 0)

? **Q3.76. Questão.** Como definarias produtórios iterativos? Verifique tua tentativa calculando um produtório curto como o $\prod_{i=1}^{3} i$ antes de continuar.

!! SPOILER ALERT !!

D3.77. Definição (Produtório iterativo). Sejam s,t inteiros e $\tau(i)$ uma expressão em qual ocorre possivelmente a variável i. Definimos recursivamente:

$$\prod_{i=s}^{t} \tau(i) \stackrel{\text{def}}{=} \begin{cases} 1, & \text{caso } s > t; \\ \left(\prod_{i=s}^{t-1} \tau(i)\right) \cdot \tau(t), & \text{caso } s \leq t. \end{cases}$$

▸ **EXERCÍCIO x3.65 (Produtório iterativo).**
Obtenha os resultados correspondente aos exercícios x3.62 e x3.64. (x3.65 H 1)

► **EXERCÍCIO x3.66.**
Adivinhe um lado direito interessante e demonstre: $\sum_{i=s}^{t} c\tau(i) = ?$. (x3.66 H 1)

► **EXERCÍCIO x3.67.**
Mesma coisa: $\sum_{i=s}^{t} (\tau(i) + \sigma(i)) = ?$. (x3.67 H 1)

► **EXERCÍCIO x3.68 (split).**
$\sum_{i=s}^{t} \tau(i) = \sum_{i=s}^{?} \tau(i) + \sum_{i=?}^{t} \tau(i)$. (x3.68 H 1)

► **EXERCÍCIO x3.69 (index shift).**
$\sum_{i=s}^{t} \tau(i) = \sum_{i=?}^{?} \tau(i-d)$. (x3.69 H 1)

► **EXERCÍCIO x3.70.**
$\sum_{i=s}^{t} 1 = ?$ (x3.70 H 1)

► **EXERCÍCIO x3.71.**
$\prod_{i=s}^{t} c\tau(i) = ?$. (x3.71 H 1)

► **EXERCÍCIO x3.72.**
$\prod_{i=s}^{t} (\tau(i) \cdot \sigma(i)) = ?$. (x3.72 H 1)

► **EXERCÍCIO x3.73 (split).**
$\prod_{i=s}^{t} \tau(i) = \prod_{i=s}^{?} \tau(i) \cdot \prod_{i=?}^{t} \tau(i)$. (x3.73 H 1)

► **EXERCÍCIO x3.74 (index shift).**
$\prod_{i=s}^{t} \tau(i) = \prod_{i=?}^{?} \tau(i-d)$. (x3.74 H 1)

► **EXERCÍCIO x3.75.**
$\prod_{i=s}^{t} c^{\tau(i)} = ?$ (x3.75 H 1)

3.78. Reclamação. Os '$\sum$' e '$\prod$' que definimos aqui estão fazendo uma mistura de trabalhos e isso não é uma idéia boa: eles mesmo geram uma lista de termos simultaneamente somando e multiplicando seus termos. Isso dificulta tanto o trabalho de definir e manipular certos objetos, quanto o trabalho de demonstrar teoremas sobre eles. Seria melhor separar o trabalho de gerar uma lista (a partir duma expressão-padrão, um início, e um fim) e o trabalho de operar em forma generalizada nos seus componentes. Faremos isso no Capítulo 4.

► **EXERCÍCIO x3.76 (Somatório de Gauss).**
Demonstre que para todo inteiro $n \geq 0$,

$$2\sum_{i=1}^{n} i = n(n+1).$$

(x3.76 H 1)

▸ **EXERCÍCIO x3.77.**
Demonstre que para todo $n \geq 0$,

$$6\sum_{i=1}^{n} i^2 = 2n^3 + 3n^2 + n.$$

(x3.77 H 0)

▸ **EXERCÍCIO x3.78.**
Demonstre que para todo inteiro n,

$$\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i\right)^2$$
$$\text{ou seja,} \qquad 1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

(x3.78 H 0)

▸ **EXERCÍCIO x3.79.**
Qualquer número inteiro positivo $n \geq 8$ pode ser escrito como somatório de 3's e 5's. (x3.79 H 0)

▸ **EXERCÍCIO x3.80.**
Seja

$$\varphi(n) \overset{\text{def}}{\iff} 8(1 + 2 + \cdots + n) = (2n + 1)^2.$$

(i) Demonstre que para todo $k \geq 0$, se $\varphi(k)$ então $\varphi(k + 1)$.
(ii) Critique a oração: *«Logo, por indução, temos que para todo $n \geq 0$, $\varphi(n)$.»*.
(iii) Mudando apenas o '=' para '>' ou '<', defina um outro predicado $\psi(-)$ tal que para todo $n \geq 0$, $\psi(n)$ (demonstre por indução).

(x3.80 H 0)

▸ **EXERCÍCIO x3.81.**
Demonstre que para todo $n \geq 0$,

$$\sum_{i=0}^{n} F_i = F_{n+2} - 1,$$

onde, novamente, F_n o n-ésimo número Fibonacci. (x3.81 H 0)

▸ **EXERCÍCIO x3.82.**
Demonstre que para todo $n \geq 0$,

$$\sum_{i=1}^{n} F_i^2 = F_n F_{n+1},$$

onde F_n o n-ésimo número Fibonacci. (x3.82 H 0)

§53. Binomial e seus coeficientes

▸ **EXERCÍCIO x3.83.**
Demonstre que para quaisquer inteiros x, y, $(x+y)^2 = x^2 + 2xy + y^2$. (x3.83 H 0)

▸ **EXERCÍCIO x3.84.**
Demonstre que para quaisquer inteiros x, y, $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$. (x3.84 H 1)

3.79. Binomial. Nosso objetivo agora é generalizar para responder ao

$$(x+y)^n = ?$$

Facilmente percebemos que

$$(x+y)^n = x^n + \cdots + y^n$$

mas esse uso de '$\cdots$' é tão abusivo que parece até piada considerar como progresso. Podemos melhorar pouco, percebendo que no final das contas nossa resposta deve ser um somatório de termos $x^i y^j$. Por exemplo, no Exercício x3.84 achamos

$$\begin{aligned}(x+y)^3 &= xxx + xxy + xyx + yxx + xyy + yxy + yyx + yyy\\ &= x^3y^0 + x^2y + x^2y + x^2y + xy^2 + xy^2 + xy^2 + x^0y^3.\end{aligned}$$

O objetivo é *achar os coeficientes* de cada termo desses:

$$\begin{aligned}&= \underbrace{x^3y^0}_{1} + \underbrace{x^2y + x^2y + x^2y}_{3} + \underbrace{xy^2 + xy^2 + xy^2}_{3} + \underbrace{x^0y^3}_{1}\\ &= 1\,x^3y^0 + 3\,x^2y + 3\,xy^2 + 1\,x^0y^3.\end{aligned}$$

Observe também como podemos melhorar os i, j no x^iy^j: temos $i+j=n$, e logo podemos escrever tudo em termos de apenas uma variável (vou escolher a 'r'): $x^{n-r}y^r$. Sabemos então que $(x+y)^n$ pode ser escrito como um somatório de termos $x^{n-r}y^r$ e o desafio é achar para um deles quantas vezes precisamos somá-lo. Em outras palavras, procuramos o coeficiente de tal termo no somatório. Vamos denotar por $\binom{n}{r}$ o coeficiente do termo $x^{n-r}y^r$:

$$\begin{aligned}(x+y)^n &= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n\\ &= \sum_{r=0}^{n}\binom{n}{r}x^{n-r}y^r.\end{aligned}$$

Θ3.80. Teorema binomial. *Para qualquer $n \geq 0$ e qualquer $0 \leq i \leq n$, temos*

$$\binom{n}{r} = C(n,r).$$

Argumentação combinatorial. Queremos achar quantas vezes o termo $x^{n-r}y^r$ aparece na expansão do binomial. Escrevendo

$$(x+y)^n = \underbrace{(x+y)(x+y)\cdots(x+y)}_{n \text{ vezes}}$$

observamos que para cada das $C(n,r)$ maneiras de escolher r dos termos acima, corresponde um termo $x^{n-r}y^r$: "escolha quais dos termos desse produtório vão oferecer seus y's (o resto dos termos oferecerá seu x)". Isso justifica o $\binom{n}{r} = C(n,r)$. (Veja o Exemplo 3.81 para um exemplo.)

Demonstração. Por indução.
Base. Calculamos:

$$(x+y)^0 = 1;$$
$$\sum_{r=0}^{0} C(0,r)x^{n-r}y^r = C(0,0)x^{0-0}y^0 = 1\cdot 1\cdot 1 = 1.$$

Passo indutivo. Seja k tal que $(x+y)^k = \sum_{r=0}^{k} C(k,r)x^{k-r}y^k$ (HI). Calculamos:

$$\begin{aligned}(x+y)^{k+1} &= (x+y)(x+y)^k \\ &= x(x+y)^k y(x+y)^k \\ &\overset{\cdots}{=} \sum_{r=0}^{k+1} C(k+1,r)x^{k-(r-1)}y^r.\end{aligned}$$

Onde o '$\overset{\cdots}{=}$' é trabalho teu (Exercício x3.85). ∎

- **EXEMPLO 3.81.**
Para $n := 7$ e $r := 4$, a escolha indicada pelos termos sublinhados no

$$(x+y)^7 = (x+y)\,\underline{(x+y)}\,(x+y)\,\underline{(x+y)}\,\underline{(x+y)}\,(x+y)\,\underline{(x+y)}$$

corresponde ao termo $xyxyyxy = x^3y^4$, e cada diferente escolha das $C(7,4)$ corresponde ao mesmo termo mas com uma maneira diferente para formá-lo:

$$\underbrace{xxxyyyy,\ xxyxyyy,\ xxyyxyy,\ xxyyyxy,\ xxyyyyx,\ xyxxyyy,\ \ldots,\ yyxyxx,\ yyyyxxx}_{C(7,4)=35 \text{ strings feitos por 3 } x\text{'s e 4 } y\text{'s}}.$$

- **EXERCÍCIO x3.85 (Teorema binomial: por indução).**
Demonstre o Teorema binomial Θ3.80. (x3.85H1234567)

§54. O lemma da divisão de Euclides

Λ3.82. Lemma da Divisão de Euclides. *Dados inteiros a e b com $b \neq 0$, existem inteiros q e r tais que:*

(EucDiv) $$a = bq + r, \qquad 0 \leq r < |b|\,.$$

Além disso, os q e r são determinados unicamente.

▸ Esboço. Existência: Considera a seqüência infinita:

$$\ldots,\ a-3b,\ a-2b,\ a-b,\ a,\ a+b,\ a+2b,\ a+3b,\ \ldots$$

Verifique que ela tem elementos não-negativos e, aplicando a PBO, considere o menor deles. Unicidade: Suponha que $a = bq + r = bq' + r'$ para alguns $q, r, q', r' \in \mathbb{Z}$ tais que satisfazem as restricções $0 \leq r < |b|$ e $0 \leq r' < |b|$. Basta mostrar que $r = r'$ e $q = q'$. □

Por causa dessa existência e unicidade, podemos definir:

D3.83. Definição (Divisão). Dados $a, b \in \mathbb{Z}$ com $b > 0$, são determinados os inteiros q e r que satisfazem a (EucDiv). Chamamos o q de *quociente* e o r de *resto* da divisão de a por b e os denotamos por $quot(a, b)$ e $rem(a, b)$ respectivamente:

$$a = b\,quot(a,b) + rem(a,b) \qquad 0 \leq rem(a,b) < |b|\,.$$

▸ **EXERCÍCIO x3.86.**
Seja n positivo. Se $a_0, a_1, \ldots, a_{n-1}$ são n inteiros consecutivos, então $n \mid a_i$ para um único $i \in \{0, \ldots, n-1\}$. (x3.86 H 1 2 3)

▸ **EXERCÍCIO x3.87.**
Demonstre que para todo $n \in \mathbb{Z}$, se $3 \nmid n$ então $3 \mid n^2 - 1$. (x3.87 H 1)

▸ **EXERCÍCIO x3.88.**
Demonstre que dado qualquer inteiro a, existem únicos inteiros q e r tais que $a = 3q + r$ e $-1 \leq r \leq 1$. (x3.88 H 1)

§55. Expansão e sistemas posicionais

Até agora temos usado os numerais que conhecemos desde crianças para referir aos números inteiros. Considerei dado que tu já sabes todos esses (infinitos!) nomes de números, e que tu entendes como interpretar e "como funciona" esse sistema de numerais. Mas suponha que um ser alienígena que usa um sistema de numerais completamente diferente do nosso acha difícil acreditar que nosso sistema funciona mesmo: «Como vós sabeis[34]

[34] os alienígenas conjugam até no segundo plural, pelo jeito...

que não tem números inteiros sem numeral?» Nesta secção estudamos esse sistema, respondemos nessa e em mais perguntas, e encontramos outros sistemas posicionais de numerais.

3.84. Símbolos para os dígitos e separadores de casas. Para os sistemas posicionais com base $b \leq 10$ usamos os símbolos

$$\mathtt{0}, \mathtt{1}, \mathtt{2}, \mathtt{3}, \mathtt{4}, \mathtt{5}, \mathtt{6}, \mathtt{7}, \mathtt{8}, \mathtt{9}.$$

como dígitos. Quando a base b é maior mas ainda $b \leq 36$ usamos os

$$\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots, \mathtt{X}, \mathtt{Y}, \mathtt{Z}$$

com valores $10, 11, 12, \ldots, 33, 34, 35$ respectivamente. O sistema mais usado com base $b > 10$ é o *hexadecimal* com $b = 16$, onde realmente usamos os dígitos

$$\mathtt{0}, \mathtt{1}, \mathtt{2}, \mathtt{3}, \mathtt{4}, \mathtt{5}, \mathtt{6}, \mathtt{7}, \mathtt{8}, \mathtt{9}, \mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D}, \mathtt{E}, \mathtt{F}.$$

Tendo estabelecido um sistema de numerais para os *valores dos dígitos*, podemos simplesmente usar esses numerais sem se preocupar com os símbolos dos dígitos para escrever numerais de outros sistemas. Nesse caso separamos as casas com um símbolo novo (que não faz parte do nosso sistema de numerais estabelecido) como separador: usando o decimal escolhemos por exemplo o símbolo : como separador das casas e assim podemos escrever o número 151208 no sistema sexagesimal assim:

$$42 : 0 : 8 = 42 \cdot 60^2 + 0 \cdot 60^1 + 8 \cdot 60^0.$$

3.85. Observação. Muitas linguagens de programação usam o prefixo `0x` como indicação que o numeral que segue é hexadecimal. Similarmente o `0o` (ou simplesmente um numeral que começa com `0`) indica octal, e o `0b` binário. Por exemplo `0x20` seria o numero $20_{(16)}$, ou seja o 32; `0b100` seria o $100_{(2)}$, ou seja o 4, e `0750` ou `0o750` seria o $750_{(8)}$, ou seja o 488. Essas são apenas convenções que certas linguagens seguem, então em forma geral não conte com nenhuma delas (a mais estabelecida sendo a do `0x`).

Θ3.86. Teorema (expansão em base). *Seja $b \geq 2$. Todo inteiro $x \geq 0$ tem uma única expansão em base b: existem únicos $m, d_0, \ldots, d_m$ tais que:*

$$x = d_m b^m + \cdots + d_1 b^1 + d_0 b^0$$

onde:

(i) para todo $i \in \{0, \ldots, m\}$, $d_i \in \{0, \ldots, b-1\}$;
(ii) $d_m = 0 \implies m = 0$.

Demonstração. Demonstrarás agora, com duas maneiras diferentes: pelo princípio da boa ordem (Exercício x3.89) e por indução (Exercício x3.90). ∎

▸ **EXERCÍCIO x3.89.**
Demonstre o Teorema Θ3.86 pelo PBO. (x3.89 H 0)

▸ **EXERCÍCIO x3.90.**
Demonstre o Teorema Θ3.86 por indução. (x3.90 H 0)

TODO mencione mais non-standard positional systems: negabinary, complex-base, gray code

§56. Quando uma base não é suficiente

D3.87. Definição (Fibonacci). Definimos a seqüência dos *números Fibonacci* recursivamente assim:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_{n+2} &= F_{n+1} + F_n. \end{aligned}$$

D3.88. Definição (Lucas). Definimos a seqüência dos *números Lucas* recursivamente assim:

$$\begin{aligned} L_0 &= 2 \\ L_1 &= 1 \\ L_{n+2} &= L_{n+1} + L_n. \end{aligned}$$

▸ **EXERCÍCIO x3.91.**
Calcule o valor L_{12}. (x3.91 H 0)

TODO Computando seus valores

3.89. Proposição. *Para todo $n \geq 1$, seja*

$$\ell_n = F_{n-1} + F_{n+1},$$

onde F_n é o n-ésimo número Fibonacci (veja Definição D3.87). Queremos mostrar que para todo $n \geq 1$, $L_n = \ell_n$, onde L_n é o n-ésimo número Lucas (veja Definição D3.88).

▸ Demonstração errada. Nos vamos demonstrar por indução que *para todo* $n \geq 1$, $L_n = \ell_n$. Vamos primeiramente verificar que para $n = 1$, realmente temos $L_n = \ell_n$:

$$\begin{aligned} \ell_1 &= F_0 + F_2 && \text{(def. de } \ell_n\text{)} \\ &= 0 + F_1 + F_0 && \text{(def. de } F_n\text{)} \\ &= 0 + 1 + 0 && \text{(def. de } F_n\text{)} \\ &= 1 \\ &= L_1. && \text{(def. de } L_n\text{)} \end{aligned}$$

Seja $k \in \mathbb{N}$ com $k \geq 2$, tal que $L_{k-1} = \ell_{k-1}$. Realmente temos

$$\begin{aligned} L_k &= L_{k-1} + L_{k-2} && \text{(def. de } L_n\text{)} \\ &= \ell_{k-1} + \ell_{k-2} && \text{(H.I.)} \\ &= (F_{k-2} + F_k) + (F_{k-3} + F_{k-1}) && \text{(def. de } \ell_n\text{)} \\ &= (F_{k-2} + F_{k-3}) + (F_k + F_{k-1}) && \text{(ass. e com. de } (+)\text{)} \\ &= F_{k-1} + F_{k+1} && \text{(def. de } F_n\text{)} \\ &= \ell_k. && \text{(def. de } \ell_n\text{)} \end{aligned}$$

que termina nossa demonstração. ↯

▸ **EXERCÍCIO x3.92.**
Na demonstração acima roubamos. Ache onde e explique como, e pense numa solução. (x3.92H0)

3.90. Proposição. *Com a notação da Proposição 3.89, para todo $n \geq 1$, $\ell_n = L_n$.*

DEMONSTRAÇÃO. Nos vamos demonstrar por indução que *para todo* $n \geq 1$, $L_n = \ell_n$. Vamos primeiramente verificar que para $n = 1$ e $n = 2$, realmente temos $L_n = \ell_n$. Para $n = 1$:

$$\begin{aligned} \ell_1 &= F_0 + F_2 && \text{(def. de } \ell_n\text{)} \\ &= 0 + F_1 + F_0 && \text{(def. de } F_n\text{)} \\ &= 0 + 1 + 0 && \text{(def. de } F_n\text{)} \\ &= 1 \\ &= L_1. && \text{(def. de } L_n\text{)} \end{aligned}$$

E para $n = 2$:

$$\begin{aligned} L_2 &= L_1 + L_0 && \text{(def. de } L_n\text{)} \\ &= 1 + 2 && \text{(def. de } L_n\text{)} \\ &= 3 \end{aligned} \qquad \begin{aligned} \ell_2 &= F_1 + F_3 && \text{(def. de } \ell_n\text{)} \\ &= 1 + F_2 + F_1 && \text{(def. de } F_n\text{)} \\ &= 1 + 1 + 1 \\ &= 3. \end{aligned}$$

Seja $k \in \mathbb{N}$ com $k \geq 3$ tal que

$$L_{k-1} = \ell_{k-1} \qquad \text{e} \qquad L_{k-2} = \ell_{k-2}$$

(nossas *duas* hipoteses indutivas). Vamos demonstrar que $L_k = \ell_k$. Calculamos:

$$\begin{aligned} L_k &= L_{k-1} + L_{k-2} && \text{(def. de } L_n\text{)} \\ &= \ell_{k-1} + \ell_{k-2} && \text{(H.I.)} \\ &= (F_{k-2} + F_k) + (F_{k-3} + F_{k-1}) && \text{(def. de } \ell_n\text{, } k \geq 3\text{)} \\ &= (F_{k-2} + F_{k-3}) + (F_k + F_{k-1}) && \text{(ass. e com. de } (+)\text{)} \\ &= F_{k-1} + F_{k+1} && \text{(def. de } F_n\text{, } k \geq 3\text{)} \\ &= \ell_k, && \text{(def. de } \ell_n\text{)} \end{aligned}$$

que termina nossa demonstração. ∎

▸ **EXERCÍCIO x3.93.**
Ache uma nova demonstração do Exercício x3.79 por indução com três bases. (x3.93H1)

3.91. Duas maneiras de organizar tua demonstração. Ok, vamos supor que tu tá tentando demonstrar algo da forma

$$(\forall n \geq 0)[\,\varphi(n)\,]$$

por indução, e que tu decidiu usar duas bases (obviamente a $\varphi(0)$ e a $\varphi(1)$). Como seria teu passo indutivo? Tem duas maneiras boas para proceder agora:

MANEIRA 1: «Seja $k \geq 2$ tal que $\varphi(k-1)$ (H.I.1) e $\varphi(k-2)$ (H.I.2). Vou demonstrar que $\varphi(k)$.» Nessa maneira, preciso tomar cuidado que nenhum inteiro menor que $k-2$ aparece em algum canto errado, pois não sei nada sobre eles; até pior pode ser que aparecem objetos que nem são definidos.

MANEIRA 2: «Seja $k \geq 0$ tal que $\varphi(k)$ (H.I.1) e $\varphi(k+1)$ (H.I.2). Vou demonstrar que $\varphi(k+2)$.» E agora preciso tomar o mesmo cuidado, só que agora com inteiros menores que k.

Ambas as maneiras são corretas e bem escritas e bem entendíveis e tudo mais—e dá pra variar mais também, pois não são únicas (Exercício x3.94). Qual vamos escolher? Depende de gosto e às vezes do contexto também. Na maioria das vezes eu vou favorecer a primeira: meus olhos gostam da associação dos (H.I.i) com os $\varphi(k-i)$. Na mesma linha de pensar, na segunda maneira as hipoteses indutivas são as $\varphi(k)$ e $\varphi(k+1)$, e o alvo seria o $\varphi(k+2)$; então a (H.I.2) parece mais com o alvo do que com a (H.I.1). Ou seja: *nos meus olhos*, os dados e o alvo ficam mais arrumados na maneira 1. Mas como falei: ambas corretas; questão de gosto; então consulte teus próprios olhos.

▸ **EXERCÍCIO x3.94.**
Qual seria a terceira "óbvia" maneira? Com que inteiros tem que tomar cuidado se escolhê-la? (x3.94 H 0)

Intervalo de problemas

▸ **PROBLEMA Π3.6.**
Retire o (Z-WOP) e para cada $\varphi : \mathsf{Int} \to \mathsf{Prop}$, adicione o axioma seguinte:

$$\text{(Z-PI}_\varphi\text{)} \qquad \varphi(1) \;\&\; (\forall k > 0)[\,\varphi(k) \implies \varphi(k+1)\,] \implies (\forall x > 0)[\,\varphi(x)\,].$$

Consegues o (Z-WOP) como teorema? (Π3.6 H 0)

▸ **PROBLEMA Π3.7.**
PIF $\iff$ PIFF. (Π3.7 H 0)

▸ **PROBLEMA Π3.8 (Cadê a base da indução forte?).**
Seguindo o teorema acima, parece que não precisamos demonstrar uma "base" na indução forte. Critique a seguinte afirmação:

> Quando quero demonstrar um teorema da forma $(\forall n)[\,\varphi(n)\,]$ usando indução, eu preciso demostrar uma(s) base(s) $\varphi(0), \varphi(1), \ldots, \varphi(b-1)$ e depois demonstrar $\varphi(k)$ para algum k sobre qual tenho dadas as b hipoteses: $\varphi(k-1), \varphi(k-2), \ldots, \varphi(k-b)$. Por outro lado, usando indução forte eu preciso mostrar menos coisas: não tenho nenhuma base para demonstrar; e, além disso, no meu esforço para demonstrar o $\varphi(k)$, eu não vou ter apenas umas poucas b hipoteses indutivas, mas sim todos os $\varphi(i)$, um para cada $i < k$. Como os dois princípios são válidos, eu vou sempre usar indução forte.

(Π3.8 H 1)

▸ **PROBLEMA Π3.9.**
Na Secção §52 generalizamos os operadores binários (+) e (·) para versões iterativas. Mostre como fazer a mesma coisa para um operador binário arbitrário (♡). Quais propriedades dele precisamos? (Π3.9 H 0)

▸ **PROBLEMA Π3.10.**
Todo conjunto finito e habitado de inteiros possui membro mínimo e membro máximo. (Π3.10 H 1)

▸ **PROBLEMA Π3.11.**
Demonstre que para todo $n \geq 5$,

$$n^2 < 2^n.$$

(Π3.11 H 0)

▸ **PROBLEMA Π3.12 (Triminôs).**

TODO Escrever

(Π3.12 H 0)

▸ **PROBLEMA Π3.13 (Cavalos e aniversários).**
Vamos demonstrar o seguinte:

> «Para todo $n \geq 0$, em qualquer conjunto de n pessoas, só tem pessoas com o mesmo dia de aniversário.»

Suposta demonstração.

> *«Por indução no n.*
> Base. *Trivial: em qualquer conjunto de 0 pessoas, só tem pessoas com o mesmo aniversário, pois não tem nenhuma pessoa e logo não tem como achar pessoas de aniversários diferentes.*
> Passo indutivo. *Seja $k \geq 0$ tal que em qualquer conjunto de k pessoas, só tem pessoas com o mesmo dia de aniversário. Seja A conjunto de $k+1$ pessoas:*
>
> $$A = \{p_0, p_1, \ldots, p_{k-1}, p_k\}.$$
>
> *Considere os conjunto*
>
> $$A' = \{p_0, p_1, \ldots, p_{k-1}\}$$
> $$A'' = \{p_1, \ldots, p_{k-1}, p_k\}.$$
>
> *Ambos os A', A'' têm k pessoas, e logo pela hipótese indutiva todos os membros de A' têm o mesmo aniversário entre si; e também todos os membros de A'' têm o mesmo aniversário entre si. Como a pessoa p_1 está no A', todos os membros de A' têm o mesmo aniversário com o p_1. Mas a pessoa p_1 também etsá no A'', e logo todos os membros de A'' têm o mesmo aniversário com o p_1. Ou seja: todos os $p_0, p_1, \ldots, p_{k-1}, p_k$ têm aniversario no mesmo dia.»*

Numa maneira parecida podemos demonstrar várias afirmações doidas, como por exemplo a seguinte:

> «Para todo $n \geq 0$, em qualquer conjunto de n cavalos, só tem cavalos da mesma cor.»

Obviamente o que "demonstramos" é errado, e logo na demonstração existe pelo menos um erro—caso contrário seria uma indicação que o princípio da indução não é válido! Qual é? (Π3.13 H 0)

▸ **PROBLEMA Π3.14 (Balanced ternary).**
Para qualquer inteiro x existem únicos $m, d_0, \ldots, d_m$ tais que

$$x = d_m 3^m + \cdots + d_1 3^1 + d_0 3^0,$$

onde:

(i) para todo $i \in \{0, \ldots, m\}$, $d_i \in \{-1, 0, 1\}$;
(ii) $d_m = 0 \implies m = 0$.

Usando como digitos os símbolos `T`, `0`, `I` com valores -1, 0, 1 respectivamente podemos então escrever qualquer inteiro sem sequer precisar um símbolo de sinal para os negativos. Uns exemplos:

$$\begin{array}{rcl} 0 &=& 0\cdot 3^0 \quad\rightsquigarrow\quad \texttt{0} \\ 1 &=& 1\cdot 3^0 \quad\rightsquigarrow\quad \texttt{I} \\ 7 &=& 1\cdot 3^2 + (-1)\cdot 3^1 + 1\cdot 3^0 \quad\rightsquigarrow\quad \texttt{ITI} \\ -7 &=& (-1)\cdot 3^2 + 1\cdot 3^1 + (-1)\cdot 3^0 \quad\rightsquigarrow\quad \texttt{TIT} \\ 26 &=& 1\cdot 3^3 + 0\cdot 3^2 + 0\cdot 3^1 + (-1)\cdot 3^0 \quad\rightsquigarrow\quad \texttt{IOOT} \end{array}$$

(Π3.14 H 0)

▸ **PROBLEMA Π3.15.**
Demonstre por indução que para todo $n \in \mathbb{N}$, $\displaystyle\sum_{i=0}^{n} i \cdot i! = (n+1)! - 1$. (Π3.15 H 0)

▸ **PROBLEMA Π3.16 (Factorial base system).**
Os sistemas posicionais de numerais que encontramos até agora usam um fixo conjunto de dígitos para cada posição. Agora vamos encontrar um onde para cada posição i, podemos usar dígitos com valores nos $0, \ldots, i$. Na posição 0 então temos apénas uma opção: o próprio 0, e logo essa posição sempre tá ocupada por 0. Na posição 1 já temos dois dígitos disponíveis, com valores 0 e 1. Na posição 42 temos quarenta e dois dígitos disponíveis; seus valores são: o 0, o 1, o 2, ..., o 40, o 41, e o 42. Cuidado, vamos usar aqui seus valores como dígitos, mesmo que no papel o 42 que acabei de escrever dá a impressão que ele mesmo é composto por dois dígitos, mas não é o caso aqui! Por isso, usamos o : para separarar "as casas". O primeiro numeral em baixo seria válido, mas o segundo não

$$4 : 0 : 2 : 2 : 0 : 0 \qquad\qquad 5 : 2 : 4 : 2 : 0 : 0$$

pois na posição 3 tem o $4 > 3$. Novamente os valores dos dígitos vão acabar sendo coeficientes de algo que depende da posição e todos os termos serão somados. Como sempre, escrevemos um número x como

$$x = d_n a_n + d_{n-1} a_{n-1} + \cdots d_2 a_2 + d_1 a_1 + d_0 a_0 \qquad\qquad 0 \leq d_i \leq D_i$$

onde D_i denota o maior valor de dígito para a i-ésima posição. Neste sistema temos:

$$a_i = i! \qquad\qquad D_i = i$$

Demonstre que tal sistema "funciona": cada inteiro pode ser escrito neste sistema numa única maneira. (Π3.16 H 0)

TODO Dar exemplos para o problema seguinte ou transformar em discussão

▸ **PROBLEMA Π3.17.**
Uns leigos divulgando o LEM (§33) estão tentando vender a idéia que seria essencial para demonstrar mais proposições do que realmente é! (Π3.17H0)

§57. Mais sobre conjuntos fechados sob subtração

Vamos finalmente responder na pergunta Questão Q3.35. Um conjunto de inteiros fechado sob a *subtração* $(-)$ (e logo sob a $(+)$ também, pois Exercício x3.29), não tem muita liberdade na "forma" dele. O lemma seguinte mostra essa forma geral que todos eles devem ter.

Λ3.92. Lema. *Seja S um conjunto de inteiros não vazio e $(-)$-fechado. Logo $S = \{0\}$ ou existe inteiro $d > 0$ tal que S é o conjunto de todos os múltiplos de d:*

$$S = \{\, md \mid m \in \mathbb{Z} \,\}.$$

Demonstração. Suponha que $S \neq \{0\}$. Basta demonstrar que existe inteiro $d > 0$ tal que

$$S = \{\, md \mid m \in \mathbb{Z} \,\}.$$

Organizamos o resto da demonstração em três partes:

(A) Definir um $d > 0$ que será o inteiro positivo desejado: Exercício x3.95.
(B) Demonstrar que todos os multiplos de d pertencem ao S: Exercício x3.96.
(C) Demonstrar que nada mais pertence ao S: Exercício x3.97.

Com isso temos que o conjunto S e o conjunto de todos os múltiplos de d possuem exatamente os mesmos membros, que foi o que precisamos demonstrar. ∎

▸ **EXERCÍCIO x3.95.**
Resolva a parte (A) da demonstração do Lema Λ3.92. (x3.95H12)

▸ **EXERCÍCIO x3.96.**
E a (B). (x3.96H1)

▸ **EXERCÍCIO x3.97.**
Preciso mesmo enunciar? (x3.97H1)

▸ **EXERCÍCIO x3.98.**
Sem usar disjunção, escreva uma proposição equivalente com a conclusão do Lema Λ3.92 e explique por que ela é equivalente. (x3.98H1)

§58. Invertíveis, units, sócios

D3.93. Definição (invertibilidade). Seja x inteiro. Dizemos que x é $(\cdot)$-*invertível na esquerda* sse existe $(\cdot)$-inverso direito de x, e simetricamente definimos o que significa $(\cdot)$-invertível na direita. Em símbolos:

$$\begin{aligned} x \text{ é invertível-L} &\stackrel{\text{def}}{\iff} (\exists x')[\, xx' = 1\,]; \\ x \text{ é invertível-R} &\stackrel{\text{def}}{\iff} (\exists x')[\, x'x = 1\,]; \\ x \text{ é invertível} &\stackrel{\text{def}}{\iff} x \text{ é invertível-L } \&\ x \text{ é invertível-R}. \end{aligned}$$

Observe que já que $(\cdot)$ é comutativa as três afirmações são equivalentes para os inteiros.

D3.94. Definição (unit). Seja u inteiro. Dizemos que u é um *unit* sse ele consegue *medir* qualquer inteiro,[35] ou seja, sse para todo x, existe k tal que $uk = x$:

$$u \text{ unit} \stackrel{\text{def}}{\iff} (\forall x)(\exists k)[\, uk = x\,] \stackrel{\text{def}}{\iff} (\forall x)[\, u \mid x\,].$$

▸ **EXERCÍCIO x3.99.**
Demonstre que invertível e unit são sinônimos nos inteiros. (x3.99 H 0)

▸ **EXERCÍCIO x3.100.**
Sejam a, b inteiros com $ab = 1$. Demonstre que $a = b = 1$ ou $a = b = -1$. Conclua que os únicos inteiros invertíveis são os $1, -1$. (x3.100 H 0)

▸ **EXERCÍCIO x3.101.**
Demonstre:

$$\begin{aligned} (\forall a, b)[\, a \mid b \ \&\ b \mid a \implies |a| = |b|\,]; \\ (\forall a, b \geq 0)[\, a \mid b \ \&\ b \mid a \implies a = b\,]. \end{aligned}$$

(x3.101 H 0)

D3.95. Definição (Sócios). Seja a, b inteiros. Dizemos que os a, b são *sócios* (entre si) sse $a \mid b$ e $b \mid a$.

▸ **EXERCÍCIO x3.102.**
Justifique o plural e o «entre si» na definição acima. (x3.102 H 1)

▸ **EXERCÍCIO x3.103 (sócios e abs).**
Demonstre ou refute: para quaisquer inteiros a, b,

$$a, b \text{ sócios} \iff |a| = |b|\,.$$

(x3.103 H 1)

[35] Euclides mesmo usou o verbo «medir» em vez do verbo «dividir» que usamos hoje.

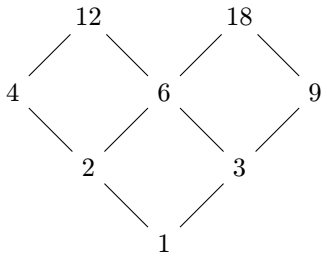
▸ **EXERCÍCIO x3.104 (sócios e units).**
Sejam $a, b \neq 0$.

$$a, b \text{ sócios} \iff (\exists u \text{ unit})[\, a = ub\,].$$

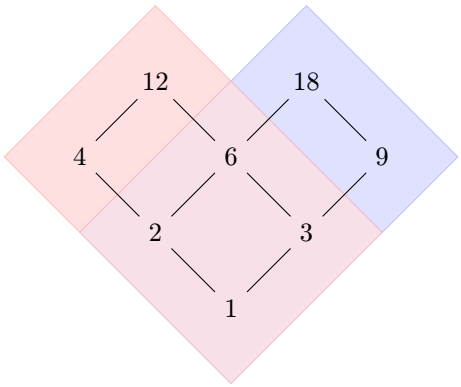
(x3.104 H 1)

§59. Desenhando ordens

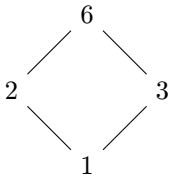
3.96. Desenhamos:



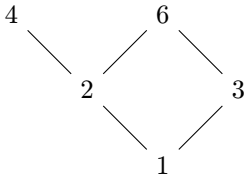
Pintamos os divisores de 12 de vermelho e os de 18 de azul,



e focamos nos divisores em comum (roxa):



3.97. E se fosse assim?. Não sempre teremos um habitante dominando seu conjunto:



TODO Continuar e conectar com mdc

§60. Melhor divisor comum

D3.98. Definição. Sejam a, b, d inteiros. O inteiro d é *um máximo divisor comum (mdc)* dos a, b sse d é um divisor comum e um multiplo de todos os divisores comuns. Em símbolos:

$$d \text{ é um mdc dos } a,b \overset{\text{def}}{\iff} \underbrace{d \mid a \;\&\; d \mid b}_{\text{divisor comun}} \;\&\; \underbrace{(\forall c \text{ divisor comum})[\, c \mid d \,]}_{\text{o “melhor” dos divisores comuns}}.$$

Nesse caso, escrevemos:

$$d = (a,b)\,.$$

Se $1 = (a,b)$, dizemos que os a, b são *coprimos* (entre si).

! **3.99. Cuidado (Disfarçando como igualdade).** Mais uma vez, abusamos aqui a notação para escrever uma proposição “com roupas de igualdade”, quando na verdade não é. Veja primeiramente (Exercício x3.105) que seu lado direito nem significa algo sozinho. Entendemos então a notação inteira como um predicado ternário nos inteiros

$$_ = (_,_) : \mathsf{Int} \times \mathsf{Int} \times \mathsf{Int} \to \mathsf{Prop}.$$

▸ **EXERCÍCIO x3.105.**
Parece que a Definição D3.98 tem um erro: o símbolo (a, b) não foi bem-definido! O que precisamos demonstrar para conseguir realmente a tipagem

$$(_,_) : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int}?$$

(x3.105 H 0)

3.100. Observação. Definimos o conceito de mdc totalmente em termos da relação $(|)$ e logo não temos chances de conseguir *unicidade* de mdc. Para qualquer inteiro d que acaba sendo um mdc dos a, b, com certeza seu sócio $-d$ também vai já que a $(|)$ não consegue distingüi-los. Então a melhor coisa que podemos esperar é uma noção de unicidade mais fraca: unicidade pelos olhos da $(|)$, ou, como falamos mesmo: *unicidade a menos de sócios:*

Θ3.101. Teorema (unicidade a menos de sócios). *Sejam a, b inteiros. Se d, d' são mdc dos a, b, então d, d' são sócios.*

▸ Esboço. Aplicamos a definição de mdc para cada um dos d e d', para chegar em $d \mid d'$ e $d' \mid d$. □ (Θ3.101P)

3.102. Corolário. *Sejam a, b inteiros. Existe único $d \in \mathbb{Z}_{\geq 0}$ tal que d é um mdc dos a, b.*

3.103. Artigo definido generalizado. Agora podemos sim definir o símbolo (a,b) e tratar a expressão $d=(a,b)$ como uma igualdade mesmo; o leitor que não quer desviar muito com a literatura popular pode fazer isso. Mas não havendo motivo de prejudicar uns inteiros contra seus sócios, e para introduzir a idéia de *um artigo definido generalizado*, vou insistir que falar *do* mdc em vez *de um* mdc, faz sentido, dado que entendemos que estamos olhando o mundo dos inteiros pelos olhos da preordem $(|)$. Nesse uso, encontrando o símbolo (a,b), a idéia é que ele denota um mdc, e que qual dos possíveis sócios ele é, não vai importar, pois não vamos sair desse mundinho. Por exemplo, não faz sentido perguntar se $(a,b)>0$ ou não, já que isso está misturando uma outra ordem (a $(>)$) com a ordem utilizada no mdc, e, querendo investigar esse tipo de perguntas, precisamos abandonar o conforto da abstração do mundinho da $(|)$.

D3.104. Definição (O máximo divisor comum). Sejam a,b inteiros.

$$d=(a,b) \overset{\text{def}}{\iff} \underbrace{d\mid a \;\&\; d\mid b}_{\text{divisor comum}} \;\&\; \underbrace{d\in\mathbb{Z}_{\geq 0} \;\&\; (\forall c)[\,(c\mid a \;\&\; c\mid b) \implies c\mid d\,]}_{\text{o máximo}}$$

▸ **EXERCÍCIO x3.106.**
Na Definição D3.98 definimos o que significa que dois inteiros a,b são coprimos (entre si). Para essa definição "compilar" algo precisa ser demonstrado. Enuncie e demonstre. (x3.106 H 0)

Podemos já demonstrar umas propriedades básicas de mdc.

▸ **EXERCÍCIO x3.107.**
Um mdc não enxerga sinais: para quaisquer inteiros a,b,

$$(a,b)=(a,-b)=(-a,b)=(-a,-b)\,.$$

(x3.107 H 0)

▸ **EXERCÍCIO x3.108.**
Sejam a,b,c inteiros. Logo:

$(a,a)=a$	idempotência
$(a,0)=a$	identidade-R
$(a,1)=1$	absorção-R
$(a,b)=(b,a)$	comutatividade
$((a,b),c)=(a,(b,c))$	associatividade

(x3.108 H 0)

• **EXEMPLO 3.105.**
Ache um mdc dos $12,18$.
Resolução. Vamos primeiramente calcular os divisores de cada um desses números:

$$\begin{aligned} \mathit{divs}(12)&=\{\pm1,\pm2,\pm3,\pm4,\pm6,\pm12\}\\ \mathit{divs}(18)&=\{\pm1,\pm2,\pm3,\pm6,\pm9,\pm18\}\,. \end{aligned}$$

Segundo a definição de mdc, se tem inteiro d que merece esse nome, ele é um dos divisores comuns:

$$\mathit{comdivs}(12,18) = \mathit{divs}(12) \cap \mathit{divs}(18) = \{\pm 1, \pm 2, \pm 3, \pm 6\}\,.$$

3.106. Mas existem?. Ainda não tratamos a *existência* de mdc. Definir o que um objeto precisa satisfazer para ser chamado por um nome não garanta que de fato existe tal objeto. Por enquanto, pode ser que para certos inteiros existe um mdc deles, mas para outros, não. Demonstraremos que não é o caso, com duas demostrações bem diferentes. Primeiramente apresentamos uma demonstração não-construtiva, que depende do princípio da boa ordem, conhecida como Lemma de Bézout. Ele não apenas garanta a existência de mdc, mas, também afirma que ele pode ser escrito numa certa forma. Na próxima secção, melhoramos a situação mostrando o *algoritmo* de Euclides, que, ainda mais mostra uma maneira efetiva de construir (achar) o mdc de quaisquer inteiros dados, e ainda-ainda mais, aproveitando sua versão "estendida", fornecer a forma de escrevê-lo garantida pelo Lemma de Bézout.

Λ3.107. Lemma de Bézout. *Sejam a, b inteiros. Logo existe d que satisfaz a definição de (a, b), e ele pode ser escrito como combinação linear dos a e b, com coeficientes inteiros; ou seja,*

$$(\exists s, t)[\, d = sa + tb\,].$$

Além disso, o (a, b) divide qualquer combinação linear dos a e b.

▸ Esboço. Considere o conjunto C de todas as combinações lineares dos a, b:

$$C \stackrel{\text{def}}{=} \{\, sa + tb \;\mid\; s, t \in \mathbb{Z}\,\}\,.$$

Infira que existe d tal que $L = d\mathbb{Z}$. Verifique que tal d é um mdc dos a, b. Como $d \in C = d\mathbb{Z}$, conclua que d divide qualquer combinação linear dos a, b. □

▸ **EXERCÍCIO x3.109.**
Investigue se a forma do (a, b) como combinação linear dos a e b é unicamente determinada. (x3.109 H 1)

3.108. Propriedade. $a \mid b \implies (a, b) = a$. *Especificamente,* $(a, 0) = a$.

▸ Esboço. Precisamos apenas verificar as condições da definição de mdc, que seguem pelas propriedades de $(|)$ que já demonstramos. □

▸ **EXERCÍCIO x3.110.**
Sejam a, b inteiros. Demonstre ou refute: para qualquer inteiro c tal que (i) c é divisor comum dos a, b e (ii) c pode ser escrito como combinação linear dos a, b, temos que c é um mdc dos a, b. (x3.110 H 1)

▸ **EXERCÍCIO x3.111.**
Sejam a, b inteiros. Demonstre que

$$(a, b) = (a, a + b)\,.$$

(x3.111 H 1 2)

▸ **EXERCÍCIO x3.112.**
Demonstre que para todo $n \in \mathbb{N}$, $(F_n, F_{n+1}) = 1$, onde F_n é o n-ésimo termo da seqüência Fibonacci (Definição D3.87). (x3.112 H 1)

§61. O algoritmo de Euclides

3.109. Idéia. Sejam a, b inteiros positivos. Como achamos o (a, b)? Nos vamos aplicar o lemma da divisão (Λ3.82) repetitivamente, até chegar em resto 0:

$$\begin{array}{rcrcrcl}
a &=& b & q_0 & + & r_0, & 0 \le r_0 < b \\
b &=& r_0 & q_1 & + & r_1, & 0 \le r_1 < r_0 \\
r_0 &=& r_1 & q_2 & + & r_2, & 0 \le r_2 < r_1 \\
r_1 &=& r_2 & q_3 & + & r_3, & 0 \le r_3 < r_2 \\
&\vdots& & & & & \vdots \\
r_{n-3} &=& r_{n-2} & q_{n-1} & + & r_{n-1}, & 0 \le r_{n-1} < r_{n-2} \\
r_{n-2} &=& \boxed{r_{n-1}} & q_n & + & \underbrace{r_n}_{0}, & 0 = r_n < r_{n-1}.
\end{array}$$

O (a, b) estará na posição marcada acima. Vamos agora descrever o algoritmo formalmente, e demonstrar (informalmente e formalmente) sua corretude!

a3.110. Algoritmo de Euclides.

EUCLID(a, b)

ENTRADA: a, b : Int
SAÍDA: (a, b)
(1) Se $b = 0$, retorna a.
(2) Retorna EUCLID(b, r), onde $r = rem(a, b)$.

• **EXEMPLO 3.111.**
Ache o $(101, 73)$ com o algoritmo de Euclides.
RESOLUÇÃO. Sabendo que os dois números são primos, fica imediato que eles são coprimos entre si também: a reposta é 1.

Aplicando o algoritmo de Euclides, para achar o $(101, 73)$, dividimos o 101 por 73:

$$101 = 73 \cdot \underbrace{\quad}_{\text{quociente}} + \underbrace{\quad}_{\text{resto}}, \qquad 0 \le \underbrace{\quad}_{\text{resto}} < 73$$

e sabemos que assim reduziremos o problema para o alvo de achar o $(73, \text{resto})$. Pensando, achamos os valores:

$$101 = 73 \cdot \underbrace{1}_{\text{quociente}} + \underbrace{28}_{\text{resto}}, \qquad 0 \le \underbrace{28}_{\text{resto}} < 73$$

ou seja, $(101, 73) = (73, 28)$. Então, repetimos:

$$73 = 28 \cdot \underbrace{2}_{\text{quociente}} + \underbrace{17}_{\text{resto}}, \qquad 0 \le \underbrace{17}_{\text{resto}} < 28$$

ou seja, $(73,28)=(28,17)$. Repetimos:

$$28 = 17\cdot \underbrace{1}_{\text{quociente}} + \underbrace{11}_{\text{resto}}, \qquad 0 \le \underbrace{11}_{\text{resto}} < 17$$

ou seja, $(28,17)=(17,11)$. Repetimos:

$$17 = 11\cdot \underbrace{1}_{\text{quociente}} + \underbrace{6}_{\text{resto}}, \qquad 0 \le \underbrace{6}_{\text{resto}} < 11$$

ou seja, $(17,11)=(11,6)$. Repetimos:

$$11 = 6\cdot \underbrace{1}_{\text{quociente}} + \underbrace{5}_{\text{resto}}, \qquad 0 \le \underbrace{5}_{\text{resto}} < 6$$

ou seja, $(11,6)=(6,5)$. Repetimos:

$$6 = 5\cdot \underbrace{1}_{\text{quociente}} + \underbrace{1}_{\text{resto}}, \qquad 0 \le \underbrace{1}_{\text{resto}} < 5$$

ou seja, $(6,5)=(5,1)$. Como $(5,1)=1$, nem precisamos repetir, mas vamos mesmo assim:

$$5 = \boxed{1}\cdot \underbrace{5}_{\text{quociente}} + \underbrace{0}_{\text{resto}}.$$

Mais compactamente, os passos são:

$$\begin{array}{rll}
101 = 73\cdot 1 + 28, & 0 \le 28 < 73 & (101,73)=(73,28)\\
73 = 28\cdot 2 + 17, & 0 \le 17 < 28 & (73,28)=(28,17)\\
28 = 17\cdot 1 + 11, & 0 \le 11 < 17 & (28,17)=(17,11)\\
17 = 11\cdot 1 + 6, & 0 \le 6 < 11 & (17,11)=(11,6)\\
11 = 6\cdot 1 + 5, & 0 \le 5 < 6 & (11,6)=(6,5)\\
6 = 5\cdot 1 + 1, & 0 \le 1 < 5 & (6,5)=(5,1)\\
5 = \boxed{1}\cdot 5 + 0 & & (5,1)=(1,0)=\boxed{1}.
\end{array}$$

Pronto: $(101,73)=1$.

3.112. Observação. Podemos utilizar o algoritmo de Euclides para achar o (a,b) onde $a,b\in\mathbb{Z}$ também, graças ao Exercício x3.107: $(a,b)=(|a|,|b|)=\textsc{Euclid}(|a|,|b|)$.

▸ **EXERCÍCIO x3.113.**
Usando o algoritmo de Euclides, ache os: (i) $(108,174)$; (ii) $(2016,305)$. (x3.113H0)

▸ **CODE-IT c3.1.**
Implemente o algoritmo de Euclides e verifique tuas soluções nos exercícios anteriores. (c3.1H0)

▸ **CODE-IT c3.2.**
Implemente um modo "verbose" no teu programa do Code-it c3.1, onde ele mostra todas as equações e desigualdades, e não apenas o resultado final. (c3.2H0)

Λ3.113. Lema (Euclides). *Se $a, b \in \mathbb{Z}$ com $b > 0$, então $(a, b) = (b, r)$, onde r o resto da divisão de a por b.*

▸ Demonstração errada. Dividindo o a por b, temos $a = bq + r$. Vamos mostrar que qualquer inteiro d satisfaz a equivalência:

$$d \mid a \;\&\; d \mid b \iff d \mid b \;\&\; d \mid r.$$

Realmente, usando as propriedades Λ3.26, temos:

$$\begin{aligned} d \mid a \;\&\; d \mid b &\implies d \mid \overbrace{a - bq}^{r} \\ d \mid \underbrace{bq + r}_{a} &\impliedby d \mid b \;\&\; d \mid r. \end{aligned}$$

Isso mostra que os divisores em comum dos a e b, e dos b e r são os mesmos, ou, formalmente:

$$\{\, c \in \mathbb{Z} \mid c \mid a \;\&\; c \mid b \,\} = \{\, c \in \mathbb{Z} \mid c \mid b \;\&\; c \mid r \,\}.$$

Logo,

$$\begin{aligned} (a, b) &= \max\{\, c \in \mathbb{Z} \mid c \mid a \;\&\; c \mid b \,\} && \text{(def. } (a, b)\text{)} \\ &= \max\{\, c \in \mathbb{Z} \mid c \mid b \;\&\; c \mid r \,\} && \text{(demonstrado acima)} \\ &= (b, r) && \text{(def. } (b, r)\text{)} \end{aligned}$$

que estabeleça a corretude do algoritmo. ↯

▸ **EXERCÍCIO x3.114.**
Qual é o problema com a demonstração do Lema Λ3.113? (x3.114H0)

Θ3.114. Teorema (Corretude do algoritmo de Euclides). *O Algoritmo de Euclides a3.110 é correto.*

▸ Esboço. Precisamos demonstrar duas coisas: *terminação* e *corretude*.

Corretude. Se o algoritmo precisou n passos, temos que verificar:

$$(a, b) = (b, r_0) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Todas as igualdades exceto a última seguem por causa do Lema Λ3.113; a última por causa da Propriedade 3.108.

Terminação. Note que a seqüência de restos $r_0, r_1, \ldots$ é estritamente decrescente, e todos os seus termos são não negativos:

$$0 \leq \cdots < r_2 < r_1 < r_0 < b.$$

Logo, essa seqüência não pode ser infinita. Realmente, o tamanho dela não pode ser maior que b, então depois de no máximo b passos, o algorítmo terminará. □ (Θ3.114P)

▸ **EXERCÍCIO x3.115.**
Explique por que as argumentações acima (Θ3.114) tanto de corretude quanto de terminação são *esboços* mesmo e não demonstrações. (x3.115H12)

3.115. Nós já demonstramos que o mdc de dois inteiros a e b pode ser escrito como uma combinação linear deles, mas como podemos realmente *achar* inteiros $s,t\in\mathbb{Z}$ que satisfazem a

$$(a,b)=as+bt,\qquad s,t\in\mathbb{Z}?$$

Surpresamente a resposta já está "escondida" no mesmo algoritmo de Euclides!

a3.116. Algoritmo (Algoritmo estendido de Euclides).
ENTRADA: $a,b\in\mathbb{Z}$, $b>0$
SAÍDA: $s,t\in\mathbb{Z}$ tais que $(a,b)=as+bt$.

• **EXEMPLO 3.117.**
Escreva o $(101,73)$ como combinação linear dos 101 e 73.
RESOLUÇÃO. Primeiramente, precisamos aplicar o algoritmo de Euclides para achar o mdc, como no Exemplo 3.111, mas vamos também resolver cada equação por o seu resto:

$$\begin{array}{rcl} 101 &=& 73\cdot 1+28\\ 73 &=& 28\cdot 2+17\\ 28 &=& 17\cdot 1+11\\ 17 &=& 11\cdot 1+6\\ 11 &=& 6\cdot 1+5\\ 6 &=& 5\cdot 1+1\\ 5 &=& \boxed{1}\cdot 5+0. \end{array}\qquad\qquad \begin{array}{rcl} 28 &=& 101-73\\ 17 &=& 73-2\cdot 28\\ 11 &=& 28-17\\ 6 &=& 17-11\\ 5 &=& 11-6\\ 1 &=& 6-5 \end{array}$$

Utilizando as equações no lado direto, de baixo para cima, calculamos:

$$\begin{array}{rll} 1 &= \underline{6}-\underline{5} & (6\text{ e }5)\\ &= \underline{6}-(\underline{11}-\underline{6})=\underline{6}-\underline{11}+\underline{6}=-\underline{11}+2\cdot\underline{6} & (11\text{ e }6)\\ &= -\underline{11}+2\cdot(\underline{17}-\underline{11})=-\underline{11}+2\cdot\underline{17}-2\cdot\underline{11}=2\cdot\underline{17}-3\cdot\underline{11} & (17\text{ e }11)\\ &= 2\cdot\underline{17}-3\cdot(\underline{28}-\underline{17})=2\cdot\underline{17}-3\cdot\underline{28}+3\cdot 17=-3\cdot\underline{28}+5\cdot\underline{17} & (28\text{ e }17)\\ &= -3\cdot\underline{28}+5\cdot(\underline{73}-2\cdot\underline{28})=-3\cdot\underline{28}+5\cdot\underline{73}-10\cdot\underline{28}=5\cdot\underline{73}-13\cdot\underline{28} & (73\text{ e }28)\\ &= 5\cdot\underline{73}-13\cdot(\underline{101}-\underline{73})=5\cdot\underline{73}-13\cdot\underline{101}+13\cdot\underline{73}=-13\cdot\underline{101}+18\cdot\underline{73} & (101\text{ e }73) \end{array}$$

No lado direto mostramos nosso progresso, no sentido de ter conseguido escrever o mdc como combinação linear de quais dois números. Sublinhamos os inteiros que nos interessam para não perder nosso foco. Em cada nova linha, escolhemos o menor dos dois números sublinhados, e o substituimos pela combinação linear que temos graças ao algoritmo de Euclides. Obviamente, essa notação e metodologia não tem nenhum sentido matematicamente falando. Serve apenas para ajudar nossos olhos humanos.

Achamos então $s,t\in\mathbb{Z}$ que satisfazem a equação $1=sa+tb$: são os $s=-13$ e $t=18$.

▸ **EXERCÍCIO x3.116.**
Usando o algoritmo estendido de Euclides, escreve: (i) o $(108,174)$ como combinação linear dos 108 e 174; (ii) o $(2016,305)$ como combinação linear dos 2016 e 305. (x3.116H0)

3.118. Equações de Diophantus.
TODO escrever e posicionar

3.119. Quantos passos precisa o Euclides. Para demonstrar a terminação do algoritmo de Euclides estabelecemos uma garantia que o EUCLID(a, b) depois b passos no máximo termina. Como o exercício seguinte mostra, o algoritmo de Euclides é *bem mais eficiente* do que isso: depois dois passos, as duas entradas, nos piores dos casos, são reduzidas à metade!

▸ **EXERCÍCIO x3.117.**
Se $a \geq b$, então $r < a/2$, onde r o resto da divisão de a por b. (x3.117H123)

? **Q3.120. Questão.** Quão eficiente é o algoritmo de Euclides?

!! SPOILER ALERT !!

TODO Sobre eficiência, operações primitivas, oráculos

Λ3.121. Lema.

TODO Eficiência de Euclides

▸ **EXERCÍCIO x3.118 (Euclides vs. Fibonacci).**
Para todo $n \geq 1$ e quaisquer inteiros $a > b > 0$, se EUCLID(a, b) precisa n passos (divisões) para terminar, então $a \geq F_{n+2}$ e $b \geq F_{n+1}$, onde F_i é o i-ésimo número Fibonacci. (x3.118H12)

▸ **EXERCÍCIO x3.119 (mdc, fibonacci).**
O fibonacci do mdc de dois números naturais é o mdc do fibonacci de cada:

$$(\forall n, m \in \mathbb{N})\big[\,(F_n, F_m) = F_{(n,m)}\,\big].$$

(x3.119H0)

§62. Fatoração

? **Q3.122. Questão.** Dado um inteiro positivo n, como podemos "quebrá-lo" em blocos de construção?

3.123. Cimento. Vamos primeiramente responder nessa questão com outra: *Qual seria nosso "cimento"?* Tome como exemplo o número $n = 28$. Usando $(+)$ para construí-lo com blocos, podemos quebrá-lo:

$$28 = 16 + 12.$$

E agora quebramos esses dois blocos:

$$= \overbrace{10+6}^{16} + \overbrace{11+1}^{12};$$

e esses:

$$= \overbrace{3+7}^{10} + \overbrace{3+3}^{6} + \overbrace{4+7}^{11} + 1$$

e o 1 não é mais "quebrável". Nesse quesito, ele é um bloco atômico, um "tijolo". Repetimos esse processo até chegar num somatório cujos termos são todos tijolos:

$$= \underbrace{1+1+1+1+\cdots+1}_{28 \text{ termos}}.$$

O leitor é convidado pensar sobre as observações seguintes:

(i) Começando com qualquer inteiro positivo n, depois um *finito* número de passos, o processo termina: nenhum dos termos que ficam pode ser quebrado.

(ii) Existe apenas um tipo de bloco atômico: o 1. Podemos então formar qualquer número n começando com n tijolos (n 1's) e usando a operação $(+)$ para juntá-los.

(iii) Não faz sentido considerar o 0 como tijolo, pois escrevendo o 1 como

$$1 = 1 + 0 \qquad \text{ou} \qquad 1 = 0 + 1$$

não conseguimos "quebrá-lo" em peças menores. Pelo contrário, ele aparece novamente, da mesma forma, no lado direito.

▸ **EXERCÍCIO x3.120.**
Qual é a melhor estratégia para desconstruir o n em 1's conseguindo o menor número de passos possível? Quantos passos precisa? Suponha que em cada passo tu tens de escolher apenas *um* termo (não atômico) e decidir em quais duas partes tu o quebrarás. (x3.120 H 1)

▸ **EXERCÍCIO x3.121.**
Demonstre formalmente tua resposta no Exercício x3.120. (x3.121 H 1 2 3)

3.124. "Vezes" em vez de "mais". Vamos agora usar como cimento a operação $(\cdot)$, ilustrando o processo com o número 2016:

$$2016 = 12 \cdot 168$$

e repetimos...

$$= \overbrace{4 \cdot 3}^{12} \cdot \overbrace{28 \cdot 6}^{168}$$

e agora vamos ver: o 4 pode ser quebrado sim ($2{\cdot}2$), mas o 3? Escrever $3 = 3{\cdot}1$ com certeza não é um jeito aceitável para quebrar o 3 em blocos de construção "mais principais": o lado direto é mais complexo! Quebrando com $(\cdot)$ então, o 3 é um bloco atômico, um tijolo! Continuando:

$$= \overbrace{2 \cdot 2}^{4} \cdot 3 \cdot (7 \cdot 4) \cdot (2 \cdot 3)$$

$$= 2 \cdot 2 \cdot 3 \cdot 7 \cdot \overbrace{2 \cdot 2}^{4} \cdot 2 \cdot 3$$

onde todos os fatores são atômicos. Podemos construir o número 2016 então assim:

$$2016 = 2 \cdot 2 \cdot 3 \cdot 7 \cdot 2 \cdot 2 \cdot 2 \cdot 3,$$

usando os tijolos 2, 3, e 7, e a operação de multiplicação. Nos vamos definir formalmente esses tijolos (que vão acabar sendo os inteiros que chamamos de *irredutíveis* ou *primos*: D3.127, D3.129, Θ3.132), e estudar suas propriedades.

Ilustrando com o mesmo número 2016, um outro caminho para processar seria o seguinte:

$$\begin{aligned} 2016 &= 48 \cdot 42 \\ &= \overbrace{8 \cdot 6}^{48} \cdot \overbrace{6 \cdot 7}^{42} \\ &= \overbrace{2 \cdot 4}^{8} \cdot \overbrace{2 \cdot 3}^{6} \cdot \overbrace{2 \cdot 3}^{6} \cdot 7 \\ &= 2 \cdot \overbrace{2 \cdot 2}^{4} \cdot 2 \cdot 3 \cdot 2 \cdot 3 \cdot 7 \end{aligned}$$

então no final temos:

$$2016 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 2 \cdot 3 \cdot 7.$$

▸ **EXERCÍCIO x3.122.**
O que tu percebes sobre as duas desconstruções?:

$$2016 = 2 \cdot 2 \cdot 3 \cdot 7 \cdot 2 \cdot 2 \cdot 2 \cdot 3;$$
$$2016 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 2 \cdot 3 \cdot 7.$$

(x3.122 H 0)

▸ **EXERCÍCIO x3.123.**
Fatore os inteiros 15, 16, 17, 81, 100, 280, 2015, e 2017 em fatores irredutíveis. (x3.123 H 0)

▸ **CODE-IT c3.3 (FactorNaive).**
Escreva um programa que mostra para cada entrada, uma fatoração em primos. Execute teu programa para verificar tuas respostas no Exercício x3.123. Note que muitos sistemas unixoides têm um programa `factor` já instalado:

```
# factor 65536 65537 65538
65536: 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
65537: 65537
65538: 2 3 3 11 331
```

(c3.3 H 0)

? **Q3.125. Questão.** Usando adição, nos precisamos apenas um tipo de tijolo para construir qualquer inteiro positivo: o 1. Usando a multiplicação nos já percebemos que vários tipos são necessários; mas quantos?

3.126. Resposta (Euclides). Essa pergunta e sua resposta não são triviais! Recomendo para ti, tentar responder e *demonstrar* tua afirmação. Logo vamos encontrar a resposta (de Euclides) que é um dos teoremas mais famosos e importantes na história de matemática (Teorema Θ3.136).

§63. Irredutíveis, primos

D3.127. Definição (Irredutível). Seja $p \neq 0$ inteiro. Chamamos o p *irredutível* sse p não é unit e para quaisquer a, b tais que $p = ab$, pelo menos um dos a, b é unit:

$$p \text{ irredutível} \overset{\text{def}}{\iff} p \text{ não unit } \& \ (\forall a, b)[\, p = ab \implies a \text{ unit ou } b \text{ unit}\,].$$

Caso contrário, p é *redutível*. Chamamos o p de *composto* sse p não é unit e existem não units a, b tais que $p = ab$.

Θ3.128. Teorema. *Seja x inteiro. Logo x irredutível sse os únicos divisores de x são os $1, -1, x, -x$.*

Demonstrarás no Exercício x3.124. ∎

▸ **EXERCÍCIO x3.124.**
Demonstre o Teorema Θ3.128. (x3.124H0)

D3.129. Definição (Primo). Seja $p \neq 0$ inteiro. Chamamos o p de *primo* sse p não é unit e para quaisquer inteiros a, b, se p divide o produto ab então p divide pelo menos um dos a, b. Em símbolos:

$$\text{Prime}(p) \overset{\text{def}}{\iff} p \text{ não unit } \& \ (\forall a, b)[\, p \mid ab \implies p \mid a \text{ ou } p \mid b\,].$$

! **3.130. Aviso.** Nossas definições de irredutível e de primo, não conseguem discriminar a partir da positividade: se um inteiro x é primo (ou irredutível), seu sócio $-x$ também é. É comum excluir os negativos dessas definições, mas não vou negá-los esse direito aqui. Mais sobre essa escolha logo depois de conhecer o teorema principal deste assunto, o Teorema fundamental da aritmética Θ3.140.

Λ3.131. Lemma de Euclides. *Todo inteiro irredutível é primo.*

▸ Esboço. Sejam a, b inteiros e p irredutível tal que $p \mid ab$. Suponha que $p \nmid a$. Logo o $(a, p) = 1$ pode ser escrito como combinação linear de a e p:

$$1 = as + pt, \qquad \text{para alguns } s, t \in \mathbb{Z}.$$

Multiplica os dois lados por b, e explica por que necessariamente $p \mid b$. □ (Λ3.131P)

O converso disso também é válido e logo as noções de irredutível e de primo coincidem no mundo dos inteiros:

Θ3.132. Teorema. *Todo inteiro é irredutível sse é primo.*

Demonstração. A direção (⇒) é o Lemma de Euclides Λ3.131. A direção (⇐) é o Exercício x3.125. ∎

▸ **EXERCÍCIO x3.125.**
Todo inteiro primo é irredutível. (x3.125 H 0)

Λ3.133. Lema. *Se $(d,a)=1$ e $d \mid ab$, então $d \mid b$.*

▸ Esboço. A demonstração é practicamente a mesma com aquela do Lemma de Euclides Λ3.131: lá nós precisamos da primalidade do p apenas para concluir que $(a,p)=1$. Aqui temos diretamente a hipótese $(a,d)=1$. □ (Λ3.133P)

3.134. Corolário. *Se $a \mid m$, $b \mid m$, e $(a,b)=1$, então $ab \mid m$.*

Demonstração. Como $a \mid m$, temos $m = au$ para algum $u \in \mathbb{Z}$. Mas $b \mid m = au$, e como $(b,a)=1$, temos $b \mid u$ (por Lema Λ3.133). Então $bv = u$ para algum $v \in \mathbb{Z}$. Substituindo, $m = au = a(bv) = (ab)v$, ou seja, $ab \mid m$. ∎

▸ **EXERCÍCIO x3.126.**
Demonstre ou refute: para quaisquer primos distintos p, q,

$$pq \mid n^2 \implies pq \mid n.$$

(x3.126 H 1 2)

▸ **EXERCÍCIO x3.127.**
O 0 é primo? Redutível? Composto? O 1? (x3.127 H 0)

▸ **EXERCÍCIO x3.128.**
2 é o "único" primo par.[36] (x3.128 H 0)

• **EXEMPLO 3.135.**
Os primeiros 31 primos positivos são os 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, e 127.

▸ **EXERCÍCIO x3.129.**
Sejam p, q primos, tais que $p \mid q$. Mostre que p, q são sócios. (x3.129 H 0)

▸ **EXERCÍCIO x3.130.**
Seja x composto. Demonstre que x tem um divisor primo p tal que $p^2 \leq x$. (x3.130 H 0)

▸ **CODE-IT c3.4 (factor).**
Use o Exercício x3.130 para melhorar teu programa do Code-it c3.3. (c3.4 H 0)

[36] Em aspas, quando eu digo 2 aqui, eu incluo seu sócio -2 também. (Óbvio?)

Θ3.136. Teorema (Euclid). *Existe uma infinidade de primos.*

▸ Esboço. Para qualquer conjunto finito de primos $P = \{p_1, \ldots, p_n\}$, considere o número $p_1 \cdots p_n + 1$ e use-o para achar um primo fora do P. □ (Θ3.136P)

? **Q3.137. Questão.** Como podemos achar todos os primos até um dado limitante b?

3.138. O crivo de Eratosthenes. Eratosthenes (276–194 a.C.) conseguiu responder com sua método conhecida como o *crivo de Eratosthenes*. Eu a aplicarei aqui para achar todos os primos menores ou iguais que $b = 128$. Primeiramente liste todos os números de 2 até $b = 128$:

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112
113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128.

Agora comece com o primeiro número na lista, o 2, e apague todos os maiores múltiplos dele:

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112
113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128.

Tome o próximo número que está ainda na lista, o 3, e faça a mesma coisa:

	2	3	5	7	9	11	13	15
17		19	21	23	25	27	29	31
33		35	37	39	41	43	45	47
49		51	53	55	57	59	61	63
65		67	69	71	73	75	77	79
81		83	85	87	89	91	93	95
97		99	101	103	105	107	109	111
113		115	117	119	121	123	125	127 .

Repita o processo (o próximo agora seria o 5) até não tem mais números para tomar. Os números que ficarão são todos os primos até o 128:

	2	3	5	7		11	13	
17		19		23	25		29	31
		35	37		41	43		47
49			53	55		59	61	
65		67		71	73		77	79
		83	85		89	91		95
97			101	103		107	109	
113		115		119	121		125	127 .

Tomando o 7:

	2	3	5	7		11	13	
17		19		23			29	31
			37		41	43		47
49			53			59	61	
		67		71	73		77	79
		83			89	91		
97			101	103		107	109	
113				119	121			127

.

Tomando o 11:

	2	3	5	7		11	13	
17		19		23			29	31
			37		41	43		47
			53			59	61	
		67		71	73			79
		83			89			
97			101	103		107	109	
113					121			127

.

E já podemos parar aqui, certos que os números que ainda ficam na lista, são todos os primos desejados.

? **Q3.139. Questão.** Por quê?

!! SPOILER ALERT !!

▸ **EXERCÍCIO x3.131.**
Seja $a > 0$ inteiro composto. Queremos dizer que a *possui fator primo* $p \leq \sqrt{a}$. Mas como não definimos a $\sqrt{_}$ nos inteiros, reformulamos nossa afirmação assim: *para todo* x*, se* $x^2 > a$*, então existe primo* $p \leq x$ *tal que* $p \mid a$. (x3.131 H 1)

▸ **CODE-IT c3.5.**
Implemente o algoritmo de Eratosthenes e o use para achar todos os primos até o 1024. (c3.5 H 0)

§64. O teorema fundamental da aritmética

Chegamos finalmente no resultado principal que esclarecerá o que percebemos no Exercício x3.122: o Teorema fundamental da aritmética Θ3.140, ilustrado (parcialmente) já por Euclides (circa 300 a.C.) nos seus *Elementos* **[Euc02]** e demonstrado completamente por Gauss (no ano 1798) no seu *Disquisitiones Arithmeticæ* **[Gau66]**.

Θ3.140. Teorema fundamental da aritmética. *Todo inteiro $x \neq 0$ pode ser escrito como um produtório de primos. Essa expressão é única a menos de sócios e desconsiderando a ordem dos fatores do produtório.*

Demonstração. Seja $x \in \mathbb{Z}$ com $x > 1$.
Existência: Usamos indução forte (veja 3.72). Caso x primo, trivialmente ele mesmo é o produtório de primos (produtório de tamanho 1). Caso contrário, $x = ab$, para uns a, b com $1 < a < x$ e $1 < b < x$, logo sabemos (hipoteses indutivas) que cada um deles pode ser escrito na forma desejada:

$$\begin{aligned} a &= p_1 p_2 \cdots p_{k_a} \quad \text{para alguns } p_i\text{'s primos;} \\ b &= q_1 q_2 \cdots q_{k_b} \quad \text{para alguns } q_j\text{'s primos.} \end{aligned}$$

Então temos

$$x = ab = (p_1 p_2 \cdots p_{k_a})(q_1 q_2 \cdots) = p_1 p_2 \cdots p_{k_a} q_1 q_2 \cdots q_{k_b}$$

que realmente é um produtório de primos.
Unicidade: Suponha que para alguns primos p_i's e q_j's, e uns naturais s, t, temos:

$$\begin{aligned} x &= p_1 p_2 \dots p_s, \\ x &= q_1 q_2 \dots q_t. \end{aligned}$$

Vamos mostrar que $s = t$ e que para todo $i \in \{1, \dots, s\}$, $p_i = q_j$. Temos

$$p_1 p_2 \dots p_s = q_1 q_2 \dots q_t,$$

e p_1 é primo que divide o lado esquerdo, então divide também o lado direito:

$$p_1 \mid q_1 q_2 \dots q_t.$$

Pelo Lemma de Euclides Λ3.131, $p_1 \mid q_{j_1}$ para algum j_1. Mas o q_{j_1}, sendo um dos q_j's, também é primo. Logo $p_1 = q_{j_1}$ (veja Exercício x3.129). Cancelando o p_1, temos:

$$p_2 \dots p_s = q_1 q_2 \cdots q_{j_1 - 1} q_{j_1 + 1} q_t,$$

Agora repetimos até um dos dois lados não ter mais fatores primos. Necessariamente, isso vai acontecer "simultaneamente" nos dois lados (caso contrário teriamos um produtório de primos igual com 1, impossível), ou seja: $s = t$. Note que as equações $p_i = q_{j_i}$ mostram a unicidade desejada. ∎

Graças ao teorema fundamental da aritmética podemos definir a:

D3.141. Definição (Representação canônica de inteiros). Seja $0 \neq n \in \mathbb{Z}$. Sua *representação canônica* é o produtório

$$n = (\pm 1) \prod_{i=1}^{k} p_i^{a_i} = (\pm 1) p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

onde os $p_1 < p_2 < \cdots < p_k$'s são primos, e $a_i \in \mathbb{N}_{>0}$ para $i = 1, \dots, k$.

Observe que se relaxar a restricção nos exponentes tal que $a_i \in \mathbb{N}$, cada $n \in \mathbb{Z}$ $(n \neq 0)$ pode ser representado (também únicamente) como o produtório

$$n = (\pm 1) \prod_{i=0}^{k} p_i^{a_i} = (\pm 1) p_0^{a_0} p_1^{a_1} \cdots p_k^{a_k},$$

onde agora os $p_0 < p_1 < \cdots < p_k$ são *todos os $k+1$ primeiros primos*, sendo então $p_0 = 2$, e p_k o maior primo divisor do n. Chamamos essa forma a *representação canônica completa* do n. (Veja também o Problema Π3.26.)

§65. Valuações

Já temos, nos inteiros, um conceito de *tamanho:* $|_|$. A partir dele, definimos uma idéia de *distância:* $|_ - _|$. Agora vamos ver uma maneira bem diferente de definir tamanho nos inteiros, e logo uma nova idéia de distância também.

D3.142. Definição (Valuação). Fixe um primo p. Definimos a função $V_p : \mathsf{Int} \to \mathsf{Int}$ pelas

$$V_p\ a = \max\left\{\, i \mid p^i \mid a \,\right\}.$$

Chamamos a V_p de *p-valuação*. Defina o *tamanho p-ádico* e a *distância p-ádica* pelas

$$\|a\|_p \stackrel{\text{def}}{=} p^{-(V_p\ a)}; \qquad\qquad d_p(x,y) \stackrel{\text{def}}{=} \|x-y\|_p .$$

Quando o '$_p$' é óbvio pelo contexto, o omitimos dessas notações.

▸ **EXERCÍCIO x3.132.**
A Definição D3.142 tem um erro. Ache e corrija! (x3.132 H 0)

▸ **EXERCÍCIO x3.133.**
Seja V uma p-valuação para algum primo p. Demonstre:
(i) $V\ (a+b) \geq \min\{V\ a, V\ b\}$;
(ii) $V\ (ab) = V\ a + V\ b$.

(x3.133 H 0)

▸ **EXERCÍCIO x3.134.**
Seja V uma p-valuação para algum primo p. Demonstre:
(i) $V\ (a,b) = \min\{V\ a, V\ b\}$;
(ii) $V\ [a,b] = \max\{V\ a, V\ b\}$.

(x3.134 H 0)

▸ **EXERCÍCIO x3.135.**
Demonstre:
(i) $\|ab\| = \|a\|\,\|b\|$;
(ii) $\|a+b\| \leq \max\{\|a\|, \|b\|\} \leq \|a\| + \|b\|$.

(x3.135 H 0)

▸ **EXERCÍCIO x3.136.**
Seja x inteiro. Demonstre:

$$\prod_{p \text{ primo}} \|x\|_p = \frac{1}{|x|}$$

(x3.136 H 0)

A partir dum primo p, definimos a função d_p que chamamos de distância p-ádica, mas devemos demonstrar que ela merece o nome *distância:*

▸ **EXERCÍCIO x3.137.**
A distância definida a partir da $\|_\|_p$ realmente é uma *função de distância*, ou seja:

(i) $d_p(x,y) \geq 0$;
(ii) $d_p(x,y) = 0 \implies x = y$;
(iii) $d_p(x,x) = 0$;
(iv) $d_p(x,y) = d_p(y,x)$;
(v) $d_p(x,z) \leq d_p(x,y) + d_p(y,z)$.

(x3.137 H 0)

§66. Conjecturas

TODO definir a função Collatz

?3.143. Conjectura (Collatz). *A função definida acima é total e (logo) igual à constante* $\lambda x\,.\,1$.

3.144. Goldbach. No ano 1742 Goldbach comunicou para Euler as conjecturas seguintes:

?3.145. Conjectura (fraca de Goldbach). *Todo número maior que* 5 *pode ser escrito como soma de três primos.*

?3.146. Conjectura (Goldbach). *Todo número par maior que* 2 *pode ser escrito como soma de dois primos.*

D3.147. Definição (Primos gêmeos). Seja p inteiro. Dizemos que p é um primo gémeo sse ambos os $p, p+2$ são primos.

?3.148. Conjectura (Twin primes). *Existe uma infinidade de primos gêmeos.*

?3.149. Conjectura (Legendre). *Para todo* $n > 0$, *existe primo entre* n^2 *e* $(n+1)^2$.

Θ3.150. Teorema (Wiles (conjectura de Fermat)). *Para qualquer* $n > 2$, *não existem inteiros* $a, b, c > 0$ *que satisfazem a equação*

$$a^n + b^n = c^n.$$

Demonstrado. A artilharia utilizada para matar este teorema fica *muito* fora do nosso alcance (e com certeza do Fermat também! O artigo principal é o [Wil95] (101 páginas!), e o [TW95] completa o que faltou para consertar e finalizar a demonstração. ∎

Intervalo de problemas

▸ **PROBLEMA Π3.18.**
Como tu percebeu resolvendo o Exercício x3.115, nenhuma das duas partes do Teorema Θ3.114 foi demonstrada mesmo. Demonstre as duas partes usando indução. (Π3.18 H 1 2 3 4)

▸ **PROBLEMA Π3.19.**
Demonstre as duas partes do Teorema Θ3.114 usando o princípio da boa ordem. (Π3.19 H 1 2 3 4 5)

▸ **PROBLEMA Π3.20.**
Para todo p primo, e todo $r \in \{1, \dots, p-1\}$,

$$p \mid C(p, r).$$

O que acontece se $r = 0$ ou $r \geq p$? (Π3.20 H 1)

▸ **PROBLEMA Π3.21.**
(Generalização do Exercício x2.4.) Para quais $u, v \in \mathbb{Z}$, a afirmação

$$a \mid b + c \;\;\&\;\; a \mid ub + vc \implies a \mid xb + yc \quad \text{para todos } x, y \in \mathbb{Z}$$

é válida? (Π3.21 H 0)

▸ **PROBLEMA Π3.22.**
Seja $n \in \mathbb{N}$, $n > 1$. Entre n e $n!$ existe primo. (Π3.22 H 1 2 3)

▸ **PROBLEMA Π3.23.**
Seja $n \in \mathbb{N}$. Ache n consecutivos números compostos. (Π3.23 H 1 2 3 4)

▸ **PROBLEMA Π3.24 (Definição alternativa de mdc).**
Uma definição alternativa do mdc é a seguinte: *Sejam $a, b \in \mathbb{Z}$. O mdc dos a e b é o maior dos divisores em comum de a e b.* Ache um problema com essa definição, corrige-o, e depois compare com a Definição D3.104. (Π3.24 H 1)

▸ **PROBLEMA Π3.25 (Contando os passos).**
O que muda no Exercício x3.120 se em cada passo podemos quebrar todos os termos que aparecem? Qual é a melhor estratégia, e quantos passos são necessários? (Π3.25 H 1 2)

▸ **PROBLEMA Π3.26 (Codificação de seqüências finitas).**
Seja S o conjunto de seqüências finitas de números naturais. Descreva uma método para "codificar" os elementos de S com os elementos de $\mathbb{N} \setminus \{0\}$. Tua método deve ser uma *revertível*, no sentido que cada seqüência finita

$$s = \langle s_0, s_1, \dots, s_{k_s} \rangle \in S$$

deve corresponder em exatamente um número natural $n_s \in \mathbb{N} \setminus \{0\}$, e, dado esse número $n_s \in \mathbb{N}_{>0}$, deveria ser possível "extrair" a seqüência s cuja codificação é o n_s. Não se preocupe se existem naturais que não são codificações de nenhuma seqüência. (Π3.26 H 1 2 3 4)

▸ **PROBLEMA Π3.27 (Representação canônica de racionais).**
Generalize a representação canônica de inteiros para racionais. (Π3.27 H 1)

▸ **PROBLEMA Π3.28.**
Seja $V : \mathsf{Int} \to \mathsf{Int}$ tal que goza das propriedades do Exercício x3.133:

(i) $V(a+b) \geq \min\{V\,a, V\,b\}$;
(ii) $V(ab) = V\,a + V\,b$.

Demonstre que existem inteiro c e primo p tais que $V = cV_p$, onde

$$V = cV_p \iff (\forall a)[\,V(a) = cV_p(a)\,].$$

(Π3.28 H 1)

§67. A idéia da relação de congruência

TODO pintar com cores, metáfora de times, planetas

Vamos fixar um inteiro positivo m. Agora graças à divisão de Euclides (Λ3.82), qualquer inteiro a pode ser escrito na forma

$$a = mk + r, \qquad 0 \leq r < m,$$

num jeito único, ou seja, os inteiros k, r são determinados pelos a, m.

Enquanto investigando a (ir)racionalidade dos $\sqrt{2}$, $\sqrt{3}$, $\sqrt{m}$, etc., nós percebemos que foi útil separar os inteiros em classes, "agrupando" aqueles que compartilham o mesmo resto quando divididos por m. Trabalhando com essa idéia nós encontramos nosso primeiro contato com *aritmética modular*.[37]

§68. Duas definições quase equivalentes

TODO reescrever para corresponder à seção anterior

Precisamos definir formalmente a noção informal de *"dois inteiros a e b pertencem à mesma classe, quando separamos eles em times usando o inteiro m"*. A primeira coisa que precisamos perceber é que essa frase é uma afirmação sobre 3 inteiros. Queremos então uma definição e uma notação que captura essa relação *de aridade* 3.

3.151. Congruência intuitivamente. Chamamos dois inteiros *congruentes* módulo um terceiro inteiro, sse eles têm o mesmo resto, quando divididos por ele.

[37] Mentira. Não foi o primeiro não: somos todos acostumados com aritmética modular mesmo sem perceber. Um desses contatos é por causa de ter que contar com horas e relógios, cuja aritmética não parece muito com aquela dos inteiros. Por exemplo: $21 + 5 = 26$, mas se agora são 21h00, que horas serão depois de 5 horas? Nossos relógios não vou mostrar 26h00, mas 02h00.

3.152. Crítica. Primeiramente, o texto da definição é bem informal e ambíguo. Para tirar essas ambigüidades, precisamos introduzir variáveis para referir sobre os "mesmos restos":

D3.153. Definição (Intuitiva). Sejam a, b, m inteiros com $m > 0$, e sejam q_a, r_a, q_b, e r_b os inteiros determinados pelas divisões:

$$\begin{aligned} a &= mq_a + r_a & 0 \leq r_a < m \\ b &= mq_b + r_b & 0 \leq r_b < m. \end{aligned}$$

Digamos que os a e b são *congruentes* módulo m, sse $r_a = r_b$.

3.154. Observação. Olhando para dois números a e b, congruêntes módulo m, o que podemos dizer sobre a diferença deles? Observe:

$$\left.\begin{aligned} a - b &= (mq_a + r_a) - (mq_b + r_b) \\ &= mq_a - mq_b + r_a - r_b \\ &= m(q_a - q_b) + (r_a - r_b) \\ &= m(q_a - q_b) + 0 \\ &= m(q_a - q_b) \end{aligned}\right\} \quad \text{ou seja, } m \mid a - b.$$

Essa observação nos mostra um caminho mais curto e elegante para definir o mesmo conceito. É o seguinte:

D3.155. Definição (Congruência (Gauss)). Sejam $a, b, m \in \mathbb{Z}$ com $m > 0$. Digamos que os a e b são *congruentes módulo* m, sse $m \mid a - b$. Em símbolos, escrevemos

$$a \equiv b \pmod{m} \overset{\text{def}}{\iff} m \mid a - b$$

e lemos: *o a é congruente com b módulo m.*

! **3.156. Cuidado.** A notação de congruência às vezes iluda de ser interpretada como se fosse uma relação entre o lado esquerdo L e o lado direito R, assim:

$$\underbrace{a}_{\text{L}} \equiv \underbrace{b \pmod{m}}_{\text{R}}.$$

Não! Principalmente, o lado direito, $b \pmod{m}$, nem é definido, então não tem significado, e nem faz sentido afirmar algo sobre ele. Prestando mais atenção, percebemos que o $_ \equiv _$ também não foi definido! O que nós definimos foi o:

$$u \equiv v \pmod{w}$$

dados $u, v, w \in \mathbb{Z}$ com $w > 1$.

3.157. Notação. Talvez ficaria mais intuitivo (e menos confúso) usar a notação

$$a \equiv_m b \overset{\text{def}}{\iff} a \equiv b \pmod{m}$$

que introduzimos aqui pois às vezes ajuda. Mas a notação mais usada é a da Definição D3.155

3.158. Intuição. Se precisamos para algum motivo pessoal—porque sim—separar mentalmente a notação de congruência em dois lados, o único jeito que faz algum sentido seria o:

$$\underbrace{a \equiv b}_{\text{L}} \quad \underbrace{\pmod m}_{\text{R}}.$$

Assim, entendemos que "algo acontece" (lado L), "dentro algo" (lado R), onde "algo acontece" seria "o a *parece* com b", e "dentro algo" seria "módulo m". Mas, claramente tudo isso é apenas uma guia (caso que queremos) e nada mais que isso. Para argumentar sobre a relação de congruência, usamos *apenas sua definição formal!*

Para ganhar o direito de usar qualquer uma das duas definições, precisamos mostrar que são equivalentes:

Θ3.159. Teorema (Equivalência das duas definições). *Sejam $a, b, m \in \mathbb{Z}$ com $m > 0$, e sejam $q_a, r_a, q_b, r_b \in \mathbb{Z}$ os números determinados por as divisões:*

$$\begin{aligned} a &= mq_a + r_a & 0 \le r_a < m \\ b &= mq_b + r_b & 0 \le r_b < m \end{aligned}$$

Temos a equivalência:

$$a \equiv b \pmod m \iff r_a = r_b.$$

▸ Esboço. Precisamos mostrar as duas direções do ($\Leftrightarrow$). A direção ($\Leftarrow$), é practicamente a Observação 3.154. Para a direção ($\Rightarrow$), vamos mostrar que $r_a - r_b = 0$. Usamos a hipótese e propriedades de ($|$) para mostrar que $m \mid r_a - r_b$, e depois as duas desigualdades para confirmar que, com suas restricções, o único inteiro múltiplo de m que as satisfaz é o 0. □ (Θ3.159P)

! 3.160. Cuidado (A operação binária "mod"). Em linguagens de programação é comum encontrar o operador *binário* "mod", frequentemente denotado com o símbolo '`%`'. Em matemática, essa função *binária* (aridade 2) é mais encontrada como '`mod`' mesmo. Cuidado não confundir a *função* $\bmod : \mathbb{Z} \times \mathbb{N}_{>0} \to \mathbb{N}$ com a *relação* $a \equiv b \pmod m$. Faz sentido escrever:

$$69 \bmod 5 = 4.$$

Isso significa apenas que o resto da divisão de 69 por 5, é 4. Por outro lado, nenhuma das expressões abaixo tem significado!:

$$69 \pmod 5 = 4 \qquad 4 = 69 \pmod 5$$

▸ **EXERCÍCIO x3.138.**
Explique o tipo da função $\bmod : \mathbb{Z} \times \mathbb{N}_{>0} \to \mathbb{N}$. (x3.138 H 1)

▸ **EXERCÍCIO x3.139 (mod vs. mod).**
Para cada uma das expressões abaixo uma das três opções é válida: (a) ela denota um termo; (b) ela denota uma afirmação; ou (c) ela não tem significado. Para cada expressão, decida qual é a opção certa e: se for a (a), ache o seu valor (qual objeto ela denota); se for a (b), ache se é válida ou não.

(1) $69 \pmod 5 = 4$

(2) $12 = 3 \pmod 8$
(3) $12 \equiv 20 \pmod 4$
(4) $8 \pmod 3 \equiv 12$
(5) $108 \equiv 208 \pmod{(43 \bmod 30)}$
(6) $x \bmod 4 = 2 \implies x \equiv 0 \pmod 2$
(7) $5^{192 \bmod 3}$
(8) $13 \pmod 8 \equiv 23 \pmod{18}$

(x3.139 H 0)

§69. Aritmética modular

3.161. Fixando um m. Observe que

$$_ \equiv _ \pmod{_} : \mathsf{Int} \times \mathsf{Int} \times \mathsf{Int} \to \mathsf{Prop}.$$

Ou seja, se trata duma relação *ternária*. Naturalmente, fixando um inteiro m, a expressão

$$_ \equiv _ \pmod m : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Prop}.$$

é uma relação binária que chamamos de *congruência módulo m* e denotamos também por $(\equiv_m)$. Suas propriedades investigamos agora.

Θ3.162. Teorema (relação de equivalência). *Fixe um inteiro m. Para todos os inteiros a, b, c, temos:*

(1)	$a \equiv_m a$	(reflexividade)
(2)	$a \equiv_m b \;\&\; b \equiv_m c \implies a \equiv_m c$	(transitividade)
(3)	$a \equiv_m b \implies b \equiv_m a.$	(simetria)

▸ Esboço. Todas são facilmente demonstradas aplicando diretamente a definição de congruência módulo m (D3.155) e as propriedades básicas da $(|)$. □ (Θ3.162P)

3.163. Observação. Uma relação que satisfaz essas três propriedades é chamada *relação de equivalência* (§234). Ou seja, o Teorema Θ3.162 que acabamos de demonstrar afirma simplesmente que $(\equiv_m)$ *é uma relação de equivalência*. Estudamos relações no Capítulo 10. Paciência!

3.164. Propriedade. *Se $a \equiv b \pmod m$, então para todo $x \in \mathbb{Z}$ temos:*

(1) $a + x \equiv b + x \pmod m$; (2) $ax \equiv bx \pmod m$; (3) $-a \equiv -b \pmod m$.

▸ Esboço. Todas seguem facilmente pela definição (D3.155) de congruência módulo m. □

Θ3.165. Teorema (congruência). *Fixe um inteiro m. Sejam a, a', b, b' tais que $a \equiv_m a'$ e $b \equiv_m b'$. Logo:*

(1)	$a + b \equiv_m a' + b'$	$(+)$-compatível
(2)	$a \cdot b \equiv_m a' \cdot b'$	$(\cdot)$-compatível
(3)	$-a \equiv_m -a'$.	$(-_)$-compatível

Demonstrarás agora. Exercício x3.140. ∎

▸ **EXERCÍCIO x3.140.**
Demonstre o Teorema Θ3.165. (x3.140 H 0)

3.166. Congruências. O que foi isso? Efetivamente, o Teorema Θ3.165 está nos permitindo substituir congruentes por congruentes em qualquer expressão de soma, de multiplicação, e de negação, garantindo que o novo resultado vai ser congruente ao original.

▸ **EXERCÍCIO x3.141.**
Suponha que $x \equiv t \pmod m$, e seja a um inteiro positivo. O que podemos concluir sobre o x módulo ma? (x3.141 H 1 2)

▸ **EXERCÍCIO x3.142 (De igualdades para congruências).**
Sejam a, b inteiros. Se $a = b$, então $a \equiv_m b$ para qualquer inteiro m. (x3.142 H 0)

▸ **EXERCÍCIO x3.143 (De congruências para igualdades?).**
Há inteiros m tais que o recíproco é válido? Ou seja, tais que podemos inferir $a = b$ a partir de apenas $a \equiv_m b$. (x3.143 H 0)

§70. Inversos e cancelamentos

D3.167. Definição (Inverso). Seja $a, a', m \in \mathbb{Z}$. Chamamos a' *um inverso (multiplicativo) de a módulo m*, sse

$$aa' \equiv 1 \pmod m.$$

Se existe inverso do a, o denotamos com a^{-1} (dado um módulo m). ↯

▸ **EXERCÍCIO x3.144.**
Qual o problema com a definição do a^{-1}? (x3.144 H 0)

Podemos falar sobre *o* inverso (em vez de *um* inverso) módulo m, graças ao teorema seguinte.

Θ3.168. Teorema (Unicidade do inverso). *Sejam $a, m \in \mathbb{Z}$. Se $b, b' \in \mathbb{Z}$ satisfazem a $ax \equiv 1 \pmod{m}$, então $b \equiv b' \pmod{m}$.*

Demonstração. Como

$$ab \equiv 1 \pmod{m} \qquad \& \qquad ab' \equiv 1 \pmod{m},$$

pela transitividade e reflexividade da congruência módulo m, temos:

$$ab \equiv ab' \pmod{m}.$$

Pelo Propriedade 3.164, podemos multiplicar os dois lados por b:[38]

$$bab \equiv bab' \pmod{m}.$$

Daí, $(ba)b \equiv (ba)b' \pmod{m}$, ou seja $b \equiv b' \pmod{m}$. ∎

- **EXEMPLO 3.169.**
O inverso de 2 módulo 9 é o 5, porque $2 \cdot 5 = 10 \equiv 1 \pmod{9}$.

Como o exemplo seguinte mostra, inversos não existem sempre:

- **EXEMPLO 3.170.**
O 4 não tem inverso módulo 6.
Resolução. Podemos verificar com força bruta:

$$\begin{aligned} 4 \cdot 1 &= 4 \equiv 4 \pmod{6} \\ 4 \cdot 2 &= 8 \equiv 2 \pmod{6} \\ 4 \cdot 3 &= 12 \equiv 0 \pmod{6} \\ 4 \cdot 4 &= 16 \equiv 4 \pmod{6} \\ 4 \cdot 5 &= 20 \equiv 2 \pmod{6} \end{aligned}$$

Pronto.

O teorema seguinte esclarece a situação:

Θ3.171. Teorema (Inverso módulo m). *Sejam $a, m \in \mathbb{Z}$.*

$$a \text{ tem inverso módulo } m \iff (a, m) = 1.$$

Demonstração. Precisamos mostrar as duas direções do ($\Leftrightarrow$).

($\Rightarrow$): Escrevemos o $(a, m) = 1$ como combinaçãolinear dos a e m (sabemos que é possível por Lemma de Bézout Λ3.107, e, até melhor construtível graças ao algoritmo estendido de Euclides, Algoritmo a3.116):

$$1 = sa + tm, \qquad \text{para alguns } s, t \in \mathbb{Z}.$$

[38] Nada especial sobre b contra o b'. Poderiamos multiplicar por qualquer inverso do a aqui.

Então temos:

$$\begin{aligned} 1 &\equiv sa + tm \pmod m \\ &\equiv sa + 0 \pmod m \\ &\equiv sa \pmod m. \end{aligned}$$

Acabamos de achar um inverso de a módulo m: o s.

($\Leftarrow$): Seja b um inverso de a módulo m; em outras palavras:

$$ab \equiv 1 \pmod m,$$

ou seja, $m \mid ab - 1$, e $mu = ab - 1$ para algum $u \in \mathbb{Z}$. Conseguimos escrever

$$1 = um - ba,$$

a combinação linear dos a e m. Pelo Lemma de Bézout Λ3.107, $(a, m) \mid 1$, logo $(a, m) = 1$. ∎

Logo (Secção §75) vamos encontrar mais uma maneira legal de achar inversos módulo um inteiro.

! **3.172. Cuidado.** A lei de cancelamento, mesmo válido nas igualdades, não é válido nas congruências em geral. Por exemplo, $3 \cdot 2 \equiv 3 \cdot 8 \pmod{18}$, mas não podemos cancelar os 3 nos dois lados: $2 \not\equiv 8 \pmod{18}$.

Felizmente, o teorema seguinte mostra quando realmente podemos cancelar:

Θ3.173. Teorema (Lei de cancelamento módulo m). *Seja m inteiro. Para todo c coprimo com m,*

$$ca \equiv cb \pmod m \implies a \equiv b \pmod m.$$

▸ Esboço. Multiplicamos tudo por c^{-1}, cuja existência (módulo m) é garantida pela hipótese (aplicando o Teorema Θ3.171). □ (Θ3.173P)

▸ **EXERCÍCIO x3.145.**
Aplicando as definições e propriedades de congruência e da relação (|), ache uma outra demonstração do Θ3.173. (x3.145 H 0)

Θ3.174. Teorema (Wilson). *Seja p inteiro.*

$$p \text{ primo} \iff (p-1)! \equiv_p -1.$$

Demonstrarás agora no Exercício x3.146. ∎

▸ **EXERCÍCIO x3.146.**
Demonstre o Teorema Θ3.174. (x3.146 H 1 2)

§71. Exponenciação

3.175. Nunca grande demais. Calculando nos inteiros (com igualdade) expressões que envolvem diversas operações os passos intermediários podem acabar precisando um espaço grande, e o processo todo um tempo longo também. Por exemplo, queremos calcular o inteiro 106^{1540}:

$$106^{1540} = 935475693614\underbrace{\ldots\ldots}_{\text{(3095 dígitos omitidos)}}159789080576.$$

O que muda quando a gente *trabalha módulo um inteiro?*

A maneira leiguíssima seria calcular o inteiro 106^{1540}, achar seu valor, e depois dividir este número—boa sorte—com o 50, para achar o resto da divisão que seria um x satisfatório para nossa busca. Observe que o problema não está apenas no último passo da exponenciação: durante esse cálculo precisamos fazer 1539 multiplicações entre números enormes. Podemos fazer melhor?

Antes de tudo, observe que graças à congruência podemos substituir o 106 por qualquer congruente seu (módulo 50), por exemplo o 6. Precisamos calcular o 6^{1540} (módulo 50) então.

Mas, seguindo fielmente a definição de exponenciação, essa melhoria não vai acabar fazendo alguma diferença grande: continuamos precisando performar 1539 multiplicações custosas.

Uma observação critical aqui é que precisando calcular várias operações "modulares", temos controle para não permitir ao tamanho dos resultados intermediários crescer muito: *em vez de deixar a modularização para o final, a performamos no fim de cada operação que chegou num resultado grande.* E o que significa grande? Bem, alguém pode ser satisfeito trabalhando com números no $\{0, 1, \ldots, 49\}$, mas eu prefiro menores ainda: dá para substituir os $49, 48, \ldots, 26$ pelos seus congruentes $-1, -2, \ldots, -24$. Assim teriamos:

$$\text{1539 multiplicações} \begin{cases} 6^2 = 6 \cdot 6 = 36 \equiv -14 \\ 6^3 = (-14) \cdot 6 = -84 \equiv 16 \\ 6^4 = 16 \cdot 6 = 96 \equiv -4 \\ 6^5 = (-4) \cdot 6 = -24 \equiv -24 \\ \quad\vdots \\ 6^{1540} = (-4) \cdot 6 = -24 \equiv -24. \end{cases}$$

? **Q3.176. Questão.** Como procederia para achar um x "pequeno" tal que $6^{1540} \equiv_{50} x$?

!! SPOILER ALERT !!

Resposta: quadrados iterados. Calculamos os quadrados

$$\begin{aligned} 6^2 &= 36 \equiv -14 & 6^{64} &\equiv -4 \\ 6^4 &= (-14)^2 = 196 \equiv -4 & 6^{128} &\equiv -16 \\ 6^8 &= (-4)^2 = 16 \equiv 16 & 6^{256} &\equiv 6 \\ 6^{16} &= 16^2 = 256 \equiv 6 & 6^{512} &\equiv -14 \\ 6^{32} &= 6^2 = 36 \equiv -14 & 6^{1024} &\equiv -4. \end{aligned}$$

E agora temos:

$$6^{1540} = 6^{1024+512+4} = 6^{1024}6^{512}6^4 = (-4)(-14)(-4) = -224 \equiv -24 \pmod{50}.$$

§72. Resolvendo umas congruências

3.177. Corolário. *Dados inteiros a, m, a congruência*

$$ax \equiv 1 \pmod{m}$$

tem resolução para x sse $(a, m) = 1$.

Demonstração. Observe que aqui «x é resolução» significa «x é o $(\cdot)$-inverso de a», e logo esta proposição é corolário imediato do Teorema Θ3.171. ∎

3.178. Corolário. *Dados inteiros a, b, m com a, m coprimos, a congruência*

$$ax \equiv b \pmod{m}$$

tem resolução para x.

▸ Esboço. Suponha a, m coprimos. Logo o a possui inverso a'. É rotina verificar que o $a'b$ satisfaz a congruência desejada. □

▸ **EXERCÍCIO x3.147.**
Enuncie o reciproco do Corolário 3.178 e demonstre ou refute. (x3.147 H 0)

▸ **EXERCÍCIO x3.148 (raizes quadradas de 1).**
Podemos, em geral, resolver a congruência $x^2 \equiv 1 \pmod{m}$? (x3.148 H 0)

§73. O teorema chinês do resto

Já sabemos como resolver congruências do tipo

$$ax \equiv b \pmod{m},$$

e agora vamos ver como resolver uns *sistemas* de congruências.

Θ3.179. Teorema chinês do resto (binário). *Sejam m_1, m_2, b_1, b_2 inteiros tais que m_1, m_2 são coprimos. Logo existe inteiro x que satisfaz o sistema de congruências*

$$x \equiv b_1 \pmod{m_1}$$
$$x \equiv b_2 \pmod{m_2}.$$

Além disso, a solução do sistema é única módulo $m_1 m_2$.

▸ Esboço. Existência: Observe que o inteiro b_1 com certeza satisfaz a primeira congruência. O problema é que talvez não satisfaça a segunda. Felizmente, temos mais inteiros que satisfazem a primeira na nossa disposição. Muito mais: uma infinidade deles: cada congruente ao b_1, ou seja os membros do conjunto

$$\{\, m_1 k + b_1 \mid k \in \mathbb{Z} \,\}$$

são exatamente todos os inteiros que satisfazem a primeira. Agora estamos numa situação bem melhor, basta achar algum deles que satisfaz a segunda. Observe que cada membro desse conjunto é determinado por uma escolha de $k \in \mathbb{Z}$. Ou seja, basta achar um inteiro k tal que $m_1 k + b_1$ satisfaz a segunda. Talvez conseguimos achar até uma infinidade de tais inteiros. Vamo lá! Procuramos inteiros k tais que

$$m_1 k + b_1 \equiv b_2 \pmod{m_2},$$

ou seja, tais que

$$m_1 k \equiv b_2 - b_1 \pmod{m_2}.$$

(Por quê?) Mas sabemos como resolver essa congruência para k. (Né? Por quê?) □

▸ **EXERCÍCIO x3.149.**
Responda no primeiro "por quê?" acima. (x3.149 H 0)

▸ **EXERCÍCIO x3.150.**
E no segundo. (x3.150 H 0)

Vamos ver isso na prática:

• **EXEMPLO 3.180.**
Ache todos os inteiros $x \in \mathbb{Z}$ que satisfazem o sistema de congruências:

$$x \equiv 1 \pmod{5}$$
$$x \equiv 7 \pmod{12}.$$

Resolução. Os inteiro que satisfazem a primeira congruência são os membros do

$$\{\, 5k + 1 \mid k \in \mathbb{Z} \,\}.$$

Basta achar os valores de k tais que $5k + 1$ também satisfaz a segunda, ou seja, resolver a congruência

$$5k + 1 \equiv 7 \pmod{12}$$

por k. Passando o $(+1)$ peloutro lado (por que podemos fazer isso numa congruência?) temos

$$\begin{aligned} 5k &\equiv 7-1 \pmod{12} \\ &\equiv 6 \qquad \pmod{12}. \end{aligned}$$

Agora basta "dividir por 5", ou seja, multiplicar ambos os lados pelo 5^{-1}, ou seja, pelo inverso de 5 módulo 12, que sabemos que existe pois $(5,12) = 1$ e logo 5 é invertível módulo 12. Percebemos que 5 é seu próprio inverso, pois $5^2 = 25 \equiv 1 \pmod{12}$, e se não percebemos isso, usamos o algoritmo de Euclides para calcular o inverso de 5 módulo 12. Temos:

$$\begin{aligned} k &\equiv 5 \cdot 6 \pmod{12} \\ &\equiv 30 \pmod{12} \\ &\equiv 6 \pmod{12}. \end{aligned}$$

Logo, para qualquer inteiro k', tomando $k = 12k' + 6$, o $5k + 1$ satisfaz ambas as congruências. Substituindo:

$$5k + 1 = 5(12k' + 6) + 1 = 60k' + 30 + 1 = 60k' + 31.$$

Em termos de classes módulo 60, achamos a única resolução:

$$x \equiv 31 \pmod{60}.$$

? **Q3.181. Questão.** E se o sistema tem mais congruências?

!! SPOILER ALERT !!

Resposta. Supondo que os módulos são *coprimos dois-a-dois*, nenhum problema! Basta só focar em duas congruências cada vez, e substituí las por uma, que corresponde na sua resolução (módulo o produto dos seus módulos).

▸ **EXERCÍCIO x3.151.**
Ache todos os inteiros $x \in \mathbb{Z}$ que satisfazem o sistema de congruências:

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 7 \pmod{12} \\ x &\equiv 3 \pmod{7}. \end{aligned}$$

(x3.151 H 1)

Θ3.182. Teorema chinês do resto. *Sejam $a_1, \ldots, a_k, m_1, \ldots, m_k \in \mathbb{Z}$, com os m_i's coprimos dois-a-dois:*

$$(\forall i, j \in \{1, \ldots, k\})[\, i \neq j \implies (m_i, m_j) = 1\,].$$

Logo existe $x \in \mathbb{Z}$ que satisfaz o sistema de congruências

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

Além disso, a solução do sistema é única módulo $m_1 \cdots m_k$.

▸ Esboço. Existência: Seja

$$M := \prod_{i=1}^{k} m_i = m_1 m_2 \cdots m_k$$

e, para todo $i \in \{1, \ldots, k\}$, defina o

$$M_i := \prod_{\substack{j=1 \\ j \neq i}}^{k} m_j = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k = \frac{M}{m_i}.$$

Observe que M_i é invertível módulo m_i, então seja B_i o seu inverso. Verificamos que o inteiro

$$x = \sum_{i=1}^{k} a_i M_i B_i$$

satisfaz todas as k congruências, e é então uma solução do sistema.

Unicidade: Suponha que $x' \in \mathbb{Z}$ é uma solução do sistema. Usando a definição de congruência e propriedades de $(|)$, mostramos que $x' \equiv x \pmod{M}$. □

• **EXEMPLO 3.183.**
Bora achar todos os inteiros x que satisfazem o sistema de congruências:

$$\begin{aligned} x &\equiv 2 \pmod{9} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 2 \pmod{4}. \end{aligned}$$

Bora. Observamos primeiramente que os módulos 9, 5, e 4 realmente são coprimos dois-a-dois. Então, pelo teorema chinês do resto, o sistema realmente tem solução. Seguindo sua método—e usando os mesmos nomes para as variáveis como no Teorema chinês do resto Θ3.182 mesmo—calculamos os:

$$\begin{aligned} M &= 9 \cdot 5 \cdot 4 = 180 \\ M_1 &= \quad 5 \cdot 4 = 20 \\ M_2 &= 9 \quad \cdot 4 = 36 \\ M_3 &= 9 \cdot 5 \quad = 45 \end{aligned} \qquad \begin{aligned} B_1 &\equiv 5 \pmod{9} \\ B_2 &\equiv 1 \pmod{5} \\ B_3 &\equiv 1 \pmod{4}, \end{aligned}$$

onde os invérsos B_i's podemos calcular usando o algoritmo estendido de Euclides (a3.116) como na prova do Teorema Θ3.171), mas nesse caso, sendo os módulos tão pequenos fez mas sentido os achar testando, com "força bruta". Então, graças ao teorema chinês, as soluções são exatamente os inteiros x que satisfazem

$$\begin{aligned} x &\equiv a_1M_1B_1 + a_2M_2B_2 + a_3M_3B_3 \pmod{M} \\ &\equiv 2\cdot 20\cdot 5 + 1\cdot 36\cdot 1 + 2\cdot 45\cdot 1 \pmod{180} \\ &\equiv 200 + 36 + 90 \pmod{180} \\ &\equiv 146 \pmod{180}. \end{aligned}$$

Para resumir, as soluções do sistema são todos os elementos do $\{\, 180k + 146 \mid k \in \mathbb{Z} \,\}$.

- **EXEMPLO 3.184.**
Vamo achar todos os inteiros x com $|x| < 64$ que satisfazem o sistema de congruências:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ 3x &\equiv 1 \pmod 4 \\ 4x &\equiv 2 \pmod 5. \end{aligned}$$

VAMO. Para aplicar o teorema chinês do resto precisamos os 3, 4, e 5 coprimos dois-a-dois, que realmente são. Mas observe que o sistema não está na forma do teorema; aí, não podemos aplicá-lo diretamente. Nosso primeiro alvo então seria transformar a segunda e a terceira congruência para equivalentes, na forma necessária para aplicar o teorema. Na segunda vamos nos livrar do fator 3, e na terceira do fator 4. Como $(3,4) = 1$,[39] o 3 é invertível módulo 4. Como o $3 \equiv -1 \pmod 4$, temos diretamente que $3^{-1} \equiv -1 \pmod 4$. Similarmente achamos o inverso $4^{-1} \equiv -1 \pmod 4$. Então temos:

$$\left.\begin{aligned} x &\equiv 1 \pmod 3 \\ 3x &\equiv 1 \pmod 4 \\ 4x &\equiv 2 \pmod 5 \end{aligned}\right\} \iff \left\{\begin{aligned} x &\equiv 1 \pmod 3 \\ 3^{-1}3x &\equiv 3^{-1}1 \pmod 4 \\ 4^{-1}x &\equiv 4^{-1}2 \pmod 5 \end{aligned}\right\} \iff \left\{\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv -1 \pmod 4 \\ x &\equiv -2 \pmod 5. \end{aligned}\right.$$

Agora sim, podemos aplicar o teorema chinês. Usando os mesmos nomes para as variáveis como no Teorema chinês do resto Θ3.182, calculamos:

$$\begin{aligned} M &= 3\cdot 4\cdot 5 = 60 & & \\ M_1 &= \quad 4\cdot 5 = 20 & B_1 &\equiv 2 \pmod 3 \\ M_2 &= 3 \quad \cdot 5 = 15 & B_2 &\equiv 3 \pmod 4 \\ M_3 &= 3\cdot 4 \quad = 12 & B_3 &\equiv 3 \pmod 5, \end{aligned}$$

onde os invérsos B_1 e B_2 calculamos percebendo que $20 \equiv -1 \pmod 3$ e $15 \equiv -1 \pmod 4$, e o B_3 com força bruta mesmo. Pronto: as soluções do sistema são exatamente os inteiros x que satisfazem:

$$\begin{aligned} x &\equiv a_1M_1B_1 + a_2M_2B_2 + a_3M_3B_3 \pmod{M} & & \\ &\equiv 1\cdot 20\cdot 2 + 3\cdot 15\cdot 3 + 3\cdot 12\cdot 3 \pmod{60} & & \\ &\equiv 40 + 135 + 108 \pmod{60} & & \\ &\equiv 40 + 15 + 108 \pmod{60} & & (135 \equiv 15 \pmod{60}) \\ &\equiv 55 + 48 \pmod{60} & & (108 \equiv 48 \pmod{60}) \\ &\equiv -5 + 48 \pmod{60} & & (\ 55 \equiv -5 \pmod{60}) \\ &\equiv 43 \pmod{60}. & & \end{aligned}$$

[39] Qual '4' foi esse?

Logo, o conjunto de todas as soluções do sistema é o $\{\,60k+43 \mid k\in\mathbb{Z}\,\}$. Facilmente verificamos que os únicos dos seus elementos que satisfazem nossa restricção $|x|<64$ são os inteiros obtenidos pelos valores de $k=0$ e -1: $x_1=43$, $x_2=-17$.

▸ **EXERCÍCIO x3.152 ("entre si" vs "dois-a-dois").**
Considere as frases:

(i) Os inteiros $a_1,a_2,\ldots,a_n$ são coprimos entre si.
(ii) Os inteiros $a_1,a_2,\ldots,a_n$ são coprimos dois-a-dois.

Mostre com um contraexemplo que as duas afirmações não são equivalentes. (x3.152 H 1)

▸ **EXERCÍCIO x3.153.**
Ache as soluções dos sistemas de congruências seguintes:

$$(1)\quad \begin{cases} x\equiv 3 \pmod 4\\ 5x\equiv 1 \pmod 7\\ x\equiv 2 \pmod 9\end{cases}\qquad (2)\quad \begin{cases} x\equiv 3 \pmod 3\\ 3x\equiv 3 \pmod 4\\ 4x\equiv 2 \pmod 5\\ 5x\equiv 1 \pmod 7).\end{cases}$$

(x3.153 H 0)

O exercício seguinte te convida descobrir que o teorema chinês pode ser aplicado em casos mais gerais do que aparece inicialmente!

▸ **EXERCÍCIO x3.154.**
Resolva os sistemas de congruências:

$$(1)\quad \begin{cases} 5x\equiv 2 \pmod 6\\ x\equiv 13 \pmod{15}\\ x\equiv 2 \pmod 7\end{cases}\qquad (2)\quad \begin{cases} x\equiv 2 \pmod 6\\ x\equiv 13 \pmod{15}\\ x\equiv 2 \pmod 7).\end{cases}$$

(x3.154 H 1 2 3 4)

§74. Critéria de divisibilidade

3.185. Critérion (Divisibilidade por potências de 10). *Um inteiro $c\neq 0$ é divisível por 10^k sse o c escrito em base decimal termina com k dígitos 0.*

3.186. Critérion (Divisibilidade por 2 ou 5). *Seja $m\in\{2,5\}$. Um inteiro c é divisível por m sse o valor do último dígito do c (em base decimal) é divisível por m.*

3.187. Critérion (Divisibilidade por 3 ou 9). *Seja $m\in\{3,9\}$. Um inteiro c é divisível por m sse o somatório dos valores dos dígitos do c (em base decimal) é divisível por m.*

3.188. Critérion (Divisibilidade por 4, 20, 25, 50). *Seja $m \in \{4, 20, 25, 50\}$. Um inteiro c é divisível por m sse o número formado pelos dois últimos dígitos do c (em base decimal) é divisível por m.*

3.189. Critérion (Divisibilidade por 11). *Um inteiro c é divisível por 11 sse o somatório dos valores dos dígitos do c (em base decimal) em posição par menos o somatório dos valores dos seus dígitos em posição ímpar é divisível por 11.*

▸ **EXERCÍCIO x3.155 (Divisibilidade por 6).**
Ache um critério (para o sistema decimal) para divisibilidade por 6. (x3.155 H 1)

3.190. Proposição (Divisibilidade por 8). *Um número c é divisível por 8 sse ele satisfaz os critéria de divisibilidade por 2 e 4.*

▸ DEMONSTRAÇÃO ERRADA. Observe que por causa do Corolário 3.134, temos:

$$8 \mid c \iff 2 \mid c \ \&\ 4 \mid c.$$

Logo, aplicamos os critéria de divisibilidade por 2 e por 4. ↯

▸ **EXERCÍCIO x3.156.**
Ache o erro no Proposição 3.190, e compare com a solução do Exercício x3.155. (x3.156 H 1)

▸ **EXERCÍCIO x3.157.**
Ache um critério (no sistema decimal) para divisibilidade por 8, e generalize para divisibilidade por 2^k (x3.157 H 1 2)

▸ **EXERCÍCIO x3.158.**
Ache um critério (no sistema decimal) para divisibilidade por $2^x 5^y$, onde $x, y \in \mathbb{N}$. (x3.158 H 1)

Intervalo de problemas

▸ **PROBLEMA Π3.29.**
Sejam a, b, c inteiros tais que $a^2 + b^2 = c^2$. Então $3 \mid abc$. (Π3.29 H 1 2)

▸ **O SONHO DO CALOURO Π3.30.**
Seja p primo, $x, y \in \mathbb{Z}$.

$$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

(Π3.30 H 1 2)

▸ **PROBLEMA Π3.31.**
Existe uma infinidade de primos "da forma $4n + 3$", ou seja, o conjunto

$$\{\, 4n + 3 \mid n \in \mathbb{N} \text{ e } 4n + 3 \text{ primo} \,\}$$

é infinito. (Π3.31 H 1 2 3 4 5 6)

▸ **PROBLEMA Π3.32.**
Depois de ter resolvido o Problema Π3.31, explique por que sua demonstração não é trivialmente adaptável para resolver a mesma questão sobre os primos da forma $4n+1$. (Π3.32 H 1)

Θ3.191. Teorema (Dirichlet). *Sejam inteiros a, m coprimos. Existe uma infinidade de primos p tal que $p \equiv a \pmod m$.*

Este teorema foi conjecturado—e usado!—por Legendre no ano 1785 e finalmente demonstrado por Dirichlet no ano 1837.

▸ CADÊ A DEMONSTRAÇÃO?. Infelizmente, não temos uma demonstração com as ferramentas elementares que temos elaborado aqui. Para matá-lo usamos artilharia pesada, *teoria dos números analítica*, que aproveita a Análise Matemática para estudar assuntos da teoria dos números. O livro **[Ser73:** Chapter VI**]** dedica um capítulo inteiro à demonstração deste teorema, e o **[Apo76:** Chapter 7**]** também! □

§75. Umas idéias de Fermat

Fermat (1607–1665) percebeu que para qualquer primo p, e qualquer inteiro a não divisível por p, o $a^p - a$ era sempre múltiplo de p:

$$p \nmid a \implies p \mid a^{p-1} - 1.$$

Observe que como $a^p - a = a(a^{p-1} - 1)$, temos

$$\begin{aligned} p \mid a^p - a &\iff p \mid a(a^{p-1} - 1) \\ &\iff p \mid a \text{ ou } p \mid a^{p-1} - 1. \end{aligned}$$

Hoje a gente escreveria a observação de Fermat

$$a^p \equiv a \pmod p,$$

notação e percepção inacessível a Fermat naquela epoca, uns 158 anos antes do **[Gau66]** (1798) de Gauss.

Θ3.192. Teorema pequeno de Fermat (Fermatinho). *Seja p primo. Logo*

$$(\forall a)[\, a^p \equiv_p a \,].$$

Fermat não demonstrou este teorema; alegou que não quis encher o saco do seu leitor com os detalhes da demonstração. Pelo contrário, eu vou encher teu saco mesmo. Quem de fato demonstrou (e publicou) esse teorema primeiro, foi o suiço Euler, no ano 1736. Leibniz tinha também escrito efetivamente a mesma demonstração de Euler em algum momento antes do ano 1683, mas nunca chegou a publicá-la. Agora chega de história, bora demonstrar.

DEMONSTRAÇÃO. Basta demonstrar o teorema para todo $a \geq 0$, ou, ainda mais, basta verificar apenas os $a \in \{0, \ldots, p-1\}$, pois estamos trabalhando módulo p.

Por indução no a. BASE. Calculamos $0^p = 0 \equiv_p 0$ e pronto. PASSO INDUTIVO. Seja k tal que $k^p \equiv_p k$. Precisamos mostrar que $(k+1)^p \equiv_p k+1$. Calculamos:

$$\begin{aligned}(k+1)^p &\equiv_p k^p + 1^p && \text{(O sonho do calouro Π3.30)}\\ &\equiv_p k + 1^p && \text{(h.i.)}\\ &\equiv_p k+1.\end{aligned}$$

∎

3.193. Corolário. *Sejam p primo e a inteiro tais que a, p são coprimos. Então*

$$a^{p-1} \equiv_p 1.$$

DEMONSTRAÇÃO. Tua: Exercício x3.159. ∎

▸ **EXERCÍCIO x3.159.**
Obtenha o Corolário 3.193 pelo Fermatinho (Θ3.192). (x3.159 H 1)

3.194. Nova maneira de calcular inversos. O Fermatinho nos permite calcular rapidamente inversos.

▸ **EXERCÍCIO x3.160.**
Como? (x3.160 H 1)

▸ **EXERCÍCIO x3.161.**
Calcule (na mão!) o $(\cdot)$-inverso de 108 módulo 241. (x3.161 H 1)

3.195. Nova maneira para exponenciação modular. O Fermatinho nos permite calcular rapidamente potências módulo um inteiro.

▸ **EXERCÍCIO x3.162.**
Como? (x3.162 H 0)

• **EXEMPLO 3.196.**
Ache o último dígito do 2^{800}.
RESOLUÇÃO. Procuramos um y tal que $2^{800} \equiv y \pmod{10}$ (por quê?). Usando o Fermatinho (Θ3.192) temos:

$$2^4 \equiv 1 \pmod 5,$$

logo

$$2^{800} = (2^4)^{200} \equiv 1 \pmod 5.$$

Então módulo 10 temos duas possibilidades (por quê?):

$$2^{800} \equiv \begin{cases} 1 \pmod{10} \\ 6 \pmod{10}. \end{cases}$$

Podemos já eliminar a primeira porque 2^{800} é par. Finalmente, o último dígito de 2^{800} é o 6.

▸ **EXERCÍCIO x3.163.**
Responda no primeiro "por quê?" do Exemplo 3.196. (x3.163 H 1 2)

▸ **EXERCÍCIO x3.164.**
Responda no segundo também, e ache um outro caminho para chegar no resultado, usando o Teorema chinês do resto Θ3.182. (x3.164 H 1)

▸ **EXERCÍCIO x3.165.**
Ache o resto da divisão de 41^{75} por 3. (x3.165 H 1 2 3 4)

§76. Primalidade

Investigamos aqui o problema seguinte: *dado um inteiro x, verifique se x é primo ou não.*

3.197. O que temos até agora. Fatore o x em primos (Teorema fundamental da aritmética Θ3.140; veja se a fatoração do x é o próprio x. Qual o problema com isso? Demora demais! Seria legal se a gente poderia decidir se x é primo ou não sem necessariamente precisar fatorá-lo. No final das contas, fatorando acabamos com *muita* mais informação do que estamos buscando aqui.

De fato, *pensando pouco*, parece que estou exagerando sobre o quão ruim que é a situação: não precisamos achar a fatoração completa do x. Assim que achar o primeiro fator primo podemos já parar o processo pois já temos nossa resposta.

De mais-fato-ainda, *pensando mais*, isso não acaba sendo tão melhor do que a idéia de achar a fatoração completa. Cada divisão custa, e se a quantidade delas fosse pequena em comparação com o tamanho do nosso número x, seria aceitável; mas não é. Aqui «pequena em comparação» significa de ordem de complexidade menor.

3.198. Critérion (Wilson). *Para qualquer inteiro p,*

$$p \text{ primo} \iff (p-1)! \equiv_p -1.$$

Demonstrado no Teorema Θ3.174. ∎

3.199. Hipotese chinesa. Começando testar uns números contra o teste de Fermat, observamos que todos que "são pegos" por ele, já estão pegos aplicando o teste 2-fermatinho. Assim parece que nem precisamos testar contra os a-fermatinhos para $a > 2$. Essa hipótese é conhecida como *hipótese chinesa:*

$$(\forall x)[\,(\exists 1 < a < x-1)[\,a^x \not\equiv_x a\,] \implies 2^x \not\equiv_x 2\,].$$

É fácil ver como tal conjectura chegou a ser estipulada: de fato, todos os inteiros até o 340 são testemunhas dela. Mas é um $(\forall x)[\dots]$ que está sendo alegado aqui, e não há quantidade suficiente de testemunhas que podemos testar para de fato confiar nela. Surpreendentemente, o próximo número, o 341 é o primeiro contraexemplo para essa hipótese: de fato, $2^3 41 \equiv_{341} 2$, mas mesmo assim tem a-fermatinho que o 341 não consegue enganar.

▸ **EXERCÍCIO x3.166 (Enganador da chinesa).**
Verique que $2^{341} \not\equiv_3 412$, e que 341 não consegue enganar mesmo o fermatinho: ache um a-fermatinho por qual o 341 é pego. (x3.166 H 0)

3.200. Números Carmichael. O 341 foi o primeiro número que conseguiu enganar o 2-fermatinho, mas mesmo assim não conseguiu enganar o próprio fermatinho, como tu descubriu no Exercício x3.166 (né?) achando um a tal que o a-fermatinho pegou o 341 em flagrante. Continuando testando os próximos números, parece de novo que ninguém consegue enganar o fermatinho. Novamente tal conclusão é errada: chegando no número 561 encontramos o primeiro exemplo de enganador de fermatinho. O 561 não é primo ($561 = 3 \cdot 11 \cdot 17$), mas mesmo assim ele consegue enganar todos os a-fermatinhos! Tais inteiros chamamos de *números Carmichael*, e eles são bem raros em comparação com os primos—algo que vai acabar facilitando nossa vida daqui a pouco. Para um tempão não sabíamos se há uma quantidade infinita deles ou não; de fato, há uma infinidade de números Carmichael, algo que foi demonstrado só em 1994; mas não vamos precisar disso aqui.

3.201. Pseudoprimos. Dado um "pseudocritério" de primalidade, como o da hipótese chinesa (o 2-fermatinho) ou o fermatinho, chamamos de *pseudoprimo* um número x que conseguiu satisfazer tal pseudocritério sem ser mesmo um primo. A noção de pseudoprimo, então, depende do pseudocritério. Percebemos então que 341 é um pseudoprimo para o 2-fermatinho, e 561 é um pseudoprimo para o fermatinho.

Θ3.202. Teorema (loop de fermatinho: eficiência). *Seja $m > 0$. Se existe inteiro a coprimo com m tal que $a^{m-1} \not\equiv_m 1$, então para pelo menos metade dos inteiros $0 \leq x < m$,*

$$x^{m-1} \not\equiv_m 1.$$

Demonstração. Seja a um tal inteiro: coprimo com m e tal que $a^{m-1} \not\equiv_m 1$. Basta associar com cada inteiro-aprovado (que conseguiu passar o teste), um que não o passou, em forma *injetiva:* associamos distintos aprovados com distintos reprovados. Isso garanta que a quantidade dos dos aprovados não pode superar a metade, que é exatamente o que precisamos demonstrar. O mapeamento que procuramos é a $(x \mapsto ax)$: associamos cada aprovado x o inteiro ax, e basta demonstrar que: (i) ax realmente é reprovado (x3.167; (ii) o mapeamento realmente é injetivo (x3.168). Deixo contigo. ∎

▸ **EXERCÍCIO x3.167.**
Demonstre a parte (i) do Teorema Θ3.202. (x3.167 H 0)

▸ **EXERCÍCIO x3.168.**
Demonstre a parte (ii) do Teorema Θ3.202. (x3.168 H 0)

§77. Geração de primos

TODO Terminar

3.203. Já temos umas maneiras de *gerar* primos à vontade. O crivo de Eratosthenes (Nota 3.138) gera todos os primos até um dado número, e a demonstração de Euclides

sobre a quantidade dos primos fornece um gerador de primos também. Mas, aqui um desafio: achar um primo grande. Nenhuma dessas idéias funciona bem aqui, pois aqui «bem» significa que tu vai achar tal primo antes de morrer. E o que significa «grande»? Depende da situação, obviamente, então vamos considerar que um desafiador escolha um comprimento ℓ e uma base b e nosso objetivo é achar um primo p cujo númeral canônico na base b tem tamanho ℓ. Efetivamente procuramos primo $b^\ell \leq p < b^{\ell+1}$. Vamo concretizar a situação? Ache um primo p que, escrito no sistema posicional binário, ocupa 4096 bits.

? **Q3.204. Questão.** Como procederias?

!! SPOILER ALERT !!

3.205. Chutando. Por incrível que pareça, uma maneira muito eficiente é *chutando*. Escolhe aleatoriamente cada bit; verifique se o número gerado é primo; se é, acabou, senão, chute novamente.

3.206. Mas isso funciona?. Essa idéia só vai funcionar se os primos não são muito raros. Apresento aqui, sem demonstração, o famoso *teorema dos números primos* que estabelece exatamente a freqüência asintótica dos primos:

Θ3.207. Teorema dos Números Primos. *Seja* $\pi(x) \stackrel{\text{def}}{=} \{\, p \leq x \mid p \text{ primo} \,\}$. *Temos*

$$\pi(x) \sim \frac{x}{\log x}.$$

Equivalentemente, $(p_n)_n \sim (n \log n)_n$.

A pergunta a qual este teorema responde tinha preocupado muitas lendas (incluindo Euler, Gauss, Legendre, Dirichlet, Chebychev, e Riemann) até finalmente foi demonstrado, por Hadamard e Poussin independentemente, no ano 1896, utilizando ferramentas de análise complexa, introduzidas pelo Riemann.

▸ Cadê a demonstração?. As demonstrações mais conhecidas utilizam ferramentas de análise complexa e, mesmo que existem umas elementares, ficam fora tanto do nosso alcance quanto do nosso foco aqui.[40] O leitor interessado pode encontrar a demonstração em textos de teoria dos números (analítica), por exemplo no **[Apo76:** Chapter 13**]** ou no **[HW79:** Chapter XXII**]**. □

[40] Análise complexa não é nada complexo nem é nada para dar medo para meu leitor. Logo depois do estudo dos reais no Capítulo 6, terás todas as ferramentas para estudar o assunto, caso quiser; e tenho umas referências pra ti no fim daquele capítulo.

3.208. O que isso significa, na prática, agora?. Que existem por volta de $1/\ell$ primos com ℓ dígitos. Ou seja, chutando ℓ algarismos b-ários, temos por volta de $1/\ell$ chances de "acertar" um primo. No Capítulo 6 (Os reais) aprendemos sobre limites de seqüências de números e o enunciado do Teorema dos Números Primos Θ3.207 vai aparecer menos obscuro. Mas por enquanto, é só entendê-lo na forma que mencionei aqui.

§78. Sistemas de resíduos

D3.209. Definição. Se $x \equiv y \pmod m$ dizemos que y é *um resíduo de x módulo m*. Seja $S = \{r_1, r_2, \ldots, r_n\}$ um conjunto de inteiros. Chamamos o S de *sistéma completo de resíduos módulo m* sse para todo inteiro x existe único $r \in S$ tal que r é um resíduo de x módulo m. Ou seja, cada inteiro tem exatamente um representante seu (do seu time) nesse conjunto R. Chamamos o S de *sistéma reduzido de resíduos módulo m* sse: (i) todos os membros de S são coprimos com m; (ii) $r_i \equiv_m r_j$ implica $i = j$ (ou seja, os membros de S são distintos dois-a-dois módulo m); (iii) para todo inteiro x coprimo com m, existe $r \in S$ tal que r é um resíduo de x módulo m. Se falar apenas de sistema completo (s.c.) ou de sistema reduzido (s.r.) sem mencionar o módulo m, é porque o consideramos implícito pelo contexto.

▸ **EXERCÍCIO x3.169.**
Todos os sistemas de resíduos módulo m do mesmo tipo (completo ou reduzido) têm a mesma cardinalidade entre si. (x3.169 H 0)

D3.210. Notação. Denotamos a cardinalide (comum) dos sistemas *reduzidos* de resíduos módulo m por $\phi(m)$. Investigamos a função ϕ logo na Secção §79.

▸ **EXERCÍCIO x3.170.**
Sejam C um sistema completo e R um sistema reduzido. O que podes afirmar sobre os

$$\sum C = ? \qquad\qquad \prod R = ?$$

Demonstre a corretude dos teus palpites. (x3.170 H 0)

3.211. Sistemas de graça. Tendo um sistema (completo ou reduzido) de resíduos módulo m, ganhamos "gratuitamente" outros sistemas (do mesmo tipo) de resíduos módulo o mesmo m. A idéia dos próximos exercícios é investigar o que podemos concluir se começar mexendo com um tal sistema S para gerar outros. O que podemos concluir sobre o $S + \ell$? Sobre o aS? Virando as mesas, se por acaso o $R + \ell$ ou o aS acaba, sendo sistemas também, o que podemos concluir sobre o ℓ? Sobre o a?

!! SPOILER ALERT !!

► **EXERCÍCIO x3.171.**
Sejam C um sistema completo de resíduos módulo m Então o conjunto $C + \ell$ também é um sistéma completo de resíduos módulo m. (x3.171 H 0)

► **EXERCÍCIO x3.172.**
Sejam C sistema completo e a inteiro. Suponha que aC também é um sistema completo. O que podes concluir sobre o a? O recíproco da tua resposta é válido? (x3.172 H 0)

► **EXERCÍCIO x3.173.**
Sejam R sistema reduzido e ℓ inteiro. Suponha que $R+\ell$ também é um sistema reduzido. O que podes concluir sobre o ℓ? (x3.173 H 0)

► **EXERCÍCIO x3.174.**
Seja R sistema reduzido e a inteiro. Suponha que aR também é um sistema reduzido. O que podes concluir sobre o a? O recíproco da tua resposta é válido? (x3.174 H 0)

3.212. Por quê «sistemas»?. Usamos a palavra "sistema" em vez da "conjunto". Por quê? A idéia é que estamos interessados não apenas nos membros de tais conjuntos, mas sim na estrutura algébrica que herdam dos inteiros. Os exercícios seguintes devem deixar isso mais claro.

► **EXERCÍCIO x3.175.**
Seja C um sistema completo de resíduos módulo m. Mostre que C é fechado módulo m sob a estrutura algébrica dos inteiros $(0,\, 1,\, (+),\, (\cdot),\, (-_))$. (x3.175 H 0)

► **EXERCÍCIO x3.176.**
Seja R um sistema reduzido de resíduos módulo m. Então R é $(1, (\cdot))$-fechado módulo m. Ainda mais, é fechado (módulo m, sempre) sob $(\cdot)$-inversos. (x3.176 H 0)

► **EXERCÍCIO x3.177.**
Sejam m, n coprimos, e sejam M e N sistemas reduzidos de resíduos módulo m e n respectivamente. Demonstre que o $nM + mN$ é um sistema reduzido de resíduos módulo mn. (x3.177 H 0)

§79. Euler entra

D3.213. Definição (Função totiente de Euler). Seja inteiro $n > 0$. Definimos

$$\phi(n) \stackrel{\text{def}}{=} |\{\, i \in \{1, \ldots, n\} \;\mid\; (i, n) = 1 \,\}| \,.$$

Em palavras, $\phi(n)$ é o número dos inteiros entre 1 e n que são coprimos com n.

► **EXERCÍCIO x3.178.**
Calcule os valores da $\phi(n)$ para $n = 1, 2, 3, 4, 8, 11, 12, 16$. (x3.178 H 0)

3.214. Propriedade. p primo $\implies \phi(p) = p - 1$.

DEMONSTRAÇÃO. Como p é primo, ele é coprimo com todos os $1, \dots, p-1$. E como $(p, p) = p \neq 1$, pela definição da ϕ temos $\phi(p) = p - 1$. ∎

▸ **EXERCÍCIO x3.179.**
Quantos multiplos de a existem no $\{1, 2, \dots, a^n\}$? (x3.179 H 0)

▸ **EXERCÍCIO x3.180.**
$\phi(n)$ é par para todo $n \geq 3$. (x3.180 H 1)

▸ **EXERCÍCIO x3.181.**
p primo $\implies \phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$. (x3.181 H 1)

▸ **EXERCÍCIO x3.182.**
Sejam p primo e $k \in \mathbb{Z}$. Calcule o valor do somatório $\sum_{i=0}^{k} \phi(p^i)$. (x3.182 H 1)

▸ **EXERCÍCIO x3.183.**
p, q primos, $p \neq q \implies \phi(pq) = (p-1)(q-1)$. (x3.183 H 0)

Θ3.215. Teorema. *A função ϕ é multiplicativa:*

$$(m, n) = 1 \implies \phi(mn) = \phi(m)\phi(n).$$

▸ ESBOÇO. Arrume todos os números $1, 2, \dots, mn$ numa tabela de dimensão $n \times m$ assim:

$$\begin{array}{rrrcrcrr}
1 & 2 & 3 & \cdots & r & \cdots & m-1 & m \\
m+1 & m+2 & m+3 & \cdots & m+r & \cdots & m+(m-1) & 2m \\
2m+1 & 2m+2 & 2m+3 & \cdots & 2m+r & \cdots & 2m+(m-1) & 3m \\
\vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots \\
(n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \cdots & (n-1)m+r & \cdots & (n-1)m+(m-1) & nm
\end{array}$$

□

TODO terminar

▸ **EXERCÍCIO x3.184.**
Obtenha o Teorema Θ3.215 como corolário do Teorema chinês do resto (binário) Θ3.179. (x3.184 H 0)

3.216. Corolário. *Se $n \geq 2$, então*

$$\phi(n) = n \prod_{\substack{p \text{ primo} \\ p \mid n}} \left(1 - \frac{1}{p}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right),$$

onde os p_i's são todos os primos divisores de n.

▸ ESBOÇO. Escrevemos o n na sua representação canônica pelo Teorema fundamental da aritmética Θ3.140 e aplicamos repetitivamente o Teorema Θ3.215. □ (3.216P)

▸ **EXERCÍCIO x3.185.**
$a \mid b \implies \phi(a) \mid \phi(b)$. (x3.185 H 0)

▸ **EXERCÍCIO x3.186.**
$\phi(2n) = \begin{cases} 2\phi(n), & n \text{ é par} \\ \phi(n), & n \text{ é ímpar.} \end{cases}$ (x3.186 H 0)

Θ3.217. Teorema (Euler, de congruência). *Sejam $a, m \in \mathbb{Z}$ com $(a, m) = 1$. Então*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

▸ Esboço. Considere o conjunto

$$R = \{r_1, r_2, \ldots, r_{\phi(m)}\}$$

de todos os inteiros r com $1 \leq r \leq m$, e $(r, m) = 1$, e o conjunto

$$\begin{aligned} aR &= \{\, ar \mid r \in R \,\} \\ &= \{ar_1, ar_2, \ldots, ar_{\phi(m)}\}. \end{aligned}$$

Observamos agora que (módulo m) os $ar_1, ar_2, \ldots, ar_{\phi(m)}$ são apenas uma permutação dos $r_1, r_2, \ldots, r_{\phi(m)}$. Logo os seus produtórios são congruentes:

$$(ar_1)(ar_2)\cdots(ar_{\phi(m)}) \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Trabalhando na última congruência chegamos na congruência desejada. □

3.218. Corolário. *Sejam p primo e $a \in \mathbb{Z}$ com $(a, p) = 1$. Então*

$$a^{p-1} \equiv 1 \pmod{p}.$$

▸ Esboço. O resultado é imediato usando o teorema de Euler (Θ3.217) e a Propriedade 3.214. □ (3.218P)

Intervalo de problemas

▸ **PROBLEMA Π3.33.**
Ache mais uma demonstração do "pequeno Fermat" usando o teorema multinominal. Essa provavelmente é a primeira demonstração do teorema, feita (sem publicar) por Leibniz, e redescoberta depois por Euler. (Π3.33 H 0)

▸ **PROBLEMA Π3.34.**
Demonstre numa linha o Exercício x4.22: *para todo $n \in \mathbb{N}$ e todo inteiro ímpar a, a^n é ímpar.* (Π3.34 H 1)

▸ **PROBLEMA Π3.35.**
(Generalização do Exercício x4.22.) Sejam $a \in \mathbb{Z}$ e $m \in \mathbb{N}$. Demonstre numa linha que para todo $n \in \mathbb{N}$, existe $b \in \mathbb{Z}$ tal que $(am+1)^n = bm+1$. (Π3.35 H 1)

▸ **PROBLEMA Π3.36.**
Demonstre que para todo $m \in \mathbb{N}$, o produto de quaisquer m consecutivos inteiros é divisível por $m!$. (Π3.36 H 0)

▸ **PROBLEMA Π3.37.**
Demonstre que

$$\phi(mn) = \phi(m)\phi(n)\frac{d}{\phi(d)}, \qquad \text{onde } d = (m,n).$$

Note quantas e quais das propriedades que já demonstramos são casos especiais dessa! (Π3.37 H 0)

▸ **PROBLEMA Π3.38.**
Sejam p, q primos com $p \neq q$. Demonstre que

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

(Π3.38 H 1 2)

▸ **PROBLEMA Π3.39.**
Ache uma generalização do Problema Π3.38 aplicável para inteiros a, b com $(a,b) = 1$. (Π3.39 H 1 2 3)

§80. Criptografia

TODO A idéia da criptografia
TODO Criptografia vs. steganografia
TODO Criptografia vs. codificação
TODO Criptografia "public-key"
TODO RSA criptografia e descriptografia

Θ3.219. Teorema. *Sejam e, M inteiros com $(e, \phi(M)) = 1$, e seja d um inverso de e módulo $\phi(M)$: $ed \equiv 1 \pmod{\phi(M)}$. Para cada x com $(x, M) = 1$,*

$$(x^e)^d \equiv m \pmod{M}.$$

Demonstração. Observe primeiramente que:

$$ed \equiv 1 \pmod{\phi(M)} \iff \phi(M) \mid ed-1 \iff (\exists k \in \mathbb{Z})[\, k\phi(M) = ed-1\,].$$

Seja $k \in \mathbb{Z}$ então um tal k, e agora resolvendo por ed:

$$(*) \qquad ed = k\phi(M) + 1.$$

Calculamos:

$$\begin{aligned}(x^e)^d &= x^{ed}\\ &= x^{k\phi(M)+1} && \text{(por (*))}\\ &= x^{k\phi(M)}x\\ &= \left(x^k\right)^{\phi(M)}x\\ &\equiv x \pmod M, && \text{(pelo teorema de Euler Θ3.217)}\end{aligned}$$

onde no último passo precisamos a hipótese que x e M são coprimos e logo, x^k e M também são. ∎

▸ **EXERCÍCIO x3.187.**
O que acontece se x e M não são coprimos? (x3.187 H 0)

§81. Assinaturas digitais

TODO Terminar

3.220. Perae!. Recebi mesmo uma mensagem que Alice mandou pra mim. Foi mesmo encryptada com minha chave pública, eu sou o único que consigo descryptar facilmente essa mensagem para ler seu conteúdo original. Mas temos um problema sério aqui. Mesmo eu sendo a única pessoa que consegue descryptar (facilmente) as mensagem que foram encryptadas com minha chave pública *qualquer pessoa* tem como encryptar qualquer mensagem. Como que eu posso saber que a mensagem que termina com «Abraço, Alice» foi escrita mesmo por Alice?

§82. Funções hash

TODO Elaborar e terminar

Problemas

Leitura complementar

Veja o [BM77b: §§1.6–1.9].
[Euc02], [Gau66].
[And94].
[NZ80], [HW79].
Se os vários sistemas de numerais te deixaram com vontade de conhecer e analisar mais, veja no [Knu97: §4.1].

CAPÍTULO 4

RECURSÃO; INDUÇÃO

TODO limpar, terminar, organizar

Vou começar definindo formalmente os naturais. Na verdade, não vou definir os próprios números naturais. Não: os *números* estão lá nas núvens do nosso coração. Não vamos nos preocupar com a questão «o que *é* o número cinco?». Vamos começar definindo uns possíveis *numerais* para tais números, que vou chamá-los de *Nats*, e a gente vai estudá-los e ver o que podemos definir, calcular, e demonstrar sobre eles.

§83. Os Nats

D4.1. Definição (Nat). Definimos o tipo de dados Nat com uma definição inductiva:

- O é um Nat;
- Se n é um Nat, então S n é um Nat;

Nada mais é um Nat.

4.2. Listando as formas. Escrevemos

$$\textbf{data}\ \mathsf{Nat}\ =\ \mathsf{O} \mid \mathsf{S}\ \mathsf{Nat}$$

e introduzimos assim o tipo Nat listando todas as formas possíveis que seus membros podem ter: cada Nat ou é o O, ou é o S de algum Nat. Pronunciamos o símbolo '|' como "ou", entendendo que separa as alternativas formas listadas.

4.3. Listando os construtores. Escrevemos

$$\begin{aligned}&\textbf{data}\ \mathsf{Nat}\\ &\quad \mathsf{O}\ :\ \mathsf{Nat}\\ &\quad \mathsf{S}\ :\ \mathsf{Nat} \to \mathsf{Nat}\end{aligned}$$

para introduzir o tipo Nat listando todos os seus *construtores* e seus tipos. Assim sabemos que o O já é um Nat (ele é um construtor de aridade 0: não precisa de argumentos). Por outro lado, o S *não* é um Nat, mas sim um Nat → Nat, ou seja precisa ser aplicado num Nat, para virar um Nat.

4.4. Com regras de inferência (1/2). Uma maneira diferente de descrever *a mesma idéia* é com *regras de inferência*. Essa abordagem combina bem com as árvores sintácticas: escrevemos

$$\frac{}{\mathsf{O} : \mathsf{Nat}}$$

e entendemos isso como

«(do nada) posso concluir que 0 é um Nat».

Esse «do nada» aqui quer dizer «sem premissa nenhuma». Vamos dar o nome Zero para essa *regra de inferência*, pois vamos precisar referir a ela depois. Escrevemos seu nome no lado direito da linha de inferência. Fica assim:

$$\frac{}{\mathsf{O} : \mathsf{Nat}}\ \textsc{Zero}$$

Olhando pra isso entendemos o seguinte: a regra Zero nos permite inferir que 0 é um Nat.

? **Q4.5. Questão.** Como tu representaria a segunda regra da Definição D4.1 como uma regra de inferência?

!! SPOILER ALERT !!

4.6. Com regras de inferência (2/2).

$$\frac{}{\mathsf{O} : \mathsf{Nat}}\ \textsc{Zero} \qquad\qquad \frac{n : \mathsf{Nat}}{\mathsf{S}\ n : \mathsf{Nat}}\ \textsc{Succ}$$

▸ **EXERCÍCIO x4.1.**
Identifique variáveis vs. metavariáveis e símbolos da linguagem-objeto vs. da metalinguagem nas definições acima. (x4.1 H 0)

• **EXEMPLO 4.7 (usando árvores).**
Vamos inferir que S (S (S O))) é um Nat mesmo.
Resolução. Vamos construir sua árvore *bottom-up*. O desafio é inferir

$$\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O}))) : \mathsf{Nat}$$

e usando a regra Succ podemos *reduzir* esse problema para

$$\frac{\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O})) : \mathsf{Nat}}{\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O}))) : \mathsf{Nat}}\ \textsc{Succ}$$

Essa árvore tem afirmações "abertas" então não terminamos ainda. Usando a mesma regra reduzimos o S (S (S O)) : Nat para:

$$\frac{\dfrac{\mathsf{S}\ (\mathsf{S}\ \mathsf{O}) : \mathsf{Nat}}{\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O})) : \mathsf{Nat}}\ \textsc{Succ}}{\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O}))) : \mathsf{Nat}}\ \textsc{Succ}$$

e continuando nessa maneira, chegamos finalmente no $0 : \mathsf{Nat}$; agora usamos a regra Zero, fechando assim a única coisa que tava aberta:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\mathsf{O} : \mathsf{Nat}}\textsc{Zero}}{\mathsf{S\ O}) : \mathsf{Nat}}\textsc{Succ}}{\mathsf{S\ (S\ O}) : \mathsf{Nat}}\textsc{Succ}}{\mathsf{S\ (S\ (S\ O})) : \mathsf{Nat}}\textsc{Succ}}{\mathsf{S\ (S\ (S\ (S\ O}))) : \mathsf{Nat}}\textsc{Succ}$$

▸ **EXERCÍCIO x4.2.**
Leia essa árvore tanto de baixo pra cima, quanto de cima pra baixo! (x4.2H0)

• **EXEMPLO 4.8 (usando palavras).**
Podemos inferir que $\mathsf{S\ (S\ (S\ (S\ O}))) : \mathsf{Nat}$ usando palavras tambem, ficando assim mais perto da Definição D4.1, mas para esse tipo de derivação fica bizarro:

> «Como O é um Nat (pela primeira cláusula), logo $\mathsf{S\ O}$ é um Nat (pela segunda com $n := \mathsf{O}$). Logo $\mathsf{S\ (S\ O})$ é um Nat, de novo pela segunda cláusula, essa vez com $n := \mathsf{S\ O}\ldots$»

E já cansei de escrever então vou parar aqui. Espero que apreciamos a laconicidade e clareza das árvores para esse tipo de inferência.

D4.9. Notação (Açúcar sintáctico). Escrever

$$\mathsf{O},\qquad \mathsf{S\ O},\qquad \mathsf{S\ (S\ O}),\qquad \mathsf{S\ (S\ (S\ O}})),\qquad \ldots$$

às vezes pode ser cansativo na mão ou nos olhos. Vamo introduzir pouco açúcar sintáctico então. Usarei as palavras

$$0,\qquad S0,\qquad SS0,\qquad SSS0,\qquad \ldots$$

como apelidos desses Nats. Ainda mais, vou usar os numerais mais populares

$$0,\qquad 1,\qquad 2,\qquad 3,\qquad \ldots$$

para denotar os mesmos objetos. Mas é importante entender que são apenas isso, um nome alternativo para os nomes "oficiais"; então quando eu peço para calcular, por exemplo, «quanto é $3 \cdot 2$», ou «quanto é $SSS0 \cdot SS0$», o que tu precisas calcular mesmo é o

$$\mathsf{S\ (S\ (S\ O}})) \cdot \mathsf{S\ (S\ O})$$

e espero que tu chegarás no resultado que eu chamaria de 6 ou de $SSSSSS0$, ou seja, no $\mathsf{S\ (S\ (S\ (S\ (S\ O}})))})$. Finalmente, estendemos este açúcar para aplicá-lo até quando temos variáveis envolvidas: tendo $n : \mathsf{Nat}$, escrevemos, por exemplo,

$$SS2 + SSSn$$

como abreviação da

$$\mathsf{S\ (S\ (S\ (S\ O}}))) + \mathsf{S\ (S\ (S}\ n)).$$

4.10. Uns apelidos com gramática BNF. Olhe na sintaxe BNF para descrever a gramática que gera as palavras-apelidos $0, S0, SS0, SSS0, \ldots$:

$$\langle Nat \rangle \ ::= \ 0 \mid S\,\langle Nat \rangle$$

Note a semelhança com o Nota 4.2. Ainda mais, para gerar a palavra $SSSS0$ a partir dessa gramática procedemos assim:

$$\begin{aligned} \langle Nat \rangle &\rightsquigarrow S\,\langle Nat \rangle \\ &\rightsquigarrow SS\,\langle Nat \rangle \\ &\rightsquigarrow SSS\,\langle Nat \rangle \\ &\rightsquigarrow SSSS\,\langle Nat \rangle \\ &\rightsquigarrow SSSS0. \end{aligned}$$

Isso corresponde à inferência `S (S (S (S O))) : Nat` do Exemplo 4.7.

- **EXEMPLO 4.11.**
Aqui os numerais de `Nat` que correspondem nos primeiros 5 números naturais:

$$0, \quad S0, \quad SS0, \quad SSS0, \quad SSSS0.$$

Escrevemos a seqüência de "primos naturais" então assim:

$$SS0, \quad SSS0, \quad SSSSS0, \quad SSSSSSS0, \quad SSSSSSSSSS0, \quad \ldots$$

Ou seja, cada número natural n corresponde numa seqüência de n cópias de S, seguidas por um 0.

4.12. Observação. Esse sistema de numerais é praticamente um sistema unário. A grande *desvantagem* dele é que o tamanho dos numerais cresce analogamente com o tamanho de números. Comparando com os sistemas mais comuns com bases $b > 1$ como o binário ou o decimal, já parece deficiente nesse sentido. Mas uma *vantagem* para a gente nesse caso é sua simplicidade na sua definição recursiva: *cada Nat ou é o zero, ou o sucessor de um Nat*. Tudo sobre os Nats é desenvolvido usando apenas essa definição simplíssima.

D4.13. Definição (Os Nats canônicos). Chamamos os termos

$$\mathsf{O}, \quad \mathsf{S\ O}, \quad \mathsf{S\ (S\ O)}, \quad \mathsf{S\ (S\ (S\ O))}, \quad \mathsf{S\ (S\ (S\ (S\ O)))}, \quad \ldots$$

de *valores canônicos* ou *literais* do tipo `Nat`.

4.14. Operador vs. construtor. Logo vamos definir operações nos Nats ($(+)$, $(\cdot)$, etc.) e vamos ter, por exemplo, que

$$S(SS0 + (SSS0 \cdot SS0)) : \mathsf{Nat}$$

também, mas obviamente faz sentido perguntar

«Quanto é $S(SS0 + (SSS0 \cdot SS0))$?»

e a resposta deve ser $SSSSSSSSS0$. Mas não faz sentido perguntar

> «Quanto é $SS0$?»

Ou seja: esse S (que vem da palavra "sucessor") não representa um operador que deve ser aplicado num argumento e que vai retornar um resultado com valor. Não! Esse S é o que chamamos de *construtor* de valores, ou seja, o $SS0$ já é um valor próprio, um valor final, um valor canônico: sem nada mais para ser calculado. Por o mesmo motivo não faz sentido perguntar

> «Quanto é 2?»

2 é 2 ué.

4.15. Naturalmente consideramos todos os valores canônicos como distintos, ou seja, para quaisquer $x, y : \mathsf{Nat}$ temos:

$$\begin{aligned} \mathsf{O} &\neq \mathsf{S}\ x && \text{disjointness} \\ \mathsf{S}\ x = \mathsf{S}\ y &\implies x = y. && \text{injectiviy} \end{aligned}$$

A segunda nos permite "cortar os S's" numa igualdade entre sucessores. Ela é freqüentemente usada na forma da sua contrapositiva:

$$x \neq y \implies \mathsf{S}\ x \neq \mathsf{S}\ y.$$

Destacamos esses dois como princípios sobre o Nat, que determinam o que significa $(=_{\mathsf{Nat}})$.

§84. Pouco de setup

Já encontramos no Igualdade entre Nats 4.15 dois princípios sobre seus construtores. Na verdade, o Nat não tem nada especial nesse quesito. Estipulamos os princípios seguintes sobre qualquer tipos de dados definido indutivamente:

4.16. Princípio (Disjointness of constructors). *Construtores distintos constroem valores distintos.*

4.17. Princípio (Injectivity of constructors). *O mesmo construtor aplicado em valores distintos constrói valores distintos.*

Veja que os dois princípios listados no 4.15 são, de fato, apenas as traduções destes princípios para o tipo Nat.

§85. Definindo funções recursivamente

D4.18. Definição. Definimos a double que retorna o dobro da sua entrada:

$$\begin{aligned}\text{double} &: \mathsf{Nat} \to \mathsf{Nat}\\ \text{double}\ \mathsf{O} &= \mathsf{O}\\ \text{double}\ (\mathsf{S}\ n) &= \mathsf{S}\ (\mathsf{S}\ (\text{double}\ n)).\end{aligned}$$

D4.19. Definição (Adição). Definimos a operação $(+)$ no Nat:

$$\begin{aligned}(+) &: \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat}\\ n + \mathsf{O} &= n\\ n + (\mathsf{S}\ m) &= \mathsf{S}\ (n + m).\end{aligned}$$

4.20. Tags implicitos. Em vez de ficar dando rótulos para cada "equação" de definições como a Definição D4.19, adotamos a convenção que usamos a notação $f.i$ para referir à i-ésima "equação" da definição da f. Assim, escrevemos '(+).1' e '(+).2' para referir às duas equações da D4.19, respeitando a ordem que elas foram escritas.

Antes de tudo, precisamos aprender bem *como calcular*. O modelo computacional que seguimos é bem simples: foque numa subexpressão e a substitua por seu igual. No exemplo seguinte calculamos e confirmamos que... $3 + 2 = 5$.

- **EXEMPLO 4.21.**
  Calcule a soma $SSS0 + SS0$.
  RESOLUÇÃO. Temos a expressão
  $$SSS0 + SS0.$$
  Qual equação aplica? Com certeza não podemos aplicar a primeira (na direção "⇒"), pois nossa expressão não tem a forma $n + 0$. Por que não? O primeiro termo na nossa expressão, o $SSS0$, não é um problema pois ele pode "casar" com o n do lado esquerdo da (+).1. Mas nosso segundo termo, o $SS0$, não pode casar com o 0, então a (+).1 não é aplicável. A segunda equação é sim, pois nossos termos podem casar assim com as variáveis da (+).2:
  $$\underbrace{SSS0}_{n} + S\,\underbrace{S0}_{m}$$
  Tomando $n := SSS0$ e $m := S0$ substituimos nossa expressão por seu igual seguindo a (+).2:
  $$\underbrace{SSS0}_{n} + S\,\underbrace{S0}_{m} = S\big(\underbrace{SSS0}_{n} + \underbrace{S0}_{m}\big) \qquad \text{(por (+).2)}$$
  Depois um passo de cálculo então chegamos na expressão $S(SSS0 + S0)$. Como nenhuma equação tem a forma $S(__) = ____$, olhamos "dentro" da nossa expressão para achar nas suas subexpressões possíveis "casamentos" com nossas equações. Focamos então na subexpressão sublinhada $S(\underline{SSS0 + S0})$: vamos tentar substituí-la por algo igual. Novamente a primeira equação não é aplicavel por causa do novo segundo termo ($S0$), mas a (+).2 é:
  $$S\big(\underbrace{SSS0}_{n} + S\,\underbrace{0}_{m}\big)$$

Tomando agora $n := SSS0$ e $m := 0$ substituimos de novo seguindo a (+).2:

$$S\overbrace{\big(\underbrace{SSS0}_{n} + S\underbrace{0}_{m}\big)}^{\text{isso}} = S\overbrace{S\big(\underbrace{SSS0}_{n} + \underbrace{0}_{m}\big)}^{\text{por isso}} \qquad \text{(por (+).2)}$$

Agora focamos na subexpressão $SS(\underline{SSS0 + 0})$ e podemos finalmente aplicar a primeira equação:

$$SS\big(\underbrace{SSS0}_{n} + 0\big)$$

então tomando $n := SSS0$ substituimos

$$SS\overbrace{\big(\underbrace{SSS0}_{n} + 0\big)}^{\text{isso}} = SS\overbrace{\underbrace{SSS0}_{n}}^{\text{por isso}} \qquad \text{(por (+).1)}$$

Finalmente chegamos no resultado: no termo $SSSSS0$. Nunca mais vamos escrever tudo isso com tanto detalhe! Esse cálculo que acabamos de fazer, escrevemos curtamente nessa forma:

$$\begin{aligned} SSS0 + SS0 &= S(SSS0 + S0) && \text{(por (+).2)} \\ &= SS(SSS0 + 0) && \text{(por (+).2)} \\ &= SSSSS0 && \text{(por (+).1)} \end{aligned}$$

escrevendo apenas em cada linha o que foi usado.

4.22. Quando termino?. Termino quando chegar num *valor canônico*. Quando eu peço para calcular quanto é $SSS0 + SS0$ por exemplo, a idéia é achar seu valor canônico, exatamente como acontece quando pedimos para uma pessoa achar

> «Quanto é $2 + 3$?»

Uma resposta

> «$2 + 3 = 2 + 3$»

não seria aceitável—mesmo assim, é correta, não é?—pois a pessoa que perguntamos não achou o valor canónico (nesse caso 5).

4.23. Dá pra terminar sempre?. Sempre tem como chegar num valor canônico? Por enquanto não sabemos! Realmente a (+) na maneira que foi definida é uma operação *total*, ou seja, sempre termina num valor canônico, mas não é algo que deve se preocupar neste momento. Estudamos muito esse assunto no Secção §368.

▸ **EXERCÍCIO x4.3.**
Calcule a soma $0 + SSSS0$. (x4.3H0)

4.24. Estratégias de evaluação. Vamos dizer que queremos calcular começando com uma expressão mais complexa, como por exemplo a

$$0 + \big(0 + S\big((SS0 + 0) + 0\big)\big).$$

Como procedimos? A expressão inteira não pode ser substituida pois nenhuma das (+).1–(+).2 tem essa forma, mas aparecem várias subexpressões em quais podemos *focar* para nosso próximo passo de cálculo:

$$\begin{aligned}
&0 + \underline{\big(0 + S\big((SS0 + 0) + 0\big)\big)}, && \text{casando com (+).2}\\
&0 + \big(0 + S\underline{\big((SS0 + 0) + 0\big)}\big), && \text{casando com (+).1}\\
&0 + \big(0 + S\big(\underline{(SS0 + 0)} + 0\big)\big), && \text{casando com (+).1.}
\end{aligned}$$

Podemos seguir uma *estratégia de evaluação* específica, por exemplo, focando sempre na expressão que aparece primeira à esquerda; ou podemos escolher cada vez onde focar aleatoriamente; etc. No Exercício x4.4 tu vai ter que escolher onde focar várias vezes.

▸ **EXERCÍCIO x4.4.**
Calcule os valores das expressões $SSS0 + (SS0 + S0)$ e $(SSS0 + SS0) + S0$. (x4.4H0)

4.25. Cadê a recursão e por quê não temos problema tipo tijolo?. Estamos definindo a própria operação (+), e na segunda linha da sua definição aparece o (+) tanto no lado esquerdo, quanto no lado direito. Por isso chamamos a definição recursiva. Se definimos (+) em termos dele mesmo, por que não temos o problema tipo *tijolo* que discutimos no Nota 1.20? (Chegou a hora que tinha prometido no 1.22.) Olhando com mais atenção, percebemos que não definimos o que significa *somar* em termos do que significa *somar* mesmo; mas definimos sim o que significa *somar os números n e Sm* em termos do que significa *somar os números n e m*. No lado direito, uma coisa nos argumentos da nossa operação está diminuindo (os S's do segundo argumento) assim evitando o loop infinito, chegando finalmente na primeira equação *depois duma quantidade finita* de perguntas «e o que é...?».

▸ **EXERCÍCIO x4.5.**
Defina (recursivamente), e sem usar a (+), uma função *double* : Nat → Nat que dobra sua entrada. Verifique que o dobro de três ($SSS0$) é seis ($SSSSSS0$). (x4.5H12)

4.26. Um programador pior. Alguém definiu a adição usando essas quatro equações:

$$\begin{aligned}
&(+) : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat}\\
&0 \;+ 0 \;\;= 0\\
&Sn + 0 \;\;= Sn\\
&0 \;+ Sm = Sm\\
&Sn + Sm = S(Sn + m).
\end{aligned}$$

Ou seja, para cada argumento da operação, ele tratou os dois casos principais separadamente, resultando assim em quatro equações. Mas, olhando nas primeiras duas, dá pra ver que ambas são casos especiais da nossa primeira equação. No final das contas, nas duas o que acontece é que o primeiro argumento acaba sendo o resultado da soma, e é exatamente isso que nossa primeira equação disse. Nossa definição é bem melhor então, mais elegante e econômica.

▸ **EXERCÍCIO x4.6.**
Defina a multiplicação no $\mathbb{N}$. (x4.6H12345)

▸ **EXERCÍCIO x4.7.**
Calcule o $2(0+1)$. (x4.7H0)

▸ **EXERCÍCIO x4.8.**
Calcule os $2 \cdot 3$ e $3 \cdot 2$. (x4.8H0)

▸ **EXERCÍCIO x4.9.**
Defina a exponenciação no $\mathbb{N}$. (x4.9H0)

▸ **EXERCÍCIO x4.10.**
Calcule o 2^3. (x4.10H0)

▸ **EXERCÍCIO x4.11.**
Defina usando equações recursivas a *seqüência Fibonacci*, como uma função de Nat para Nat. (x4.11H0)

▸ **EXERCÍCIO x4.12.**
Considere as funções seguintes definidas recursivamente:

$$\begin{array}{ll|ll}
q : \mathsf{Nat} \to \mathsf{Nat} & & r : \mathsf{Nat} \to \mathsf{Nat} & \\
q\ \mathsf{O} & = \mathsf{O} & r\ \mathsf{O} & = \mathsf{O} \\
q\ (\mathsf{S}\ \mathsf{O}) & = \mathsf{O} & r\ (\mathsf{S}\ \mathsf{O}) & = \mathsf{S}\ \mathsf{O} \\
q\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O})) & = \mathsf{O} & r\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O})) & = \mathsf{S}\ (\mathsf{S}\ \mathsf{O}) \\
q\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ n))) & = \mathsf{S}\ (q\ n) & r\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ n)))) & = r\ n
\end{array}$$

(i) Re-escreva essas definições numa maneira mais abreviada.
(ii) O que cada função calcula?

(x4.12H1)

§86. Demonstrando propriedades de naturais sem indução

4.27. Convenção. Nessa secção todos os quantificadores que aparecem "nus" *quantificam sobre os naturais*. Por exemplo

$$(\forall x)(\forall y)(\exists z)(\forall w)[\,\varphi(x,y,z,w)\,]$$

significa

$$(\forall x : \mathsf{Nat})(\forall y : \mathsf{Nat})(\exists z : \mathsf{Nat})(\forall w : \mathsf{Nat})[\,\varphi(x,y,z,w)\,].$$

Vamos primeiramente *definir* recursivamente as tres operações de adição, multiplicação, e exponenciação:

D4.28. Definição. Definimos as operações de adição, multiplicação, e exponenciação recursivamente assim:

$$\begin{array}{lll} (+) : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat} & (\cdot) : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat} & (\hat{}) : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat} \\ n + 0 \quad = n & n \cdot 0 \quad = 0 & n \hat{} 0 \quad = S0 \\ n + Sm = S(n + m) & n \cdot Sm = (n \cdot m) + n & n \hat{} Sm = (n \hat{} m) \cdot n. \end{array}$$

Observe que cada uma dessas equações tem um implícito $(\forall n)$ ou $(\forall n)(\forall m)$ na frente dela.

4.29. Convenções. Seguindo a convenção comum, escrevemos o $x \hat{} y$ como x^y, mas mesmo assim consideramos isso como um açúcar sintáctico para a expressão $x \hat{} y$. Entendemos então que no x^y temos uma aplicação duma operação binária (aplicada nos argumentos x e y). Vamos seguir também a convenção que a exponenciação "pega mais forte" que as outras duas operações, e que multiplicação pega mais forte que a adição: $a \cdot b^c$ escrito sem parênteses significa $a \cdot (b \hat{} c)$ e não $(a \cdot b) \hat{} c$; e $a + b \cdot c$ significa $a + (b \cdot c)$. Graças às associatividades das $(+)$ e $(\cdot)$ (Teorema Θ4.39 e Exercício x4.16) podemos escrever $a + b + c$ e $a \cdot b \cdot c$, mas para a exponenciação que não é associativa escolhemos a associatividade-direita: a^{b^c} significa $a \hat{} (b \hat{} c)$ e não $(a \hat{} b) \hat{} c$.

4.30. Proposição. *A $(+)$ é associativa.*

(Θ4.39) ◁ **4.31. Tentativa de demonstração.** Vamos tentar demonstrar essa proposição. Primeiramente, o que a afirmação significa? A adição é essa operação $(+)$ que definimos na Definição D4.28. Vamos tentar escrever essa afirmação numa maneira mais formal para expor sua estrutura lógica:

$$(\forall n)(\forall m)(\forall k)[\,(n + m) + k = n + (m + k)\,].$$

Nosso alvo tem a forma

$$(\forall x : \mathsf{Nat})[\,\varphi(x)\,]$$

olhando como

$$(\forall n)\big[\underbrace{(\forall m)(\forall k)[\,(n + m) + k = n + (m + k)\,]}_{\varphi_1(n)}\big]$$

podemos atacá-la tomando um arbitrario Nat e mostrando que ele goza da propriedade φ:

Seja $a : \mathsf{Nat}$. Agora precisamos mostrar que $\varphi(a)$, ou seja nosso alvo é

$$(\forall m)(\forall k)[\,(a + m) + k = a + (m + k)\,].$$

Observe que nosso alvo é apenas uma afirmação sobre o natural a. Beleza. Mas nosso alvo tem a mesma forma,

$$\underbrace{(\forall m)\big[\underbrace{(\forall k)[\,(a + m) + k = a + (m + k)\,]}_{\varphi_2(m)}\big]}_{\varphi_1(a)}$$

então podemos atacar novamente com a mesma idéia, "sejando" mais um natural.

Seja m : Nat. Preciso demonstrar que

$$\underbrace{(\forall k)\big[\underbrace{(a+m)+k = a+(m+k)}_{\varphi_3(k)}\big]}_{\varphi_2(m)}.$$

Atacamos uma última vez com a mesma estratégia:

Seja y : Nat. Agora precisamos demonstrar

$$\underbrace{(a+m)+y = a+(m+y)}_{\varphi_3(y)}.$$

E agora? Como chegamos numa igualdade, precisamos verificar que seus dois lados realmente denotam o mesmo valor. Vamos calcular então. Tomando o lado esquerdo, $(a+m)+y$, tantamos casá-lo com as equações $(+).1$–$(+).2$, mas ele não casa com nenhuma delas, então não tem como simplificá-lo.[41]

? **Q4.32. Questão.** Parece que chegamos num "dead end". Tem como continuar?

!! SPOILER ALERT !!

Resposta. Tem! O problema foi que não sabemos nem sobre o m nem sobre o y se são da forma O ou da forma S _ e por isso não conseguimos aplicar nenhuma das $(+).1$–$(+).2$. Mas podemos *separar em casos*. Vamos escolher um desses Nats então, o y, e considerar:

- Caso $y = 0$: ...
- Caso $y = Sy'$ para algum y': ...

Lembre-se que cada vez que separamos em casos, nosso alvo tá sendo *copiado e colado* para cada um deles.

▸ **EXERCÍCIO x4.13 (O primeiro caso).**
Demonstre que

$$(a+m)+y = a+(m+y)$$

no primeiro caso. (x4.13H123)

[41] Isso não é exatamente verdade, pois o lado direito da $(+).1$, sendo apenas uma variável, casa com qualquer coisa. Mas escolhendo qualquer (sub)expressão da $(a+m)+y$, para casar com n, não vamos ter progresso nenhum, pois vamos acabar adicionando apenas uns "+0" até cansar, sem nenhuma mudança na posição das parenteses que nos importam aqui.

4.33. O segundo caso. Sabemos que y é o sucessor de algum natural, então vamos escolher um nome pra denotá-lo: *seja y' natural tal que $y = Sy'$* $^{(1)}$. Calculamos:

$$\begin{aligned}(a+m)+y &= (a+m)+Sy' && \text{(hipótese (1))}\\ &= S((a+m)+y') && \text{((+).2, com } n := (a+m),\ m := y')\end{aligned}$$

e o outro lado

$$\begin{aligned}a+(m+y) &= a+(m+Sy') && \text{(hipótese (1))}\\ &= a+S(m+y') && \text{((+).2 com } n := m,\ m := y')\\ &= S(a+(m+y')) && \text{((+).2 com } n := a,\ m := m+y')\end{aligned}$$

E agora peguntamos

$$S((a+m)+y') \stackrel{?}{=} S(a+(m+y'))$$

e para resolver isso basta "cortar os S's" e demonstrar que

$$(a+m)+y' = a+(m+y').$$

E estamos onde estávamos! Só com a, m, y' em vez de a, m, y. E daí? Podemos separar esse caso em dois subcasos:

- Caso $y' = 0$: ...
- Caso $y' = Sy''$ para algum y'': ...

O primeiro subcaso vamos conseguir matar, pois é igual ao primeiro caso. Mas a melhor coisa que conseguimos no segundo caso seria chegar ate o alvo

$$(a+m)+y'' \stackrel{?}{=} a+(m+y'').$$

E depois? Considerar dois casos novamente? Não importa quantas vezes repetir essa idéia, a gente sempre vai conseguir matar apenas um dos sub-(sub-sub-...)-casos, e chegar num

$$(a+m)+y''^{\cdots\prime} \stackrel{?}{=} a+(m+y''^{\cdots\prime}).$$

Obviamente precisamos uma outra técnica para demonstrar esse teorema.

§87. Indução

4.34. Princípio (Indução). *Seja* $\varphi : \mathsf{Nat} \to \mathsf{Prop}$. *Para demonstrar* $(\forall n : \mathsf{Nat})[\,\varphi(n)\,]$, *basta demonstrar* $\varphi(0)$ *e* $(\forall k : \mathsf{Nat})[\,\varphi(k) \implies \varphi(Sk)\,]$.

4.35. Indução: regra de inferência. Em forma de regra de inferência, o princípio da indução é o seguinte:

$$\frac{\varphi(0) \qquad (\forall k : \mathsf{Nat})[\,\varphi(k) \implies \varphi(Sk)\,]}{(\forall n : \mathsf{Nat})[\,\varphi(n)\,]}\ \textsc{Ind}_\varphi$$

onde chamamos a proposição $\varphi(0)$ de *base* e a $(\forall k)[\,\varphi(k) \implies \varphi(Sk)\,]$ de *passo indutivo*:

$$\frac{\overbrace{\varphi(0)}^{\text{(Base)}} \qquad \overbrace{(\forall k : \mathsf{Nat})[\,\varphi(k) \implies \varphi(Sk)\,]}^{\text{(Passo indutivo)}}}{(\forall n : \mathsf{Nat})[\,\varphi(n)\,]}\ \textsc{Ind}_\varphi$$

Mas esses são apenas os apelidos que usamos freqüentemente; nada mais que isso. Como vamos ver logo, a proposição $\varphi(k)$ no esquema acima também tem um apelido: *hipótese indutiva (H.I.)*.

4.36. Novo ataque. Sabemos que regras de inferência correspondem em "comandos" do nosso low-level sistema de demonstrações. Precisamos então um comando para essa, e isso será um pleno "Por indução." Para utilizá-lo, nosso algo *precisa* ter essa forma:

Demonstração	**Dados**	**Alvos**
		$(\forall n : \mathsf{Nat})[\,\varphi(n)\,]$

Demonstração	**Dados**	**Alvos**
Por indução.		~~$(\forall n : \mathsf{Nat})[\,\varphi(n)\,]$~~ $\varphi(0)$ $(\forall k : \mathsf{Nat})[\,\varphi(k) \implies \varphi(Sk)\,]$

Demonstração	**Dados**	**Alvos**
Por indução. Base.		$\varphi(0)$ $(\forall k : \mathsf{Nat})[\,\varphi(k) \implies \varphi(Sk)\,]$

Demonstração	**Dados**	**Alvos**
Por indução. Base. ⋮ (demonstração de $\varphi(0)$)	$\varphi(0)$	~~$\varphi(0)$~~ $(\forall k : \mathsf{Nat})[\,\varphi(k) \implies \varphi(Sk)\,]$

Demonstração	**Dados**	**Alvos**
Por indução. Base. ⋮ (demonstração de $\varphi(0)$) Passo indutivo.	$\varphi(0)$	$(\forall k : \mathsf{Nat})[\,\varphi(k) \implies \varphi(Sk)\,]$

Demonstração	**Dados**	**Alvos**
Por indução. BASE. ⋮ (demonstração de $\varphi(0)$) PASSO INDUTIVO. Seja $k : \mathsf{Nat}$.	$\varphi(0)$ $k : \mathsf{Nat}$	~~$(\forall k : \mathsf{Nat})[\varphi(k) \implies \varphi(Sk)]$~~ $\varphi(k) \implies \varphi(Sk)$

Demonstração	**Dados**	**Alvos**
Por indução. BASE. ⋮ (demonstração de $\varphi(0)$) PASSO INDUTIVO. Seja $k : \mathsf{Nat}$ tal que $\varphi(k)$ (HI).	$\varphi(0)$ $k : \mathsf{Nat}$ $\varphi(k)$	~~$\varphi(k) \implies \varphi(Sk)$~~ $\varphi(Sk)$

Demonstração	**Dados**	**Alvos**
Por indução. BASE. ⋮ (demonstração de $\varphi(0)$). PASSO INDUTIVO. Seja $k : \mathsf{Nat}$ tal que $\varphi(k)$ (HI). ⋮ (demonstração de $\varphi(Sk)$) ∎	$\varphi(0)$ $k : \mathsf{Nat}$ $\varphi(k)$ $\varphi(Sk)$	~~$\varphi(Sk)$~~

4.37. Observação. Observe que no momento que escrevemos

«Seja $k : \mathsf{Nat}$ tal que $\varphi(k)$ (HI).»

no 4.36 não fizemos nada especial relacionado à indução! Isso é o "ataque padrão" duma proposição da forma

$$(\forall x : A)[\,\varphi(x) \implies \psi(x)\,]$$

onde juntamos os passos de atacar o '$\forall$' e o '$\implies$' numa frase só. Em geral, podes considerar a indução como um comando que quando usado transforma um alvo da forma

$$(\forall x : \mathsf{Nat})[\,\varphi(x)\,]$$

para *dois* novos alvos (com nomes chique):

$$\begin{aligned} \text{BASE:} \quad & \varphi(0) \\ \text{PASSO INDUTIVO:} \quad & (\forall k : \mathsf{Nat})[\,\varphi(k) \implies \varphi(Sk)\,] \end{aligned}$$

(exatamente como a regra do 4.35 disse, lida de baixo para cima). Fora disso, *não tem nada mais mágico* que acontece: o comando já foi executado e seu efeito já aconteceu. E depois? Depois *continuamos normalmente para matar esses dois alvos.*

4.38. Observação (Indução numa variável?). No Nota 4.36 escrevemos «Indução no n». Como assim «no n»? Quem é esse n? Não tem n no nosso escopo! Sim, realmente não faz sentido no pé da letra essa frase, mas ajudamos nosso leitor entender qual quantificador estamos atacando do nosso alvo, caso que aparecem mais que um. Talvez ficaria (pouco) mais correto escrever «Indução no $\forall n$.» (No final das contas, é o quantificador que estamos atacando.) De qualquer forma, isso é apenas um modo de falar, e presuponha que nosso leitor tem acesso no nome da variável ligada que escolhemos quando escrevemos nosso alvo. (Muitas vezes isso faz parte do enunciado.)

§88. Demonstrando propriedades de naturais com indução

Θ4.39. Teorema (Associatividade da adição). *A operação* $(+)$ *da Definição D4.28 é associativa:*

$$(\forall n)(\forall m)(\forall k)[\, n+(m+k) = (n+m)+k \,].$$

Vamos demonstrar esse teorema duas vezes. É importantíssimo entender a diferença e seguir todos os detalhes. Antes de começar, lembre nossa tentativa 4.31 e como e onde exatamente a gente travou:

Demonstração	**Dados**	**Alvos**
Seja n natural. Seja m natural. Seja k natural. Separamos em casos: Caso $k = 0$: (resolvido no Exercício x4.13) Caso $k = Sk'$ para algum k': (caimos num caminho infinito aqui)	$n : \mathsf{Nat}$ $m : \mathsf{Nat}$ $k : \mathsf{Nat}$	$n+(m+k) = (n+m)+k$

E como caimos num caminho de sempre separar em dois novos casos sem fim, percebemos que algo deu errado; queremos tentar nossa nova técnica, indução. Neste momento na nossa prova, podemos atacar nosso alvo por indução? Não! Para atacar um alvo por indução ele precisa ter a forma

$$(\forall x : \mathsf{Nat})[\, \varphi(x) \,]$$

e nosso alvo não é um '$\forall$' mas uma igualdade! Vamos fazer uns "undo" então na nossa demonstração e voltar nesse momento:

	Demonstração	**Dados**	**Alvos**
1	Seja n natural.	$n : \mathsf{Nat}$	$(\forall k)\big[\underbrace{n+(m+k) = (n+m)+k}_{\varphi(k)}\big]$
2	Seja m natural.	$m : \mathsf{Nat}$	
3	~~Seja k natural.~~		
4	~~Separamos em casos:~~		

Agora sim! Nosso alvo tem uma forma que casa com o padrão que precisamos para aplicar indução. Bora ver essa demonstração primeiro então.

Primeira demonstração. Sejam n, m naturais. Vamos demonstrar por indução no k

que

$$(\forall k)\big[\underbrace{n+(m+k)=(n+m)+k}_{\varphi(k)}\big].$$

Base. Precisamos mostrar que

$$n+(m+0)=(n+m)+0.$$

Calculamos:

$$\begin{aligned} n+(m+0)&=n+m && \text{(pela (+).1 com } n:=m)\\ (n+m)+0&=n+m && \text{(pela (+).1 com } n:=n+m)\end{aligned}$$

Passo indutivo. Precisamos mostrar que

$$(\forall t)\big[\underbrace{n+(m+t)=(n+m)+t}_{\varphi(t)} \implies \underbrace{n+(m+St)=(n+m)+St}_{\varphi(St)}\big].$$

Seja w natural tal que

(HI) $$n+(m+w)=(n+m)+w.$$

Precisamos mostrar que

$$n+(m+Sw)=(n+m)+Sw.$$

Calculamos:

$$\begin{aligned} n+(m+Sw)&=n+S(m+w) && ((+).2:\ n:=m;\ m:=w)\\ &=S(n+(m+w)) && ((+).2:\ n:=n;\ m:=m+w)\\ (n+m)+Sw&=S((n+m)+w) && ((+).2:\ n:=n+m;\ m:=w)\end{aligned}$$

Basta então mostrar

$$S(n+(m+w))=S((n+m)+w)$$

que segue pela (HI). (Como?) ∎

▸ **EXERCÍCIO x4.14.**
Como mesmo? (x4.14H1)

4.40. Precisamos discutir o que acabou de acontecer. Agora bora ver uma demonstração que também usa indução, mas numa maneira bem diferente: Queremos demonstrar a afirmação

$$(\forall n)(\forall m)(\forall k)[\,\psi(n,m,k)\,]$$

onde

$$\psi(x,y,z) \overset{\text{abbr}}{\iff} x+(y+z)=(x+y)+z.$$

Talvez parece que ela não está no formato $(\forall n)[\,\varphi(n)\,]$ e que não podemos atacá-la diretamente com indução. Mas, na verdade, reescrevendo como

$$(\forall n)\,\underbrace{(\forall m)(\forall k)[\,\psi(n,m,k)\,]}_{\varphi_1(n)}$$

já percebemos que tem a forma certa. E podemos trocar a ordem de quantificadores consecutivos *do mesmo tipo*, então o que queremos demonstrar é equivalente aos

$$(\forall n)\underbrace{(\forall m)(\forall k)[\,\psi(n,m,k)\,]}_{\varphi_1(n)};\qquad (\forall m)\underbrace{(\forall n)(\forall k)[\,\psi(n,m,k)\,]}_{\varphi_2(m)};\qquad (\forall k)\underbrace{(\forall n)(\forall m)[\,\psi(n,m,k)\,]}_{\varphi_3(k)};$$

etc. (tem ainda mais três opções que não escrevi), onde em cada caso o φ_i tem uma definição diferente, mas o ψ tem sempre a mesma. Escolhemos demonstrar a

$$(\forall k)\underbrace{(\forall n)(\forall m)[\,\psi(n,m,k)\,]}_{\varphi(k)}$$

por indução. Vamos ver o que vai acontecer.

(Θ4.39) ◁ **4.41.** Segunda demonstração. Por indução no k.
Base. Precisamos demonstrar que

$$\underbrace{(\forall n)(\forall m)[\,n+(m+0)=(n+m)+0\,]}_{\varphi(0)}.$$

Sejam n, m naturais. Calculamos os dois lados:

$$\begin{aligned}\underline{(n+m)+0} &= n+m && ((+).1)\\ n+\underline{(m+0)} &= n+m && ((+).1)\end{aligned}$$

Ou seja, a $\varphi(0)$ realmente é válida.
Passo indutivo. Precisamos demonstrar a afirmação:

$$(\forall t)[\,\varphi(t) \implies \varphi(St)\,],$$

ou seja,

$$(\forall t)[\,((\forall n)(\forall m)[\,(n+m)+t=n+(m+t)\,]) \implies ((\forall u)(\forall v)[\,(u+v)+St=u+(v+St)\,])\,]$$

onde escolhi nomes diferentes nas variáveis quantificadas apenas para enfatizar que são realmente diferentes! Bora demonstrar isso então. Seja w natural tal que

(H.I.) $$(\forall n)(\forall m)[\,(n+m)+w=n+(m+w)\,].$$

Preciso mostrar que:

$$(\forall u)(\forall v)[\,(u+v)+Sw=u+(v+Sw)\,].$$

Sejam u, v naturais. Calculamos:

$$\begin{aligned}\underline{(u+v)+Sw} &= S(\underline{(u+v)+w}) && ((+).2)\\ &= \underline{S(u+(v+w))} && (\text{H.I., com } n:=u,\ m:=v)\\ &= u+\underline{S(v+w)} && ((+).2^{\leftarrow})\\ &= u+(v+Sw). && ((+).2^{\leftarrow})\end{aligned}$$

Isso termina nossa demonstração. ∎

? **Q4.42. Questão.** Acabamos de escolher para demonstrar por indução no k. Por que k? Faz diferença ou não? Como escolherias qual dos $\forall$ seria o melhor para atacar por indução?

!! SPOILER ALERT !!

4.43. Como escolher a variável da indução. Como a definição da adição foi recursiva no segundo argumento da função, vai nos ajudar se a indução é feita numa variável que aparece mais como segundo argumento da adição do que como primeiro. Aqui por exemplo, a k aparece duas vezes como argumento da $(+)$, e as duas vezes ela é o segundo argumento da $(+)$. Perfeito. O n no outro lado aparece duas vezes como primeiro argumento, e o m uma como primeiro e uma como segundo.

Θ4.44. Teorema (Comutatividade da adição). *A operação* $(+)$ *da Definição D4.28 é comutativa:*

$$(\forall n)(\forall m)[\, n + m = m + n \,].$$

▸ Demonstração errada. Demonstramos a

$$(\forall n) \underbrace{(\forall m)[\, n + m = m + n \,]}_{\varphi(n)}.$$

Base. Queremos demonstrar o $\varphi(0)$, ou seja, o seguinte:

$$(\forall m) \underbrace{[\, 0 + m = m + 0 \,]}_{\psi(m)}.$$

Vamos demonstrar por indução!
Sub-base. Trivial, pois o que queremos demonstrar é $0 + 0 = 0 + 0$ e os dois lados são a mesma expressão.
Sub-passo indutivo. Precisamos demonstrar que:

$$\forall k \Big[\underbrace{0 + k = k + 0}_{\psi(k)} \implies \underbrace{0 + Sk = Sk + 0}_{\psi(Sk)} \Big].$$

Seja $k \in \mathbb{N}$ tal que

(S.H.I.) $$0 + k = k + 0.$$

Queremos mostrar que

$$0 + Sk = Sk + 0.$$

Calculamos:

$$\begin{aligned} 0 + Sk &= S(0 + k) && ((+).2) \\ &= S(k + 0) && ((\text{S.H.I.})) \\ &= Sk && ((+).1) \\ &= Sk + 0. && ((+).1) \end{aligned}$$

Isso termina nossa base. Passo indutivo. Queremos demonstrar:

$$\forall k\Big[\underbrace{\forall m(k+m=m+k)}_{\varphi(k)} \implies \underbrace{\forall m(Sk+m=m+Sk)}_{\varphi(Sk)}\Big].$$

Seja $k \in \mathbb{N}$ tal que

(H.I.) $$\underbrace{\forall m(k+m=m+k)}_{\varphi(k)}$$

então. Basta demonstrar que

$$\underbrace{\forall m(Sk+m=m+Sk)}_{\varphi(Sk)}.$$

Seja $m \in \mathbb{N}$. Calculamos:

$$\begin{aligned} Sk+m &= S(k+m) && ((+).2)\\ &= S(m+k) && ((\text{H.I.}))\\ &= m+Sk. && ((+).2) \end{aligned}$$

Isso termina nossa demonstração. ↯

▸ **EXERCÍCIO x4.15.**
A demonstração do Teorema Θ4.44 tem um erro! Ache o erro. (x4.15 H 1 2)

Λ4.45. Lema. *A operação* $(+)$ *satisfaz:*

$$(\forall a)(\forall b)[\,Sa+b=a+Sb\,].$$

Demonstração. Demonstramos por indução que

$$(\forall b)\,\underbrace{(\forall a)[\,Sa+b=a+Sb\,]}_{\varphi(b)}.$$

Base. Precisamos demonstrar que

$$\underbrace{(\forall a)[\,Sa+0=a+S0\,]}_{\varphi(0)}.$$

Calculamos:

$$\begin{aligned} Sa+0 &= Sa && ((+).1)\\ a+S0 &= S(a+0) && ((+).2)\\ &= Sa. && ((+).1) \end{aligned}$$

Passo indutivo. Queremos demonstrar:

$$(\forall k)\Big[\underbrace{(\forall a)[\,Sa+k=a+Sk\,]}_{\varphi(k)} \implies \underbrace{(\forall a)[\,Sa+Sk=a+SSk\,]}_{\varphi(Sk)}\Big].$$

Seja $k : \mathsf{Nat}$ tal que

(H.I.) $$\underbrace{(\forall a)[\, Sa + k = a + Sk \,]}_{\varphi(k)}.$$

Basta mostrar que

$$\underbrace{(\forall a)[\, Sa + Sk = a + SSk \,]}_{\varphi(Sk)}.$$

Seja $a : \mathsf{Nat}$. Calculamos

$$\begin{aligned} Sa + Sk &= S(Sa + k) && ((+).2) \\ &= S(a + Sk) && (\text{H.I. com } a := a) \\ &= a + SSk. && ((+).2) \end{aligned}$$

Isso termina nossa demonstração, e logo substituindo a justificativa «(+).2» na demonstração do Teorema Θ4.44 por «pelo Lema Λ4.45» ganhamos também o direito de substituir seu ‘ ↯ ’ por um legítimo ‘ ∎ ’: ∎

TODO Sketch da comutatividade da adição com indução dupla

▸ **EXERCÍCIO x4.16 (Associatividade da multiplicação).**
$(\forall n)(\forall m)(\forall k)[\, (n \cdot m) \cdot k = n \cdot (m \cdot k) \,]$. (x4.16H12)

▸ **EXERCÍCIO x4.17 (Comutatividade da multiplicação).**
$(\forall n)(\forall m)[\, n \cdot m = m \cdot n \,]$. (x4.17H123)

▸ **EXERCÍCIO x4.18 (Distributividade).**
$(\forall x)(\forall y)(\forall z)[\, x \cdot (y + z) = (x \cdot y) + (x \cdot z) \,]$. (x4.18H1)

Θ4.46. Teorema (Identidade da multiplicação). $(\forall x)[\, x \cdot S0 = x = S0 \cdot x \,]$.

Demonstração. Seja $x : \mathsf{Nat}$. Calculamos:

$$\begin{aligned} x \cdot S0 &= (x \cdot 0) + x && ((\cdot).2,\ n := x,\ m := 0) \\ &= 0 + x && ((\cdot).1) \\ &= x + 0 && ((+) \text{ comut. } (\Theta 4.44)) \\ &= x. && ((+).1) \end{aligned}$$

Como já demonstramos a comutatividade da $(\cdot)$ (x4.17) isso termina nossa demonstração. ∎

TODO easy equivalence of two ways to define exponenciation of Exercício x4.9

TODO still, there is reason to choose one over the other

▸ **EXERCÍCIO x4.19 (Lei de exponenciação 1).**
$(\forall x)(\forall a)(\forall b)\big[\, x^{a+b} = (x^a) \cdot (x^b) \,\big]$. (x4.19H123)

▸ **EXERCÍCIO x4.20 (Lei de exponenciação 2).**
$(\forall a)(\forall b)(\forall c)\big[\, a^{b \cdot c} = (a^b)^c \,\big]$. (x4.20H123)

▸ **EXERCÍCIO x4.21 (Lei de exponenciação 3).**
$(\forall n)[\, S0^n = S0 \,]$ (x4.21 H 1 2 3)

▸ **EXERCÍCIO x4.22.**
Demonstre que para todo n, e todo ímpar x, x^n é ímpar.[42] (x4.22 H 0)

4.47. Observação. Parece que o Problema Π3.34 é demonstrar esse teorema numa linha só! Mas não exatamente. Aqui demonstramos uma propriedade que envolve uma operação nos Nat. Por outro lado, no Π3.34 demonstramos algo sobre as potências de certos inteiros. Veja que definimos as potências x^n para qualquer *inteiro* x e qualquer $n \in \mathbb{N}$ recursivamente; mas não temos (nem teremos) uma *operação* entre inteiros de exponenciação.

§89. Por que aceitar o princípio da indução?

4.48. Intuição. Por que demonstrar $\varphi(0)$ e $(\forall k \in \mathbb{N})[\, \varphi(k) \implies \varphi(Sk) \,]$ é suficiente para demonstrar o $(\forall n \in \mathbb{N})[\, \varphi(n) \,]$? Estabelecendo esses dois alvos significa que ganhamos como regras de inferência as seguintes:

$$\frac{}{\varphi(\mathsf{O})}\ \textsc{IndZero}_\varphi \qquad\qquad \frac{\varphi(n)}{\varphi(\mathsf{S}\ n)}\ \textsc{IndSucc}_\varphi$$

onde n é uma metavariável pegando valores em todos os naturais, e onde eu escolhi esses rótulos talvez estranhos para nomear essas regras. Vamos ver o que podemos demonstrar graças essas duas regras agora: com certeza temos o próprio $\varphi(0)$ pela primeira que não tem nenhuma premissa. Mas, agora, usando a segunda com $n := 0$ temos uma demonstração do $\varphi(S0)$:

$$\dfrac{\dfrac{}{\varphi(0)}\ \textsc{IndZero}_\varphi}{\varphi(S0)}\ \textsc{IndStep}_\varphi$$

Ou seja, ganhamos o $\varphi(S0)$. Então podemos usar a regra $\textsc{IndZero}_\varphi$ agora com $n := S0$ para ganhar o $\varphi(SS0)$:

$$\dfrac{\dfrac{\dfrac{}{\varphi(0)}\ \textsc{IndZero}_\varphi}{\varphi(S0)}\ \textsc{IndStep}_\varphi}{\varphi(SS0)}\ \textsc{IndStep}_\varphi$$

E por aí vai! Olhando para as duas regras

$$\frac{}{\varphi(\mathsf{O})}\ \textsc{IndZero}_\varphi \qquad\qquad \frac{\varphi(n)}{\varphi(\mathsf{S}\ n)}\ \textsc{IndSucc}_\varphi$$

observamos que são bem parecidas com as

$$\frac{}{\mathsf{O} : \mathsf{Nat}}\ \textsc{Zero} \qquad\qquad \frac{n : \mathsf{Nat}}{\mathsf{S}\ n : \mathsf{Nat}}\ \textsc{Succ}$$

[42] Aqui consideramos a seguinte definição de «ímpar»: *um* $n : \mathsf{Nat}$ *é ímpar sse existe* k *tal que* $n = S(k + k)$.

e logo dado qualquer natural n, o desafio de estabelecer que n tem a propriedade φ, acaba sendo o mesmo com o "desafio" de estabelecer que n é um natural mesmo! Em outras palavras, assim que demonstrar os dois alvos da indução para matar o $(\forall n \in \mathbb{N})[\,\varphi(n)\,]$, temos:

$$n : \mathsf{Nat} \implies \varphi(n).$$

Ou seja: *todos os naturais têm a propriedade φ mesmo.*

4.49. Esse bla-bla presta mesmo?. O leitor alerto justamente ficaria com dúvidas sobre o texto acima. Realmente faz sentido essa descripção e essa intuição, mas todo esse "bla-bla" serve como uma demonstração mesmo do princípio da indução? Serve não. E por isso que o chamamos de *princípio*, ou seja axioma! Mas calma: dependendo na fundação de matemática que trabalhamos, o princípio pode virar teorema mesmo! No Capítulo 16 por exemplo, vamos *demonstrar mesmo* o princípio da indução para os naturais. Mas por enquanto não temos as ferramentas nem a maturidade que precisamos para entender essas idéias; então paciência. O que podes mesmo fazer desde já é demonstrar a equivalência desse princípio com um outro, que também é facilmente aceitável: o princípio da boa ordem (Problema Π3.6).

§90. Ordem nos naturais

D4.50. Definição. Definimos a relação de ordem $(\leq)$ nos Nats pela:

$$n \leq m \stackrel{\text{def}}{\iff} (\exists k : \mathsf{Nat})[\,n + k = m\,].$$

▸ **EXERCÍCIO x4.23 (Bottom).**
$(\forall x)[\,\mathsf{O} \leq x\,]$. (x4.23H0)

Λ4.51. Lema. *Para quaisquer $n, m : \mathsf{Nat}$,*

$$n \leq \mathsf{S}\, m \iff n \leq m \text{ ou } n = \mathsf{S}\, m.$$

Demonstração. Sejam n, m naturais.
($\Rightarrow$): Suponha $n \leq Sm$. Logo seja u tal que $n + u = Sm$. Separamos em casos. Caso $u = 0$. Logo $Sm = n + u = n + 0 = n$ e temos o que queremos demonstrar. Caso $u = Su'$ para algum u'. Logo $Sm = n + Su' = S(n + u')$. Agora, como $Sm = S(n + u')$, logo $m = n + u'$. Ou seja, $n \leq m$.
($\Leftarrow$): Tua: Exercício x4.24. ∎

▸ **EXERCÍCIO x4.24.**
Demonstre que

$$(\forall n)(\forall m)[\,n \leq \mathsf{S}\, m \iff n \leq m \text{ ou } n = \mathsf{S}\, m\,].$$

(x4.24H1)

Nos exercícios seguintes vamos demonstrar que $(\leq)$ é uma *ordem linear*, i.e., $(\leq)$ é...

▸ **EXERCÍCIO x4.25 (Reflexiva).**
$(\forall x)[\, x \leq x \,]$. (x4.25H0)

▸ **EXERCÍCIO x4.26 (Transitiva).**
$(\forall x)(\forall y)(\forall z)[\, x \leq y \;\&\; y \leq z \implies x \leq z \,]$. (x4.26H0)

▸ **EXERCÍCIO x4.27 (Antissimétrica).**
$(\forall x)(\forall y)[\, x \leq y \;\&\; y \leq x \implies x = y \,]$. (x4.27H0)

▸ **EXERCÍCIO x4.28 (Total).**
$(\forall x)(\forall y)[\, x \leq y \text{ ou } y \leq x \,]$. (x4.28H1)

Na verdade, $(\leq)$ é ainda mais legal: olhe no Problema Π4.5.

De uma ordem para outra. Simplesmente trocando a $(+)$ pela $(\cdot)$ na definição (D4.50) de $(\leq)$ obtemos uma definição (D4.52) duma outra relação de ordem (parcial) nos Nats:

D4.52. Definição. Definimos a relação de ordem $(|)$ nos Nats pela:

$$n \mid m \overset{\text{def}}{\iff} (\exists k : \mathsf{Nat})[\, n \cdot k = m \,].$$

que, naturalmente[43] chamamos de *divide*.

▸ **EXERCÍCIO x4.29.**
Verifique que a relação $(|) : \mathsf{Nat} \times \mathsf{Nat} \to \mathsf{Prop}$ é uma relação de ordem parcial, ou seja, ela é: reflexiva, transitiva, antissimétrica. Ela não é total. (x4.29H0)

▸ **EXERCÍCIO x4.30.**
O Nat possui bottom (mínimo) *e* top (máximo) com a ordem $(|)$ (quais são?), enquanto ordenado pela $(\leq)$ só tem bottom (Exercício x4.23). (x4.30H0)

Intervalo de problemas

D4.53. Definição (Ackermann). Seja ack a função definida por *recursão aninhada* pelas:

$$\begin{aligned}
&\mathrm{ack} : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat} \\
&\mathrm{ack}\ \mathsf{O}\ \ x\ \ = \mathsf{S}\ x \\
&\mathrm{ack}\ (\mathsf{S}\ n)\ \mathsf{O}\ \ = \mathrm{ack}\ n\ 1 \\
&\mathrm{ack}\ (\mathsf{S}\ n)\ (\mathsf{S}\ x) = \mathrm{ack}\ n\ (\mathrm{ack}\ (\mathsf{S}\ n)\ x).
\end{aligned}$$

[43] pun intended

A função ack é conhecida como função de Ackermann, e vamos encontrá-la novamente bem depois, no Secção §368.

Aqui um pequeno tira-gosto: implemente a definição ack na tua linguagem de programação favorita e use teu programa para calcular uns valores dela. O que percebes?

▸ **PROBLEMA Π4.1 (Ackermann).**
Investigue a função ack:

(i) Calcule o valor ack 3 2, indicando para cada passo qual equação foi usada.
(ii) Demonstre que ack 1 = (+ 2), ou seja, que para todo $x : \mathsf{Nat}$, ack 1 $x = x + 2$.
(iii) Demonstre que para todo $x : \mathsf{Nat}$, ack 2 $x = 2x + 3$.
(iv) Demonstre que ack, vista como função binária, é estritamente crescente no seu segundo argumento.
(v) Conclua que ack $n\ x \geq x$,
(vi) Mostre que ack é estritamente crescente no seu primeiro argumento também.
(vii) Mostre que $(\text{ack}\ n)^2$ é pointwise-$(<)$ que ack $(n + 2)$.
(viii) Demonstre que para todo $x : \mathsf{Nat}$, ack 2 $x = 2x + 3$.

(Π4.1H0)

▸ **PROBLEMA Π4.2.**
Definimos as operações binárias de adição, multiplicação, e exponenciação no Nat. Descubra um "padrão" nas definições dessas operações, e defina a próxima operação, *tetração*, nessa seqüência de operações. (Π4.2H0)

▸ **PROBLEMA Π4.3.**
Defina recursivamente as funções $t : (\mathbb{N} \to \mathbb{N}) \to \mathbb{N} \to \mathbb{N}$ e $T : (\mathbb{N} \to \mathbb{N}) \to \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ que satisfazem:

$$t\ h\ n = h(0)h(1)\cdots h(n-1) = \prod_{i=0}^{n-1} h(i);$$

$$T\ h\ (m,n) = h(m)h(m+1)\cdots h(m+n-1) = \prod_{i=m}^{m+n-1} h(i).$$

(Π4.3H12)

▸ **PROBLEMA Π4.4.**
Tentando resolver o Problema Π4.3, um aluno definiu corretamente a t e depois a usou na sua definição de T, assim:

$$T(m,n) = t(m+n)/t(m).$$

Qual o problema com essa definição? (Suponha como conhecida uma definição recursiva da operação / de divisão inteira.) (Π4.4H123)

▸ **PROBLEMA Π4.5.**
Demonstre por indução que a $(\leq)$ (definida na Definição D4.50) é uma bem-ordem, i.e.,

para todo habitado $A : \mathsf{Set\ Nat}$, $\quad A$ tem membro mínimo.

Dizemos que m é um *membro mínimo de* A sse $m \in A$ e $(\forall a \in A)[\, m \leq a \,]$. (Π4.5H12345)

▸ **PROBLEMA Π4.6.**
Qualquer Nat é par ou ímpar. (Π4.6H1)

§91. Abusando tipos e seus habitantes

▸ **EXERCÍCIO x4.31 (Par ou ímpar).**
Implemente funções $\mathrm{ev}, \mathrm{od} : \mathsf{Nat} \to \mathsf{Nat}$ que poderiam ser usadas para decidir se um Nat é par ou ímpar. (x4.31H0)

▸ **EXERCÍCIO x4.32 (Os inteiros como nats).**
Implemente o tipo de inteiros Int como type synonym do $\mathsf{Nat} \times \mathsf{Nat}$. (x4.32H0)

§92. Os Bools

D4.54. Definição (Bool). Definimos o tipo de dados Bool:

$$\begin{array}{l}\textbf{data}\ \mathsf{Bool}\\ \quad \mathsf{False}\ :\ \mathsf{Bool}\\ \quad \mathsf{True}\ \ :\ \mathsf{Bool}\end{array}$$

Tendo Bool, definimos as ev, od, agora sem abusos. Encontramos aqui três diferentes maneiras de definí-las, a primeira sendo efetivamente a mesma que fizemos no Exercício x4.33, só nos livrando do seu abuso:

▸ **EXERCÍCIO x4.33 (Par ou ímpar).**
Implemente funções $\mathrm{ev}, \mathrm{od} : \mathsf{Nat} \to \mathsf{Bool}$, poderiam ser usadas para decidir se um Nat é par ou ímpar. (x4.33H0)

§93. Internalização de conceitos

D4.55. Definição (leq). Com o que temos já definido podemos definir recursivamente a função

$$\begin{aligned}&\mathrm{leq} : \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Bool}\\ &\mathrm{leq}\ 0\quad m\quad = \mathsf{True}\\ &\mathrm{leq}\ Sn\ 0\quad = \mathsf{False}\\ &\mathrm{leq}\ Sn\ Sm = \mathrm{leq}\ n\ m.\end{aligned}$$

• **EXEMPLO 4.56.**
Calcule os $\mathrm{leq}\ SS0\ SSSS0$ e $\mathrm{leq}\ SSSS0\ SS0$.
RESOLUÇÃO. Calculamos:

$$\begin{aligned}
&\mathrm{leq}\ SS0\ SSSS0 \\
&\quad = \mathrm{leq}\ S0\ SSS0 && \text{(leq.3)} \\
&\quad = \mathrm{leq}\ 0\ SS0 && \text{(leq.3)} \\
&\quad = \mathsf{True}. && \text{(leq.1)}
\end{aligned}
\qquad\qquad
\begin{aligned}
&\mathrm{leq}\ SSSS0\ SS0 \\
&\quad = \mathrm{leq}\ SSS0\ S0 && \text{(leq.3)} \\
&\quad = \mathrm{leq}\ SS0\ 0 && \text{(leq.3)} \\
&\quad = \mathsf{False}. && \text{(leq.2)}
\end{aligned}$$

Podemos demonstrar que leq "é uma ordem linear", demonstrando cada uma das propriedades como fizemos sobre a $(\leq)$ nos exercícios (x4.25, x4.27, x4.26, x4.28) mas uma maneira melhor que vai nos permitir ganhar bem mais resultados de graça é demonstrar que $(\leq)$ e leq são na verdade a mesma relação. Ou seja, as definições D4.50 e D4.55 são equivalentes. Tu demonstrarás isso no Exercício x4.34.

▸ **EXERCÍCIO x4.34 (internal-leq).**
Na Definição D4.50 definimos a ordem $(\leq)$ nos naturais. Na Definição D4.55 definimos a relação $(\preceq)$ nos naturais. Obviamente não podemos dar duas definições diferentes para a mesma coisa. Demonstre que as duas definições sempre concordam:

$$\text{para todo } n, m \in \mathbb{N}, \quad n \leq m \iff n \preceq m.$$

(x4.34H0)

▸ **EXERCÍCIO x4.35 (internal-eq).**
Internalize a relação $(=)$ entre Nats. (x4.35H12)

§94. O Unit

D4.57. Definição (Unit). Definimos o tipo de dados Unit:

$$\begin{aligned}
&\textbf{data}\ \mathsf{Unit} \\
&\quad \star\ :\ \mathsf{Unit}
\end{aligned}$$

▸ **EXERCÍCIO x4.36.**
Defina funções saindo do e entrando no tipo Unit, ou seja, funções que tem tipos

$$\mathsf{Unit} \to \beta \qquad \text{e} \qquad \alpha \to \mathsf{Unit}.$$

O que percebes? (x4.36H0)

§95. O Empty

D4.58. Definição (Empty). Definimos o tipo de dados Empty:

$$\textbf{data}\ \mathsf{Empty}$$

Sim. Não tem nenhum construtor, e logo não tem nenhum habitante!

▸ **EXERCÍCIO x4.37.**
Defina funções saindo do e entrando no tipo Empty, ou seja, funções que tem tipos

$$\mathsf{Empty} \to \beta \qquad \text{e} \qquad \alpha \to \mathsf{Empty}.$$

O que percebes? (x4.37 H 0)

§96. O ListNat

D4.59. Definição (ListNat). Definimos o tipo de dados ListNat:

$$\begin{aligned}&\textbf{data}\ \mathsf{ListNat}\\ &\quad \mathsf{Nil}\ \ : \mathsf{ListNat}\\ &\quad \mathsf{Cons}\ : \mathsf{Nat} \to \mathsf{ListNat} \to \mathsf{ListNat}\end{aligned}$$

D4.60. Definição (length).

$$\begin{aligned}&\mathrm{length} : \mathsf{ListNat} \to \mathsf{Nat}\\ &\mathrm{length}\ \mathsf{Empty} \quad\ = \mathsf{O}\\ &\mathrm{length}\ (\mathsf{Cons}\ n\ ns) = \mathsf{S}\ (\mathrm{length}\ ns).\end{aligned}$$

▸ **EXERCÍCIO x4.38.**
Defina as funções: $\mathrm{sum}, \mathrm{product} : \mathsf{ListNat} \to \mathsf{Nat}$. (x4.38 H 0)

▸ **EXERCÍCIO x4.39.**
Defina as funções: $\mathrm{addNat}, \mathrm{mulNat}, \mathrm{expNat}, \mathrm{powNat} : \mathsf{Nat} \to \mathsf{ListNat} \to \mathsf{ListNat}$. (x4.39 H 0)

▸ **EXERCÍCIO x4.40.**
Defina as funções:

$$\mathrm{pwAdd}, \mathrm{pwMul}, \mathrm{pwExp} : \mathsf{ListNat} \to \mathsf{ListNat} \to \mathsf{ListNat}.$$

O «pw» vem de *pointwise*, a idéia sendo que aplicamos uma certa operação *ponto a ponto* numa lista inteira, chegando numa nova lista. Exemplos de input–output:

$$\begin{aligned}&\mathrm{pwAdd}\ [3,6,2]\ \ [100,500,7] = [103,506,9]\\ &\mathrm{pwAdd}\ [1,2,3,4]\ [100,40]\ \ \ \ = [101,42]\\ &\mathrm{pwMul}\ [1,2,3,4]\ [100,40,50] = [100,80,150]\\ &\mathrm{pwExp}\ [5,2,3,4]\ [2,8,3]\ \ \ \ = [25,256,27].\end{aligned}$$

(x4.40 H 0)

▸ **EXERCÍCIO x4.41.**
Defina as funções

$$\mathrm{stretch} : \mathsf{Nat} \to \mathsf{ListNat} \to \mathsf{ListNat} \qquad \mathrm{countdown} : \mathsf{Nat} \to \mathsf{ListNat}$$

com exemplos de input–output

$$\begin{array}{ll} \mathrm{stretch}\ 3\ [2,8] = [2,2,2,8,8,8] & \mathrm{countdown}\ 4 = [4,3,2,1,0] \\ \mathrm{stretch}\ 2\ [1,9,8,3] = [1,1,9,9,8,8,3,3] & \mathrm{countdown}\ 1 = [1,0]. \end{array}$$

(x4.41 H 0)

§97. Princípio da indução estrutural

4.61. Indução no ListNat. O que nos permite usar recursão e indução nos naturais é sua definição inductiva. Ou seja, podemos usar essas ferramentas em qualquer tipo que foi definido assim.

4.62. Com de inferência. Em forma de regra de inferência, o princípio da indução do ListNat é o seguinte:

$$\frac{\overbrace{\varphi(\mathsf{Nil})}^{(\mathsf{Nil}\text{ preserva a }\varphi)} \qquad \overbrace{(\forall ks : \mathsf{ListNat})[\,\varphi(ks) \implies (\forall k : \mathsf{Nat})[\,\varphi(\mathsf{Cons}\ k\ ks)\,]\,]}^{(\mathsf{Cons}\text{ preserva a }\varphi)}}{(\forall ns : \mathsf{ListNat})[\,\varphi(ns)\,]}\ \textsc{Ind}^{\mathsf{ListNat}}_{\varphi}$$

TODO Escrever

Intervalo de problemas

▸ **PROBLEMA Π4.7 (Listas de nats como nats).**
Implemente o tipo de listas-de-nats ListNat como type synonym do Nat. (Π4.7 H 0)

▸ **PROBLEMA Π4.8 (Os PairNats como Nats).**
Implemente o tipo de parzinhos-de-nats $\mathsf{Nat} \times \mathsf{Nat}$ como type synonym do Nat. (Π4.8 H 0)

§98. Listas

D4.63. Definição (List). Para qualquer $\alpha : \mathsf{Type}$, definimos o tipo de dados $\mathsf{List}\ \alpha$:

data $\mathsf{List}\ \alpha$
  $\mathsf{Nil}\ \ : \mathsf{List}\ \alpha$
  $\mathsf{Cons}\ : \alpha \to \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha$

Note que $\mathsf{List} : \mathsf{Type} \to \mathsf{Type}$. O contexto permitindo, podemos abreviar o $\mathsf{List}\ \alpha$ por $\mathsf{L}\ \alpha$.

4.64. List-induction. Em forma de regra de inferência, o princípio da indução do $\mathsf{List}\alpha$ é o seguinte:

$$\frac{\overbrace{\varphi([\,])}^{([\,]\text{ preserva a }\varphi)} \qquad \overbrace{(\forall xs : \mathsf{List}\ \alpha)[\,\varphi(xs) \implies (\forall x : \alpha)[\,\varphi(x :: xs)\,]\,]}^{((::)\text{ preserva a }\varphi)}}{(\forall ns : \mathsf{Nat})[\,\varphi(ns)\,]}\ \textsc{Ind}_{\varphi}^{\mathsf{List}\ \alpha}$$

D4.65. Length. Definimos a versão polimófica da length:

$$\begin{aligned}
&\mathrm{length} : \mathsf{List}\ \alpha \to \mathsf{Nat}\\
&\mathrm{length}\ [\,] \qquad\ = \mathsf{O}\\
&\mathrm{length}\ (x :: xs) = \mathsf{S}\ (\mathrm{length}\ xs).
\end{aligned}$$

D4.66. Reverse. Definimos a função reverse:

$$\begin{aligned}
&\mathrm{reverse} : \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha\\
&\mathrm{reverse}\ [\,] \qquad\ = [\,]\\
&\mathrm{reverse}\ (x :: xs) = \mathrm{reverse}\ xs +\!\!+ [x].
\end{aligned}$$

D4.67. Concat. Definimos a função $(+\!\!+)$:

$$\begin{aligned}
&(+\!\!+) : \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha\\
&[\,] +\!\!+ ys \qquad\ = ys\\
&(x :: xs) +\!\!+ ys = x :: (xs +\!\!+ ys).
\end{aligned}$$

TODO Terminar

§99. Destrutores

4.68. Observação (De quem é o destrutor?). Mesmo que às vezes dá para ver head e tail sendo referidos como "destrutores do tipo $\mathsf{List}\ \alpha$", isso é um abuso pesado de linguagem. Não são os tipos que têm destrutores, mas sim os seus construtores! E quantos destrutores tem, cada construtor? Tantos quantos argumenos ele precisa para construir um habitante do tipo! Olhando ao tipo $\mathsf{List}\ \alpha$ como exemplo, ele tem 2 construtores:

$$\begin{aligned}
&\mathsf{Nil} : \mathsf{List}\ \alpha\\
&\mathsf{Cons} : \alpha \to \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha.
\end{aligned}$$

Deles, o Nil tem aridade 0 e logo 0 destrutores também; mas o Cons tem aridade 2 e voilá: 2 destrutores. Considere uma lista $\ell : \mathsf{List}\ \alpha$ que foi construida pelo Cons. Isso significa que no processo de construí-la duas informações entraram nela: uma de tipo α, e uma de tipo $\mathsf{List}\ \alpha$, já que esses são os tipos dos argumentos do seu construtor Cons. Cada

destruidor é responsável para extrair a correspondente inforação: aqui o $\mathtt{head} : \mathsf{List}\ \alpha \rightharpoonup \alpha$ é responsável para extrair a primeira e o $\mathtt{tail} : \mathsf{List}\ \alpha \rightharpoonup \mathsf{List}\ \alpha$ extrai a segunda. Os nomes que escolhemos para eles são indicativos sobre o que e como pensamos sobre os objetos construidos por tal construtor: o que acabam sendo essas informações que o construtor coloca dentro do objeto construido, para o próprio objeto? No exemplo atual, os visualizamos como cabeça e rabo da lista construida, e logo os nomes.

TODO Escrever

§100. Dois lados da mesma moeda

TODO conectar 3-eq defs com 3-pattern induction, match-with, etc

TODO quais são os presentes numa dessas; teaser wf-induction

4.69. Definição inductiva. Definimos o tipo Nat listando suas formas (4.2) assim:

```
data Nat = O | S Nat
```

Note o Nat que aparece no lado direito também; é nesse sentido podemos dizer que essa foi uma definição recursiva. Alternativamente, optando para listar seus construtores (4.3) foi assim:

```
data Nat
  O : Nat
  S : Nat → Nat
```

Aqui note o Nat que reaparece *como argumento* para um dos seus próprios construtores. Esse tipo de definição chamamos de *definição inductiva*. Ela libera duas ferramentas poderosas: definir operações e relações por recursão; e demonstrar propriedades por indução. Na verdade se trata da mesma ferramenta; dois lados da mesma moeda.

! **4.70. Cuidado.** Muitas vezes *definição inductiva* acaba sendo chamada *definição recursiva*. Vários autores, dependendo da área que estão trabalhando adoptam um uso ou o outro, ou ambos, ou até diferenciando o que cada um significa. Tradicionalmente o slogan é:

> «defina por recursão; demonstre por indução».

4.71. O presente da recursão. Estamos tentando *definir algo por recursão*, por exemplo a operação de multiplicação (Exercício x4.6). Escrevemos já

$$n \cdot 0 = 0$$
$$n \cdot Sm = ____$$

e estamos pensando em como completar nossa definição. E a Recursão chega e nos oferece um presente:

> «Para definir o $n \cdot Sm$, considere o valor do $n \cdot m$ como dado, de graça por mim; e veja se tu consegues definir o valor de $n \cdot Sm$ com isso.»

E é exatamente o que fizemos. É isto o *poder da recursão*.

4.72. O presente da indução. Estamos tentando *demonstrar algo por indução* por exemplo a associatividade da adição. Já demonstramos a base (o $\varphi(0)$), e queremos demonstrar o $\varphi(Sn)$. E a Indução chega e nos oferece um presente:

> «Para demonstrar a $\varphi(Sn)$, considere a $\varphi(n)$ como dado, de graça por mim; e veja se tu consegues demonstrar a $\varphi(Sn)$ com isso agora.»

E é exatamente o que fizemos. É isto o *poder da indução*. Compare com nossa primeira tentativa de demonstrar a associatividade da adição (sem indução) onde nossa única maneira de andar era separar em casos, mas cada vez que conseguimos matar o "caso 0", o "caso sucessor" tava sempre gerando mais dois subcasos: um novo "caso 0" e um novo "caso sucessor". E nossos dados continuavam insuficientes para matar o segundo.

4.73. E a recursão? Não tem princípio não?. Se recursão e indução são dois lados da mesma moeda mesmo, e já encontramos e enunciamos o princípio da indução; a gente não deveria ter analogamente um princípio da recursão também? Tem sim, e temos o usado repetidamente cada vez que definimos uma função por recursão. Dependendo de quais são os fundamentos matemáticos em cima de quais estamos trabalhando e do contexto também, os "dois" princípios podem ser, de fato, apenas um e o mesmo, ou pode ser que um tem papel de princípio e o outro é demonstrável a partir dele (e vice versa), ou que ambos acabam sendo teoremas. Encontramos essas situações mais pra frente: no Capítulo 9 voltamos a esse assunto de justificar definições recursivas (Secção §221); no Capítulo 14 obtemos resultados que garantam e mostram como computar funções assim definidas (Secção §301); no Capítulo 16 demonstramos o teorema da indução dos naturais (Secção §324) e o teorema da recursão dos naturais (Secção §325). Sugiro paciência pois precisamos mais ferramentas e maturidade. O ponto, agora, é que não precisamos nada disso para conseguir trabalhar em forma correta com demonstrações indutivas e definições recursivas.

§101. Umas funções de ordem superior

D4.74. Definição (map). Definimos a função map:

$$\begin{aligned}
&\mathrm{map} : (\alpha \to \beta) \to (\mathsf{List}\ \alpha) \to (\mathsf{List}\ \beta)\\
&\mathrm{map}\ f\ [\,] \quad\ = [\,]\\
&\mathrm{map}\ f\ (x :: xs) = f\ x : \mathrm{map}\ f\ xs
\end{aligned}$$

D4.75. Definição (filter). Definimos a função filter:

$$\begin{aligned}
&\mathrm{filter} : (\alpha \to \mathsf{Bool}) \to (\mathsf{List}\ \alpha) \to (\mathsf{List}\ \alpha)\\
&\mathrm{filter}\ p\ [\,] \quad\ = [\,]\\
&\mathrm{filter}\ p\ (x :: xs) = \textbf{if}\ p\ x\ \textbf{then}\ x :: \mathrm{filter}\ p\ xs\ \textbf{else}\ \mathrm{filter}\ p\ xs
\end{aligned}$$

Ou, usando *guards*,

$$\begin{aligned}
&\mathrm{filter} : (\alpha \to \mathsf{Bool}) \to (\mathsf{List}\ \alpha) \to (\mathsf{List}\ \alpha)\\
&\mathrm{filter}\ p\ [\,] \quad\ = [\,]\\
&\mathrm{filter}\ p\ (x :: xs)\\
&\quad \mid p\ x \quad\ = x :: \mathrm{filter}\ p\ xs\\
&\quad \mid \mathrm{otherwise} = \mathrm{filter}\ p\ xs
\end{aligned}$$

▸ **EXERCÍCIO x4.42 (DRY).**
Elimine a repetição na Definição D4.75. (x4.42 H 1)

Θ4.76. Teorema.

(filter-map) $(\forall f : \alpha \to \beta)(\forall p : \beta \to \mathsf{Bool})[\,\mathrm{filter}\ p \circ \mathrm{map}\ f = \mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f)\,].$

Demonstração. Sejam $f : \alpha \to \beta$ e $p : \beta \to \mathsf{Bool}$. Para demonstrar

$$\mathrm{filter}\ p \circ \mathrm{map}\ f = \mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f)$$

pela definição de igualdade entre funções, preciso demonstrar

$$(\forall \ell : \mathsf{List}\ \alpha)[\,(\mathrm{filter}\ p \circ \mathrm{map}\ f)\ \ell = (\mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f))\ \ell\,]$$

Por indução no ℓ.
Caso $[\,]$. Precisamos demonstrar:

$$(\mathrm{filter}\ p \circ \mathrm{map}\ f)\ [\,] \stackrel{?}{=} (\mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f))\ [\,].$$

Calculamos os dois lados:

$(\mathrm{filter}\ p \circ \mathrm{map}\ f)\ [\,]$		$(\mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f))\ [\,]$	
$= \mathrm{filter}\ p\ (\mathrm{map}\ f\ [\,])$	$((\circ).1)$	$= \mathrm{map}\ f\ (\mathrm{filter}\ (p \circ f)\ [\,])$	$((\circ).1)$
$= \mathrm{filter}\ p\ [\,]$	$(\mathrm{map}.1)$	$= \mathrm{map}\ f\ [\,]$	$(\mathrm{filter}.1)$
$= [\,]$	$(\mathrm{filter}.1)$	$= [\,].$	$(\mathrm{map}.1)$

Caso $(x :: xs)$. Aqui temos a hipótese indutiva

$$(\mathrm{filter}\ p \circ \mathrm{map}\ f)\ xs = (\mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f))\ xs.$$

Separamos em casos:
Caso $(p \circ f)\ x = \mathsf{True}$, e logo $p\ (f\ x) = \mathsf{True}$. Calculamos:

$(\mathrm{filter}\ p \circ \mathrm{map}\ f)\ (x :: xs)$	
$= \mathrm{filter}\ p\ (\mathrm{map}\ f\ (x :: xs))$	$((\circ).1)$
$= \mathrm{filter}\ p\ (f\ x :: \mathrm{map}\ f\ xs)$	$(\mathrm{map}.2)$
$= f\ x :: \mathrm{filter}\ p\ (\mathrm{map}\ f\ xs)$	$(\mathrm{filter}.2$ e HC$)$
$= f\ x :: (\mathrm{filter}\ p \circ \mathrm{map}\ f)\ xs$	$((\circ).1)$
$= f\ x :: (\mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f))\ xs$	(HI)
$= f\ x :: (\mathrm{map}\ f\ (\mathrm{filter}\ (p \circ f)\ xs))$	$((\circ).1)$
$= \mathrm{map}\ f\ (x :: \mathrm{filter}\ (p \circ f)\ xs)$	$(\mathrm{map}.2)$
$= \mathrm{map}\ f\ (\mathrm{filter}\ (p \circ f)\ (x :: xs)))$	$(\mathrm{filter}.2$ e HC$)$
$= (\mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f))\ (x :: xs)$	$((\circ).1)$

Caso $(p \circ f)\ x = \mathsf{False}$, e logo $p\ (f\ x) = \mathsf{False}$.

$(\mathrm{filter}\ p \circ \mathrm{map}\ f)\ (x :: xs)$	
$= \mathrm{filter}\ p\ (\mathrm{map}\ f\ (x :: xs))$	$((\circ).1)$
$= \mathrm{filter}\ p\ (f\ x :: \mathrm{map}\ f\ xs)$	$(\mathrm{map}.2)$
$= \mathrm{filter}\ p\ (\mathrm{map}\ f\ xs)$	$(\mathrm{filter}.2$ e HC$)$
$= (\mathrm{filter}\ p \circ \mathrm{map}\ f)\ xs$	$((\circ).1)$
$= (\mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f))\ xs$	(HI)
$= \mathrm{map}\ f\ (\mathrm{filter}\ (p \circ f)\ xs$	$((\circ).1)$
$= \mathrm{map}\ f\ (\mathrm{filter}\ (p \circ f)\ (x :: xs)$	$(\mathrm{filter}.2$ e HC$)$
$= (\mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f))\ (x :: xs)$	$((\circ).1)$

4.77. Na demonstração do Teorema Θ4.76, escolhi separar em casos, para evitar carregar a expressão com o if-then-else nas costas. Sem separar em casos, este cálculo ficaria assim:

$$
\begin{aligned}
& (\mathrm{filter}\ p \circ \mathrm{map}\ f)\ (x :: xs) \\
= \quad & ((\circ).1) \\
& \mathrm{filter}\ p\ (\mathrm{map}\ f\ (x :: xs)) \\
= \quad & (\mathrm{map}.2) \\
& \mathrm{filter}\ p\ (f\ x :: \mathrm{map}\ f\ xs) \\
= \quad & (\mathrm{filter}.2) \\
& \textbf{if}\ p\ (f\ x)\ \textbf{then}\ f\ x :: \mathrm{filter}\ p\ (\mathrm{map}\ f\ xs)\ \textbf{else}\ \mathrm{filter}\ p\ (\mathrm{map}\ f\ xs) \\
= \quad & ((\circ).1) \\
& \textbf{if}\ p\ (f\ x)\ \textbf{then}\ f\ x :: (\mathrm{filter}\ p \circ \mathrm{map}\ f)\ xs\ \textbf{else}\ (\mathrm{filter}\ p \circ \mathrm{map}\ f)\ xs \\
= \quad & (\mathrm{HI}) \\
& \textbf{if}\ p\ (f\ x)\ \textbf{then}\ f\ x :: (\mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f))\ xs\ \textbf{else}\ (\mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f))\ xs \\
= \quad & ((\circ).1) \\
& \textbf{if}\ (p \circ f)\ x\ \textbf{then}\ f\ x :: (\mathrm{map}\ f\ (\mathrm{filter}\ (p \circ f)\ xs))\ \textbf{else}\ \mathrm{map}\ f\ (\mathrm{filter}\ (p \circ f)\ xs) \\
= \quad & (\mathrm{map}.2) \\
& \textbf{if}\ (p \circ f)\ x\ \textbf{then}\ \mathrm{map}\ f\ (x :: \mathrm{filter}\ (p \circ f)\ xs)\ \textbf{else}\ \mathrm{map}\ f\ (\mathrm{filter}\ (p \circ f)\ xs) \\
= \quad & (\mathrm{ifthenelse\text{-}distr}) \\
& \mathrm{map}\ f\ (\textbf{if}\ (p \circ f)\ x\ \textbf{then}\ x :: \mathrm{filter}\ (p \circ f)\ xs\ \textbf{else}\ \mathrm{filter}\ (p \circ f)\ xs) \\
= \quad & ((\circ).1) \\
& \mathrm{map}\ f\ (\textbf{if}\ (p \circ f)\ x\ \textbf{then}\ \mathrm{filter}\ (p \circ f)\ (x :: xs)\ \textbf{else}\ \mathrm{filter}\ (p \circ f)\ xs) \\
= \quad & (\mathrm{filter}.2) \\
& \mathrm{map}\ f\ (\mathrm{filter}\ (p \circ f)\ (x :: xs)) \\
= \quad & ((\circ).1) \\
& (\mathrm{map}\ f \circ \mathrm{filter}\ (p \circ f))\ (x :: xs).
\end{aligned}
$$

▸ **EXERCÍCIO x4.43 (ifthenelse-distr).**
Enuncie e demonstre o (ifthenelse-distr) citado acima. (x4.43H0)

D4.78. Definição (folds). Definimos as funções foldl e foldr:

$$
\begin{array}{ll}
\mathrm{foldl} : (\beta \to \alpha \to \beta) \to \beta \to (\mathsf{List}\ \alpha \to \beta) & \mathrm{foldr} : (\alpha \to \beta \to \beta) \to \beta \to (\mathsf{List}\ \alpha \to \beta) \\
\mathrm{foldl}\ f\ z\ [\,] = z & \mathrm{foldr}\ f\ z\ [\,] = z \\
\mathrm{foldl}\ f\ z\ (x :: xs) = \mathrm{foldl}\ f\ (f\ z\ x)\ xs & \mathrm{foldr}\ f\ z\ (x :: xs) = f\ x\ (\mathrm{foldr}\ f\ z\ xs)
\end{array}
$$

Ou, reescrevendo usando *where*, e trocando uns nomes:

$$
\begin{array}{ll}
\mathrm{foldl} : (\beta \to \alpha \to \beta) \to \beta \to (\mathsf{List}\ \alpha \to \beta) & \mathrm{foldr} : (\alpha \to \beta \to \beta) \to \beta \to (\mathsf{List}\ \alpha \to \beta) \\
\mathrm{foldl}\ f\ v\ [\,] = v & \mathrm{foldr}\ c\ n\ [\,] = n \\
\mathrm{foldl}\ f\ v\ (x :: xs) = \mathrm{foldl}\ f\ v'\ xs & \mathrm{foldr}\ c\ n\ (x :: xs) = c\ x\ t \\
\quad \textbf{where}\ \ v' = f\ z\ x & \quad \textbf{where}\ \ t = \mathrm{foldr}\ c\ n\ xs
\end{array}
$$

TODO Elaborar

§102. Polimorfísmo

TODO Escrever

§103. Somatórios e produtórios

TODO Escrever

Intervalo de problemas

▸ **PROBLEMA Π4.9 (IList).**
Defina o construtor de tipos $\mathsf{IList} : \mathsf{Type} \to \mathsf{Type}$, que construa tipos de listas *habitadas*. Defina também funções head e tail pare este tipo, e uma função

$$\mathrm{toList} : \mathsf{IList} \to \mathsf{List}.$$

(Π4.9H0)

▸ **PROBLEMA Π4.10 (EList, OList).**
Defina *usando recursão mútua* os construtores de tipos $\mathsf{EList}, \mathsf{OList} : \mathsf{Type} \to \mathsf{Type}$, que construam tipos de listas de tamanhos garantidamente par (a OList) e ímpar (a EList). Defina também funções head e tail para cada uma dessas listas, e funções toList. (Π4.10H0)

▸ **PROBLEMA Π4.11.**
No Capítulo 9 aprendemos que conseguir uma função $(\circ)$-L-inversa duma função $f : \alpha \to \beta$, i.e., uma $f' : \alpha \leftarrow \beta$ tal que

$$f' \circ f = \mathrm{id}_\alpha$$

é suficiente para garantir que f é *injetiva:*

$$(\forall a, a' : \alpha)[\, f\ a = f\ a' \implies a = a' \,].$$

Dado isso, uma aluna tentou demonstrar a S-injetividade assim:

> Injetividade de S. Considere a $\mathrm{pred} : \mathsf{Nat} \leftarrow \mathsf{Nat}$. Basta mostrar que ela é uma $(\circ)$-L-inversa da S: $(\mathrm{pred} \circ \mathsf{S})\ n = \mathrm{pred}\ (\mathsf{S}\ n) = n = \mathrm{id}\, n$.

A demonstração é válida? Se não, especifique o erro; senão, por que estipulamos tal injetividade como princípio em vez de consegui-la como teorema? (Π4.11H123)

▸ **PROBLEMA Π4.12.**
(Apenas depois de resolver o Problema Π4.11.)
Responda na pergunta surgida no fim da minha resolução de Problema Π4.11. (Π4.12H1)

§104. Tipos de Maybe

D4.79. Definição (Maybe). Definimos o construtor de tipos Maybe assim:

$$\begin{aligned}&\textbf{data}\ \mathsf{Maybe} : (\alpha : \mathsf{Type}) \to \mathsf{Type}\\ &\quad \mathsf{Nothing} \ : \ \mathsf{Maybe}\ \alpha\\ &\quad \mathsf{Just} \quad : \ \alpha \to \mathsf{Maybe}\ \alpha\end{aligned}$$

Podemos abreviar o $\mathsf{Maybe}\,\alpha$ por $\mathsf{M}\,\alpha$ quando o contexto permite, a seus construtores também, por N e J respectivamente.

TODO Gambiarra (1): $\mathrm{safeHead}_1 : \mathsf{ListNat} \to \mathsf{ListNat}$
TODO Gambiarra (2): $\mathrm{junkHead} : \mathsf{ListNat} \to \mathsf{Bool} \times \mathsf{Nat}$
TODO Gambiarra (3): $\mathrm{defaultHead} : \mathsf{Nat} \to \mathsf{ListNat} \to \mathsf{Nat}$
TODO Terminar

§105. Tipos de Either

D4.80. Definição (Either). Para quaisquer $\alpha, \beta : \mathsf{Type}$, definimos o tipo de dados $\mathsf{Either}\ \alpha\ \beta$:

$$\begin{aligned}&\textbf{data}\ \mathsf{Either}\ \alpha\ \beta\\ &\quad \mathsf{Left} \ : \ \alpha \to \mathsf{Either}\ \alpha\ \beta\\ &\quad \mathsf{Right} \ : \ \beta \to \mathsf{Either}\ \alpha\ \beta\end{aligned}$$

Note que $\mathsf{Either} : \mathsf{Type} \to \mathsf{Type} \to \mathsf{Type}$. Como esperado, quando o contexto permite podemos abreviar os Either, Left, Right por E, L, R respectivamente.[44]

TODO Terminar

§106. Produtos, somas, etc.

TODO Escrever

Intervalo de problemas

TODO Add problems

[44] o meio ambiente agradece

§107. Functors

S4.81. Especificação (Functor). Considere os

$$F : \mathsf{Type} \to \mathsf{Type}$$
$$\mathrm{map}_F : (\alpha \to \beta) \to (F\ \alpha \to F\ \beta)$$

Dizemos que o F com a map_F é um *functor* sse as duas *leis de functor* são satisfeitas:

(functor-id) $\quad \mathrm{map}_F\ \mathrm{id} = \mathrm{id}$

(functor-comp) $\quad \mathrm{map}_F\ (f \circ g) = \mathrm{map}_F\ f \circ \mathrm{map}_F\ g.$

Escrevemos apenas map quando o F é inferível pelo contexto.

Θ4.82. Teorema (List-functor). *O* $\mathsf{List} : \mathsf{Type} \to \mathsf{Type}$ *com sua* $\mathrm{map} : (\alpha \to \beta) \to (\mathsf{List}\ \alpha \to \mathsf{List}\ \beta)$ *é um functor.*

Demonstração. Precisamos demonstrar as duas leis de functors. A primeira é pra ti (Exercício x4.44), e a segunda, i.e.,

$$\big(\forall \alpha \xrightarrow{g} \beta \xrightarrow{f} \gamma\big)\big[\,\mathrm{map}\ (f \circ g) = \mathrm{map}\ f \circ \mathrm{map}\ g\,\big],$$

pra mim. Sejam $\alpha \xrightarrow{g} \beta \xrightarrow{f} \gamma$. Agora, pela definição da igualdade sobre funções, preciso demonstrar

$$(\forall \ell : \mathsf{List}\ \alpha)[\,\mathrm{map}\ (f \circ g)\ \ell = (\mathrm{map}\ f \circ \mathrm{map}\ g)\ \ell\,].$$

Seja $\ell : \mathsf{List}\ \alpha$. Por indução.
Caso $[\,]$. Calculamos:

$$\begin{aligned}
\mathrm{map}\ (f \circ g)\ [\,] &= [\,] && (\mathrm{map}.1)\\
(\mathrm{map}\ f \circ \mathrm{map}\ g)\ [\,] &= \mathrm{map}\ f\ (\mathrm{map}\ g\ [\,]) && ((\circ).1)\\
&= \mathrm{map}\ f\ [\,] && (\mathrm{map}.1)\\
&= [\,]. && (\mathrm{map}.1)
\end{aligned}$$

Caso $(x :: xs)$. Calculamos os dois lados:

$$\begin{aligned}
&\mathrm{map}\ (f \circ g)\ (x :: xs)\\
&\quad = (f \circ g)\ x :: \mathrm{map}\ (f \circ g)\ xs && (\mathrm{map}.2)\\
&\quad = (f \circ g)\ x :: (\mathrm{map}\ f\ xs \circ \mathrm{map}\ g\ xs) && (\mathrm{HI})\\
&\quad = f\ (g\ x) :: (\mathrm{map}\ f\ xs \circ \mathrm{map}\ g\ xs) && ((\circ).1)\\
&\quad = f\ (g\ x) :: \mathrm{map}\ f\ (\mathrm{map}\ g\ xs) && ((\circ).1)
\end{aligned}$$

$$\begin{aligned}
&(\mathrm{map}\ f \circ \mathrm{map}\ g)\ (x :: xs)\\
&\quad = \mathrm{map}\ f\ (\mathrm{map}\ g\ (x :: xs)) && ((\circ).1)\\
&\quad = \mathrm{map}\ f\ (g\ x :: \mathrm{map}\ g\ xs) && (\mathrm{map}.2)\\
&\quad = f\ (g\ x) :: \mathrm{map}\ f\ (\mathrm{map}\ g\ xs) && (\mathrm{map}.2)
\end{aligned}$$

∎

▸ **EXERCÍCIO x4.44.**
Demonstre a primeira lei de functor para o List com sua map. (x4.44H0)

▸ **EXERCÍCIO x4.45.**
Para cada um dos

$$(\alpha\ +), \quad (+\ \beta), \quad (\alpha\ \times), \quad (\times\ \beta), \quad (\gamma\ \to), \quad (\to\ \delta) \quad : \mathsf{Type} \to \mathsf{Type}$$

verifique se pode fazer parte dum functor: se pode, defina correspondente map que satisfaz as leis de functor (assim satisfazendo a Especificação S4.81); senão, explique o porquê. (x4.45 H 1)

4.83. E os Nat, Bool, List Nat, etc.? Será que são functors também? A resposta imediata nesse momento deve ser que até a pergunta tem um type error, pois, pela especificação de functor (S4.81) apenas coisas de tipo Type → Type tem chances de ser functor (sim, junto com uma map apropriada), mas esses bichos que botei na mesa na minha pergunta todos são tipos, ou seja, tem tipo Type, ou seja, não tem como eles serem considerados functors. Ou tem? Lembre que o 0 : Nat também não é uma função, como nenhuma constante é, mas podemos considerá-la como se fosse, com o simples hackinho de considerar a 0 : Unit → Nat em vez do próprio 0 : Nat. Podemos fazer algo parecido com os tipos e aproveitar uma maneira de considerá-los como possíveis functors. Diga «bem vindo» ao functor-constante:

D4.84. Definição (Konst). Dado qualquer tipo κ, o Konst κ : Type → Type simplesmente ignora seu argumento e retorna o próprio κ:

$$\begin{aligned} &\mathsf{Konst} : \mathsf{Type} \to \mathsf{Type} \to \mathsf{Type} \\ &\mathsf{Konst}\ \kappa\ \alpha \stackrel{\mathsf{def}}{=} \kappa. \end{aligned}$$

Observe o tipo do próprio Konst : Type → Type → Type; o aplicando (parcialmente) a um tipo κ, obtemos o Konst κ : Type → Type, e esse tem o tipo certo para ter chances de fazer parte dum functor! Será que ele faz?

▸ **EXERCÍCIO x4.46 (Konst-functor).**
Faz sim! (x4.46 H 0)

▸ **EXERCÍCIO x4.47 (Id).**
Definimos já o functor constante Konst κ : Type → Type, agora queremos definir um tal de Id : Type → Type. Defina. (x4.47 H 0)

▸ **EXERCÍCIO x4.48 (Id-functor).**
Preciso enunciar? (x4.48 H 0)

▸ **EXERCÍCIO x4.49.**
Ache tipos α e β tais que as tipagens seguintes são válidas:

$$\begin{aligned} &\mathsf{Just}\ [5,6,1], \quad \mathsf{Just}\ [7], \quad \mathsf{Just}\ [\,], \quad \mathsf{Nothing}, \quad \ldots \quad : \alpha \\ &[\mathsf{Just}\ 3, \mathsf{Just}\ 1, \mathsf{Just}\ 3], \quad [\mathsf{Just}\ 4], \quad [\mathsf{Nothing}], \quad [\mathsf{Just}\ 5, \mathsf{Nothing}, \mathsf{Just}\ 1], \quad [\,], \quad \ldots \quad : \beta \end{aligned}$$

(x4.49 H 0)

▸ **EXERCÍCIO x4.50.**
Defina funções $\mathrm{map}_1, \mathrm{map}_2$ tais que para qualquer $f : \mathsf{Nat} \to \gamma$ a $\mathrm{map}_1\ f$ será aplicável nos objetos da primeira linha do Exercício x4.49 retornando

$$\mathsf{Just}\ [f\ 5, f\ 6, f\ 1], \quad \mathsf{Just}\ [f\ 7], \quad \ldots$$

e a $\mathrm{map}_2\ f$ nos objetos da segunda retornando

$$[\mathsf{Just}\ (f\ 3), \mathsf{Just}\ (f\ 1), \mathsf{Just}\ (f\ 3)], \quad [f\ 4], \quad \ldots$$

(x4.50H1)

▸ **EXERCÍCIO x4.51.**
Escreva uns habitantes dos tipos seguintes:

$$\ldots \ : \mathsf{List}\ (\mathsf{List}\ (\mathsf{Bool} \to \mathsf{Nat}))$$
$$\ldots \ : \mathsf{List}\ (\mathsf{Either}\ \mathsf{Nat}\ (\mathsf{Maybe}\ (\mathsf{List}\ \mathsf{Bool}))).$$

(x4.51H0)

4.85. Considere tipos como os

$$\mathsf{Maybe}\ (\mathsf{List}\ \mathsf{Nat}) : \mathsf{Type} \qquad \mathsf{List}\ (\mathsf{Maybe}\ \mathsf{Nat}) : \mathsf{Type}$$
$$\mathsf{List}\ (\mathsf{List}\ (\mathsf{Bool} \to \mathsf{Nat})) : \mathsf{Type} \qquad \mathsf{List}\ (\mathsf{Either}\ \mathsf{Nat}\ (\mathsf{Maybe}\ (\mathsf{List}\ \mathsf{Bool}))) : \mathsf{Type}.$$

e observe que, de fato, todos eles são tipos mesmo. Uns habitantes desses tipos encontrou nos exercícios x4.49 e x4.51. Mesmo que o Exercício x4.50 não foi nada difícil pra ti—confio no teu potencial—e mesmo que tu gastou pouquíssimas linhas para definir essas map's que ele pediu, deves concordar que se conseguir a mesma funcionalidade com 0 (zero) linhas, seria bem melhor. Isso que faremos agora, demonstrando apenas um teorema. Ainda mais, essa método é aplicável para todos os tipos "desse tipo": tipos como esses que escrevi acima. O primeiro passo é conseguir descrever esse tipo de tipo. O que eles têm em comum mesmo?

!! SPOILER ALERT !!

Resposta. Todos eles são construidos aplicando uns functors em outros tipos, que também foram construidos via functors, e por aí vai. Ou seja: *são composições de functors* aplicadas num tipo. Eu vou explicitar as duas primeiras, que são mais simples, e deixar as outras duas e ainda mais umas pra ti—acho justo:

$$\mathsf{Maybe}\ (\mathsf{List}\ \mathsf{Nat}) = (\mathsf{Maybe} \circ \mathsf{List})\ \mathsf{Nat} \qquad \mathsf{List}\ (\mathsf{Maybe}\ \mathsf{Nat}) = (\mathsf{List} \circ \mathsf{Maybe})\ \mathsf{Nat}.$$

▸ **EXERCÍCIO x4.52.**
Escreva os tipos seguintes como composições de functors aplicados num tipo só (tua escolha, se tiver), como eu acabei de fazer:

$$\mathsf{List}\ (\mathsf{List}\ (\mathsf{Bool} \to \mathsf{Nat})) : \mathsf{Type} \qquad \mathsf{List}\ (\mathsf{Either}\ \mathsf{Nat}\ (\mathsf{Maybe}\ (\mathsf{List}\ \mathsf{Bool}))) : \mathsf{Type}$$
$$\mathsf{Nat} \times \mathsf{List}\ (\mathsf{Maybe}\ \mathsf{Nat}) : \mathsf{Type} \qquad \mathsf{Either}\ \mathsf{Weekday}\ (\mathsf{Nat} \times \mathsf{Bool}) : \mathsf{Type}.$$

(x4.52H1)

§108. Árvores

TODO Desenhar uns exemplos de árvores

D4.86. Definição (BinTree). Para qualquer $\alpha : \mathsf{Type}$, definimos o tipo

$$\begin{aligned}&\textbf{data}\ \mathsf{BinTree}\ \alpha\\ &\quad \mathsf{Tip}\ \ : \alpha \to \mathsf{BinTree}\ \alpha\\ &\quad \mathsf{Fork}\ : \mathsf{BinTree}\ \alpha \to \mathsf{BinTree}\ \alpha \to \mathsf{BinTree}\ \alpha\end{aligned}$$

Chamamos o tipo de *binary tree*, por causa da quantidade de filhos que cada nó dele tem (exatamente 2).

4.87. Observação (Tree). Economizando minha tinta e teu cansaço visual, vou escrever $\mathsf{Tree}\ \alpha$ ou até $\mathsf{T}\ \alpha$, quando é implicito qual de todas as árvores está sendo considerada.

▸ **EXERCÍCIO x4.53 (nodes, leaves, depth).**
Defina as funções

$$\mathrm{nodes} : \mathsf{Tree}\ \alpha \to \mathsf{Nat} \qquad \mathrm{leaves} : \mathsf{Tree}\ \alpha \to \mathsf{Nat} \qquad \mathrm{depth} : \mathsf{Tree}\ \alpha \to \mathsf{Nat}.$$

que contam os nós, as folhas, e os andares duma árvore. (x4.53H123)

Θ4.88. Teorema (nodes-leaves). *Para toda árvore* $t : \mathsf{Tree}\ \alpha$,

$$\mathrm{leaves}\ t = 1 + \mathrm{nodes}\ t.$$

Demonstrarás agora no Exercício x4.54. ∎

▸ **EXERCÍCIO x4.54.**
Demonstre o Teorema Θ4.88. (x4.54H12)

Θ4.89. Teorema (leaves-depth). *Para toda árvore* $t : \mathsf{Tree}\ \alpha$,

$$\mathrm{leaves}\ t \leq 2\ \hat{}\ \mathrm{depth}\ t.$$

Demonstração. Seja $t : \mathsf{Tree}\ \alpha$. Por indução no t.

Caso (Tip x). Calculamos:

$$\begin{aligned} \text{leaves } (\mathsf{Tip}\ x) &= 1 && \text{(leaves.1)} \\ 2 \mathbin{\wedge} \text{depth } (\mathsf{Tip}\ x) &= 2 \mathbin{\wedge} 0 = 1. && \text{(depth.1)} \end{aligned}$$

Caso (Fork ℓ r). Calculamos:

$$\begin{aligned} &\text{leaves } (\mathsf{Fork}\ \ell\ r) \\ &\quad = \text{leaves } \ell + \text{leaves } r && \text{(leaves.2)} \\ &\quad \le 2 \mathbin{\wedge} \text{depth } \ell + \text{leaves } r && \text{(hi-}\ell\text{)} \\ &\quad \le 2 \mathbin{\wedge} \text{depth } \ell + 2 \mathbin{\wedge} \text{depth } r && \text{(hi-}r\text{)} \\ &\quad \vdots && \text{(Exercício x4.55)} \\ &\quad = 2 \mathbin{\wedge} \text{depth } (\mathsf{Fork}\ \ell\ r). && \text{(depth.2)} \end{aligned}$$

∎

▸ **EXERCÍCIO x4.55.**
Feche o que faltou para fechar na demonstração de Teorema Θ4.89. (x4.55 H 0)

▸ **EXERCÍCIO x4.56 (subtrees).**
Defina a $\mathit{subtrees} : \mathsf{Tree}\ \alpha \to \mathsf{List}\ (\mathsf{Tree}\ \alpha)$ que retorna uma lista com todas as subárvores da sua entrada. (x4.56 H 0)

▸ **EXERCÍCIO x4.57 (flatten).**
Defina a $\mathit{flatten} : \mathsf{Tree}\ \alpha \to \mathsf{List}\ (\mathsf{Tree}\ \alpha)$ que retorna o *achatamento* da sua entrada: uma lista com todos os valores das folhas, na ordem que aparecem projetando a árvore a um piso horizontal. (x4.57 H 0)

▸ **EXERCÍCIO x4.58 (search, fetch).**
Queremos definir funções

$$\mathit{search} : \alpha \to \mathsf{Tree}\ \alpha \to \mathsf{List}\ (\mathsf{Path}) \qquad \mathit{fetch} : \mathsf{Path} \to \mathsf{Tree}\ \alpha \to \mathsf{Maybe}\ \alpha$$

para árvores. No caso de listas, a busca da search retorna uma lista de Nats, já que cada tal Nat visto como índice é a informação que corresponde numa posição numa lista. Numa árvore não faz sentido perguntar «quem está na posição 4?». Ou seja, o Nat não serve como tipo para descrever uma posição. Cada posição é descrita por um caminho, ou seja, uma lista de direções (esquerda–direita). Usamos o tipo Path de caminhos então, que é definido apenas como um sinônimo

$$\mathsf{Path} \stackrel{\text{def}}{=} \mathsf{List\ Dir} \qquad \text{onde} \qquad \begin{array}{l} \textbf{data}\ \mathsf{Dir} \\ \quad \mathsf{L} \ : \mathsf{Dir} \\ \quad \mathsf{R} \ : \mathsf{Dir} \end{array}$$

Agora defina as search e fetch. (x4.58 H 0)

▸ **EXERCÍCIO x4.59 (subtree).**
Defina a $\mathit{subtree}$ que, dado um caminho e uma árvore retorna a subárvore que começa a parir do ponto descrito pelo caminho. Faz parte deste exercício pensar num tipo legal para tal função. (x4.59 H 1)

▸ **EXERCÍCIO x4.60 (functor).**
O BinTree : Type → Type pode ser um functor? Se sim, defina o que precisa ser definido e demonstre o que precisa ser demonstrado. Senão, por que não? (x4.60 H 1 2)

▸ **EXERCÍCIO x4.61 (LBinTree).**
Defina o LBinTree, capaz de representar árvores binárias com rótulos, ou seja, que carregam informação tanto nos seus forks, quanto nos seus tips. Observe que tais informações, em geral, podem ser de tipos diferentes. (x4.61 H 0)

▸ **EXERCÍCIO x4.62 (flatten).**
Adapte a flatten para funcionar em árvores de tipo LBinTree α α, projetando as informações tanto dos forks quanto dos tips na mesma lista. O que faria se quisesse adaptá-la para árvores de tipo LBinTree α β mesmo? (x4.62 H 0)

▸ **EXERCÍCIO x4.63 (GenTree).**
Defina o GenTree, capaz de representar árvores gerais, que carregam informação nos seus nós e cada nó pode ter 0 ou mais filhos (suas folhas são seus nós sem filhos). (x4.63 H 0)

§109. Ordenando

TODO Escrever

§110. Um toque de complexidade

Nosso foco tem sido definir funções corretamente e demonstrar suas propriedades, incluindo a corretude dos nossos programas. Sem aprofundar nos terrenos da complexidade computational, quero aproveitar o momento para falar de eficiência.

4.90. Length. Lembre a definição da length (D4.65):

$$\begin{aligned}
&\text{length} : \mathsf{List}\ \alpha \to \mathsf{Nat}\\
&\text{length}\ [\,] \qquad\ = \mathsf{O}\\
&\text{length}\ (n :: ns) = \mathsf{S}\ (\text{length}\ ns).
\end{aligned}$$

Quantos passos precisamos para calcular o valor da length $[1,2,3,4]$ ficando fieis na sua definição? Calculamos:

$$\begin{aligned}
&\text{length}\ [1,2,3,4]\\
&\quad = \mathsf{S}\ (\text{length}\ [1,2,3]) && (\text{length.2})\\
&\quad = \mathsf{S}\ (\mathsf{S}\ (\text{length}\ [1,2])) && (\text{length.2})\\
&\quad = \mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\text{length}\ [1]))) && (\text{length.2})\\
&\quad = \mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\text{length}\ [\,])))) && (\text{length.2})\\
&\quad = \mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O}))). && (\text{length.1})
\end{aligned}$$

Precisou 5 passos: 4 usos de length.2 e 1 uso de length.1. É fácil perceber a maneira certa de generalizar isso para contar os passos de cálculo da length ℓ, onde ℓ é uma lista arbitrária: vamos precisar $|\ell| + 1$ passos, onde $|\ell|$ denota o tamanho da lista ℓ.

▸ **EXERCÍCIO x4.64 (Concatenação).**
Lembre a definição (D4.67) da $(+\!\!+)$:

$$\begin{aligned}(+\!\!+) &: \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha\\ [\,] +\!\!+ ys &= ys\\ (x :: xs) +\!\!+ ys &= x :: (xs +\!\!+ ys).\end{aligned}$$

Quantos passos precisamos para calcular o valor da $xs +\!\!+ ys$? Tua resposta deve depender dos tamanhos das listas xs e ys. (x4.64H0)

4.91. Complexidade de Reverse. Lembre a definição da reverse. Quantos passos precisamos para calcular seu valor, ficando fieis na sua definição? Calculamos:

$$\begin{aligned}&\mathrm{reverse}\ [1,2,3,4,5]\\ &= \mathrm{reverse}\ [1,2,3,4] +\!\!+ [5] && (\mathrm{reverse}.2)\\ &= (\mathrm{reverse}\ [1,2,3] +\!\!+ [5]) +\!\!+ [4] && (\mathrm{reverse}.2)\\ &= ((\mathrm{reverse}\ [1,2] +\!\!+ [5]) +\!\!+ [4]) +\!\!+ [3] && (\mathrm{reverse}.2)\\ &= (((\mathrm{reverse}\ [1] +\!\!+ [5]) +\!\!+ [4]) +\!\!+ [3]) +\!\!+ [2] && (\mathrm{reverse}.2)\\ &= ((((\mathrm{reverse}\ [\,] +\!\!+ [5]) +\!\!+ [4]) +\!\!+ [3]) +\!\!+ [2]) +\!\!+ [1] && (\mathrm{reverse}.2)\\ &= (((([\,] +\!\!+ [5]) +\!\!+ [4]) +\!\!+ [3]) +\!\!+ [2]) +\!\!+ [1] && (\mathrm{reverse}.1)\\ &\eqqcolon (((([5] +\!\!+ [4]) +\!\!+ [3]) +\!\!+ [2]) +\!\!+ [1] && ((+\!\!+).2;\ (+\!\!+).1)\\ &\eqqcolon (([5,4] +\!\!+ [3]) +\!\!+ [2]) +\!\!+ [1] && ((+\!\!+).2;\ (+\!\!+).1)\\ &\eqqcolon ([5,4,3] +\!\!+ [2]) +\!\!+ [1] && ((+\!\!+).2;\ (+\!\!+).1)\\ &\eqqcolon [5,4,3,2] +\!\!+ [1] && ((+\!\!+).2;\ (+\!\!+).1)\\ &\eqqcolon [5,4,3,2,1]. && ((+\!\!+).2;\ (+\!\!+).1)\end{aligned}$$

Vamos separar esse cálculo em duas partes. Na primeira (onde aparecem só $(=)$) cada linha corresponde em exatamente um passo, em qual aplicamos a definição de reverse para efetuar uma substituição. Na segunda (onde aparecem só $(\eqqcolon)$) cada linha corresponde numa seqüência de passos, em quais aplicamos repetidamente a $(+\!\!+).2$ até esvasiar a lista à esquerda para finalmente aplicar a $(+\!\!+).1$. Queremos contar a quantidade de passos que todo esse cálculo precisou até terminar. A primeira parte é fácil: de fato, cada $(=)$ é 1 passo, e tem 6 em total; então vou escrever

$$\begin{aligned}&\mathrm{reverse}\ [1,2,3,4,5]\\ &\overset{6}{=} (((([\,] +\!\!+ [5]) +\!\!+ [4]) +\!\!+ [3]) +\!\!+ [2]) +\!\!+ [1]. && ((4\times)\ \mathrm{reverse}.2;\ (1\times)\ \mathrm{reverse}.1)\end{aligned}$$

Agora precisamos contar quantas $(=)$'s estão escondidas atrás de cada uma das $(\eqqcolon)$'s. Lembrando que o cálculo de $\ell_1 +\!\!+ \ell_2$ precisa de $|\ell_1|+1$ passos, chegamos na conta seguinte:

$$\begin{aligned}&\mathrm{reverse}\ [1,2,3,4,5]\\ &\overset{6}{=} (((([\,] +\!\!+ [5]) +\!\!+ [4]) +\!\!+ [3]) +\!\!+ [2]) +\!\!+ [1] && ((5\times)\ \mathrm{reverse}.2;\ (1\times)\ \mathrm{reverse}.1)\\ &\overset{1}{=} ((([5] +\!\!+ [4]) +\!\!+ [3]) +\!\!+ [2]) +\!\!+ [1] && ((0\times)\ (+\!\!+).2;\ (1\times)\ (+\!\!+).1)\\ &\overset{2}{=} (([5,4] +\!\!+ [3]) +\!\!+ [2]) +\!\!+ [1] && ((1\times)\ (+\!\!+).2;\ (1\times)\ (+\!\!+).1)\\ &\overset{3}{=} ([5,4,3] +\!\!+ [2]) +\!\!+ [1] && ((2\times)\ (+\!\!+).2;\ (1\times)\ (+\!\!+).1)\\ &\overset{4}{=} [5,4,3,2] +\!\!+ [1] && ((3\times)\ (+\!\!+).2;\ (1\times)\ (+\!\!+).1)\\ &\overset{5}{=} [5,4,3,2,1]. && ((4\times)\ (+\!\!+).2;\ (1\times)\ (+\!\!+).1)\end{aligned}$$

Assim, a primeira parte precisou 6 passos e a segunda $1 + \cdots + 5 = 15$ passos, isto é, 21 passos para uma lista de tamanho 5.

§111. Eficiênia via indução

Vamos ver como podemos usar a teoria que temos elaborado aqui para ganhar versões bem mais eficientes dumas funções com quais nos sofreríamos se iríamos trabalhar com suas versões originais.

4.92. Melhor não pensar tanto. Descubrimos (Nota 4.91) que nossa $\mathrm{reverse}$ tem complexidade de tempo $O(n^2)$: para reverter uma lista de tamanho n ela precisa $\frac{1}{2}n^2 + \frac{3}{2}n + 1$ passos. Uma alternativa sensata agora seria pensar criativamente para achar uma nova definição de $\mathrm{reverse}$, mais eficiente. Mas com o que temos estudado até agora, dá para evitar esse processo, limitando a inspiração necessária. Vamos ver como aproveitar nossa experiência com indução e usá-la como guia para chegar quase gratuitamente numa nova definição de $\mathrm{reverse}$ que vai acabar sendo *muito* mais eficiente!

4.93. O que deu errado? O que seria legal?. O problema visto na Nota 4.91 é que temos dois trabalhos acontecendo e gastando tempo: reverter e concatenar. Que tal imaginar uma função revcat que retornaria seu primeiro argumento revertido e já concatenado com seu segundo? Tipo assim:

$$\mathrm{revcat} : \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha$$
$$(\forall xs, ys : \mathsf{List}\ \alpha)[\,\mathrm{revcat}\ xs\ ys = \mathrm{reverse}\ xs +\!\!+\ ys\,].$$

Note que isso não é uma definição, mas sim uma especificação que tal desejada revcat precisa atender. Vamos fingir por um momento que alguém já definiu uma tal função, e que ela é rápida. Observe que tendo uma tal revcat, podemos definir nossa $\mathrm{reverse}$ para ser simplesmente uma aplicação parcial da revcat:

$$\mathrm{reverse}\ xs \stackrel{\mathsf{def}}{=} \mathrm{revcat}\ xs\ [\,].$$

Então basta definir uma eficiente revcat. Bora.

4.94. Revcat via indução. Por que não usar simplesmente sua especificação como definição mesmo? Se tentar definir

$$\mathrm{revcat}\ xs\ ys = \mathrm{reverse}\ xs +\!\!+\ ys$$

onde $\mathrm{reverse}$ e $(+\!\!+)$ são nossas funções já definidas, a revcat vai ser lenta, mas isso nem é o maior problema: queremos usar a revcat para definir a $\mathrm{reverse}$ na maneira escrita acima, e se tentar usar essas duas definições mesmo, vamos ter uma tijolada. Mesmo que não serve como definição, a especificação precisa ser satisfeita por qualquer implementação de revcat, e logo temos sim as igualdades

$$\mathrm{revcat}\ [\,]\ ys = \mathrm{reverse}\ [\,] +\!\!+\ ys$$
$$\mathrm{revcat}\ (x :: xs)\ ys = \mathrm{reverse}\ (x :: xs) +\!\!+\ ys.$$

Basta substituir cada uma delas por algo igual que não envolve nem reverse nem (++):

$$\begin{aligned} \mathrm{revcat}\ [\,]\ ys &\stackrel{\mathsf{def}}{=} ? \quad (= \mathrm{reverse}\ [\,] +\!\!+ ys) \\ \mathrm{revcat}\ (x :: xs)\ ys &\stackrel{\mathsf{def}}{=} ? \quad (= \mathrm{reverse}\ (x :: xs) +\!\!+ ys). \end{aligned}$$

A parte criativa que queremos evitar é pensar nesses ? aí. Usaremos indução como guia para chegar em tal definição, sem pecisar pensar muito. Começa fingindo que estamos tentando demonstrar por indução que, de fato,

$$(\forall xs : \mathsf{List}\ \alpha)(\forall ys : \mathsf{List}\ \alpha)[\,\mathrm{revcat}\ xs\ ys = \mathrm{reverse}\ xs +\!\!+ ys\,].$$

Seja $xs : \mathsf{List}\ \alpha$ então. Por indução no xs.
Caso $[\,]$. Seja $ys : \mathsf{List}\ \alpha$.

$$\mathrm{revcat}\ [\,]\ ys \stackrel{?}{=} \mathrm{reverse}\ [\,] +\!\!+ ys.$$

Não tendo como trabalhar no lado esquerdo, trabalhamos no lado direito:

$$\begin{aligned} &\mathrm{reverse}\ [\,] +\!\!+ ys \\ &\quad = [\,] +\!\!+ ys \quad (\mathrm{reverse}.1) \\ &\quad = ys \qquad ((+\!\!+).1) \end{aligned}$$

E assim a "base da indução" nos fornece a primeira das duas linhas que precisamos para definir a desejada revcat:

$$\mathrm{revcat}\ [\,]\ ys \stackrel{\mathsf{def}}{=} ys.$$

Agora falta o "passo indutivo" nos fornecer a segunda linha.
Caso $(x :: xs)$. Nossa "hipótese indutiva" aqui é que a lista xs é *legalzona*, ou seja:

$$(\forall \ell : \mathsf{List}\ \alpha)[\,\mathrm{revcat}\ xs\ \ell = \mathrm{reverse}\ xs +\!\!+ \ell\,].$$

Vamos brincar de demonstradores de

$$(\forall ys : \mathsf{List}\ \alpha)[\,\mathrm{revcat}\ (x :: xs)\ ys = \mathrm{reverse}\ (x :: xs) +\!\!+ ys\,].$$

Seja $ys : \mathsf{List}\ \alpha$. Calculamos novamente no lado direito:

$$\begin{aligned} &\mathrm{revcat}\ (x :: xs)\ ys \\ &\quad \stackrel{!}{=} \mathrm{reverse}\ (x :: xs) +\!\!+ ys && (\text{especificação da revcat}) \\ &\quad = (\mathrm{reverse}\ xs +\!\!+ [x]) +\!\!+ ys && (\mathrm{reverse}.2) \\ &\quad = \mathrm{reverse}\ xs +\!\!+ ([x] +\!\!+ ys) && ((+\!\!+)\text{-assoc.}) \\ &\quad = \mathrm{reverse}\ xs +\!\!+ (x :: ([\,] +\!\!+ ys)) && ((+\!\!+).2) \\ &\quad = \mathrm{reverse}\ xs +\!\!+ (x :: ys) && ((+\!\!+).1) \\ &\quad = \mathrm{revcat}\ xs\ (x :: ys) && (\text{h.i. com } \ell := x :: ys) \end{aligned}$$

finalmente chegando numa expressão que não envolve nem reverse nem (++), que usamos para completar nossa definição de revcat, cuja versão final fica assim:

D4.95. Definição (revcat).

$$\begin{aligned} &\mathrm{reverse} : \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha && \mathrm{revcat} : \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha \to \mathsf{List}\ \alpha \\ &\mathrm{reverse}\ xs = \mathrm{revcat}\ xs\ [\,] && \mathrm{revcat}\ [\,]\ ys = ys \\ & && \mathrm{revcat}\ (x :: xs)\ ys = \mathrm{revcat}\ xs\ (x :: ys). \end{aligned}$$

4.96. Reverse: new and improved. Quantos passos precisamos para calcular o valor da $\mathrm{reverse}[1,2,3,4,5]$ com nossa nova Definição D4.95? Calculamos:

$$\begin{aligned}
&\mathrm{reverse}\ [1,2,3,4,5] \\
&\quad = \mathrm{revcat}\ [1,2,3,4,5]\ [\,] && (\mathrm{reverse}.1)\\
&\quad = \mathrm{revcat}\ [2,3,4,5]\ [1] && (\mathrm{revcat}.2)\\
&\quad = \mathrm{revcat}\ [3,4,5]\ [2,1] && (\mathrm{revcat}.2)\\
&\quad = \mathrm{revcat}\ [4,5]\ [3,2,1] && (\mathrm{revcat}.2)\\
&\quad = \mathrm{revcat}\ [5]\ [4,3,2,1] && (\mathrm{revcat}.2)\\
&\quad = \mathrm{revcat}\ [\,]\ [5,4,3,2,1] && (\mathrm{revcat}.2)\\
&\quad = [5,4,3,2,1]. && (\mathrm{revcat}.1)
\end{aligned}$$

Precisou 7 passos: 1 no início para chamar a revcat, 5 chamadas da revcat.2, e finalmente 1 chamada da revcat.1. Em forma geral, sendo aplicada numa lista de tamanho n, vai precisar apenas $n+2$ passos. Ou seja conseguimos uma implementação de tempo $O(n)$, em vez da velha e lenta versão que precisa $O(n^2)$.

§112. Eficiência via álgebra

TODO Escrever

§113. Folding

TODO Escrever

Problemas

▸ **PROBLEMA Π4.13 (Unfolding).**

TODO Escrever

(Π4.13H0)

TODO Leftovers to be tidied up, expanded upon, and complemented

§114. A notação BNF

4.97. Uma primeira tentativa. Vamos começar diretamente com um exemplo de uso da notação *BNF* (Backus–Naur form), para descrever uma linguagem de expressões aritméticas:

4.98. ArEx (1).

(1) $\langle ArEx\rangle \ ::= \ 0 \mid 1 \mid 2 \mid 3 \mid \cdots$

(2) $\langle ArEx\rangle \ ::= \ (\langle ArEx\rangle + \langle ArEx\rangle)$

O que tudo isso significa? A primeira linha, é uma regra dizendo: uma expressão aritmética pode ser um dos 0, 1, 2, 3, ... A segunda linha é mais interessante: uma expressão aritmética pode começar com o símbolo ‘ (’, depois ter uma expressão aritmética, depois o símbolo ‘ + ’, depois mais uma expressão aritmética, e finalmente o símbolo ‘) ’. A idéia é que o que aparece com ângulos é algo que precisa ser substituido, com uma das opções que aparecem no lado direito de alguma regra que começa com ele.

Começando com o $\langle ArEx\rangle$ ficamos substituindo até não aparece mais nada em ângulos. Et voilà: neste momento temos criado uma expressão aritmética.

• **EXEMPLO 4.99.**
Use as regras (1)–(2) da Nota 4.98 acima para criar duas expressões aritmética.
RESOLUÇÃO. Começando usando a regra (2), temos:

$$\begin{aligned}\underline{\langle ArEx\rangle} &\overset{(2)}{\rightsquigarrow} (\langle ArEx\rangle + \underline{\langle ArEx\rangle})\\ &\overset{(1)}{\rightsquigarrow} (\underline{\langle ArEx\rangle} + 3)\\ &\overset{(2)}{\rightsquigarrow} ((\underline{\langle ArEx\rangle} + \langle ArEx\rangle) + 3)\\ &\overset{(1)}{\rightsquigarrow} ((128 + \underline{\langle ArEx\rangle}) + 3)\\ &\overset{(1)}{\rightsquigarrow} ((128 + 0) + 3)\end{aligned}$$

Começando usando a regra (1), temos:

$$\underline{\langle ArEx\rangle} \overset{(1)}{\rightsquigarrow} 17$$

Isto sendo nosso primeiro exemplo de uso de BNF, em cada expressão que fica na parte esquerda dum ‘ $\rightsquigarrow$ ’ sublinhei o foco atual (o que escolhi para ser substituido nesse passo). Em geral, não vamos fazer isso.

▸ **EXERCÍCIO x4.65.**
Mostre como usar a Nota 4.98 para gerar a expressão aritmética $((1 + (2 + 2)) + 3)$. (x4.65 H 0)

! **4.100. Cuidado.** Essa coisinha aí, a ‘$(\langle ArEx\rangle + \langle ArEx\rangle)$’ que parece no lado direito da Nota 4.98 pode dar a impressão errada que só podemos criar expressões de aritmética onde a soma é aplicada nos mesmos termos, por exemplo, $(1+1)$, $(5+5)$, $((1+1)+(1+1))$, etc. *Não é o caso!* Isso deve ser óbvio já pelo Exemplo 4.99. Não pense então nos ‘ $\langle Bla\rangle$ ’ como variáveis, nem no ‘ ::= ’ como igualdade. Numa expressão como a ‘$y = x + x$’ o termo ‘x’ deve denotar o mesmo objeto em ambas as suas instâncias.

? **Q4.101. Questão.** Quais são uns defeitos dessa primeira tentativa? O que podemos fazer para a melhorar?

!! SPOILER ALERT !!

Resposta. Umas deficiências são:
(1) A linguagem gerada por essa gramática não é suficiente para representar expressões que envolvem outras operações, como $-$, $(\cdot)$, $\div$, etc.
(2) A regra (1) tem uma infinitade de casos (graças aos '$\cdots$').
(3) As regras e os nomes escolhidos não refletem bem nossa idéia.

▸ **EXERCÍCIO x4.66.**
Apenas alterando a segunda regra da Nota 4.98, resolva a primeira deficiência. (x4.66H1)

4.102. Uma segunda tentativa. A solução que encontramos no Exercício x4.66 não é a coisa mais elegante do mundo. Tem muita repetição que podemos evitar, definindo uma nova regra em nossa gramática:

Γ4.103. Gramática (ArEx (2)).

(1) $\langle ArEx\rangle ::= 0 \mid 1 \mid 2 \mid 3 \mid \cdots$
(2) $\langle ArEx\rangle ::= (\langle ArEx\rangle\,\langle BinOp\rangle\,\langle ArEx\rangle)$
(3) $\langle BinOp\rangle ::= + \mid - \mid \cdot \mid \div$

Bem melhor! Mas ainda a gramática não refleta bem nossa idéia. Podemos melhorá-la, com mais regras e com nomes melhores que deixam mais claras nossas intenções:

Γ4.104. Gramática (ArEx (3)).

(0) $\langle ArEx\rangle ::= \langle Num\rangle \mid \langle OpEx\rangle$
(1) $\langle Num\rangle ::= 0 \mid 1 \mid 2 \mid 3 \mid \cdots$
(2) $\langle OpEx\rangle ::= (\langle ArEx\rangle\,\langle BinOp\rangle\,\langle ArEx\rangle)$
(3) $\langle BinOp\rangle ::= + \mid - \mid \cdot \mid \div$

Falta achar um jeito para remover esses '$\cdots$' ainda, mas vamos deixar isso para depois (Problema Π4.14).

! **4.105. Cuidado.** Como conseguimos separar o que é sintaxe da linguagem que estamos definindo a partir duma gramática da sintaxe da *metalinguagem* que usamos para descrever essa gramática? Por exeplo, na (2) da Gramática Γ4.104, na sua parte direita,temos uma expressão cujo primeiro caracter é o '(' e depois... continua com o caracter '$\langle$'?

Claro que não, e parece que necessitamos esses ângulos na nossa metalinguagem para tirar essa ambigüidade. Mas muitas vezes não existe esse perigo, pois podemos inferir se algo é para ser substituido ou se é sintaxe da linguagem-objeto mesmo: *caso que aparece no lado esquerdo de alguma das regras da nossa gramática, é para ser substituido.* Aqui um exemplo duma gramática escrita nesse jeito que define uma linguagem importantíssima que vamos amar bastante, logo no Capítulo 4:

Γ4.106. Gramática (N, de «Não vou dizer»).

$$N \ ::= \ \mathrm{O} \mid \mathrm{S}N$$

▸ **EXERCÍCIO x4.67.**
Quais são umas das palavras que podes gerar com a Gramática Γ4.106? Podes pensar de algum uso para essa linguagem? (x4.67 H 0)

Problemas

▸ **PROBLEMA Π4.14.**
Usando BNF, defina uma gramática para a linguagem de todos os numerais que representam os naturais no sistema decimal. A embuta na gramática das expressões aritméticas Gramática Γ4.104 chegando assim numa gramática que gera a mesma linguagem, mas sem usar "$\cdots$". (Π4.14 H 0)

▸ **PROBLEMA Π4.15.**
Aumente tua gramática do Problema Π4.14 para gerar expressões aritméticas que usam o operador unitário (e postfixo) do factorial, que denotamos com !, escrevendo por exemplo $8!$ para o factorial de 8. Note que não usamos parenteses para aplicar o factorial:

$$((2+3!)! \cdot 0!!)$$

(Π4.15 H 0)

▸ **PROBLEMA Π4.16.**
Aumenta tua gramática do Problema Π4.15 para gerar expressões aritméticas que usam as variáveis

$$x, y, z, x', y', z', x'', y'', z'', x''', y''', z''', \ldots$$

(Π4.16 H 0)

▸ **PROBLEMA Π4.17 (Notação polonesa).**
Demonstre que não podemos simplesmente apagar as parenteses da nossa gramática de $\langle ArEx \rangle$ sem perder uma propriedade importantíssima da nossa linguagem (qual?). Experimente com a gramática

$$\begin{aligned}
(0) \qquad \langle PolArEx \rangle &::= \langle Num \rangle \mid \langle OpEx \rangle \\
(1) \qquad \langle Num \rangle &::= 0 \mid 1 \mid 2 \mid 3 \mid \cdots \\
(2) \qquad \langle OpEx \rangle &::= \langle BinOp \rangle \langle PolArEx \rangle \langle PolArEx \rangle \\
(3) \qquad \langle BinOp \rangle &::= + \mid - \mid \cdot \mid \div
\end{aligned}$$

Escreva uns dos seus termos. Supondo que cada símbolo de $\langle Num \rangle$ é apenas um símbolo (por exemplo o ‘ 15 ’ é um símbolo atômico e não algo composto dos ‘ 1 ’ e ‘ 5 ’), observe que com essa notação (chamada *notação Polonesa* ou *notação Łukasiewicz*) não precisamos de parenteses! Como escreverias nessa linguagem as expressões correspondentes às:

$$1 + 2; \qquad 3 \cdot (2 + 4) + 6; \qquad 2 \cdot 3 + 3 \cdot (7 + 8 \cdot 2)\,?$$

(Π4.17H0)

▸ **PROBLEMA Π4.18.**
Defina linguagens: uma de logica proposicional e uma de lógica de predicados que usam notação Polonesa (Problema Π4.17). Faça um bom trabalho, definindo açúcares sintácticos e abreviações. E sobre precedências e associatividades sintácticas? (Π4.18H0)

§115. Uma linguagem de numerais binários

§116. Tipos de expressões

• **EXEMPLO 4.107.**
Defina uma função $f : \mathfrak{L}_0 \to \mathbb{N}$ que calcula o número de conectivos binários que aparecem na sua entrada. Use-lá para calcular os conectivos binários da expressão

$$\neg(P_4 \to (P_9 \wedge \neg P_9)).$$

Resolução. Seguindo a definição de $\mathfrak{L}_0$, cada um dos seus elementos é formado por uma de certas regras. Basta escrever então como calcular o número desejado para cada um desses casos:

$$\begin{array}{lcl}
(\mathrm{BC}_P) & f(p) = 0, & (p \in \mathrm{Pvar}) \\
(\mathrm{BC}_\neg) & f(\neg A) = f(A), & (A \in \mathfrak{L}_0) \\
(\mathrm{BC}_\to) & f((A \to B)) = f(A) + 1 + f(B), & (A, B \in \mathfrak{L}_0) \\
(\mathrm{BC}_\wedge) & f((A \wedge B)) = f(A) + 1 + f(B), & (A, B \in \mathfrak{L}_0) \\
(\mathrm{BC}_\vee) & f((A \vee B)) = f(A) + 1 + f(B), & (A, B \in \mathfrak{L}_0)
\end{array}$$

Preguiçosamente, podemos condensar as três últimas equações em úma só, assim:

$$f((A \heartsuit B)) = f(A) + 1 + f(B), \quad (A, B \in \mathfrak{L}_0, \text{ e } \heartsuit \in \{\to, \wedge, \vee\})$$

Aplicando nossa função na fórmula dada calculamos:

$$\begin{array}{rll}
f(\neg(P_4 \to (P_9 \wedge \neg P_9))) &= f((P_4 \to (P_9 \wedge \neg P_9))) & (\text{por } \mathrm{BC}_\neg) \\
&= f(P_4) + 1 + f((P_9 \wedge \neg P_9)) & (\text{por } \mathrm{BC}_\to) \\
&= 0 + 1 + f((P_9 \wedge \neg P_9)) & (\text{por } \mathrm{BC}_P) \\
&= 0 + 1 + (f(P_9) + 1 + f(\neg P_9)) & (\text{por } \mathrm{BC}_\wedge) \\
&= 0 + 1 + (0 + 1 + f(\neg P_9)) & (\text{por } \mathrm{BC}_P) \\
&= 0 + 1 + (0 + 1 + f(P_9)) & (\text{por } \mathrm{BC}_\neg) \\
&= 0 + 1 + (0 + 1 + 0) & (\text{por } \mathrm{BC}_P) \\
&= 2 &
\end{array}$$

§117. Uma pequena linguagem de programação

§118. Indução em tal coisa

4.108. Indução em tal coisa. Até agora usamos indução para demonstrar proposições da forma

$$\text{para todo } x : \alpha,\ \varphi(x)$$

onde α sempre é um tipo que definimos indutivamente ou da forma

$$\text{para todo } x \in S,\ \varphi(x)$$

onde S é um conjunto como o dos inteiros positivos, sobre qual temos demonstrado um teorema de induç ou um Também já encontramos como "hackear a regra" escolhendo um apropriado $\varphi(-)$, conseguindo assim demonstrar proposições que variaram um pouco do padrão original. Bora hackear pouco mais!

4.109. Todo conjunto finito. Vamos supor que estamos tentando demostrar algo da forma

$$\text{para todo conjunto } S,\ \varphi(S).$$

Podemos usar indução? Parece que estamos bem longe do padrão permitido, essa mudança de «todo inteiro positivo» para «todo conjunto» não vai ser tão fácil de hackear como quando mudamos para conseguir um «todo natural maior que ℓ». E se for realmente «todo conjunto» podemos esquecer a indução que aprendemos até agora; mas se for «todo conjunto *finito*»? Tipo assim:

$$\text{para todo conjunto finito } S,\ \varphi(S).$$

? **Q4.110. Questão.** Agora podemos usar indução sim, mas em que?

!! SPOILER ALERT !!

Resposta. Indução *no tamanho de* S.

▸ **EXERCÍCIO x4.68.**
Podemos demonstrar o princípio da boa ordem usando indução no tamanho do subconjunto A? (x4.68H0)

D4.111. Definição (Cardinalidade). Definimos a cardinalidade $|A|$ dum conjunto finito e habitado A pelas:

$$|A| = 1 \iff A \text{ é um singleton}$$

$$|A| = n+1 \iff (\exists a \in A)(\exists A' \subseteq A)\left[a \notin A' \;\&\; |A'| = n \;\&\; \underbrace{(\forall x \in A)[\, x = a \text{ ou } x \in A'\,]}_{A \subseteq \{a\} \cup A'} \right]$$

Se existe $n \in \mathbb{N}$ tal que $|A| = n$ dizemos que A é *finito*.

Λ4.112. Lema. *Qualquer conjunto finito de números A habitado, possui mínimo.*

▸ Esboço. Por indução no tamanho do conjunto. A base é trivial: um conjunto com apenas um membro a, tem o a como mínimo. Seja $k \geq 1$ tal que

(HI) todos os conjuntos de tamanho k possuem mínimo.

Considere um conjunto A de tamanho $k+1$, ou seja,

$$A = \{a_1, \ldots, a_k, a_{k+1}\}.$$

Pela hipótese indutiva sabemos que $\{a_1, \ldots, a_k\}$ possui mínimo m. Agora o menor membro do A é o menor dos m e a_{k+1}. □ (Λ4.112P)

▸ **EXERCÍCIO x4.69.**
Faria sentido trocar o '$(\exists a \in A)$' por '$(\forall a \in A)$' na fim do Lema Λ4.112? (x4.69H0)

Intervalo de problemas

▸ **PROBLEMA Π4.19.**
Denotamos a operação de concatenação de strings por $(+\!\!+)$. Dois alunos definiram com as maneiras seguintes a "exponenciação":

(L1) ${}^0s = \varepsilon$ $\qquad$ $s^0 = \varepsilon$ (R1)

(L2) ${}^ns = {}^{n-1}s +\!\!+ s$ $\qquad$ $s^n = s +\!\!+ s^{n-1}$ (R2)

onde ε é o string vazio "", que é uma *identidade* da concatenação, ou seja, que satisfaz:

(E) $$(\forall s)[\, \varepsilon +\!\!+ s = s = s +\!\!+ \varepsilon\,].$$

Demonstre que as duas definições são equivalentes, ou seja, que para todo string s e todo $n \geq 0$, ${}^ns = s^n$. Cuidado: a operação $+\!\!+$ é associativa mas não comutativa: 'oimundo' e 'mundooi' são palavras diferentes! (Π4.19H123)

Problemas

Leitura complementar

Recursão e indução vamos ficar usando o tempo todo. Mais pra frente vamos mergulhar na teoria desses assuntos; mas sugiro paciência por enquanto, e *ganhar experiência trabalhando* com recursão e indução.

Sobre o princípio da boa ordem e indução, dê uma olhada no **[BM77b: §§1.4–1.5]**.

Neste capítulo tivemos nosso primeiro contato com *programação funcional*. Para o ansioso e animado-para-programar leitor recomendo se jogar no **[BW88]**. Além disso, obviamente brincar com uma linguagem puramente funcional é essencial; sobre programação funcional em Haskell: **[Bir14]**, **[Hut16]**, **[Bir98]**, **[Lip12]**.

TODO Divulgar Lean and SML

Vale muito a pena investir em trabalhar com uma implementação como a Agda ou o Coq. Ambos podem ser vistos tanto como uma linguagem de programação funcional, quanto como um *proof assistant*. Dois textos excelentes para inciantes que meu leitor é muito recomendado começar desde já estudar são os **[PdAC+17]** (que usa Coq) e o **[WK18]** (que usa Agda).

Para aprofundar ainda mais em recursão e indução consulte os **[Acz77]** e **[Mos14]**, mas sugiro fazer isso bem depois, pois podem aparecer pesados demais neste momento.

CAPÍTULO 5

COMBINATÓRIA ENUMERATIVA

TODO terminar e arrumar

§119. Princípios de contagem

5.1. Informalmente. Queremos contar todas as maneiras possíveis para algo acontecer, certas configurações, certos objetos ser escolhidos, ou ordenados, etc. Baseamos nossas idéias em dois princípios de contagem: da *adição* e da *multiplicação*.

O princípio da adição, informalmente: Se podemos agrupar todos esses objetos em grupos *distintos*, tais que cada objeto pertence em *exatamente um* grupo, o número total dos objetos é igual o somatório dos tamanhos dos grupos.

O princípio da multiplicação, informalmente: Se cada configuração pode ser descrita completamente em n passos, onde para o primeiro passo temos a_1 opções, para o segundo passo temos a_2 opções, etc., e *em cada passo a quantidade das opções disponíveis não depende nas escolhas anteriores*, então existem em total $a_1 a_2 \cdots a_n$ configurações possíveis.

5.2. Princípio da adição. *Seja A conjunto finito, e $A_1, \ldots, A_n$ subconjuntos dele tais que cada elemento $a \in A$, pertence em exatamente um dos A_i. Logo,*

$$|A| = \sum_{i=1}^{n} |A_i|.$$

5.3. Princípio da multiplicação. *Sejam $A_1, \ldots, A_n$ conjuntos finitos. Logo*

$$|A_1 \times \cdots \times A_n| = |A_1| \cdots |A_n|.$$

- **EXEMPLO 5.4.**

De quantas maneiras podemos escrever um string de tamanho 3...

(i) Usando o alfabeto $\{\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots, \mathtt{X}, \mathtt{Y}, \mathtt{Z}\}$?
(ii) Usando o mesmo alfabeto, mas proibindo o mesmo caractere se repetir no string?

RESOLUÇÃO. Consideramos a formação de cada string em passos, caractere a caractere. Temos 3 posições para colocar os caracteres: $_\,_\,_$.

Para a questão (i), temos: 26 maneiras para escolher o primeiro caractere, 26 para o segundo, e 26 para o último:

$$\underbrace{_}_{26}\ \underbrace{_}_{26}\ \underbrace{_}_{26}.$$

A escolha em cada passo não é afeitada por as escolhas dos passos anteriores. Logo, pelo princípio da multiplicação tem

$$26 \cdot 26 \cdot 26 = 26^3$$

strings possíveis.

Para a questão (ii), temos: 26 maneiras para escolher o primeiro caractere, 25 para o segundo (todos menos aquele que escolhemos no passo anterior), e 24 para o último (similarmente):

$$\underbrace{_}_{26}\ \underbrace{_}_{25}\ \underbrace{_}_{24}\,.$$

Agora a escolha em cada passo realmente *é afeitada* por as escolhas dos passos anteriores! Por exemplo, se no primeiro passo escolher o caractere `C`, para o segundo passo as opções incluem o caractere `A`; mas se no primeiro passo escolher o caractere `A`, as opções para o segundo mudam: não temos essa opção mais. *Mesmo assim, podemos usar o princípio da multiplicação!* Por quê? As escolhas dos passos anteriores afeitam *quais* são as escolhas do passo atual, mas não afeitam *quantas* elas são! Por isso, chegamos no resultado aplicando mais uma vez o princípio da multiplicação: temos

$$26 \cdot 25 \cdot 24$$

maneiras possíveis.

▸ **EXERCÍCIO x5.1.**
Temos 4 presentes e queremos dar para 3 crianças tal que cada criança vai receber apenas um presente.

(i) De quantas maneiras podemos disribuir os presentes para as crianças?
(ii) O que muda se as crianças são 4? Explique.

(x5.1H0)

▸ **EXERCÍCIO x5.2.**
De quantas maneiras podemos escrever strings de tamanho 2 usando o alfabeto

$$\{\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D}\}\,,$$

tais que as letras aparecem em ordem que concorda com a do alfabeto? Por exemplo os string `AC`, `BB`, e `CD` são aceitáveis, mas os `DC` e `BA`, não. (x5.2H12)

§120. Permutações e combinações

? **Q5.5. Questão.** De quantas maneiras podemos escolher r objetos de n?

Essa questão é bastante ambígua; por exemplo: Os n objetos são todos distintos? Podemos repetir o mesmo objeto na nossa escolha?

D5.6. Definição. Usamos os símbolos:

$$\begin{aligned} P_{\mathsf{tot}}(n): &\quad \text{o número de permutações totais de } n \text{ objetos} \\ P(n,r): &\quad \text{o número de } r\text{-permutações de } n \text{ objetos} \\ C(n,r): &\quad \text{o número de } r\text{-combinações de } n \text{ objetos} \end{aligned}$$

Onde entendemos que:

(i) os n objetos são distíntos;
(ii) não podemos repeti-los.

Observe que as permutações totais são apenas casos especiais de r-permutações. Na literatura encontramos r-permutações também com o nome *arranjos*, mas nós vamos evitar esse termo aqui para evitar confusão.

5.7. Proposição (Permutações totais).

$$P_{\mathsf{tot}}(n) = n!.$$

5.8. Proposição (Permutações).

$$P(n,r) = \frac{n!}{(n-r)!}.$$

5.9. Proposição (Combinações).

$$C(n,r) = \frac{n!}{(n-r)!\,r!}.$$

- **EXEMPLO 5.10.**

10 amigos têm vontade viajar com um carro de 5 vagas. De quantas maneiras diferentes 5 deles podem entrar no carro? Considere que o que diferencia mesmo a configuração são apenas a posição do motorista e do copiloto.

RESOLUÇÃO. Vamos ver dois jeitos diferentes para contar essas configurações:

JEITO 1: Escrevendo

$$C(10,1)\cdot C(9,1)\cdot C(8,3)$$

já é meio auto-explicativo: formamos cada configuração em passos: (i) escolher o motorista; (ii) escolher o copiloto; (iii) escolher os passangeiros de trás.

JEITO 2: Outra método para formar cada configuração seria: (i) escolher os 5 que vão entrar no carro; (ii) escolher qual vai ser o motorista; (iii) escolher qual vai ser o copiloto. pensando assim chegamos no cálculo

$$\underbrace{C(10,5)}_{\text{(i)}}\cdot\underbrace{C(5,1)}_{\text{(ii)}}\cdot\underbrace{C(4,1)}_{\text{(iii)}}.$$

Olhando para os dois cálculos

$$C(10,1)\cdot C(9,1)\cdot C(8,3) \stackrel{?}{=} C(10,5)\cdot C(5,1)\cdot C(4,1)$$

não é óbvio que seus valores são iguais. Calculamos

$$C(10,1)\cdot C(9,1)\cdot C(8,3) = 10\cdot 9\cdot \frac{8!}{5!\,3!} = \frac{10!}{5!\,3!}$$
$$C(10,5)\cdot C(5,1)\cdot C(4,1) = \frac{10!}{5!\,5!}\cdot 5\cdot 4 \;\; = \frac{10!}{5!\,3!}$$

e respondemos (felizmente) que em total temos

$$\frac{10!}{5!\,3!} = \frac{10\cdot 9\cdot 8\cdot 7\cdot 6}{3!} = 10\cdot 9\cdot 8\cdot 7 = 5040$$

configurações diferentes.

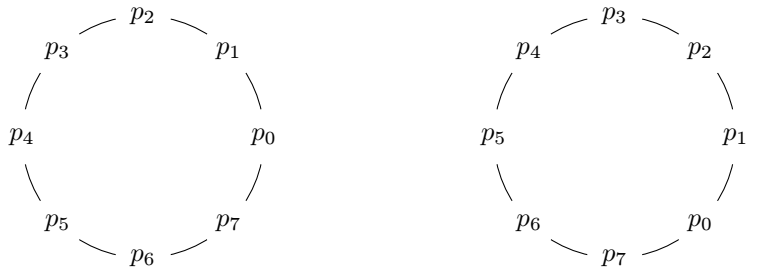
§121. Permutações cíclicas

• **EXEMPLO 5.11.**
8 pessoas querem dançar uma dança em qual todos precisam formar um ciclo pegando as mãos (e olhando para o interior do ciclo). Em quantas configurações diferentes essa dança pode começar?

RESOLUÇÃO. Vamos resolver esse problema seguindo duas idéias bem diferentes:

IDÉIA 1. Consideramos primeiro a questão: "*de quantas maneiras podemos permutar as* 8 *pessoas numa ordem?*" Respondemos 8!, o número das permutações totais de 8 objetos (sabendo que hipercontamos para o problema original). Mas podemos calcular *exatamente quanto* hipercontamos: cada resposta do problema original corresponde em exatamente 8 respostas do problema novo (uma para cada "circular shift"). Então basta só dividir a "hiperconta" por 8, e chegamos no resultado final: 8!/8, ou seja, 7!.

IDÉIA 2. *Fixamos uma pessoa como "determinante" da configuração;* a idéia sendo que para comparar duas configurações nós vamos começar com o determinante, e depois comparar em ordem fixa o resto da configuração (por exemplo indo cada vez de uma pessoa para quem tá no lado direito dela). Assim, para cada permutação total das 7 outras pessoas, temos uma permutação circular das 8 e vice-versa, ou seja, a resposta final é 7!.



Uma configuração do 5.11 representada em dois jeitos diferentes no papel.

Generalizando concluimos que:

5.12. Proposição. *As configurações circulares diferentes de n objetos, $n > 0$ são*

$$(n-1)!.$$

▸ **EXERCÍCIO x5.3.**
O que mudará na contagem do Exemplo 5.11, se cada dançador pode olhar ou para o interior ou para o exterior do círculo? (x5.3H12)

▸ **EXERCÍCIO x5.4.**
O que mudará na contagem do Exemplo 5.11, se temos 4 mulheres e 4 homens e as regras da dança mandam alternar os sexos na configuração? (x5.4H12)

▸ **EXERCÍCIO x5.5.**
Temos 8 miçangas diferentes, e queremos pôr todas numa corrente para criar uma pulseira. Quantas maneiras diferentes temos para o criar? (x5.5 H 1 2)

§122. Juntos ou separados

• **EXEMPLO 5.13.**
Suponha que 8 pessoas A, B, C, D, E, F, G, H querem sentar num bar mas C e D querem sentar juntos. De quantas maneiras isso pode acontecer?
Resolução. *Vamos imaginar que C e D são uma pessoa, chamada CD.* Nos perguntamos de quantas maneiras as 7 pessoas A, B, CD, E, F, G, H podem sentar numa mesa de bar com 7 banquinhos. A resposta é os permutações totais de tamanho 7, ou seja, $7!$. Mas para cada configuração desse problema, correspondem *duas* configurações do problema original, porque os C e D podem sentar em duas ordens diferentes juntos. A resposta final: $7! \cdot 2$.

▸ **EXERCÍCIO x5.6.**
Suponha que 8 pessoas A, B, C, D, E, F, G, H querem jantar numa mesa de bar. Em quantas configurações diferentes eles podem sentar se. . . :
(1) os C e D e E querem sentar juntos;
(2) os F e G não podem sentar juntos;
(3) as duas restricções (1) e (2).

(x5.6 H 1)

Generalizando:

5.14. Proposição. *O número das permutações totais de m objetos distintos com a restricção que certos c deles tem que estar consecutivos é*

$$(m - c + 1)!\, c!.$$

§123. Permutações de objetos não todos distintos

? **Q5.15. Questão.** De quantas maneiras podemos permutar n objetos se eles não são todos distíntos?

• **EXEMPLO 5.16.**
Conte todas as palavras feitas por permutações das 12 letras da palavra

PESSIMISSIMO.

Resolução. Vamos contar em dois jeitos diferentes:

Idéia 1: Construimos cada palavra possível "em passos", usando o princípio da multplicação para achar o número total.

Começamos com 12 espaços:	_ _ _ _ _ _ _ _ _ _ _ _	
escolhemos onde colocar o P:	_ _ _ _ _ _ _ _ P _ _ _	tivemos $C(12,1)$ opções;
depois o E:	_ _ _ _ _ _ _ _ P _ E _	tivemos $C(11,1)$ opções;
depois os 4 S:	_ _ S S _ S S _ P _ E _	tivemos $C(10,4)$ opções;
depois os 3 I:	_ I S S I S S I P _ E _	tivemos $C(6,3)$ opções;
depois os 2 M:	M I S S I S S I P _ E M	tivemos $C(3,2)$ opções;
e finalmente o O:	M I S S I S S I P O E M	tivemos $C(1,1)$ opção.

Pelo princípio da multiplicação, a resposta é o produto

$$\underbrace{C(12,1)}_{\texttt{P}}\underbrace{C(11,1)}_{\texttt{E}}\underbrace{C(10,4)}_{\texttt{4S}}\underbrace{C(6,3)}_{\texttt{3I}}\underbrace{C(3,2)}_{\texttt{2M}}\underbrace{C(1,1)}_{\texttt{O}} = \frac{12!}{11!\,1!}\frac{11!}{10!\,1!}\frac{10!}{6!\,4!}\frac{6!}{3!\,3!}\frac{3!}{1!\,2!}\frac{1!}{0!\,1!}$$
$$= \frac{12!}{1!\,1!\,4!\,3!\,2!\,1!} = \frac{12!}{4!\,3!\,2!}.$$

Idéia 2: Contamos as maneiras como se todas as letras fossem distintas, por exemplo marcando cada letra com índices:

$$\texttt{P}_1\ \texttt{E}_1\ \texttt{S}_1\ \texttt{S}_2\ \texttt{I}_1\ \texttt{M}_1\ \texttt{I}_2\ \texttt{S}_3\ \texttt{S}_4\ \texttt{I}_3\ \texttt{M}_2\ \texttt{O}_1\,.$$

Sabemos que são 12! e que assim temos *hipercontado* para nosso problema. Por exemplo, a palavra MISSISSIPOEM corresponde em várias palavras do problema novo; escrevemos três delas aqui como exemplos:

$$\texttt{M I S S I S S I P O E M} \rightsquigarrow \left\{\begin{array}{l} \texttt{M}_1\ \texttt{I}_1\ \texttt{S}_1\ \texttt{S}_2\ \texttt{I}_2\ \texttt{S}_3\ \texttt{S}_4\ \texttt{I}_3\ \texttt{P}_1\ \texttt{O}_1\ \texttt{E}_1\ \texttt{M}_2 \\ \texttt{M}_2\ \texttt{I}_1\ \texttt{S}_1\ \texttt{S}_2\ \texttt{I}_2\ \texttt{S}_3\ \texttt{S}_4\ \texttt{I}_3\ \texttt{P}_1\ \texttt{O}_1\ \texttt{E}_1\ \texttt{M}_1 \\ \texttt{M}_2\ \texttt{I}_1\ \texttt{S}_4\ \texttt{S}_3\ \texttt{I}_2\ \texttt{S}_2\ \texttt{S}_1\ \texttt{I}_3\ \texttt{P}_1\ \texttt{O}_1\ \texttt{E}_1\ \texttt{M}_1 \\ \vdots \end{array}\right\} \ldots \text{quantas?}$$

Mas é fácil calcular quanto hipercontamos: *cada* palavra do problema original corresponde em exatamente tantas palavras quantas as maneiras de permutar cada grupo de letras "subindicadas" entre si, ou seja:

$$\underbrace{1!}_{\texttt{P}} \cdot \underbrace{1!}_{\texttt{E}} \cdot \underbrace{4!}_{\texttt{S}} \cdot \underbrace{3!}_{\texttt{I}} \cdot \underbrace{2!}_{\texttt{M}} \cdot \underbrace{1!}_{\texttt{O}}$$

maneiras. Para responder então, basta dividir o número da "hipercontagem" por esse:

$$\frac{12!}{4!\,3!\,2!}.$$

Pronto.

▸ **EXERCÍCIO x5.7.**
Escolhendo outra ordem de colocar as letras na Idéia 1 do Problema Π5.12 nossas opções em cada passo seriam diferentes. Explique porque podemos usar o princípio da multiplicação mesmo assim. (x5.7 H 1)

§124. Número de subconjuntos

? **Q5.17. Questão.** Quantos subconjuntos dum conjunto finito existem?

5.18. Idéia 1. Começamos com um exemplo de um conjunto A de tamanho 6:

$$A = \{a, b, c, d, e, f\}.$$

Uns subconjuntos de A são os:

$$\{a, d, e\}, \qquad \emptyset, \qquad \{a\}, \qquad \{b, c, e, f\}, \qquad A, \qquad \{f\}, \qquad \dots$$

Queremos contar todos os subconjuntos de A. Vamos *traduzir o problema* de contar os subconjuntos do A para um problema que envolve n-tuplas de dois símbolos "0" e "1", "sim" e "não", "$\in$" e "$\notin$", etc. (Obviamente *quais* são esses símbolos não afeita nada; o que importa é que são dois símbolos distintos.) Podemos associar agora cada dessas tuplas (ou strings) de tamanho n para um subconjunto de A, e vice-versa, chegando numa correspondência entre as duas colecções de objetos. Naturalmente associamos, por exemplo,

a	b	c	d	e	f
1	0	0	1	1	0
0	0	0	0	0	0
1	0	0	0	0	0
0	1	1	0	1	1
1	1	1	1	1	1
0	0	0	0	0	1
⋮	⋮	⋮	⋮	⋮	⋮

Strings de tamanho 6 do alfabeto $\{0,1\}$

$\leftrightsquigarrow$

$\{a, d, e\}$
$\emptyset$
$\{a\}$
$\{b, c, e, f\}$
A
$\{f\}$
⋮

Subconjuntos de A

e verificamos que realmente cada configuração do problema original de subconjuntos corresponde exatamente numa configuração do problema novo dos strings e vice-versa.

O que ganhamos? Sabemos como contar todos esses strings: são 2^6. Concluimos que os subconjuntos do A são 2^6 também.

Generalizando essa idéia chegamos no resultado:

5.19. Proposição. *Seja A conjunto finito.*

$$|\wp A| = 2^{|A|}.$$

5.20. Idéia 2. Um outro jeito para contar todos os subconjuntos dum dado conjunto A, seria os separar em grupos baseados no seu tamanho. Assim, percebos que esses subconjuntos são naturalmente divididos em $n+1$ colecções: subconjuntos com 0 elementos, com 1 elemento, ..., com n elementos.

O que ganhamos? Sabemos como contar os elementos de cada uma dessas colecções: para formar um subconjunto de tamanho r, precisamos escolher r dos n elementos, ou seja, existem $C(n, r)$ subconjuntos de tamanho r. Agora, pelo princípio da adição basta apenas somar: são $\sum_{i=0}^{n} C(n, i)$.

Qual o problema? Comparando essa solução com a do item 5.18, aqui temos a dificuldade de realmente calcular todos os n números $C(n,i)$ para os somar. O Exercício x5.8 mostre que na verdade, não é nada dificil calcular o somatório diretamente sem nem calcular nenhum dos seus termos separadamente!

5.21. Proposição. *Seja A conjunto finito.*

$$|\wp A| = \sum_{i=0}^{n} C(n,i), \qquad \text{onde } n = |A|.$$

Combinando as duas proposições chegamos num resultado interessante:

5.22. Corolário. *Para todo $n \in \mathbb{N}$,*

$$\sum_{i=0}^{n} \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

▸ **EXERCÍCIO x5.8.**
Esqueça o corolário e demonstre que:

$$\sum_{i=0}^{n} \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} \qquad = 2^n$$
$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0$$

(x5.8H1234)

§125. O triângulo de Pascal

5.23. As primeiras potências do binomial. Calculamos:

$$\begin{aligned}
(x+y)^0 &= 1\\
(x+y)^1 &= 1x + 1y\\
(x+y)^2 &= 1x^2 + 2xy + 1y^2\\
(x+y)^3 &= 1x^3 + 3x^2y + 3xy^2 + 1y^3\\
(x+y)^4 &= 1x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + 1y^4\\
(x+y)^5 &= 1x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + 1y^5\\
(x+y)^6 &= 1x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + 1y^6\\
(x+y)^7 &= 1x^7 + 7x^6y + 21x^5y^2 + 35x^4y^3 + 35x^3y^4 + 21x^2y^5 + 7xy^6 + 1y^7\\
(x+y)^8 &= 1x^8 + 8x^7y + 28x^6y^2 + 56x^5y^3 + 70x^4y^4 + 56x^3y^5 + 28x^2y^6 + 8xy^7 + 1y^8.
\end{aligned}$$

5.24. O triângulo de Pascal. Tomando os coeficientes acima criamos o triângulo seguinte, conhecido como *triângulo de Pascal*:

$$\begin{array}{ccccccccccc}
1 & & & & & & & & & & \\
1 & 1 & & & & & & & & & \\
1 & 2 & 1 & & & & & & & & \\
1 & 3 & 3 & 1 & & & & & & & \\
1 & 4 & 6 & 4 & 1 & & & & & & \\
1 & 5 & 10 & 10 & 5 & 1 & & & & & \\
1 & 6 & 15 & 20 & 15 & 6 & 1 & & & & \\
1 & 7 & 21 & 35 & 35 & 21 & 7 & 1 & & & \\
1 & 8 & 28 & 56 & 70 & 56 & 28 & 8 & 1 & & \\
\vdots & & & & & & & & & \ddots &
\end{array}$$

Observando o triângulo, percebemos que com umas exceções—quais?—cada número é igual à soma de dois números *na linha em cima*: aquele que fica na mesma posição, e aquele que fica na posição anterior. (Consideramos os "espaços" no triângulo como se fossem 0's.)

▸ **EXERCÍCIO x5.9.**
Escreva essa relação formalmente. (x5.9 H 1)

Θ5.25. Teorema. *Para todos inteiros positivos n e r temos:*

$$C(n,r) = C(n-1,r) + C(n-1,r-1).$$

▸ Esboço. Lembramos que $C(n,r)$ é o número das maneiras que podemos escolher r de n objetos. Fixe um dos n objetos e o denote por s, para agir como "separador de maneiras": separamos as maneiras de escolher em dois: aquelas que escolhem (entre outros) o s e aquelas que não o escolhem. Contamos cada colecção separadamente e somamos (princípio da adição) para achar o resultado:

$$C(n,r) = \underbrace{C(n-1,r)}_{\text{escolhas sem } s} + \underbrace{C(n-1,r-1)}_{\text{escolhas com } s}.$$

□

▸ **EXERCÍCIO x5.10.**
Demonstre o Teorema Θ5.25 para todos os $n, r \in \mathbb{N}$ com $0 < r < n$, usando como definição do símbolo $C(n,r)$ a

$$C(n,r) = \frac{n!}{(n-r)!\,r!}.$$

(x5.10 H 1)

▸ **EXERCÍCIO x5.11.**
Redefina o símbolo $C(n,r)$ para todo $n, r \in \mathbb{N}$ recursivamente com

$$\begin{aligned}
C(0,0) &= 1\\
C(0,r) &= 0\\
C(n,r) &= C(n-1,r) + C(n-1,r-1),
\end{aligned}$$

e demonstre que para todo $n, r \in \mathbb{N}$, $C(n,r) = \dfrac{n!}{(n-r)!\,r!}$. (x5.11 H 1)

5.26. Observação (Axiomas mais fortes do que precisamos). Para cada inteiro positivo, quantas vezes aparece no triângulo de Pascal? É imediato que o 1 aparece uma infinidade de vezes. Além disso, qualquer inteiro $x > 1$ só pode aparecer nas primeiras x linhas do triângulo—e de fato aparece pelo menos uma vez na própria x-ésima linha—algo que garanta também que nenhum outro inteiro pode aparecer uma infinidade de vezes. Até o momento que esta parágrafo foi escrita, o número com a maioria de ocorrências que conhecemos é o 3003, que ocorre 8 vezes:

$$3003 = \binom{3003}{1} = \binom{78}{2} = \binom{15}{5} = \binom{14}{6} = \binom{14}{8} = \binom{15}{10} = \binom{78}{76} = \binom{3003}{2}.$$

Para qualquer $x > 0$, denote por $m(x)$ a quantidade de vezes que x aparece no triângulo de Pascal até a x-ésima linha; assim

$$m(1) = 3, \quad m(2) = 1, \quad m(3) = 2, \quad m(4) = 2, \quad m(5) = 2,$$

e, visto como uma seqüência $(m_x)_x$, seus primeiros valores são[45]

$$(m_x)_x = 3, 1, 2, 2, 2, 3, 2, 2, 2, 4, 2, 2, 2, 2, 4, 2, 2, 2, 2, 3, 4, 2, 2, 2, \ldots$$

Singmaster conjecturou que existe uma cota superior para o conjunto dos seus valores $\{m_x\}_x$ e até este momento continua aberta. Sabemos apenas que $1, 2, 3, 4, 6, 8 \in \{m_x\}_x$.

?5.27. Conjectura (Singmaster). *A $(m_x)_x$ é cotada por cima, ou seja:*

$$(\exists b > 0)[\,\{m_x\}_x \leq b\,], \qquad \text{ou seja,} \qquad (\exists b > 0)(\forall x > 0)[\,m_x \leq b\,].$$

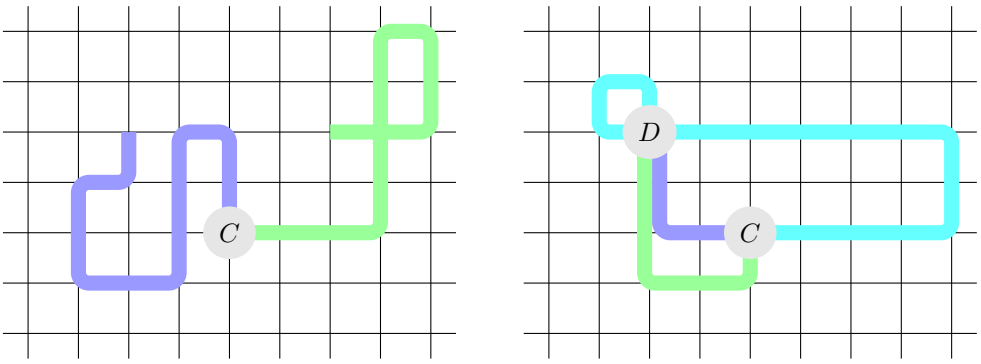
§126. Contando recursivamente

▸ **EXERCÍCIO x5.12.**
Defina uma função $f : \mathbb{N} \to \mathbb{N}$ que conta as seqüências feitas por os números 2 e 3 com soma sua entrada. Quantas seqüências de 2's e 3's existem cujos termos somam em 17? (x5.12H1234)

▸ **EXERCÍCIO x5.13.**
Defina uma função $g : \mathbb{N} \to \mathbb{N}$ que conta as seqüências feitas por os números 2 e 3 com soma sua entrada, em quais aparecem os dois números (2 e 3). Quantas seqüências de 2's e 3's existem cujos termos somam em 18? (x5.13H1234)

▸ **EXERCÍCIO x5.14 (Dirigindo na cidade infinita (sem destino)).**
No "meio" duma "cidade infinita", tem um motorista no seu carro. Seu carro tá parado numa intersecção onde tem 3 opções: virar esquerda; dirigir reto; virar direita. No seu depósito tem a unidades de combustível, e sempre gasta 1 para dirigir até a próxima intersecção. De quantas maneiras diferentes ele pode dirigir até seu combustível acabar? (Veja na figura, dois caminhos possíveis com $a = 12$.)

[45] A no(ta)ção de seqüências é introduzida pela Definição D6.35.



Caminhos possíveis para os exercícios x5.14 e x5.16 respectivamente.

(x5.14 H 1 2)

▸ **EXERCÍCIO x5.15 (Dirigindo na montanha infinita).**
No "meio" duma montanha de altura infinita, tem um motorista no seu carro. Seu carro tá parado numa intersecção onde tem 4 opções: dirigir subindo (gasta 4 unidades de combutível); dirigir descendo (gasta 1); dirigir na mesma altura clockwise (gasta 2); dirigir na mesma altura counter-clockwise (gasta 2). No seu depósito tem a unidades de combistível. De quantas maneiras diferentes ele pode dirigir até seu combustível acabar? (x5.15 H 1 2 3)

▸ **EXERCÍCIO x5.16 (Dirigindo na cidade infinita (com destino)).**
No "meio" duma "cidade infinita", tem um motorista no seu carro. Seu carro tá parado numa intersecção onde tem 4 opções: dirigir na direção do norte; do leste; do sul; do oeste. No seu depósito tem c unidades de combustível e sempre gasta 1 para dirigir até a próxima intersecção. De quantas maneiras diferentes ele pode dirigir até chegar no seu destino, que fica numa distância y unidades para norte e x para leste? Considere que números negativos representam descolamento para a direção oposta. (Veja na figura onde o carro C tem destino D, ou seja, seu descolamento desejado é de $x = -2$, $y = 2$.) (x5.16 H 1 2 3)

§127. Soluções de equações em inteiros

§128. Combinações com repetições

§129. O princípio da inclusão–exclusão

▸ **EXERCÍCIO x5.17.**
42 passangeiros estão viajando num avião.

- 11 deles não comem beef.
- 10 deles não comem peixe.

- 12 deles não comem frango.
- Os passangeiros que não comem nem beef nem frango são 6.
- O número de passangeiros que não comem nem beef nem peixe, é o mesmo com o número de passangeiros que não comem nem peixe nem frango.
- Os passangeiros que não comem nada disso são 3.
- Os passangeiros que comem tudo são 22.

Quantos são os passangeiros que não comem nem beef nem peixe? (x5.17 H 0)

§130. Probabilidade elementar

▸ **EXERCÍCIO x5.18 (Roleta russa).**
(Não tente isso em casa; vai acordar os vizinhos.) No jogo da roleta russa, uma única bala é posicionada num revolver de 6 balas e logo após o moinho é girado com força em tal forma que a posição da bala é desconhecida e "justa", ou seja, cada posição é igualmente provável de ter a bala. A partir disso, o jogador 1 pega a arma e atira na sua própria cabeça. Caso que sobreviveu, o jogador 2 faz a mesma coisa, e o jogo continua assim alterando esse processo até um jogador acaba se matando. Logo, a duração desse jogo é de 1 a 6 rodadas. Supondo que ambos os jogadores querem viver, algum dos dois tem vantagem? (x5.18 H 0)

▸ **EXERCÍCIO x5.19.**
O que muda se os jogadores giram o moinho do revolver antes de cada rodada e não apenas no começo do jogo? (x5.19 H 0)

§131. Desarranjos

§132. O princípio da casa dos pombos

§133. Funções geradoras e relações de recorrência

Problemas

▸ **PROBLEMA П5.1.**
Uma turma de 28 alunos tem 12 mulheres e 16 homens.

(a) De quantas maneiras podemos escolher 5 desses alunos, para formar um time de basquete? (Considere que as posições de basquete não importam).

(b) De quantas maneiras podemos escolher 6 desses alunos, para formar um time de volei, tal que o time tem pelo menos 4 homens? (Considere que as posições de volei não importam).
(c) De quantas maneiras podemos escolher 11 desses alunos, para formar um time de futebol, tal que o time tem exatamente 3 mulheres, e um homem goleiro? (Considere que a única posição de futebol que importa é do goleiro.)
(d) De quantas maneiras podemos escolher 3 times, um para cada esporte, sem restricção de sexo?

(Π5.1 H 0)

▸ **PROBLEMA Π5.2.**
Uma noite, depois do treino 3 times (uma de basquete, uma de vólei, e uma de futebol), foram beber num bar que foi reservado para eles. Como os jogadores de cada time querem sentar juntos, o dono arrumou duas mesas cíclicas, uma com 5 e outra com 6 cadeiras, e 11 cadeiras no bar.

De quantas maneiras diferentes eles podem sentar? (Considere que nas mesas cíclicas o que importa é apenas quem tá no lado de quem, mas no bar o que importa é a posição da cadeira mesmo.) (Π5.2 H 0)

▸ **PROBLEMA Π5.3.**
Considere os inteiros $1, 2, \ldots, 30$. Quantas das suas 30! permutações totais têm a propriedade que não aparecem múltiplos de 3 consecutivamente? (Π5.3 H 1 2 3)

▸ **PROBLEMA Π5.4.**
Numa turma de 28 alunos precisamos formar duas comissões de 5 e 6 membros. Cada comição tem seu presidente, seu vice-presidente, e seus membros normais. De quantas maneiras podemos formar essas comissões...

(a) ...sem restricções (cada um aluno pode participar nas duas comissões simultaneamente)?
(b) ...se nenhum aluno pode participar simultaneamente nas duas comissões?
(c) ...se os dois (únicos) irmãos entre os alunos não podem participar na mesma comissão, e cada aluno pode participar simultaneamente nas duas?

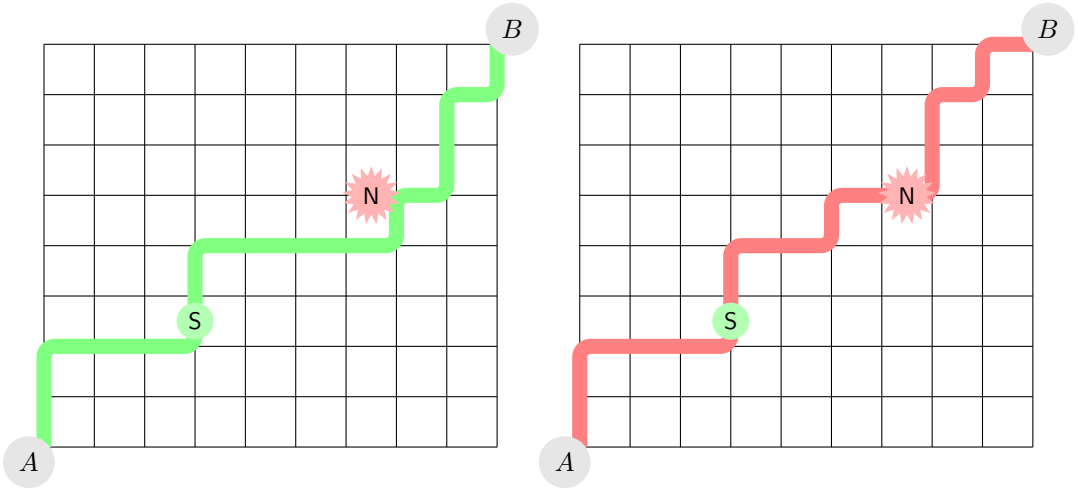
(Π5.4 H 0)

▸ **PROBLEMA Π5.5.**
Do alfabeto $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ desejamos formar strings de tamanho ℓ onde não aparece o substring `ab`. Em quantas maneiras podemos fazer isso? (Π5.5 H 0)

▸ **PROBLEMA Π5.6.**
Conte em quantas maneiras podemos cobrir um tabuleiro de dimensão $2 \times n$ com peças-dominô (ou seja, peças de dimensão 2×1). (Π5.6 H 1 2)

▸ **PROBLEMA Π5.7.**
Na figura abaixo temos um mapa (as linhas correspondem em ruas). Nikos quer caminhar do ponto A para o ponto B, *o mais rápido possível*.

(1) De quantas maneiras ele pode chegar?
(2) Se ele precisa passar pelo ponto S?
(3) Se ele precisa passar pelo ponto S mas quer evitar o ponto N?



Um caminho aceitável e um inaceitável no caso (3) do Problema Π5.7.

(Π5.7 H 0)

▸ **PROBLEMA Π5.8.**
Num jogo de lotéria, tem os números de 1 até 60:

01	02	03	04	05	06	07	08	09	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

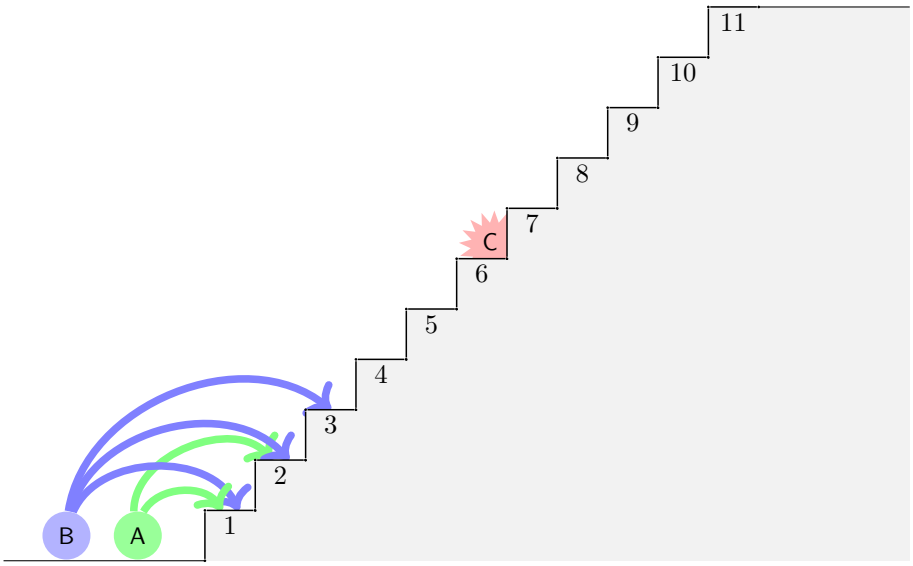
Os organizadores do jogo, escolhem aleatoriamente 6 números deles (sem repetições). Esses 6 números são chamados "a megasena". Um jogador marca pelo menos 6 números na sua lotéria e se conseguir ter marcados todos os 6 da megasena, ganha.(Marcando mais que 6 números, as chances do jogador aumentam, mas o preço da lotéria aumenta também.)

(1) Um jogador marcou 6 números. Qual a probabilidade que ele ganhe?
(2) Uma jogadora marcou 9 números. Qual a probabilidade que ela ganhe?
(3) Generalize para um jogo com N números, onde w deles são escolhidos, e com um jogador que marcou m números, sendo $w \leq m \leq N$.

(Π5.8 H 0)

▸ **PROBLEMA Π5.9.**
Aleco e Bego são dois sapos. Eles estão na frente de uma escada com 11 degraus. No 6o degrau, tem Cátia, uma cobra, com fome. Aleco pula 1 ou 2 degraus para cima. Bego, 1, 2 ou 3. E ele é tóxico: se Cátia comê-lo, ela morre na hora.

(1) Por enquanto, Cátia está dormindo profundamente.
   a. De quantas maneiras Aleco pode subir a escada toda?
   b. De quantas maneiras Bego pode subir a escada toda?
(2) Cátia acordou!
   a. De quantas maneiras Aleco pode subir a escada toda?



Os dois sapos do Problema Π5.9 e suas possibilidades para começar.

b. De quantas maneiras Bego pode subir a escada toda?

(3) Bego começou subir a escada... Qual é a probabilidade que Cátia morra? (Considere que antes de começar, ele já decidiu seus saltos e não tem percebido a existência da cobra.)

(Π5.9 H 1 2 3)

▸ **PROBLEMA Π5.10.**
Temos 6 músicos disponíveis, onde cada um toca:

Alex:	violão, guitarra, baixo	Daniel:	guitarra
Beatriz:	bateria	Eduardo:	piano, teclado, violão, fláuto
Cynthia:	saxofone, clarineto	Fagner:	guitarra, baixo, teclado

(Considere que uma banda precisa *pelo menos um membro*, todos os membros duma banda *precisam tocar pelo menos algo na banda*, e que cada banda é diferenciada pelos músicos e suas funções. Por exemplo: uma banda onde Alex toca o violão (apenas) e Beatriz a bateria, é diferente duma banda onde Alex toca o violão *e* a guitarra, e Beatriz a bateria, mesmo que seus membros são os mesmos.

(1) Quantas bandas diferentes podemos formar?
(2) Quantas bandas diferentes podemos formar com a restricção que nenhum músico tocará mais que um instrumento na banda (mesmo se em geral sabe tocar mais)?
(3) Quantas bandas diferentes podemos formar onde todos os músicos fazem parte da banda?

(Π5.10 H 0)

▸ **PROBLEMA Π5.11.**
De quantas maneiras podemos escrever um string ternário (usando o alfabeto $\{0, 1, 2\}$) de tamanho 7, tais que *não aparece neles o substring* 00.

Por exemplo:

0112220	é um string aceitável;
2001000	não é.

(Π5.11 H 1 2 3)

▸ **PROBLEMA Π5.12.**
Contar todas as palavras feitas por permutações das 12 letras da palavra

PESSIMISSIMO

onde...

(1) a palavra começa com P;
(2) todos os I aparecem *juntos*;
(3) os M aparecem *separados*;
(4) nenhum dos S aparece ao lado de outro S.

(Π5.12 H 1)

▸ **PROBLEMA Π5.13.**
De quantas maneiras podemos escrever um string usando o alfabeto de 26 letras

$$\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots, \mathtt{X}, \mathtt{Y}, \mathtt{Z},$$

tais que as vogais aparecem na ordem estrita alfabética, e as consoantes na ordem oposta? (As vogais sendo as letras A, E, I, O, U, Y.) Por exemplo:

TEDUCY	é um string aceitável;
DETUCY	não é ($\mathtt{D} \not> \mathtt{T}$);
TEDUCA	não é ($\mathtt{U} \not< \mathtt{A}$).

(1) ...se os strings são de tamanho 26 e os vogais aparecem todos juntos;
(2) ...se os strings são de tamanho 12 e aparecem todos os vogais;
(3) ...se os strings são de tamanho 3;
(4) ...se os strings são de tamanho ℓ, com $0 \leq \ell \leq 26$.

(Π5.13 H 0)

▸ **PROBLEMA Π5.14.**
Numa roleta dum cassino tem "pockets" (ou "casas") numerados com:

$$00, 0, 1, 2, \ldots, 36$$

e cada um deles é suficientemente profundo para caber até 8 bolinhas. O crupiê joga 8 bolinas na roleta no mesmo tempo. De quantas maneiras elas podem cair nos pockets se...

(i) ...as bolinhas são distintas e não importa sua ordem dentro um pocket.
(ii) ...as bolinhas são todas iguais.

(Π5.14 H 0)

▸ **PROBLEMA Π5.15.**
De quantas maneiras podemos escrever um string usando letras do alfabeto $\{\mathtt{A}, \mathtt{B}, \mathtt{C}, \mathtt{D}\}$, tais que *cada letra é usada exatamente duas vezes mas não aparece consecutivamente no string*? Por exemplo:

ABADCDBC	é um string aceitável;
ABAC<u>DD</u>BC	não é.

(Π5.15 H 1 2)

▸ **PROBLEMA Π5.16.**
De quantas maneiras podemos escrever um string binário (usando o alfabeto $\{0,1\}$) de tamanho 12, tais que:

(i) os 0's aparecem apenas em grupos maximais de tamanho par;
(ii) os 1's aparecem apenas em grupos maximais de tamanho ímpar.

Por exemplo:

000000111001	é um string aceitável;
100110010001	não é.

(Π5.16 H 1 2)

▸ **PROBLEMA Π5.17.**
Xÿźźÿ o Mago Bravo decidiu matar todos os lemmings que ele guarda no seu quintal. Seus feitiços são os:

- "magic missile", que mata 2 lemmings simultaneamente, e gasta 1 ponto "mana";
- "fireball", que mata 3 lemmings simultaneamente, e gasta 2 pontos mana.

Além dos feitiços, Xÿźźÿ pode usar seu bastão para matar os lemmings (que não custa nada, e mata 1 lemming com cada batida).

Suponha que o mago *nunca* lançará um feitiço que mataria mais lemmings do que tem (ou seu quintal vai se queimar). Ele tem m pontos mana e existem n lemmings no seu quintal. Em quantas maneiras diferentes ele pode destruir todos os lemmings se...

(i) os lemmings são indistinguíveis?
(ii) os lemmings são distinguíveis?
(iii) os lemmings são distinguíveis e cada vez que Xÿźźÿ mata um usando seu bastão, ele *ganha* um ponto de mana?

(Para os casos que os lemmings são distinguíveis, o mago escolhe também *quais* dos lemmings ele matará cada vez.) (Π5.17 H 1 2)

Notas históricas

Pascal não foi o primeiro de estudar o "triângulo aritmético", cuja existência e sua relação com o teorema binomial já eram conhecidas desde uns séculos antes do seu nascimento. Mesmo assim, seu estudo *"Traité du triangle arithmétique, avec quelques autres petits traitez sur la mesme matière"*, publicado no ano 1654 (depois da sua morte) popularizou o triângulo e suas diversas aplicações e propriedades (**[Pas65]**).

Leitura complementar

Veja o **[Niv65]**.

CAPÍTULO 6

OS REAIS

TODO limpar, terminar, organizar

Os reais formam um *corpo ordenado completo*. Neste capítulo vamos estudar o que isso significa e investigar umas conseqüências dos axiomas dos reais. Além disso, vamos definir e estudar os conceitos fundamentais de limites e séries.

§134. Construindo os racionais

TODO x to Q

▸ **EXERCÍCIO x6.1.**
O que acontece se relaxar a restricção nos exponentes ainda mais?: $a_i \in \mathbb{Z}$.[46] (x6.1 H 0)

§135. De volta pra Grécia antiga: racionais e irracionais

6.1. O $\sqrt{2}$ não é racional.

TODO Escrever

6.2. Mas o $\sqrt{2}$ com certeza é um número.

TODO Escrever

6.3. Números irracionais.

TODO Escrever

6.4. O $\sqrt{3}$ é irracional.

TODO Escrever

6.5. Um lemma.

TODO Escrever

6.6. O que acontece com $\sqrt{4}$ e $\sqrt{5}$.

TODO Escrever

[46] Essa pergunta é para o leitor que já viu algo que não encontramos ainda aqui.

6.7. Um teorema de generalização.

TODO Escrever

6.8. Mais números irracionais.

TODO Escrever

6.9. Números algébricos e transcendentais.

TODO Escrever

§136. A reta real

TODO Escrever

§137. Primeiros passos

S6.10. Especificação (Os reais (1/3)). Usamos Real para denotar um tipo cujos membros chamamos de (números) reais e onde temos os seguintes componentes primitivos:

$$(+), (\cdot) : \mathsf{Real} \times \mathsf{Real} \to \mathsf{Real} \qquad 0, 1 : \mathsf{Real} \qquad (-) : \mathsf{Real} \to \mathsf{Real}.$$

Estipulamos as proposições seguintes como axiomas:

(RA-Ass) $(\forall a, b, c)[\,(a + b) + c = a + (b + c)\,]$
(RA-Id) $(\forall a)[\,0 + a = a = a + 0\,]$
(RA-Com) $(\forall a, b)[\,a + b = b + a\,]$
(RA-Inv) $(\forall a)[\,(-a) + a = 0 = a + (-a)\,]$

(RM-Ass) $(\forall a, b, c)[\,a \cdot (b \cdot c) = (a \cdot b) \cdot c\,]$
(RM-Id) $(\forall a)[\,1 \cdot a = a = a \cdot 1\,]$
(RM-Com) $(\forall a, b)[\,a \cdot b = b \cdot a\,]$
(RM-Inv*) $(\forall a)[\,a \neq 0 \implies (\exists a')[\,a' \cdot a = 1 = a \cdot a'\,]\,]$

(R-Dist) $(\forall d, a, b)[\,d \cdot (a + b) = (d \cdot a) + (d \cdot b) \;\;\&\;\; (a + b) \cdot d = (a \cdot d) + (b \cdot d)\,]$

(R-NZero) $0 \neq 1.$

6.11. Observação (Axiomas mais fortes do que precisamos). Observe que tanto sobre as identidades quanto sobre os inversos, optamos para incluir nos axiomas "ambos os lados". Compare isso com os axiomas que tivemos sobre os inteiros, onde *demonstramos como teorema* que 0 é uma (+)-identidade-L, e as demais versões esquerdas (Exercício x3.1). A demonstração foi simplíssima, graças às comutatividades das operações, que

aqui também temos. Ou seja, a gente poderia ter escolhido uma abordagem parecida aqui, mas não é sempre tão importante se obsecar economizando nos axiomas. Listados na maneira que tenho acima, tem uma outra vantagem: não passam uma informação falsa sobre nossa pretenção, e, além disso, seria mais facil se perguntar «o que acontece se apagar comutatividade de tal lista?», sem precisar nos preocupar para adicionar explicitamente as identidades e inversos esquerdos.

6.12. Considerações sintácticas. Atribuimos as mesmas *associatividades sintácticas* e as mesmas *precedências sintácticas* nas operações $(+)$ e $(\cdot)$ que atribuimos no Capítulo 3 (Nota 3.4, Nota 3.5, Nota 3.6). Similarmente usamos as abreviações

$$\begin{array}{llll} 2 : \mathsf{Real} & 3 : \mathsf{Real} & 4 : \mathsf{Real} & \cdots \\ 2 \stackrel{\mathsf{def}}{=} 1+1 & 3 \stackrel{\mathsf{def}}{=} 2+1 & 4 \stackrel{\mathsf{def}}{=} 3+1 & \cdots \end{array}$$

como fizemos no Nota 3.8.

D6.13. Definição (Açúcar sintáctico: subtração). Como nos inteiros (Nota 3.7), definimos a operação *binária*

$$(-) : \mathsf{Real} \times \mathsf{Real} \to \mathsf{Real}$$

de subtração pela

$$a - b \stackrel{\mathsf{def}}{=} a + (-b).$$

Novamente o símbolo '$-$' tá sendo *sobrecarregado* mas o contexto sempre deixa claro qual das

$$(-_) : \mathsf{Real} \to \mathsf{Real} \qquad\qquad (_ - _) : \mathsf{Real} \times \mathsf{Real} \to \mathsf{Real}$$

está sendo usada.

▸ **EXERCÍCIO x6.2 (Unicidade da identidade aditiva).**
Existe único z tal que para todo x, $z + x = x = x + z$. (x6.2H0)

▸ **EXERCÍCIO x6.3 (Unicidade dos inversos aditivos).**
Para todo x, existe único x' tal que $x' + x = 0 = x + x'$. (x6.3H0)

▸ **EXERCÍCIO x6.4 (Unicidade de resoluções).**
Para quaisquer a, b, existe único x tal que $a + x = b$ e existe único y tal que $y + a = b$. (x6.4H0)

▸ **EXERCÍCIO x6.5 (Negação de negação).**
Para todo x, $-(-x) = x$. (x6.5H0)

▸ **EXERCÍCIO x6.6 (Negação de soma).**
Para quaisquer a, b, temos $-(a - b) = b - a$ e $-(a + b) = -a - b$. (x6.6H0)

► **EXERCÍCIO x6.7 (Lei de cancelamento aditivo).**
Temos:

(RA-Can) $\quad (\forall a,b,c)[\,(c+a=c+b \implies a=b) \;\&\; (a+c=b+c \implies a=b)\,].$

(x6.7 H 0)

► **EXERCÍCIO x6.8 (Anulador).**
Demonstre que 0 é um $(\cdot)$-anulador:

(R-Ann) $\quad (\forall a)[\,0\cdot a=0=a\cdot 0\,].$

(x6.8 H 0)

► **EXERCÍCIO x6.9.**
Demonstre que 0 não possui $(\cdot)$-inverso. (x6.9 H 0)

► **EXERCÍCIO x6.10.**
Para todo a real, $-a=(-1)a$. (x6.10 H 0)

► **EXERCÍCIO x6.11.**
$(\forall a,b)[\,(-a)b=-(ab)=a(-b)\,].$ (x6.11 H 0)

► **EXERCÍCIO x6.12.**
Para quaisquer a,b, $(-a)(-b)=ab$. (x6.12 H 0)

► **EXERCÍCIO x6.13 (Unicidade da identidade multiplicativa).**
Existe único u tal que para todo x, $ux=x=xu$. (x6.13 H 0)

► **EXERCÍCIO x6.14 (Unicidade dos inversos multiplicativos).**
Para todo $x\neq 0$, existe único x' tal que $x'x=1=xx'$. (x6.14 H 0)

D6.14. Notação (Inverso multiplicativo). Seja $a\neq 0$. Denotamos por a^{-1} o seu $(\cdot)$-inverso, ou seja, o único real a' tal que $a'a=1=aa'$.

► **EXERCÍCIO x6.15 (Lei de cancelamento multiplicativo).**
Temos:

(R-Can) $\quad (\forall c,a,b)[\,c\neq 0 \implies (ca=cb \implies a=b) \;\&\; (ac=bc \implies a=b)\,].$

(x6.15 H 0)

► **EXERCÍCIO x6.16 (Inverso de inverso).**
Para todo $x\neq 0$, $\left(x^{-1}\right)^{-1}=x$. (x6.16 H 0)

► **EXERCÍCIO x6.17 (Inverso de produto).**
Para quaisquer $a,b\neq 0$, $(ab)^{-1}=a^{-1}b^{-1}$. (x6.17 H 0)

▸ **EXERCÍCIO x6.18 (R-NZD).**
$(\forall a, b)[\, ab = 0 \implies a = 0 \text{ ou } b = 0\,]$. (x6.18 H 0)

D6.15. Definição (Açúcar sintáctico: fracção). Dados a, b com $b \neq 0$, escrevemos a/b ou $\frac{a}{b}$ como açúcar sintáctico para o produto $a \cdot b^{-1}$. Note que as notações $1/b$ e $\frac{1}{b}$ são casos especiais disso.

▸ **EXERCÍCIO x6.19 (Produto de fracções).**
Para quaisquer a, b, c, d com $b, d \neq 0$, temos:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

(x6.19 H 0)

▸ **EXERCÍCIO x6.20 (Soma de fracções).**
Para quaisquer a, b, c, d com $b, d \neq 0$, temos:

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}.$$

(x6.20 H 0)

▸ **EXERCÍCIO x6.21 (Fracção de frações).**
Para quaisquer a, b, c, d com $b, c, d \neq 0$, temos:

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}.$$

(x6.21 H 0)

D6.16. Definição (Potências naturais). Já que agora possuimos mesmo o tipo Nat, podemos definir mesmo as potências naturais de qualquer real x, recursivamente, como uma operação de tipo:

$$(\hat{}) : \mathsf{Real} \to \mathsf{Nat} \to \mathsf{Real}$$

definida pelas

$$x^0 \stackrel{\mathsf{def}}{=} 1$$
$$x^{n+1} \stackrel{\mathsf{def}}{=} x \cdot x^n.$$

Como acabemos de fazer aqui, denotamos a aplicação da $(\hat{})$ nos argumentos a, b por a^b.

▸ **EXERCÍCIO x6.22.**
Uma alternativa para definir as potências naturais dum real x seria a seguinte:

$$x^0 \stackrel{\mathsf{def}}{=} 1$$
$$x^{n+1} \stackrel{\mathsf{def}}{=} x^n \cdot x.$$

Demonstre que essas duas definições são equivalentes. Mas cuidado! Duas definições alternativas usando a mesma notação não ajuda em demonstrar que são equivalentes.

Tu vai acabar escrevendo que precisa demonstrar que $x^n = x^n$, parecendo algo trivial (por reflexividade), só que não é o caso, pois num lado o x^n é para seguir uma definição, e no outro outra! Por isso precisamos alterar a notação da definição alternativa. Sugiro assim:

$$\begin{aligned} {}^0x &\stackrel{\text{def}}{=} 1 \\ {}^{n+1}x &\stackrel{\text{def}}{=} {}^nx \cdot x. \end{aligned}$$

Agora sim, o que precisas demonstrar é fácil de escrever:

$$(\forall x : \mathsf{Real})(\forall n : \mathsf{Nat})[\, {}^nx = x^n \,].$$

(x6.22 H 0)

▸ **EXERCÍCIO x6.23.**
Sejam a real e n, m naturais. Logo:

$$\begin{aligned} a^{n+m} &= a^n \cdot a^m \\ a^{n \cdot m} &= (a^n)^m. \end{aligned}$$

(x6.23 H 0)

6.17. Observação (Potências integrais: qual definição escolher?). Tendo o tipo dos inteiros Int gostaríamos de estender as potências dum real x para permitir expoentes inteiros. Parece que temos dois significados razoáveis para atribuir ao x^{-n}:

$$x^{-n} \stackrel{?}{=} \begin{cases} \left(x^{-1}\right)^n & \text{(o inverso de } x\text{, elevado ao natural } n\text{)} \\ \text{...ou...} & \\ (x^n)^{-1} & \text{(o inverso de } x^n\text{)} \end{cases}$$

Felizmente as duas alternativas são equivalentes, e logo não importa tanto qual das duas vamos escolher. Demonstrarás isso agora no Exercício x6.24, e logo depois (Definição D6.18) eu vou escolher uma para ser a definição mesmo.

▸ **EXERCÍCIO x6.24.**
Demonstre que as duas interpretações da Observação 6.17 são equivalentes. (x6.24 H 0)

D6.18. Definição (Potências integrais). Definimos

$$x^{-n} \stackrel{\text{def}}{=} (x^n)^{-1}.$$

▸ **EXERCÍCIO x6.25.**
Observando os valores de:

$$\begin{aligned} 1 + \frac{1}{2} &= 2 - \frac{1}{2} \\ 1 + \frac{1}{2} + \frac{1}{4} &= 2 - \frac{1}{4} \\ 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} &= 2 - \frac{1}{8}, \end{aligned}$$

adivinhe uma fórmula geral para o somatório

$$1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} = ?$$

e demonstre que ela é válida para todo $n \in \mathbb{N}$. (x6.25 H 0)

§138. Subconjuntos notáveis e inaceitáveis

D6.19. Definição. Definimos os subconjuntos de reais seguintes:

os reais naturais: $\mathbb{R}_{\mathbb{N}} \overset{\text{“def”}}{=} \{0, 1, 2, 3, \dots\}$

os reais inteiros: $\mathbb{R}_{\mathbb{Z}} \overset{\text{def}}{=} \mathbb{R}_{\mathbb{N}} \cup \{ -n \mid n \in \mathbb{R}_{\mathbb{N}} \}$

os reais racionais: $\mathbb{R}_{\mathbb{Q}} \overset{\text{def}}{=} \{ m/n \mid m \in \mathbb{R}_{\mathbb{Z}}, n \in \mathbb{R}_{\mathbb{Z}_{>0}} \}$

os reais algébricos: $\mathbb{R}_{\mathbb{A}} \overset{\text{def}}{=} \{ x \mid x \text{ é raiz dum polinómio com coeficientes inteiros} \}$.

Definimos também os *reais irracionais* $\mathbb{R} \setminus \mathbb{R}_{\mathbb{Q}}$ e os *reais transcendentais* $\mathbb{R} \setminus \mathbb{R}_{\mathbb{A}}$. Quando pelo contexto é inferível que estamos referindo a um conjunto de reais, é conveniente abusar a notação e escrever $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{A}$ em vez de $\mathbb{R}_{\mathbb{N}}, \mathbb{R}_{\mathbb{Z}}, \mathbb{R}_{\mathbb{Q}}, \mathbb{R}_{\mathbb{A}}$, respectivamente.

! 6.20. Cuidado (Um mal-entendido comum). É comum ouvir e ler a seguinte bobagem matemática:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

e outras bizarrices similares. Tais inclusões de conjuntos não fazem sentido. Todos os números seguintes são pronunciados do mesmo jeito, «zero», e denotados pelo mesmo símbolo, ‘0’:

$$0 : \mathsf{Nat} \qquad 0 : \mathsf{Int} \qquad 0 : \mathsf{Rat} \qquad 0 : \mathsf{Real} \qquad 0 : \mathsf{Complex}.$$

Mas seria errado pensar que se trata do mesmo objeto, já que são objetos de tipos diferentes e logo sequer faz sentido formular a pergunta se são iguais! Por outro lado, no conjunto $\mathbb{Z}$ de inteiros existe um subconjunto dele que serve como *representação do conjunto dos naturais*, e que chamamos de *inteiros naturais:*

$$\mathbb{Z}_{\mathbb{N}} \overset{\text{def}}{=} \{ x \in \mathbb{Z} \mid x \geq 0 \}.$$

E agora sim temos $\mathbb{Z}_{\mathbb{N}} \subseteq \mathbb{Z}$. Similarmente, dentro do conjunto dos racionais, encontramos um subconjunto para representar os inteiros, e logo herdamos também seu subconjunto como representante dos naturais também:

$$\mathbb{Q}_{\mathbb{N}} \subseteq \mathbb{Q}_{\mathbb{Z}} \subseteq \mathbb{Q}.$$

E nos reais temos

$$\mathbb{R}_{\mathbb{N}} \subseteq \mathbb{R}_{\mathbb{Z}} \subseteq \mathbb{R}_{\mathbb{Q}} \subseteq \mathbb{R}.$$

Mas sobre os

$$\mathbb{N}, \quad \mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{R},$$

o que podemos afirmar mesmo? E o que nos permite abusar a notação e a linguagem os tratando como se fossem subconjuntos mesmo? O que temos mesmo são *embutimentos que respeitam as estruturas*

$$\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R}$$

mas para entender o que essa frase significa vamos precisar de pouca paciência pois as ferramentas necessárias encontraremos nos Capítulo 9, Capítulo 11, e Capítulo 12. A situação vai ser esclarecida ainda mais no Capítulo 16 onde vamos *construir* mesmo todos esses conjuntos numéricos, em vez de tratá-los axiomaticamente, como fazemos neste

capítulo por exemplo sobre os reais, e no Capítulo 3 sobre os inteiros. O contexto de tal construção é de fundamentos sem tipos (a teoria dos conjuntos), então as perguntas são perguntáveis e mesmo assim todas vão acabar sendo refutáveis com nossas construções:

$$\mathbb{N} \not\subseteq \mathbb{Z} \not\subseteq \mathbb{Q} \not\subseteq \mathbb{R}$$

teremos testemunhas para cada uma dessas ($\not\subseteq$): membros do conjunto à esquerda que não pertencem ao conjunto à direita.

§139. Ordem e positividade

6.21. Observação (Axiomatização alternativa). Como discutimos no Nota 3.38, podemos optar para adicionar um predicado de positividade como noção primitiva, e *definir* as relações binárias $(<), (\leq), (>), (\geq)$, ou escolher uma das relações binárias como primitiva e definir o resto. Nos inteiros escolhemos a primeira abordagem. Para variar, vamos tomar a $(>)$ como primitiva nos reais. Mas, realmente, tanto faz.

S6.22. Especificação (Os reais (2/3)). Aumentamos a estrutura dos reais para

$$(\mathbb{R}\,;\, 0, 1, +, -, \cdot, >)$$

adicionando um predicado binário:

$$(>) : \mathsf{Real} \times \mathsf{Real} \to \mathsf{Prop}.$$

Estipulamos os axiomas seguintes:

(RO-Trans)	$(\forall a, b, c)[\, a > b \;\&\; b > c \implies a > c\,]$
(RO-Tri)	$(\forall a, b)[\,\text{e.u.d.: } a > b;\ a = b;\ b > a\,]$
(RO-A)	$(\forall a, b, c)[\, a > b \implies a + c > b + c\,]$
(RO-M)	$(\forall a, b, c)[\, a > b \;\&\; c > 0 \implies ac > bc\,].$

onde lembramos que «e.u.d.» significa *exatamente uma das*.

D6.23. Definição. Definimos as relações binárias $(<), (\leq), (\geq)$ pelas

$$x < y \overset{\text{def}}{\iff} y > x \qquad x \geq y \overset{\text{def}}{\iff} x > y \text{ ou } x = y \qquad x \leq y \overset{\text{def}}{\iff} y \geq x,$$

e o predicado unário $\mathrm{Pos} : \mathsf{Real} \to \mathsf{Prop}$ pela

$$\mathrm{Pos}(x) \overset{\text{def}}{\iff} x > 0.$$

▸ **EXERCÍCIO x6.26.**
$(\forall a, b, c, d)[\, a > b \;\&\; c > d \implies a + c > b + d\,].$ (x6.26 H 0)

► **EXERCÍCIO x6.27.**
$(\forall a)[\, a > 0 \implies -a < 0\,]$. (x6.27 H 0)

► **EXERCÍCIO x6.28.**
$(\forall a)[\, a < 0 \implies -a > 0\,]$. (x6.28 H 0)

► **EXERCÍCIO x6.29.**
$(\forall a, b)[\, a > b \implies a - b > 0\,]$. (x6.29 H 0)

► **EXERCÍCIO x6.30.**
$(\forall a, b)[\, a < 0 \ \&\ b < 0 \implies ab > 0\,]$. (x6.30 H 0)

► **EXERCÍCIO x6.31.**
Se $a \neq 0$ então $a^2 > 0$. (x6.31 H 0)

► **EXERCÍCIO x6.32.**
$(\forall a)\big[\, 0 < a < 1 \implies 0 < a^2 < a < 1\,\big]$. (x6.32 H 0)

► **EXERCÍCIO x6.33.**
$1 > 0$. (x6.33 H 0)

► **EXERCÍCIO x6.34.**
$(\forall a, b)[\, b > 0 \implies a + b > a\,]$. (x6.34 H 0)

► **EXERCÍCIO x6.35 (Tricotomia da positividade).**
Para todo a, exatamente uma das: a é positivo; $a = 0$; $-a$ é positivo. (x6.35 H 0)

► **EXERCÍCIO x6.36.**
O conjunto Pos é $(+)$-fechado. (x6.36 H 0)

► **EXERCÍCIO x6.37.**
O conjunto Pos é $(\cdot)$-fechado. (x6.37 H 0)

► **EXERCÍCIO x6.38.**
Se $a < b \ \&\ c < 0$ então $ac > bc$. (x6.38 H 0)

► **EXERCÍCIO x6.39.**
Se $a < b$ então $-a > -b$. (x6.39 H 0)

► **EXERCÍCIO x6.40.**
Se $ab > 0$ então a, b são ou ambos positivos ou ambos negativos. (x6.40 H 0)

► **EXERCÍCIO x6.41.**

A função $(_^2)$ *preserve* e *reflete* a $(\leq)$ no $\mathbb{R}_{\geq 0}$:

$$(\forall a, b \geq 0)\big[\, a \leq b \implies a^2 \leq b^2 \,\big]; \qquad (_^2) \text{ preserve a } (\leq)$$
$$(\forall a, b \geq 0)\big[\, a \leq b \impliedby a^2 \leq b^2 \,\big]. \qquad (_^2) \text{ reflete a } (\leq)$$

E a mesma coisa sobre as outras ordens que temos definido até agora: $(<), (\geq), (>)$. (x6.41 H 0)

► **EXERCÍCIO x6.42.**
Para todo a, b, temos $a^2 + b^2 \geq 0$. Ainda mais: $a^2 + b^2 = 0$ sse $a = b = 0$. (x6.42 H 0)

► **EXERCÍCIO x6.43.**
Não existe x tal que $x^2 + 1 = 0$. (x6.43 H 0)

► **EXERCÍCIO x6.44.**
$(\forall a)\big[\, a > 0 \iff a^{-1} > 0 \,\big]$. (x6.44 H 0)

► **EXERCÍCIO x6.45.**
$(\forall a, b)\big[\, 0 < a < b \implies 0 < b^{-1} < a^{-1} \,\big]$. (x6.45 H 0)

► **EXERCÍCIO x6.46.**
$(\forall a, b)\big[\, a < b \implies a < \frac{1}{2}(a+b) < b \,\big]$. (x6.46 H 0)

► **EXERCÍCIO x6.47.**
$(\forall a)\big[\, 0 < a \implies 0 < \frac{1}{2}a < a \,\big]$. (x6.47 H 0)

► **EXERCÍCIO x6.48.**
Calculando os valores de:

$$\left(1 - \frac{1}{2}\right), \qquad \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right), \qquad \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{4}\right),$$

adivinhe uma fórmula geral para o produtório

$$\prod_{i=2}^{n}\left(1 - \frac{1}{i}\right) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{4}\right)\cdots\left(1 - \frac{1}{n}\right)$$

e demonstre que ela é válida para todo inteiro $n \geq 2$. (x6.48 H 0)

► **EXERCÍCIO x6.49.**
Demonstre que para todo inteiro $n \geq 1$,

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

(x6.49 H 0)

► **EXERCÍCIO x6.50 (desigualdade Bernoulli (0)).**
Demonstre usando o teorema binomial que para todo real $x \geq 0$, e todo $n \geq 0$, temos

$$(1+x)^n \geq 1 + xn.$$

(x6.50 H 0)

▸ **EXERCÍCIO x6.51 (desigualdade Bernoulli (1)).**
Demonstre por indução que para todo real $x > -1$, e todo $n \geq 1$, $(1+x)^n \geq 1 + xn$. (x6.51 H 0)

▸ **EXERCÍCIO x6.52 (desigualdade Bernoulli (2)).**
Demonstre por indução que para todo real $x > -2$, e todo $n \geq 0$, $(1+x)^n \geq 1 + xn$. (x6.52 H 1)

§140. Valor absoluto

D6.24. Definição. Definimos a operação $|-| : \mathsf{Real} \to \mathsf{Real}$

$$|x| \stackrel{\text{def}}{=} \begin{cases} x, & \text{caso } x \geq 0; \\ -x, & \text{caso } x < 0. \end{cases}$$

▸ **EXERCÍCIO x6.53.**
$|a| = 0 \iff a = 0$; $\quad |a| \geq 0$. (x6.53 H 0)

▸ **EXERCÍCIO x6.54.**
$|x| \leq a \iff -a \leq x \leq a$. (x6.54 H 1)

▸ **EXERCÍCIO x6.55.**
$|-a| = |a|\,; \quad |a \cdot b| = |a| \cdot |b|\,; \quad |a+b| \leq |a| + |b|\,; \quad |a-b| \leq |a| + |b|\,.$ (x6.55 H 0)

▸ **EXERCÍCIO x6.56.**
Sejam a, b reais. Logo:

$$\big||a| - |b|\big| \leq |a+b| \leq |a| + |b|\,;$$
$$\big||a| - |b|\big| \leq |a-b| \leq |a| + |b|\,.$$

(x6.56 H 0)

▸ **EXERCÍCIO x6.57.**
Sejam a, b, c reais. Logo:

$$|a-c| \leq |a-b| + |b-c|\,.$$

(x6.57 H 0)

▸ **EXERCÍCIO x6.58.**
Sejam c, r, x reais com $r > 0$. Logo:

$$|x-c| < r \iff c - r < x < c + r$$

(x6.58 H 0)

▸ **EXERCÍCIO x6.59.**
Sejam a : Real, x : Int.

$$|a|^x = |a^x| = \begin{cases} a^x, & x \text{ par;} \\ a^x, & x \text{ ímpar, } a \geq 0; \\ -a^x, & x \text{ ímpar, } a < 0. \end{cases}$$

(x6.59 H 0)

6.25. Observação. Uma maneira de interpretar o valor absoluto dum real x é como uma medida de quão distante é o x do real 0. Ainda mais, podemos *usar* o valor absoluto para falar sobre *distâncias* entre quaisquer dois reais. Fazemos isso na Secção §150.

§141. Conjuntos de reais

Conjuntos e seqüências mesmo, em forma geral, vamos estudar no Capítulo 8. Aqui vamos só usar um pouco uns conjuntos e logo depois umas seqüências *de reais*

Set Real : Type Seq Real : Type

e uns conjuntos e umas seqüências *de conjuntos de reais*

Set (Set Real) : Type Seq (Set Real) : Type

e, acho que pronto, parou! Nada mais profundo que isso.

6.26. Saber um conjunto de reais. O que precisamos fazer para ter o direito de dizer que *definimos* um conjunto de reais A? Precisamos definir o que significa *pertencer ao conjunto* A. Se, e somente se, para qualquer x real sabemos o que significa a afirmação $x \in A$, temos o direito de falar que sabemos quem é o A. E para falar que entendemos o que significa conjunto mesmo, precisamos saber o que significa a afirmação $A = B$, para quaisquer conjuntos A, B. Vamos lembrar isso agora:

$$A = B \overset{\text{def}}{\iff} (\forall x)[\, x \in A \iff x \in B\,].$$

E para formar (definir) um conjunto A, o que precisamos fazer? Simplesmente definir o que $x \in A$ significa:

$$x \in A \overset{\text{def}}{\iff} \ldots$$

pois saber o que $x \in A$ significa, é saber o que A significa.

6.27. Set-builder. Quando o conjunto tem uma quantidade finita de membros, podemos simplesmente listar todos eles entre chaves:

$$A \overset{\text{def}}{=} \{5, 7, 2\}\,.$$

Com essa definição definimos sim a proposição $x \in A$ para qualquer x real para ser a seguinte:

$$x \in A \iff x = 5 \text{ ou } x = 7 \text{ ou } x = 2.$$

Usamos a notação *set-builder*

$$\{\, x \in \mathbb{R} \mid \varphi(x) \,\}$$

para denotar o conjunto de todos os reais x tais que $\varphi(x)$. Dado qualquer real a, então, a proposição

$$a \in \{\, x \in \mathbb{R} \mid \varphi(x) \,\}$$

reduz-se à proposição $\varphi(a)$. Dado um conjunto de reais D, escrevemos

$$\{\, x \in D \mid \varphi(x) \,\}$$

para referir ao conjuto de todos os membros de D que, ainda mais, possuem a propriedade φ. Todos os usos até agora dessa notação usam apenas uma variável na sua parte esquerda, mas podemos escrever termos mais interessantes. Por exemplo

$$\{\, 2^n + 1 \mid n \in \mathbb{N} \,\} = \{2^0 + 1, 2^1 + 1, 2^2 + 1, 2^3 + 1, \dots\} = \{2, 3, 5, 9, \dots\}.$$

Quando um conjunto é definido nesta forma dizemos que é *indexado*, aqui pelo conjunto $\mathbb{N}$. Isso significa que para solicitar membros arbitrários deste conjunto basta solicitar indices arbitrários do conjunto de índices. Escrevendo «Sejam $i, j \in \mathbb{N}$», então, querendo ou não, temos acesso em dois membros arbitrários do nosso conjunto: $2^i + 1, 2^j + 1$. O conjunto $\mathbb{N}$ nesse exemplo também é chamado de *gerador*, visto como um fornecedor de valores para a variável n que aparece na parte esquerda, para formar os membros do conjunto mesmo. Podemos usar mais que um gerador, e quando isso acontece a idéia é que para cada escolha de membro por cada gerador fornece um membro do nosso conjunto. Por exemplo:

$$\begin{aligned}\{\, n^2 + 2m \mid n \in \mathbb{N}, m \in \{10, 20\} \,\} &= \{0^2 + 2 \cdot 10, 0^2 + 2 \cdot 20, 1^2 + 2 \cdot 10, 1^2 + 2 \cdot 20, \dots\} \\ &= \{20, 40, 21, 41, 24, 44, \dots\}.\end{aligned}$$

D6.28. Definição (Intervalos). Sejam a, b reais. Definimos os conjuntos de reais seguintes, que chamamos de *intervalos:*

$$\begin{aligned}(a,b) &\stackrel{\text{def}}{=} \{\, x \mid a < x < b \,\} & [a,b] &\stackrel{\text{def}}{=} \{\, x \mid a \le x \le b \,\} \\ (a,b] &\stackrel{\text{def}}{=} \{\, x \mid a < x \le b \,\} & [a,b) &\stackrel{\text{def}}{=} \{\, x \mid a \le x < b \,\}.\end{aligned}$$

Pronunciamos as parentêses de «aberto» e os colchetes de «fechado». Definimos também:

$$\begin{aligned}(-\infty,b) &\stackrel{\text{def}}{=} \{\, x \mid x < b \,\} & (a,+\infty) &\stackrel{\text{def}}{=} \{\, x \mid a < x \,\} \\ (-\infty,b] &\stackrel{\text{def}}{=} \{\, x \mid x \le b \,\} & [a,+\infty) &\stackrel{\text{def}}{=} \{\, x \mid a \le x \,\}.\end{aligned}$$

É conveniente também definir $(-\infty, +\infty) \stackrel{\text{def}}{=} \mathbb{R}$.

! 6.29. Cuidado. Não definimos os $-\infty, +\infty$ como objetos matemáticos aqui. Por enquanto fazem parte de notação, e com certeza *não* se trata de números reais.

§142. Mínima e máxima

D6.30. Definição. Definimos as funções:

$$\min : \mathsf{Real} \times \mathsf{Real} \to \mathsf{Real} \qquad\qquad \max : \mathsf{Real} \times \mathsf{Real} \to \mathsf{Real}$$
$$\min(a,b) \stackrel{\text{def}}{=} \begin{cases} a, & \text{se } a \leq b; \\ b, & \text{senão;} \end{cases} \qquad \max(a,b) \stackrel{\text{def}}{=} \begin{cases} b, & \text{se } a \leq b; \\ a, & \text{senão.} \end{cases}$$

▸ **EXERCÍCIO x6.60.**
Sejam a, b reais. Logo

$$\min(a,b) = \frac{a+b-|b-a|}{2} \qquad\qquad \max(a,b) = \frac{a+b+|b-a|}{2}.$$

(x6.60 H 0)

▸ **EXERCÍCIO x6.61.**
Sejam a, b, c, d reais. Logo

$$\max(a+c, b+d) \leq \max(a,b) + \max(c,d).$$

(x6.61 H 0)

▸ **EXERCÍCIO x6.62.**
Qual a correspondente afirmação que podes demonstrar sobre a min? (x6.62 H 0)

D6.31. Definição. Sejam A um conjunto de reais e x um real. Dizemos que:

$$m \text{ é um mínimo de } A \stackrel{\text{def}}{\iff} m \in A \;\&\; m \leq A$$
$$m \text{ é um máximo de } A \stackrel{\text{def}}{\iff} m \in A \;\&\; m \geq A.$$

▸ **EXERCÍCIO x6.63 (Unicidades de máxima e mínima).**
Seja A conjunto de reais. Se A possui um mínimo membro m, então m é o único mínimo membro de A. Similarmente sobre os máxima. (x6.63 H 0)

D6.32. Notação. Quando um conjunto A de reais possui mínimo, denotamos por $\min A$ o seu único membro mínimo. Similarmente, quando A possui máximo, o denotamos por $\max A$.

▸ **EXERCÍCIO x6.64.**
O $\mathbb{R}$ não tem nem mínimo, nem máximo. (x6.64 H 0)

▸ **EXERCÍCIO x6.65.**
Todo conjunto finito e habitado de reais possui membro mínimo e membro máximo. (x6.65 H 0)

D6.33. Definição (piso, teto). Seja a real. Associamos com a dois reais inteiros, que chamamos de *piso* e *teto* de a e denotamos por $\lfloor a \rfloor$ e $\lceil a \rceil$ respectivamente. Suas definições:

$$\lfloor a \rfloor \stackrel{\text{def}}{=} \max \{\, x \in \mathbb{R}_{\mathbb{Z}} \mid x \leq a \,\} \qquad\qquad \lceil a \rceil \stackrel{\text{def}}{=} \min \{\, x \in \mathbb{R}_{\mathbb{Z}} \mid a \leq x \,\}.$$

▸ **EXERCÍCIO x6.66.**
A definição Definição D6.33 é potencialmente perigosa. Qual o perigo? Identifique e demonstre que não há tal perigo mesmo. (x6.66 H 0)

• **EXEMPLO 6.34.**
Temos:

$$\begin{array}{lllll} \lceil 4 \rceil = 4 & \lceil 1/2 \rceil = 1 & \lceil -3/2 \rceil = -1 & \lceil 0.99 \rceil = 1 & \lceil 0.999\ldots \rceil = 1 \\ \lfloor 4 \rfloor = 4 & \lfloor 1/2 \rfloor = 0 & \lfloor -3/2 \rfloor = -2 & \lfloor 0.99 \rfloor = 0 & \lfloor 0.999\ldots \rfloor = 1. \end{array}$$

As duas últimas colunas envolvem *numerais de reais em notação decimal*, algo que não temos discutido ainda, mas encontraremos daqui a pouco, neste mesmo capítulo. Inclui essas duas colunas aqui para o leitor que já é acostumado com eles.

▸ **EXERCÍCIO x6.67.**
Adivinhe os '...?...' e demonstre:

$$(\forall x \in \mathbb{R})[\, \lfloor \lceil x \rceil \rfloor = \ldots ?\ldots] \qquad\qquad (\forall x \in \mathbb{R})[\, \lceil \lfloor x \rfloor \rceil = \ldots ?\ldots].$$

(x6.67 H 0)

▸ **EXERCÍCIO x6.68.**
Adivinhe os '...?...' e demonstre:

$$(\forall x \in \mathbb{R})(\forall k \in \mathbb{R}_{\mathbb{Z}})[\, \lfloor x + k \rfloor = \ldots ?\ldots] \qquad (\forall x \in \mathbb{R})(\forall k \in \mathbb{R}_{\mathbb{Z}})[\, \lceil x + k \rceil = \ldots ?\ldots].$$

(x6.68 H 0)

§143. Seqüências

D6.35. Definição (seqüência). Considere que temos definido os reais

$$x_0, x_1, x_2, x_3, \ldots$$

Temos então, para cada $n \in \mathbb{N}$, determinado um certo real x_n. Dizemos que temos uma *seqüência de reais*, que denotamos por qualquer uma das

$$(x_n)_{n=0}^{\infty} \qquad (x_n)_{n\in\mathbb{N}} \qquad (\, x_n \mid n \in \mathbb{N}\,) \qquad (\, x_n \mid n \geq 0\,) \qquad (x_n)_n,$$

dependendo de quanta informação podemos deixar implicita sem haver confusão ou ambigüidade. Dizemos que o x_i é o i-ésimo *componente* ou *termo* da seqüência $(x_n)_n$. A pergunta primitiva que podemos fazer numa seqüência é a seguinte: «qual é teu i-ésimo componente?». Consideramos duas seqüências como *iguais* sse concordam em todas as posições, ou seja:

$$(x_n)_n = (y_n)_n \iff (\forall n)[\, x_n = y_n\,].$$

! 6.36. Cuidado (Seqüências não são conjuntos). Mesmo que uma seqüência tem componentes (um para cada "posição" dela) reservamos o verbo «pertencer» e o símbolo ($\in$) apenas para *conjuntos*:

$$(\in) : \mathsf{Object} \times \mathsf{Set} \to \mathsf{Prop}$$

ou, até melhor, trabalhando numa maneira mais cuidadosa com tipagens para cada tipo α teremos um $(\in_\alpha)$:

$$(\in_\alpha) : \alpha \times \mathsf{Set}\ \alpha \to \mathsf{Prop}.$$

De qualquer forma, seria um *type error* escrever $1 \in (x_n)_n$. Aquele *tão errado que nem chega a ser falso*. Simplesmente sem significado.

6.37. Type coercion: seqüências como conjuntos. Mesmo assim, é comum ver uma seqüência aparecendo num lugar onde pelo contexto é inferível que deveria aparecer um conjunto. Provavelmente o que tá sendo referido nesses casos não é a seqüência em si mas sim o *conjunto do seus termos:*

$$(x_n)_{n\in\mathbb{N}} \qquad \rightsquigarrow \qquad \{\, x_n \mid n \in \mathbb{N} \,\}, \qquad \text{que também denotamos por } \{x_n\}_n.$$

- **EXEMPLO 6.38.**
Aqui umas seqüências e seus primeiros componentes:

$$\begin{aligned}
(1/2^n)_{n=0}^{\infty} &= 1, 1/2, 1/4, 1/8, \dots & (3n+1)_n &= 1, 4, 7, 10, \dots \\
(1)_{n\in\mathbb{N}} &= 1, 1, 1, 1, \dots & ((-1)^n)_{n=8}^{\infty} &= 1, -1, 1, -1, \dots \\
(n(-1)^n)_{n\geq 3} &= -3, 4, -5, 6, \dots & \left(\frac{n+1}{n}\right)_{n=1}^{\infty} &= 2, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \dots \\
(x_{2n})_{n=0}^{\infty} &= x_0, x_2, x_4, x_6, \dots & \left(y_n z_{n+1}^2\right)_{n=1}^{\infty} &= y_1 z_2^2, y_2 z_3^2, y_3 z_4^2, y_4 z_5^2, \dots \\
(a_{n_i})_i &= a_{n_0}, a_{n_1}, a_{n_2}, a_{n_3}, \dots & (a_{n^2})_n &= a_0, a_1, a_4, a_9, \dots \\
\left(\prod_{i=2}^{n-1} a_i\right)_{n\geq 1} &= 1, 1, a_2, a_2a_3, \dots & \left(\sum_{n=1}^{3} n\right)_{n=0}^{\infty} &= 6, 6, 6, 6, \dots
\end{aligned}$$

- **EXEMPLO 6.39.**
Definimos a seqüência de reais $(b_n)_n$ pela:

$$b_n \stackrel{\text{def}}{=} 1 + 1/n.$$

Observe que aqui consideramos como primeiro termo da seqüência o b_1, e não o b_0. Se, por motivos religiosos, queremos defini-la em tal forma que seu primeiro termo é o b_0 mesmo, basta definir pela $b_n \stackrel{\text{def}}{=} 1 + 1/(n+1)$.

- **EXEMPLO 6.40.**
Definimos a seqüência de reais $(a_n)_n$ recursivamente pelas:

$$\begin{aligned}
a_0 &\stackrel{\text{def}}{=} 0 \\
a_{n+1} &\stackrel{\text{def}}{=} 1 - a_n.
\end{aligned}$$

• **EXEMPLO 6.41.**
Definimos a seqüência de reais $(x_n)_n$ recursivamente pelas:

$$x_0 \stackrel{\text{def}}{=} 0$$
$$x_{n+1} \stackrel{\text{def}}{=} (1/2)x_n + 1.$$

Seus primeiros termos então são os:

$$0, \quad 1, \quad 1+1/2, \quad 1+3/4, \quad 1+7/8, \quad \ldots$$

ou, igualmente,

$$0, \quad 1, \quad 2-1/2, \quad 2-1/4, \quad 2-1/8, \quad \ldots$$

▸ **EXERCÍCIO x6.69.**
Demonstre que a $(x_n)_n$ definida no Exemplo 6.41 é *crescente*, i.e.:

$$(\forall n)[\, x_n \leq x_{n+1}\,].$$

(x6.69 H 0)

! **6.42. Cuidado (Crescente não implica ilimitada).** Mesmo sabendo que cada termo duma seqüência é *estritamente menor* que o próximo, não podemos inferir que a seqüência não é cotada por cima: pode ser que existe um real M, tal que todos os termos dela são menores que M.

▸ **EXERCÍCIO x6.70.**
Ache um tal M para essa mesma seqüência do Exemplo 6.41, e demonstre que realmente serve. (x6.70 H 0)

▸ **EXERCÍCIO x6.71.**
Agora considere a seqüência $(x_n)_n$ definida pelas

$$x_0 \stackrel{\text{def}}{=} 1$$
$$x_{n+1} \stackrel{\text{def}}{=} (3x_n + 4)/4.$$

Resolva sobre esta as mesmas duas questões: ela é crescente? ela é cotada? (x6.71 H 0)

▸ **EXERCÍCIO x6.72.**
Seja ϑ um real pequeno: $0 < \vartheta < 1$. Definimos a seqüência $(t_n)_n$ pelas

$$t_0 \stackrel{\text{def}}{=} 0;$$
$$t_{n+1} \stackrel{\text{def}}{=} t_n + \frac{1}{2}(\vartheta - t_n^2).$$

Demonstre que $(t_n)_n$ é cotada por cima. (x6.72 H 0)

▸ **EXERCÍCIO x6.73.**
Demonstre que a mesma seqüência é crescente. (x6.73 H 0)

§144. Uniões e interseções

6.43. União e interseção de colecções de conjuntos. Tendo uns conjuntos de reais queremos definir a *união* e a *intersecção* deles; ou seja: definir o que significa *pertencer à união deles* e o que significa *pertencer à interseção deles*. Caso que a quantidade dos conjuntos é apenas 2, vamos dizer A_1, A_2, já conhecemos até uma notação para sua união e sua interseção: $A_1 \cup A_2$ e $A_1 \cap A_2$ respectivamente. Lembramos as suas definições:

$$x \in A_1 \cup A_2 \iff^{\text{def}} x \in A_1 \text{ ou } x \in A_2$$
$$x \in A_1 \cap A_2 \iff^{\text{def}} x \in A_1 \ \& \ x \in A_2.$$

Mas se temos mais que dois conjuntos? As definições acima não são aplicáveis nesse caso. Precisamos generalizá-las. Se temos uma quantidade finita de conjuntos para unir ou para intersectar, até que dá para fazer aproveitando as $(\cup)$ e $(\cap)$—e faremos isso no Capítulo 8 mesmo—mas aqui não nos interessa, pois não será suficiente considerar colecções de *apenas* 8, 84, ou 4208 conjuntos. Freqüentemente teremos uma infinidade de conjuntos, ou arrumada assim

$$A_1, A_2, A_3, \ldots$$

numa seqüência $(A_n)_n$, ou até sem sequer ter nomes legais para esses conjuntos: considere que temos uma colecção (possivelmente infinita) $\mathcal{A}$ de conjuntos de reais. Dizemos que

$$x \text{ pertence à união de uns conjuntos} \iff^{\text{def}} x \text{ pertence àlgum deles}$$
$$x \text{ pertence à interseção de uns conjuntos} \iff^{\text{def}} x \text{ pertence a todos eles}$$

Denotando a colecção de tais conjuntos por $\mathcal{A}$:

$$x \text{ pertence à união dos conjuntos da } \mathcal{A} \iff^{\text{def}} (\exists A \in \mathcal{A})[\, x \in A \,]$$
$$x \text{ pertence à interseção dos conjuntos da } \mathcal{A} \iff^{\text{def}} (\forall A \in \mathcal{A})[\, x \in A \,]$$

E se temos nomes indexados de tais conjuntos $A_0, A_1, A_2, \ldots$:

$$x \text{ pertence à união dos } A_0, A_1, A_2, \ldots \iff^{\text{def}} (\exists i \in \mathbb{N})[\, x \in A_i \,]$$
$$x \text{ pertence à interseção dos } A_0, A_1, A_2, \ldots \iff^{\text{def}} (\forall i \in \mathbb{N})[\, x \in A_i \,].$$

Para referir à união ou à interseção de uma colecção de conjuntos usamos os símbolos $\bigcup$ e $\bigcap$, assim:

$$\bigcup \mathcal{A} \stackrel{\text{def}}{=} \text{a união dos conjuntos da colecção } \mathcal{A}$$
$$\bigcap \mathcal{A} \stackrel{\text{def}}{=} \text{a interseção dos conjuntos da colecção } \mathcal{A}$$
$$\bigcup_{n\in\mathbb{N}} A_n \stackrel{\text{def}}{=} \bigcup_{i=0}^{\infty} A_i \stackrel{\text{def}}{=} \text{a união dos conjuntos } A_0, A_1, A_2, \ldots$$
$$\bigcap_{n\in\mathbb{N}} A_n \stackrel{\text{def}}{=} \bigcap_{i=0}^{\infty} A_i \stackrel{\text{def}}{=} \text{a interseção dos conjuntos } A_0, A_1, A_2, \ldots.$$

Quando é claro pelo contexto quais são "os A_n's" que estamos unindo ou intersetando escrevemos apenas

$$\bigcup_n A_n \stackrel{\text{def}}{=} \text{a união dos } A_n\text{'s}$$
$$\bigcap_n A_n \stackrel{\text{def}}{=} \text{a interseção dos } A_n\text{'s.}$$

Seqüências de conjuntos. Toda a notação e terminologia sobre seqüências de reais que elaboramos aqui aplica *mutatis mutandis* para seqüências de *conjuntos de reais*.

▸ **EXERCÍCIO x6.74.**
Seja $(A_n)_n$ uma seqüência de conjuntos de reais, tal que

$$A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$$

e tal que cada um deles possui uma infinidade de membros. Podemos concluir que sua intersecção

$$A_1 \cap A_2 \cap A_3 \cap \cdots$$

também possui uma infinidade de reais? (x6.74 H 0)

▸ **EXERCÍCIO x6.75.**
E se, em vez de infinito, cada um dos A_i é finito e habitado, podemos concluir que a interseção também é finita e habitada? (x6.75 H 0)

▸ **EXERCÍCIO x6.76.**
Para $n = 1, 2, 3, \ldots$ defina os intervalos de reais

$$F_n = \left[-1 + \frac{1}{n},\ 1 - \frac{1}{n}\right] \qquad\qquad G_n = \left(-1 - \frac{1}{n},\ 1 + \frac{1}{n}\right).$$

Calcule os conjuntos $\bigcup_n F_n$ e $\bigcap_n G_n$. (x6.76 H 1)

▸ **EXERCÍCIO x6.77.**
Para todo real $\varepsilon > 0$ e todo $n \in \mathbb{N}$, sejam os intervalos de reais

$$I_\varepsilon = [0, 1 + \varepsilon) \qquad\qquad J_n = [0, 1 + 1/n] \qquad\qquad U_n = [n, +\infty).$$

Calcule os conjuntos: (i) $\bigcap \{\, I_\varepsilon \mid \varepsilon > 0 \,\}$; (ii) $\bigcap_{n=0}^{\infty} J_n$; (iii) $\bigcap_{n=2}^{\infty} U_n$. (x6.77 H 0)

§145. Operações e relações entre seqüências

D6.44. Definição (ordem pointwise). Aproveitando as ordens que já temos nos reais, as elevamos para definir correspondentes ordens entre seqüências de reais, em forma *pointwise:*

$$(a_n)_n \le (b_n)_n \iff (\forall n)[\, a_n \le b_n \,],$$

e similarmente para as outras ordens que definimos: $(<)$, $(\ge)$, etc.

! **6.45. Cuidado.** Antes da Definição D6.44, a expressão

$$(a_n)_n \leq (b_n)_n$$

seria interpretada através de *type coercion* como

$$\{a_n\}_n \leq \{b_n\}_n$$

pois temos estabelecido já o que $A \leq B$ significa para conjuntos de reais A, B:

$$A \leq B \iff (\forall a \in A)[\, a \leq B \,] \iff (\forall a \in A)(\forall b \in B)[\, a \leq b \,].$$

Mas a partir da Definição D6.44 a expressão

$$(a_n)_n \leq (b_n)_n$$

já ganhou seu próprio significado, e logo não entra mais nenhum *type coercion* nesse processo. Mas será que as duas interpretações acabam sendo equivalentes?

▸ **EXERCÍCIO x6.78.**
Será? (x6.78 H 1)

§146. Os reais naturais

D6.46. Definição (naturalmente indutivo). Seja A um conjunto de reais. Chamamos o A de (naturalmente) *indutivo* sse: (i) A é 0-fechado: $0 \in A$; (ii) A é $(+1)$-fechado: $(\forall a)[\, a \in A \implies a+1 \in A \,]$.

• **EXEMPLO 6.47.**
O próprio conjunto $\mathbb{R}$ com certeza é indutivo. Os conjuntos $\mathbb{R}_{\geq 0}, \mathbb{R}_{\geq -1}$ também. Os conjuntos

$$H \stackrel{\text{def}}{=} \left\{ \ldots -3, -\frac{5}{2}, -2, -\frac{3}{2}, -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, 3, \ldots \right\}$$
$$H_{\geq 0} \stackrel{\text{def}}{=} \{\, h \in H \mid h \geq 0 \,\}$$

também.

• **NÃOEXEMPLO 6.48.**
Nenhum dos conjuntos seguintes é indutivo:

$$\{0\}, \quad \{0, 1, 2, 3, \ldots, 83\}, \quad \mathbb{R}_{\neq 0}, \quad \mathbb{R}_{\leq 0}, \quad \mathbb{R}_{>0}, \quad \mathbb{R}_{\neq -1}.$$

▸ **EXERCÍCIO x6.79.**
Por quê? (x6.79 H 0)

D6.49. Definição (Os reais naturais). Seja $\mathcal{I}$ a colecção de todos os conjuntos indutivos de reais. Sabemos que $\mathbb{R} \in \mathcal{I}$. Considere a interseção de todos os conjuntos indutivos de reais, ou seja, o conjunto

$$\mathbb{R}_{\mathbb{N}} \stackrel{\text{def}}{=} \{\, x \in \mathbb{R} \mid x \text{ pertence a todo conjunto indutivo de reais} \,\}$$

que denotaremos por $\mathbb{R}_{\mathbb{N}}$ e cujos membros chamamos de *reais naturais*. Seus membros são os

$$\mathbb{R}_{\mathbb{N}} = \{0, 1, 2, 3, 4, \dots\}.$$

Θ6.50. Teorema. *O conjunto $\mathbb{R}_{\mathbb{N}}$ é indutivo.*

Demonstração. Precisamos verificar que: (i) $0 \in \mathbb{R}_{\mathbb{N}}$; (ii) $(\forall x)[\, x \in \mathbb{R}_{\mathbb{N}} \implies x+1 \in \mathbb{R}_{\mathbb{N}}\,]$. Lembre-se que para demonstrar que um real a pertence ao $\mathbb{R}_{\mathbb{N}}$ basta demonstrar que a pertence a todos os conjuntos indutivos, já que $\mathbb{R}_{\mathbb{N}}$ foi definido como interseção de todos eles.

(i) Seja I conjunto indutivo de reais. Logo $0 \in I$. (ii) Seja $x \in \mathbb{R}_{\mathbb{N}}$, ou seja, x pertence em qualquer conjunto indutivo. Preciso mostrar que $x+1 \in \mathbb{R}_{\mathbb{N}}$. Para conseguir isso, seja I um conjunto indutivo de reais. Logo $x \in I$. Como I é indutivo, $x+1 \in I$, que é o que precisava mostrar. ∎

6.51. Corolário. *O conjunto $\mathbb{R}_{\mathbb{N}}$ é o $(\subseteq)$-menor conjunto indutivo, i.e.,*

$$(\forall I \text{ indutivo})[\, \mathbb{R}_{\mathbb{N}} \subseteq I \,].$$

Demonstração. Seja I indutivo e $n \in \mathbb{R}_{\mathbb{N}}$. Logo $n \in I$. ∎

6.52. Observação. É muito fácil subestimar ou até descartar o que acabamos de obter (tão facilmente) sem perceber sua importância: *ele é o princípio da indução* para o $\mathbb{R}_{\mathbb{N}}$! Compare com o Teorema Θ3.68 dos inteiros.

Tendo finalmente definido os reais naturais $\mathbb{R}_{\mathbb{N}}$, ganhamos o resto dos subconjuntos da Definição D6.19.

▸ **EXERCÍCIO x6.80.**
Os $\mathbb{R}_{\mathbb{Z}}, \mathbb{R}_{\mathbb{Q}}, \mathbb{R}_{\mathbb{A}}$ são conjuntos indutivos. (x6.80 H 0)

▸ **EXERCÍCIO x6.81.**
Daria certo utilizar a mesma idéia para definir os inteiros naturais $\mathbb{ZN} \subseteq \mathbb{Z}$? Os racionais naturais $\mathbb{Q}_{\mathbb{N}} \subseteq \mathbb{Q}$? (x6.81 H 1)

§147. Sobre modelos

6.53. Modelos. Qualquer $(X\,; 0, 1, +, -, \cdot, >)$ com

$$0, 1 : X \qquad (+), (\cdot) : X \times X \to X \qquad (-) : X \to X \qquad (>) : X \times X \to \mathsf{Prop}$$

que satisfaz todos os axiomas que temos estipulado até agora neste capítulo sobre os reais é chamado um *corpo ordenado*. Ou seja: até agora temos exigido que o $(\mathbb{R}\,;0,1,+,-,\cdot,>)$ é *um* corpo ordenado. Conhecendo o conjunto $\mathbb{Q}$ dos *racionais*, percebemos que o $(\mathbb{Q}\,;0,1,+,-,\cdot,>)$ também é um corpo ordenado. Em palavras mais formais, tanto os reais quanto os racionais são o que a gente chama de *modelos* de corpos ordenados. O que temos estipulado então, não é suficiente para *determinar os reais*, pois nem consegue diferenciá-los dos racionais.

? **Q6.54. Questão.** Podemos adicionar alguma lei capaz de separar os reais dos racionais? Ou seja, chegar numa lista de leis mais exigentes, tais que os reais vão ser um modelo, mas os racionais não.

!! SPOILER ALERT !!

A verdade é que falta só um axioma que realmente vai determinar os reais. Mas conseguir enxergá-lo neste momento é um grande desafio.[47] Pelo menos já estamos prontos para conhecer o que falta para a pergunta virar mais fácil: o *supremum* e seu conceito dual, o *infimum*. Conhecemos logo (§148) para finalmente chegar numa resposta (§154). Mas antes de tudo isso, vamos falar de distâncias.

Intervalo de problemas

TODO Add problems

§148. Infimum e supremum

D6.55. Definição (cotas). Seja $A \subseteq \mathbb{R}$. Dizemos que c é uma *cota inferior* (ou *lower bound*) de A sse $c \leq A$; e, *dualmente*, c é uma *cota superior* (ou *upper bound*) de A sse $c \geq A$:

$$c \text{ é uma cota inferior de } A \overset{\text{def}}{\iff} c \leq A \iff (\forall a \in A)[\, c \leq a \,];$$
$$c \text{ é uma cota superior de } A \overset{\text{def}}{\iff} A \leq c \iff (\forall a \in A)[\, a \leq c \,].$$

Denotamos o conjunto de todas as cotas inferiores de A por $(\leq A)$ ou $(A \geq)$ e dualmente usamos $(A \leq)$ ou $(\geq A)$ para o conjunto de todas as suas cotas superiores:

$$(\leq A) \overset{\text{def}}{=} \{\, x \mid x \leq A \,\};$$
$$(A \leq) \overset{\text{def}}{=} \{\, x \mid A \leq x \,\}.$$

[47] Vai desistir de pensar em alguma resposta por causa disso?

Se um conjunto A tem pelo menos uma cota inferior, dizemos que A é *cotado inferiormente* (ou, *bounded below*); e se tem pelo menos uma cota superior, ele é *cotado superiormente* (ou, *bounded above*). Chamamos um conjunto de *cotado* se é cotado inferiormente e superiormente; senão, ele é um conjunto *ilimitado*.[48]

D6.56. Definição (infimum; supremum). A *melhor cota inferior* é chamada *ínfimo* ou *infimum*, e a *melhor cota superior* é chamada *supremo* ou *supremum*:

$$\begin{aligned} c \text{ é um infimum de } A &\overset{\text{def}}{\iff} \overbrace{c \le A}^{\text{cota inferior}} \;\&\; \overbrace{(\forall c' \le A)[\, c \ge c' \,]}^{\text{a melhor}}; \\ c \text{ é um supremum de } A &\overset{\text{def}}{\iff} \underbrace{c \ge A}_{\text{cota superior}} \;\&\; \underbrace{(\forall c' \ge A)[\, c \le c' \,]}_{\text{a melhor}}. \end{aligned}$$

Escrevemos $c = \inf A$ e $c = \sup A$ respectivamente, mas, como o leito deve ter suspeitado, *não se tratam literamente de igualdades,* pois suas partes direitas sequer foram definidas "em isolação" mesmo—veja mais sobre essa possibilidade no Cuidado 6.59. As tipagens corretas aqui então são as:

$$_ = \inf _ : \mathsf{Real} \times \mathsf{Set\ Real} \to \mathsf{Prop} \qquad _ = \sup _ : \mathsf{Real} \times \mathsf{Set\ Real} \to \mathsf{Prop}.$$

▸ **EXERCÍCIO x6.82.**
O que *devemos* demonstrar agora para justificar esse abuso notacional que criou essas "conjunções disfarçadas com roupas de igualdades"? (x6.82H1)

Θ6.57. Teorema (Unicidade de inf e sup). *Seja A : Set Real. Se A tem infimum, ele é único. Dualmente, se A tem supremum, ele é único.*

Demonstração. Por fight club: suponha ℓ, ℓ' são infima, logo $\ell \le \ell'$ pois ℓ' é maior que qualquer cota inferior, e ℓ é uma cota inferior. No outro lado $\ell' \le \ell$ pois ℓ é maior que qualquer cota inferior, e ℓ' é uma cota inferior. Logo $\ell \le \ell'$ e $\ell' \le \ell$ e pela antissimetria da $(\le)$ temos $\ell = \ell'$.

A unicidade dos supremos é *dual*.[49] ∎

D6.58. Notação (Açúcar sintáctico). Com as unicidades estabelecidas podemos introduzir realmente os símbolos

$$\inf A \overset{\text{def}}{=} \max(\le A) \qquad \sup A \overset{\text{def}}{=} \min(\ge A).$$

Outros nomes (e notações correspondentes) desses dois conceitos são muito comuns e vamos ficar os usando também: o infimum é chamado também de *greatest lower bound* e o supremum de *least upper bound*, e denotados por glb e lub respectivamente:

$$\operatorname{glb} A \overset{\text{def}}{=} \inf A \qquad \operatorname{lub} A \overset{\text{def}}{=} \sup A.$$

E olha que no Capítulo 14 encontramos ainda mais nomes e notações!

[48] O que chamamos aqui de *cota* e de *cotado* são também chamados *limitante* e *limitado*, mas vou evitar esses termos por causa da conexão etimológica que essas palavras têm com a palavra «limite».

[49] Finja que leu a palavra *similar* aqui.

! **6.59. Cuidado.** Assim, inf e sup não são operações totais nos reais, mas sim *parciais:*

$$\inf, \sup : \mathsf{Set}\ \mathsf{Real} \rightharpoonup \mathsf{Real}.$$

Ou seja, ninguém garanta que para qualquer $A : \mathsf{Set}\ (\mathsf{Real})$ existe mesmo um real x que satisfaz as condições das definições acima, traduzidas aqui assim:

$$\inf A \stackrel{\text{def}}{=} \text{o único infimum de } A, \text{ se existe;}$$
$$\sup A \stackrel{\text{def}}{=} \text{o único supremum de } A, \text{ se existe.}$$

6.60. Os reais estendidos. Agora, se A não é cotado inferiormente e se A não é cotado superiormente escrevemos

$$\inf A = -\infty \qquad \text{e} \qquad \sup A = +\infty$$

respectivamente. Isso é bem justificável se pensar no $\mathbb{R}$ apenas como um conjunto ordenado sendo enriquecido por dois novos objetos distintos que denotamos por '$-\infty$' e '$+\infty$' chegando assim no conjunto

$$\{-\infty\} \cup \mathbb{R} \cup \{+\infty\}$$

que ordenamos assim:

$$-\infty < x < +\infty, \quad \text{para todo } x \in \mathbb{R}.$$

Chamamos os membros do $\mathbb{R} \cup \{-\infty, +\infty\}$ de *reais estendidos* e denotamos esse conjunto por $\overline{\mathbb{R}}$ e $[-\infty, +\infty]$ também. Então podemos considerar ambas as operações agora como

$$\inf, \sup\ : \mathsf{Set}\ \mathsf{Real} \rightharpoonup [-\infty, +\infty].$$

6.61. Observação (Type errors?). Meu leitor alerto talvez teve uns suspeitos de type errors na Nota 6.60. De fato tem, mas felizmente são todos resolvíveis com uns type castings. Tecnicamente precisamos de um novo tipo ExtReal de dados para os reais extendidos, e umas funções para os trabalhos burocráticos que precisam ser feitos quando ocorre real num contexto onde esperamos real estendido e vice versa. O Exercício x6.83 é dedicado a isso:

▸ **EXERCÍCIO x6.83.**
Defina um tipo de ExtReal e mostra como ler a Nota 6.60 sem cair em type errors. (x6.83 H 1)

▸ **EXERCÍCIO x6.84.**
Seja $A \subseteq \mathbb{R}$. Demonstre que: (i) se $\inf A \in A$ então $\inf A = \min A$; (ii) a dual da (i). (x6.84 H 0)

▸ **EXERCÍCIO x6.85.**
Seja $A \subseteq \mathbb{R}$. Demonstre que $(\leq A)$ é vazio ou infinito, e a mesma coisa sobre o $(A \leq)$. (x6.85 H 0)

▸ **EXERCÍCIO x6.86.**
Demonstre ou refute: para quaisquer A, B habitados e sup-cotados,

$$A \subseteq B \implies \sup A \leq \sup B.$$

O que podemos dizer se remover a hipotese de habitados? E de cotados? (x6.86 H 0)

▸ **EXERCÍCIO x6.87.**
O sobre o inf? (x6.87 H 0)

▸ **EXERCÍCIO x6.88.**
Considere o conjunto

$$A = \left\{ m + \frac{1}{2^n} \;\middle|\; m \in \mathbb{N}, n \in \mathbb{N}_{>0} \right\}.$$

(i) Visualize o A na linha dos reais, e rascunhe seu desenho. (ii) Ache o $\inf A$ e $\sup A$ se existem. (x6.88 H 0)

▸ **EXERCÍCIO x6.89.**
Pode acontecer que para algum $A \subseteq \mathbb{R}$ temos...

(i) $\inf A = \sup A$?
(ii) $\inf A > \sup A$?

Se sim, quando? Se não, por que não? (x6.89 H 0)

▸ **EXERCÍCIO x6.90.**
No Capítulo 17 aumentaremos nosso vocabulário do nível-coração com bem mais gírias relacionadas às distâncias. Por enquanto tente adivinhar as definições dos conceitos seguintes: distância entre dois conjuntos de reais; distância entre um real e um conjunto de reais; diâmetro dum conjunto de reais; ponto isolado; ponto interior; ponto exterior; ponto de borda; conjunto cotado (esta última noção deve acabar sendo extensionalmente mas não intensionalmente equivalente à noção de conjunto inferiormente e superiormente fechado). (x6.90 H 0)

E agora... Será que podes pensar numa resposta para a Questão Q6.54? A resposta demora pouco ainda (§154), mas este ponto é um ponto bom para formar uma tentativa boa de palpite. Tente!

§149. Epsilons

Θ6.62. Teorema. *Seja x real tal que para todo $\varepsilon > 0$, $0 \leq x < \varepsilon$. Logo $x = 0$.*

Demonstração. Como $x \geq 0$, basta eliminar o caso $x > 0$ (Exercício x6.91). ∎

▸ **EXERCÍCIO x6.91.**
Elimine! (x6.91 H 1)

6.63. Corolário. *Sejam a, b reais tais que para todo $\varepsilon > 0$, $a - \varepsilon < b < a + \varepsilon$. Logo $a = b$.*

Demonstração. Tua: Exercício x6.92. ∎

▸ **EXERCÍCIO x6.92.**
Demonstre. (x6.92 H 1)

▸ **EXERCÍCIO x6.93.**
Sejam a, b reais. Se para todo $\varepsilon > 0$, $a < b + \varepsilon$, então $a \leq b$. (x6.93 H 0)

§150. Distância

S6.64. Especificação (distância). Seja $d : \alpha \times \alpha \to \mathsf{Real}$. Dizemos que d é uma *distância* (ou *métrica*) no α sse todas as propriedades seguintes são satisfeitas:

(D-Range)	$d(x, y) \geq 0$	positividade (1)
(D-Sym)	$d(x, y) = d(y, x)$	simetria
(D-Tri)	$d(x, y) \leq d(x, w) + d(w, y)$	triangular
(D-EqZero)	$d(x, x) = 0$	positividade (2)
(D-ZeroEq)	$d(x, y) = 0 \implies x = y.$	positividade (3)

Chamamos a d de *pré-distância* (ou *pré-métrica*, ou *pseudométrica*) sse ela satisfaz as primeiras quatro dessas propriedades.

6.65. Observação. Qual propriedade exatamente está sendo referida pelo termo «positividade» varia na literatura, mas costuma ser uma ou uma combinação das (1)–(3) anotadas acima; eu vou evitar esse termo aqui. A (D-EqZero) é equivalente à recíproca da (D-ZeroEq), e por isso às vezes são juntadas em uma proposição só:

$$d(x, y) = 0 \iff x = y.$$

A contrapositiva da (D-ZeroEq), graças à (D-Range) acaba sendo equivalente à

$$x \neq y \implies d(x, y) > 0.$$

que deixa mais clara a escolha do seu rótulo; em muitos textos é apresentada assim—aqui não. A (D-Tri) é conhecida como *desigualdade triangular*, um nome melhor justificado quando consideramos distâncias num plano, onde corresponde à idéia que o melhor (mais curto) caminho entre dois pontos é aquele que vai direto de um (x) para o outro (y); medindo via terceiros pontos (w), em geral, pode aumentar a distância.

D6.66. Definição (distância euclideana). Chamamos a função

$$\begin{aligned} d &: \mathsf{Real} \times \mathsf{Real} \to \mathsf{Real} \\ d(a, b) &\stackrel{\text{def}}{=} |a - b| \,. \end{aligned}$$

de *distância eulideana*.

D6.67. Definição (distância discreta). Chamamos a função

$$\begin{aligned} d_0 &: \mathsf{Real} \times \mathsf{Real} \to \mathsf{Real} \\ d_0(a, b) &\stackrel{\text{def}}{=} \begin{cases} 0, & \text{se } a = b; \\ 1, & \text{se } a \neq b. \end{cases} \end{aligned}$$

de *distância discreta*.

Decidir chamar uma função de «distância» não signifia que, de fato é. Precisamos verificar que ela atende a Especificação S6.64. «Precisamos»? Quis dizer, precisas. Agora.

▸ **EXERCÍCIO x6.94.**
Justifique: a distância euclideana, de fato, é uma distância, ou seja, atende a Especificação S6.64. (x6.94 H 0)

▸ **EXERCÍCIO x6.95.**
A distância discreta também. (x6.95 H 0)

6.68. Qual distância?. O estudo abstrato de distâncias, viz., a teoria dos espaços métricos, é o assunto do Capítulo 17. Para meus propósitos neste capítulo vamos concordar que quando é envolvida uma métrica ou mencionada a palavra distância na conversa, sempre será a distância euclideana (D6.66) exceto se especificamente mencionar outra. No que segue, d denota uma métrica, ou seja, uma função que satisfaz a Especificação S6.64.

D6.69. Definição (ε-perto). Seja x, y reais e $\varepsilon > 0$. Dizemos que

$$\text{o } x \text{ é } \varepsilon\text{-perto do } y \iff^{\text{def}} d(x,y) < \varepsilon.$$

Observe que a relação é simétrica (Exercício x6.97) e logo podemos escrever também:

$$\text{os } x, y \text{ são } \varepsilon\text{-perto (entre si)}.$$

• **EXEMPLO 6.70.**
Os 1 e 2/3 são 1/2-perto (com a distância euclideana, mas não com a distância discreta).

▸ **EXERCÍCIO x6.96.**
Dado $\varepsilon > 0$, seja $(\sim_\varepsilon)$ a relação definida pela

$$x \sim_\varepsilon y \iff^{\text{def}} x \text{ é } \varepsilon\text{-perto do } y.$$

Demonstre que $(\sim_\varepsilon)$ é reflexiva. (x6.96 H 1)

▸ **EXERCÍCIO x6.97.**
Dado $\varepsilon > 0$, a $(\sim_\varepsilon)$ do Exercício x6.96 é simétrica, e logo podemos escrever frases como

$$\text{«os } x, y \text{ são } \varepsilon\text{-perto (entre si)»}.$$

(x6.97 H 0)

▸ **EXERCÍCIO x6.98.**
Existe algum $\varepsilon > 0$ para qual a $(\sim_\varepsilon)$ do Exercício x6.96 é uma relação *transitiva*?

$$(\sim_\varepsilon) \text{ é transitiva} \iff (\forall a, b, c)[\, a \sim_\varepsilon b \;\&\; b \sim_\varepsilon c \implies a \sim_\varepsilon c\,].$$

(x6.98 H 1)

D6.71. Definição (ε-bola). Dado um ponto c, chamamos o conjunto de todos os pontos que são ε-perto do c de *ε-bola do c*:

$$\mathcal{B}_\varepsilon(c) \stackrel{\text{def}}{=} \{\, x \mid x \text{ é } \varepsilon\text{-perto de } c \,\}.$$

Também chamamos de *bola com centro c e raio ε*.

• **EXEMPLO 6.72.**
A 1/3-bola do 7 é o intervalo $(7 - 1/3, 7 + 1/3)$ e a 2-bola do 0 o $(-2, 2)$.

▸ **EXERCÍCIO x6.99.**
Ache as mesmas bolas mas considerando como distância a discreta. (x6.99 H 0)

Λ6.73. Lema (bolas nos reais). *Nos reais, bolas são intervalos da forma (u, v) (com u, v reais) e vice-versa.*

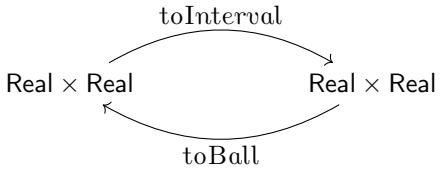
Demonstração. Associamos cada bola com um intervalo e vice versa (quase isso: Observação 6.74).
De bola $\mathcal{B}_r(c)$ para intervalo $(_, _)$. A bola $\mathcal{B}_r(c)$ é o intervalo $(c - r, c + r)$:

$$\begin{aligned}\mathcal{B}_r(c) &= \{\, x \mid d(x, c) < r \,\} \\ &= \{\, x \mid |x - c| < r \,\} \\ &= \{\, x \mid c - r < x < c + r \,\} \\ &= (c - r, c + r).\end{aligned}$$

De intervalo (u, v) para bola $\mathcal{B}_(_)$. Essa parte é tua (Exercício x6.100). ∎

▸ **EXERCÍCIO x6.100.**
Termine a demonstração do Lema Λ6.73. (x6.100 H 1)

6.74. Observação. Efetivamente definimos funções



entre centros-raios (de bolas) e inícios-fins (de intervalos), e tais funções são inversas entre si (são?—x6.101). Note que esses nomes não são exatamente honestos: bolas e intervalos são conjuntos de reais, não parzinhos de reais. Cada um desses conjuntos (tanto bola quanto intervalo), se é habitado, tem uma única representação como parzinho de centro-raio, e uma única representação como parzinho de início-fim. Essas funções efetivamente traduzem entre tais representações. E uma bola vazia? E um intervalo vazio? Ambos são o mesmo conjunto: o $\emptyset$: Set Real; só que, visto como bola, ele tem uma infinidade de representações (quais?—x6.101) e visto como intervalo, também (quais?—x6.101). As traduções estabelecidas mantêm a correspondência até entre tais representações, algo que nem seria necessário para o objetivo de demonstrar o Lema Λ6.73.

▸ **EXERCÍCIO x6.101.**
São? Quais? Quais? (x6.101 H 0)

D6.75. Definição (diâmetro). Seja A um conjunto de reais. Se o conjunto de todas as possíveis distâncias entre seus membros

$$\{\, d(a,b) \mid a,b \in A \,\}$$

possui supremum, o chamamos de *diâmetro* de A. Ou seja,

$$s = \operatorname{diam} A \overset{\text{def}}{\iff} s = \sup\{\, d(a,b) \mid a,b \in A \,\}$$

escrevendo também

$$\operatorname{diam} A = -\infty \overset{\text{def}}{\iff} \sup A = -\infty; \qquad \operatorname{diam} A = +\infty \overset{\text{def}}{\iff} \sup A = +\infty.$$

Aproveitando a ordem dos reais estendidos escrevemos

$$\operatorname{diam} A < +\infty$$

quando $\operatorname{diam} A = -\infty$ ou quando para algum real s temos $s = \operatorname{diam} A$.

D6.76. Definição (cercado). Chamamos um conjunto de reais de *cercado* sse ele está contido numa bola:

$$A \text{ cercado} \overset{\text{def}}{\iff} (\exists c)(\exists M)[\, A \subseteq \mathcal{B}_M(c) \,].$$

▸ **EXERCÍCIO x6.102.**
Seja A conjunto de reais.

$$A \text{ cotado} \overset{?}{\iff} A \text{ cercado}.$$

(x6.102 H 0)

▸ **EXERCÍCIO x6.103.**
No Exercício x6.102 a resposta depende da métrica escolhida? Justifique tua resposta com um contraexemplo ou com uma demonstração, dependendo de se foi «sim» ou «não». Lembre-se que implicitamente munimos os reais com a métrica euclideana (Definição D6.66). (x6.103 H 0)

§151. Limites

D6.77. Definição (pvsgd). Sejam $\varphi : \mathsf{Real} \to \mathsf{Prop}$ um predicado sobre reais e $(a_n)_n$ uma seqüência de reais. Dizemos que *para valores suficientemente grandes de* n, $\varphi(a_n)$ sse a partir de um natural N "todos os $a_$'s" satisfazem a φ, ou seja, sse

$$(\exists N)(\forall n \geq N)[\, \varphi(a_n) \,].$$

• **EXEMPLO 6.78.**
Para valores suficientemente grandes de n, $2^n > n^4 > 8n$. Por outro lado, não é o caso que para valores suficientemente grandes de n, o ano n é bissexto.

D6.79. Definição (eventualmente). Seja um predicado $\varphi : \mathsf{Seq}\ \mathsf{Real} \to \mathsf{Prop}$ sobre seqüências de reais, e seja $(a_n)_n$ uma seqüência de reais. Dizemos que a $(a_n)_n$ *eventualmente* satisfaz o φ sse para algum N, a subseqüência $(a_n)_{n\geq N}$ satisfaz o φ, ou seja,

$$\text{eventualmente } \varphi\,((a_n)_n) \iff^{\mathsf{def}} (\exists N)\Big[\,\varphi\,\Big((a_n)_{n\geq N}\Big)\,\Big].$$

• **EXEMPLO 6.80.**
A seqüência $\big(\lfloor 2^8/n \rfloor\big)_n$ é eventualmente constante (ainda mais, ela é eventualmente 0). Para qualquer $\varepsilon > 0$, ela não está eventualmente contida no $(\varepsilon, +\infty)$; ainda mais, ela fica eventualmente fora dele!

6.81. Corolário. *Seja $(a_n)_n$ uma seqüência legal (qualquer coisa que isso significa). Logo $(a_n)_n$ é eventualmente legal.*

DEMONSTRAÇÃO. Basta escolher $N := 0$, já que a subseqüência $(a_n)_{n\geq 0}$ é a própria seqüência $(a_n)_n$. ∎

6.82. Observação. Usamos as mesmas gírias sobre $\mathsf{Seq}\,\alpha$; nada especial sobre o Real aqui.

D6.83. Definição (limite). Sejam $(a_n)_n$ uma seqüência de reais e ℓ um real. Dizemos que $(a_n)_n$ *tende ao* ℓ (ou *converge ao* ℓ) sse para qualquer bola de ℓ, a seqüência $(a_n)_n$ eventualmente fica dentro dela. Escrevemos $(a_n)_n \to \ell$; ou seja, definimos o

$$_ \to _ : \mathsf{Seq}\ \mathsf{Real} \times \mathsf{Real} \to \mathsf{Prop}$$

assim:

$$\begin{aligned}
(a_n)_n \to \ell &\iff^{\mathsf{def}} \text{qualquer bola de } \ell \text{ eventualmente contem a seqüência } (a_n)_n \\
&\iff (\forall \varepsilon > 0)[\,(a_n)_n \text{ está eventualmente contida na } \mathcal{B}_\varepsilon(\ell)\,] \\
&\iff (\forall \varepsilon > 0)[\,(a_n)_n \text{ eventualmente fica } \varepsilon\text{-perto de } \ell\,] \\
&\iff (\forall \varepsilon > 0)[\,\text{para valores suficientemente grandes de } n,\ a_n \text{ é } \varepsilon\text{-perto de } \ell\,] \\
&\iff (\forall \varepsilon > 0)(\exists N)\Big[\,(a_n)_{n\geq N} \subseteq \mathcal{B}_\varepsilon(\ell)\,\Big] \\
&\iff (\forall \varepsilon > 0)(\exists N)[\,\text{a partir de } N, \text{ todos os } a_n\text{'s são } \varepsilon\text{-perto de } \ell\,] \\
&\iff (\forall \varepsilon > 0)(\exists N)(\forall n \geq N)[\,a_n \text{ é } \varepsilon\text{-perto de } \ell\,] \\
&\iff (\forall \varepsilon > 0)(\exists N)(\forall n \geq N)[\,d(a_n, \ell) < \varepsilon\,].
\end{aligned}$$

Escrevemos também

$$\lim_n a_n = \ell \qquad \text{ou} \qquad \lim (a_n)_n = \ell$$

como sinônimo de $(a_n)_n \to \ell$, e caso que isso aconteça referimos a tal ℓ como um *limite* da $(a_n)_n$. Dizemos que uma seqüência é *convergente* sse ela converge àlgum real:

$$(a_n)_n \text{ é convergente} \iff^{\mathsf{def}} (\exists \ell)[\,(a_n)_n \to \ell\,].$$

Senão, ela é *divergente*. Destacamos um especial de seqüência divergente: dizemos que $(a_n)_n$ *diverge ao* $+\infty$ (ou até *tende ao* $+\infty$) sse para qualquer $M > 0$ ela eventualmente fica acima do M, ou seja definimos o

$$_ \to +\infty : \mathsf{Seq\ Real} \to \mathsf{Prop}$$

assim:

$$\begin{aligned}(a_n)_n \to +\infty &\overset{\text{def}}{\iff} \text{a seqüência } (a_n)_n \text{ eventualmente supera qualquer } M > 0\\ &\iff (\forall M > 0)[\,\text{eventualmente } (a_n)_n > M\,]\\ &\iff (\forall M > 0)(\exists N)\Big[\,(a_n)_{n\geq N} > M\,\Big]\\ &\iff (\forall M > 0)(\exists N)(\forall n \geq N)[\,a_n > M\,].\end{aligned}$$

Escrevemos também

$$\lim_n a_n = +\infty \qquad \text{ou} \qquad \lim (a_n)_n = +\infty.$$

Similarmente definimos o $_ \to -\infty : \mathsf{Seq\ Real} \to \mathsf{Prop}$.

6.84. Observação. É muito comum usar o nome 'n_0' onde usei o 'N' nessas definições. O 'n_0' é freqüêntemente lido «n nought» em inglês.

• **EXEMPLO 6.85.**
Dizemos que:

a seqüência	$(1)_n = 1, 1, 1, \ldots$	tende ao 1;
a seqüência	$(1/n)_n = 1, 1/2, 1/3, 1/4, \ldots$	tende ao 0;
a seqüência	$((-1)^n)_n = 1, -1, 1, -1, \ldots$	diverge;
a seqüência	$(n)_n = 0, 1, 2, 3, \ldots$	diverge ao $+\infty$.

▸ **EXERCÍCIO x6.104.**
Uma notação introduzida na Definição D6.83 é problemática; qual o problema e o que devemos fazer para resolvê-lo? (x6.104 H 1)

6.86. Quantificadores alternantes. Provavelmente essa foi a primeira definição que tu encontraste que necessitou três alternações de quantificadores:

$$\forall \ldots \exists \ldots \forall \ldots$$

Para cada alteração de quantificação que seja adicionada numa afirmação, o processo de digeri-la naturalmente fica mais complicado para nossa mente! Com experiência, *matemalhando*, essas definições com três quantificadores ficarão mais e mais digeríveis. Mesmo com essa experiência, num momento vamos encontrar uma afirmação com *quatro* quantificações alternantes, e a dificuldade vai voltar e te lembrar dessa dificuldade que talvez sentes agora. Felizmente, temos duas ferramentas indispensáveis que deixam o processo bem mais tranqüilo do que talvez parece: (i) *as ferramentas formais dos fundamentos matemáticos* que nos permitem trabalhar com proposições sem necessariamente digeri-las completamente; (ii) *as ferramentas informais das gírias* que estamos desenvolvendo com e para nosso coração matemático que nos ajudam entender, visualizar, e pensar sobre as noções e proposições sobre quais estamos trabalhando. (Divulguei isso na Secção §19 mas provavelmente era cedo demais para ser devidamente entendido e apreciado.)

6.87. Jogos e estratégias. Considere que quero demonstrar que $(a_n)_n \to 4$. Meu alvo então, olhando na última linha da Definição D6.83, é

$$(\forall \varepsilon > 0)(\exists N)(\forall i \geq N)[\, d(a_i, 4) < \varepsilon \,].$$

Considere um jogo, onde eu estou jogando contra meu inimigo, o jogador-($\exists$) debatendo a vericidade dessa proposição. (Eu sou o jogador-($\forall$).) Cada troca de tipo-de-quantificador corresponde em troca de jogador para jogar. O jogo começa então com o ($\forall$) escolhendo um $\varepsilon > 0$: vamos dizer o $1/2$; interpretamos seu movimento como um desafio. Respondemos a ele escolhendo um N (vamos dizer o 6) e agora novamente é a vez do ($\forall$) jogar. Ele precisa escolher um $i \geq 6$, e ele escolhe o 8. Agora acabaram os quantificadores, e logo podemos olhar na proposição formada por essas escolhas:

$$d(a_8, 4) < 1/2.$$

Se ela é válida, ganhei. Senão, perdi. O dialogo desta jogada ficou assim:

- Duvido que para o $1/2 > 0$ tu consegue escolher um N que serve.
- Escolho o 6.
- Escolho o 8 (posso pois $8 \geq 6$).

Note que não podemos inferir a corretude duma proposição dessas a partir duma partida. Talvez eu perdi só porque fui burro enquanto se tivesse jogado melhor eu teria ganhado. Mas também talvez ganhei só porquê meu inimigo foi burro, e jogando contra um jogador melhor eu ia perder. O que podemos de fato usar (para inferir em forma correta que uma tal proposição é válida) é a existência duma *estratégia vencedora* para mim, ou seja, uma estratégia que determina como eu preciso jogar contra qualquer possível movimento do meu inimigo e chegar numa vitória.

• **EXEMPLO 6.88.**
A seqüência $1, 1, 1, \ldots$ tende a 1.
RESOLUÇÃO. Seja $\varepsilon > 0$. O desafio é achar um N tal que a partir de N, todos os membros da seqüência são ε-perto de 1. Tome $N := 0$, e seja $n \geq N$. Obviamente o n-ésimo termo da seqüência é ε-perto do 1, pois ele é igual ao 1 mesmo, e logo a distância deles é 0, e logo menor que ε. Observe que qualquer escolha de N aqui funcionaria para fechar a demonstração.

▸ **EXERCÍCIO x6.105.**
$(a_n)_n$ eventualmente convergente $\iff$ $(a_n)_n$ convergente. (x6.105 H 0)

▸ **EXERCÍCIO x6.106.**
$(a_n)_n$ constante $\implies$ $(a_n)_n$ convergente. (x6.106 H 0)

▸ **EXERCÍCIO x6.107.**
$(a_n)_n$ eventualmente constante $\implies$ $(a_n)_n$ convergente. (x6.107 H 0)

▸ **EXERCÍCIO x6.108.**
Toda seqüência que diverge ao $+\infty$, diverge. (x6.108 H 0)

Como tu já resolveste o Exercício x6.104—né?—tu sabes que precisamos demonstrar a unicidade dos limites. E a existência? A existência não é garantida (vamos descobrir isso agora no Exemplo 6.89), então precisamos tomar os mesmos cuidados com o símbolo lim que tomamos com os sup, min, etc.; e precisando vê-lo como operador, é um operador *parcial*.

- **EXEMPLO 6.89.**
A seqüência $0, 1, 0, 1, \ldots$, definida pela

$$a_n \stackrel{\text{def}}{=} \begin{cases} 0, & \text{se } n \text{ par;} \\ 1, & \text{caso contrário;} \end{cases}$$

é divergente.
DEMONSTRAÇÃO. Primeiramente: o que precisamos demonstrar? Que para qualquer possível limite ℓ,

$$(a_n)_n \not\to \ell.$$

Seja ℓ tal que $(a_n)_n \to \ell$. O que isso significa?

$$(a_n)_n \to \ell \stackrel{\heartsuit}{\iff} (\forall \varepsilon > 0)(\exists N)[\, N \text{ garanta que a partir dele todos são } \varepsilon\text{-perto de } \ell\,].$$

Para conseguir usar esse dado (um $(\forall)$), basta aplicá-lo em qualquer real positivo que queremos, e ele vai fornecer de volta um novo dado. Por exemplo, o aplicando no 1 (que de fato é positivo: x6.33) obtemos o novo dado

$$(\exists N)[\, N \text{ garanta que a partir dele todos os } a_i\text{'s são 1-perto de } \ell\,].$$

Para aproveitar esse novo dado agora, solicitamos tal N. Seja N tal que

$$(\forall n \geq N)[\, a_n, \ell \text{ são 1-perto}\,].$$

Novamente um $(\forall)$; essa vez para utilizá-lo precisamos o aplicar em naturais a partir do N. Agora a idéia é conseguir dois membros da seqüência que são suficientemente longe entre si para garantir que não tem como ambos estar 1-perto de ℓ.

Refletindo pouco deve parecer óbvio que não temos como conseguir isso. Nossa seqüência só pega os valores $0, 1$, cuja distância é 1, e logo considerando o $\frac{1}{2}$ como um possível ℓ percebemos que ambos conseguem ficar 1-perto dele. Qual foi o problema?

Nossa escolha de $\varepsilon > 0$ foi grande demais. A gente poderia ter escolhido um epsilonzinho melhor, como por exemplo o $1/2$ ou o $1/4$. Precisamos um tal que, para qualquer candidato ℓ, a ε-bola dele vai ser tão pequena que seria impossível possuir dois membros com distança 1, como os únicos membros da nossa seqüência tem $(d(0,1) = 1)$. Aqui poderíamos escolher o $1/2$, e daria certo, mas não existe motivo de ser tão dramáticos. Vamo escolher algo menor ainda; que tal $1/3$. Obtemos assim um novo N, essa vez garantindo que a partir dele todos os membros da seqüência são $1/3$-perto de ℓ. Como $2N, 2N+1 \geq N$, logo os a_{2N} e a_{2N+1} ambos são $1/3$-perto de ℓ. Calculamos:

$$d(a_{2N}, a_{2N+1}) = d(0,1) = |0 - 1| = 1;$$

mas também:

$$\begin{aligned} d(a_{2N}, a_{2N+1}) &\leq d(a_{2N}, \ell) + d(\ell, a_{2N+1}) \qquad ((\leq)\text{-triangular}) \\ &< 1/3 + d(\ell, a_{2N+1}) \\ &< 1/3 + 1/3 \\ &= 2/3, \end{aligned}$$

chegando assim na contradição $1 < \frac{2}{3}$.

Θ6.90. Teorema (unicidade de limites). *Seja* $(a_n)_n$ *seqüência de reais tal que*

$$(a_n)_n \to \ell_1 \qquad\qquad (a_n)_n \to \ell_2.$$

Logo $\ell_1 = \ell_2$.

Demonstração. Graças ao Teorema Θ6.62 basta demonstrar que $d(\ell_1, \ell_2) < \varepsilon$ para todo $\varepsilon > 0$. Seja $\varepsilon > 0$ então, e agora observe que para quaisquer $\varepsilon_1, \varepsilon_2 > 0$ podemos escolher N_1, N_2 tais que:

$$(\forall i \geq N_1)[\, d(a_i, \ell_1) < \varepsilon_1 \,] \qquad\qquad (\forall i \geq N_2)[\, d(a_i, \ell_2) < \varepsilon_2 \,].$$

Seja $N = \max\{N_1, N_2\}$. Logo

$$d(a_N, \ell_1) < \varepsilon_1 \qquad\qquad d(a_N, \ell_2) < \varepsilon_2.$$

Calculamos

$$\begin{aligned} d(\ell_1, \ell_2) &\leq d(\ell_1, a_N) + d(a_N, \ell_2) && \text{((D-Tri))} \\ &= d(\ell_1, a_N) + d(\ell_2, a_N) && \text{((D-Sym))} \\ &< \varepsilon_1 + \varepsilon_2. && \text{(escolha dos } \varepsilon_1, \varepsilon_2\text{)} \end{aligned}$$

Lembre-se que isso é válido para quaisquer $\varepsilon_1, \varepsilon_2 > 0$, então basta selecioná-los para satisfazer $\varepsilon_1 + \varepsilon_2 \leq \varepsilon$ (tome por exemplo ambos (menores ou) iguais ao $\varepsilon/2$). Assim demonstramos que para todo $\varepsilon > 0$,

$$0 \leq d(\ell_1, \ell_2) < \varepsilon, \qquad\qquad \text{(a } (0 \leq) \text{ vem pela (D-Range))}$$

e logo $d(\ell_1, \ell_2) = 0$ (pelo Teorema Θ6.62), e portanto $\ell_1 = \ell_2$ (pela (D-ZeroEq)). ∎

6.91. Teaser (conjuntos dirigidos). Com a linha

> «Seja $N = \max\{N_1, N_2\}$.»

eu apenas escolhi um nome ('N') para referir ao $\max(N_1, N_2)$—só para facilitar minha escrita mesmo. Note que esta linha *não foi* uma solicitação feita usando um dado existencial ($\exists$).[50] Mas a única propriedade que precisei desse N na demonstração foi a $N \geq \{N_1, N_2\}$ e logo eu poderia ter usado a linha

> «Seja N tal que $N \geq \{N_1, N_2\}$.»,

essa vez usando mesmo um teoreminha que garanta tal existência. Considere um conjunto habitado $D : \mathsf{Set}\ \mathsf{Nat}$ e membros dele $d_1, d_2 \in D$. O mundo dos naturais já garanta que, sem precisar saber nada mais sobre o D nem sobre os d_1, d_2, existe membro $d \in D$ que *domina* ambos: um d tal que $d_1 \leq d$ e $d_2 \leq d$, uma cota superior deles dentro do próprio D. Como conseguir tal d? Simplesmente tome o máximo dos d_1, d_2, aproveitando que a ordem dos naturais é total e, o máximo sendo um dos dois, com certeza é um membro do D. Note que a mesma coisa vale sobre conjuntos de inteiros, de reais, e em geral conjuntos munidos com uma ordem total. E se não tiver essa totalidade aí? Muitas vezes basta saber a existência dum bicho no D com essa propriedade do d sem precisar ser o máximo, nem (menos forte) a melhor cota superior (o supremum), mas apenas (ainda menos forte) *uma cota superior* deles. Conjuntos como o D, cuja ordem garanta essa existência, são chamados *dirigidos* (ou *directed*) e seu papel vai acabar sendo critical mais que uma vez neste texto.

[50] Essa parte já foi feita quando definimos (D6.30) *a função* max.

▸ **EXERCÍCIO x6.109.**
Ache algo interessante para o «. . . ?. . . » e demonstre sua afirmação:

$$(a_n)_n \text{ convergente } \&\ \text{eventualmente } (a_n)_n \subseteq \mathbb{R}_{\mathbb{Z}} \implies \ldots ?\ldots$$

(x6.109 H 1)

▸ **EXERCÍCIO x6.110.**
$(a_n)_n$ eventualmente constante $\implies$ $(a_n)_n$ cotada. (x6.110 H 0)

Θ6.92. Teorema. *Toda seqüência de reais convergente é cercada.*

Demonstração. Seja $(a_n)_n$ convergente e logo seja ℓ seu limite. Logo, usando $\varepsilon := 1$ seja N tal que a partir do a_N todos os a_n's são 1-perto de ℓ, ou seja, $(a_n)_{n\geq N} \subseteq \mathcal{B}_1(\ell)$. Possivelmente precisamos um raio maior que 1 para conseguir conter a seqüência inteira. Observe que o conjunto $\{\, d(\ell, a_i) \mid i \leq N \,\}$ das distâncias entre o ℓ e seus primeiros termos (até o N-ésimo) é finito e habitado, e logo (pelo Exercício x6.65) seja M seu máximo.

$$M = \max\{\, d(\ell, a_i) \mid i \leq N \,\}.$$

Agora só basta verificar que a bola $\mathcal{B}_{M+1}(\ell)$ cerca a seqüência inteira (Exercício x6.111). ∎

▸ **EXERCÍCIO x6.111.**
Feche a demonstração do Teorema Θ6.92. (x6.111 H 0)

6.93. Corolário. *Toda seqüência convergente é cotada.*

Demonstração. Graças à equivalência entre cercada e cotada (Exercício x6.102) seque imediatamente pelo Teorema Θ6.92. ∎

▸ **EXERCÍCIO x6.112.**
Demonstre o Corolário 6.93 em forma direta, adaptando o que precisa na demonstração do Teorema Θ6.92. (x6.112 H 0)

§152. Limites e a estrutura atual

6.94. Comportamento respeituoso. Nossa estrutura atual de reais tem uma parte algébrica $(0, 1, +, \cdot, -)$ e uma parte relacional $(>)$. Estabelecemos agora que os limites se comportam bem (de forma *respeituosa*) com ambas as partes. Vamo começar com a parte algébrica.

▸ **EXERCÍCIO x6.113.**
Sejam $(a_n)_n$ seqüência de reais e a tal que $(a_n)_n \to a$. Seja c real. Logo:

$$(c + a_n)_n \to c + a.$$

(x6.113 H 0)

▸ **EXERCÍCIO x6.114.**
Sejam $(a_n)_n$ seqüência de reais e a tal que $(a_n)_n \to a$. Seja c real. Logo:

$$(ca_n)_n \to ca.$$

(x6.114 H 0)

▸ **EXERCÍCIO x6.115.**
Sejam $(a_n)_n, (b_n)_n$ seqüências de reais e a, b tais que $(a_n)_n \to a$ e $(b_n)_n \to b$. Logo:

$$(a_n + b_n)_n \to a + b.$$

(x6.115 H 0)

TODO analisar o próximo exercício

▸ **EXERCÍCIO x6.116.**
Sejam $(a_n)_n, (b_n)_n$ seqüências de reais e a, b tais que $(a_n)_n \to a$ e $(b_n)_n \to b$. Logo:

$$(a_n b_n)_n \to ab.$$

(x6.116 H 0)

▸ **EXERCÍCIO x6.117.**
Sejam $(a_n)_n, (b_n)_n$ seqüências de reais e a, b tais que $(a_n)_n \to a$ e $(b_n)_n \to b$. Considere a proposição:

$$(a_n/b_n)_n \to a/b.$$

Enuncie uma hipótese adicional necessária para sua demonstração e demonstre. (x6.117 H 0)

Θ6.95. Teorema. *Sejam $(a_n)_n, (b_n)_n$ seqüências de reais convergentes. Logo*

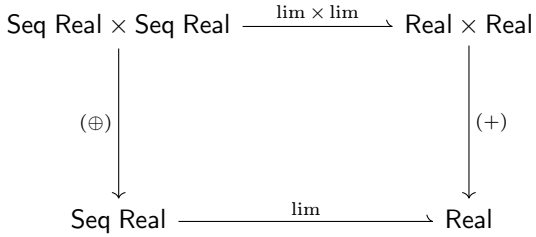
$$\lim_n(a_n + b_n) = \lim_n a_n + \lim_n b_n; \qquad \lim_n(-a_n) = -\lim_n a_n;$$
$$\lim_n(a_n \cdot b_n) = \lim_n a_n \cdot \lim_n b_n; \qquad \lim_n({b_n}^{-1}) = (\lim_n b_n)^{-1};$$
$$\lim_n(a_n/b_n) = \lim_n a_n / \lim_n b_n.$$

onde nas duas últimas supomos adicionalmente que todos os b_n's são não nulos, e o b também.

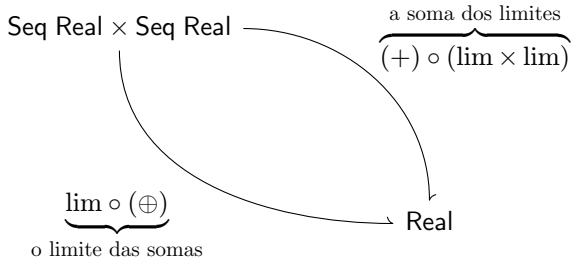
6.96. Diagramas comutativos. Podemos expressar o teorema

$$\frac{(a_n)_n \to a \qquad (b_n)_n \to b}{(a_n)_n \oplus (b_n)_n \to a + b}$$

(que acabei de expressar em forma de regra de inferência aqui) em forma dum *diagrama comutativo*, assim:



Mas o que significa que o diagrama acima comuta? Observe que temos duas maneiras de começar na esquina superior-esquerda e chegar na esquina inferior-direita: (i) atravessar à direita, e depois descer; ou (ii) descer, e depois atravessar. Observe que cada um desses caminhos determina uma função de tipo



e, afirmando que *o diagrama comuta*, afirmamos que esses caminhos correpondem em funções iguais.[51] Nesse diagrama, atravessar à direita corresponde em "pegar limites", enquanto descer corresponde em "somar". Note que não são exatamete as mesmas funções as correspondem no «atravessar à direita»: tendo um par de seqüências, denotamos por

$$\lim \times \lim \ : \mathsf{Seq\ Real} \times \mathsf{Seq\ Real} \rightharpoonup \mathsf{Real} \times \mathsf{Real}$$

a função que aplica a lim em cada componente da sua entrada e retorna o par das saidas:

$$(\lim \times \lim)\ ((a_n)_n, (b_n)_n) \stackrel{\mathsf{def}}{=} (\lim (a_n)_n, \lim (b_n)_n).$$

E sobre o «descer» também não é exatamente a mesma coisa nos dois lados: descer no lado direito é a soma $(+)$ entre reais, mas descer no lado esquerdo é a soma pointwise $(\oplus)$ entre seqüências de reais:

$$(\oplus) \ : \mathsf{Seq\ Real} \times \mathsf{Seq\ Real} \to \mathsf{Seq\ Real}$$
$$(\oplus) \stackrel{\mathsf{def}}{=} \mathfrak{pw}\ (+).$$

Tendo investigado a parte algébrica da estrutura dos reais tornamos agora para investigar a parte relacional.

▸ **EXERCÍCIO x6.118.**
Sejam $(a_n)_n, (b_n)_n$ seqüências de reais e a, b tais que $(a_n)_n \to a$ e $(b_n)_n \to b$. Adivinhe algo interessante que podemos inferir se $a < b$; enuncie e demonstre. (x6.118H123)

▸ **EXERCÍCIO x6.119.**
E o recíproco? (x6.119H0)

Θ6.97. Teorema Sanduíche. *Sejam* $(a_n)_n, (b_n)_n, (c_n)_n : \mathsf{Seq\ Real}$ *tais que*

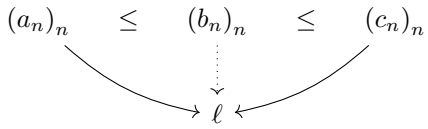
$$(a_n)_n \leq (b_n)_n \leq (c_n)_n.$$

Logo se $(a_n)_n$ *e* $(c_n)_n$ *tendem ao mesmo real* ℓ*, então* $(b_n)_n$ *também tende ao* ℓ*.*
DEMONSTRARÁS AGORA NO EXERCÍCIO x6.120. ∎

[51] Lembre que usamos o $(\rightharpoonup)$ quando se trata e função *parcial*, possivelmente não conseguindo retornar um valor do seu codomínio.

▸ **EXERCÍCIO x6.120.**
Demonstre o Teorema Sanduíche Θ6.97. (x6.120 H 0)

? **Q6.98. Questão.** No diagrama seguinte as setas denotam o «_ tende a _»:



Qual tua acha que é a interpretação da seta pontilhada?

!! SPOILER ALERT !!

6.99. Setas pontilhadas. A idéia é ler esses diagramas em dois tempos. No primeiro tempo ignore as setas pontilhadas: o que fica é o contexto, os dados, e as hipoteses. Leia isso como um «se a gente tem tudo isso...». As setas pontilhadas entram no segundo tempo, completando a implicação assim: «...então temos essas setas (pontilhadas) também.».

Θ6.100. Teorema. *Seja* $0 < \vartheta < 1$. *Logo* $(\vartheta^n)_n \to 0$.

Demonstração. Como $\vartheta < 1$, logo $1/\vartheta > 1$, e logo seja $\delta > 0$ tal que $1/\vartheta = 1 + \delta$. Seja $n \in \mathbb{N}$. Usando a desigualdade Bernoulli obtemos

$$0 \leq \vartheta^n = \frac{1}{(1+\delta)^n} \overset{(x6.50)}{\leq} \frac{1}{1+n\delta}.$$

Temos então

$$(0)_n \leq (\vartheta^n)_n \leq \left(\frac{1}{1+n\delta}\right)_n$$

com as seqüências à esquerda e à direita tendendo ao mesmo limite 0, e logo a $(\vartheta^n)_n$ que fica no meio também tende ao 0 pelo Teorema Sanduíche Θ6.97. ∎

§153. Seqüências autoconvergentes

D6.101. Definição (autoconvergente). Seja $(a_n)_n$ uma seqüência de reais. Dizemos que $(a_n)_n$ é *autoconvergente* (ou *Cauchy*) sse para qualquer $\varepsilon > 0$ existe um membro da seqüência tal que a partir dele, todos os seus membros são ε-perto entre si (dois a dois). Formalmente:

$$(a_n)_n \text{ autoconvergente} \overset{\text{def}}{\iff} (\forall \varepsilon > 0)(\exists N \in \mathbb{N})(\forall i, j \geq N)[a_i, a_j \text{ são } \varepsilon\text{-perto}].$$

Θ6.102. Teorema. *Toda seqüência de reais convergente é autoconvergente.*

▸ Esboço. Seja $(a_n)_n$ convergente com limite ℓ. Dado um desafio $\varepsilon > 0$, precisamos achar N tal que a partir de N os membros da $(a_n)_n$ ficam ε-perto entre si. A idéia é obter um índice tal que a partir dele todos os membros dá $(a_n)_n$ são $\frac{\varepsilon}{2}$-perto de ℓ. Assim quaisquer dois deles não podem ter distância maior que $\frac{\varepsilon}{2} + \frac{\varepsilon}{2}$. □

Θ6.103. Teorema. *Toda seqüência de reais autoconvergente é cercada.*

▸ Esboço. Suponha $(a_n)_n$ autoconvergente. Logo seja N tal que a partir de N, todos os a_n's ficam 1-perto entre si. Ou seja: $(\forall i, j \geq N)[\, d(a_i, a_j) < 1\,]$. Vou achar uma bola para cercar a seqüência. Basta determinar seu centro e seu raio. Como centro, tome o a_N. Observe (x6.121) que a bola $\mathcal{B}_1(a_N)$ contem todos os membros da $(a_n)_{n\geq N}$, mas não garanta nada sobre os $a_0, \ldots, a_{N-1}$. Como $\{a_i\}_{i\leq N}$ é finito e habitado, logo seja $r = \max\{\, d(a_N, a_i) \mid i \leq N \,\} + 1$. Observe (x6.121) que a bola $\mathcal{B}_r(a_N)$ contem todos os membros do $\{a_i\}_{i<N}$ mas não garanta nada sobre os $a_N, a_{N+1}, \ldots$. Basta então considerar a bola com raio o maior dos dois raios $M = \max(1, r)$ e verificar (x6.121) que, de fato, $(a_n)_n \subseteq \mathcal{B}_M(a_N)$. □

▸ **EXERCÍCIO x6.121.**
"Observe" o que ficou para observar, e verifique o que ficou para verificar na demonstração do Teorema Θ6.103. (x6.121 H 0)

6.104. Corolário. *Toda seqüência de reais autoconvergente é cotada.*

Demonstração. Imediato pois já demonstramos que nos reais cotada e cercada são noções equivalentes (Exercício x6.102). ▮

▸ **EXERCÍCIO x6.122.**
Demonstre o Corolário 6.104 em forma direta, adaptando o que precisa na demonstração do Teorema Θ6.103. (x6.122 H 0)

Tendo demonstrado as implicações

$$\text{convergente} \overset{\Theta 6.102}{\Longrightarrow} \text{autoconvergente} \begin{array}{l} \overset{\Theta 6.103}{\Longrightarrow} \text{cercada} \\ \overset{6.104}{\Longrightarrow} \text{cotada} \end{array}$$

obtemos novas demonstrações dos

$$\text{convergente} \begin{array}{l} \overset{\Theta 6.92}{\Longrightarrow} \text{cercada} \\ \overset{6.93}{\Longrightarrow} \text{cotada.} \end{array}$$

▸ **EXERCÍCIO x6.123.**
Demonstre: toda seqüência autoconvergente de reais inteiros é convergente. (x6.123 H 0)

D6.105. Definição (Subseqüência). Seja $(a_n)_n$: Seq Real. Dada qualquer estritamente crescente $(n_i)_i$: Seq Nat, chamamos a $(a_{n_i})_i$ de *subseqüência* da $(a_n)_n$. Equivalentemente, dizemos que uma seqüência $(b_n)_n$ é uma subseqüência da $(a_n)_n$ sse existem

$$n_0 < n_1 < n_2 < \dots$$

tais que para todo i, temos $b_i = a_{n_i}$.

▸ **EXERCÍCIO x6.124.**
Sejam $(a_n)_n \to \ell$. Logo toda subseqüência de $(a_n)_n$ também tende ao ℓ. (x6.124 H 0)

▸ **EXERCÍCIO x6.125.**
Verifique: toda seqüência cotada possui subseqüência autoconvergente. (x6.125 H 0)

6.106. Autoconvergente vs. convergente. Demonstramos no Teorema Θ6.102 que

$$\text{autoconvergente} \impliedby \text{convergente}.$$

Por enquanto não conseguimos demonstrar a recíproca

$$\text{autoconvergente} \overset{?}{\implies} \text{convergente}$$

mas também não conseguimos encontrar nenhum contraexemplo. Agora vamos investigar o que acontece se acrescentar a hipótese que a seqüência possui subseqüência convergente e vamos pelo menos conseguir a implicação

$$\left.\begin{array}{c}\text{autoconvergente}\\ +\\ \text{subseqüência convergente}\end{array}\right\} \implies \text{convergente}:$$

Θ6.107. Teorema. *Toda seqüência autoconvergente que possui subseqüência convergente é convergente.*

Demonstração. Seja $(a_n)_n$ autoconvergente e seja uma subseqüência convergente dela $(a_{k_i})_i$, e logo seja ℓ seu limite. Vou demonstrar que $(a_n)_n \to \ell$. Seja $\varepsilon > 0$. Como $(a_n)_n$ autoconvergente, seja N tal que

$$(\forall m, n \geq N)[\, d(a_m, a_n) < \varepsilon_1 \,].$$

Como $(a_{k_i})_i \to \ell$, seja I tal que

$$(\forall i \geq I)[\, d(a_{k_i}, \ell) < \varepsilon_2 \,].$$

Seja $J \geq I$ tal que $k_J \geq N$. (Justifique!) Vou demonstrar que a partir do k_J-ésimo termo da $(a_n)_n$, todos os seus termos ficam ε-perto do ℓ. Seja $n \geq k_J$ então, e logo $n \geq N$ também. Calculamos:

$$\begin{aligned} d(a_n, \ell) &\leq d(a_n, a_{k_J}) + d(a_{k_J}, \ell) && (\text{(D-Tri)})\\ &< \varepsilon_1 + d(a_{k_J}, \ell) && (\text{pois } n, k_J \geq N)\\ &< \varepsilon_1 + \varepsilon_2 && (\text{pois } J \geq I)\\ &= \varepsilon. \end{aligned}$$

∎

Θ6.108. Teorema. *Toda seqüência de reais tem subseqüência crescente ou decrescente.*

DEMONSTRAÇÃO. Introduzimos o conceito de posição de pico de seqüência: dizemos que P é uma *posição de pico* para a $(a_n)_n$ sse $a_P \geq (a_n)_{n\geq P}$. Para achar uma subseqüência desejada, separamos em casos a partir da quantidade de posições de pico da $(a_n)_n$.
CASO FINITA: teu (Exercício x6.126).
CASO CONTRÁRIO: também teu (Exercício x6.127). ∎

▸ **EXERCÍCIO x6.126.**
Feche o primeiro caso. (x6.126 H 1)

▸ **EXERCÍCIO x6.127.**
E o segundo. (x6.127 H 1)

TODO Terminar
Última chance: será que podes pensar numa resposta para a Questão Q6.54?

Intervalo de problemas

TODO Add problems

▸ **PROBLEMA Π6.1.**
(i) Demonstre que

$$\lim_n \frac{2^n}{n!} = 0.$$

(ii) Podemos trocar esse '2' por quais números mantendo esse limite? (Π6.1 H 1 2)

▸ **PROBLEMA Π6.2.**
Tem como definir uma distância no ExtReal com qual o sigificado de $(a_n)_n \to +\infty$ acabaria sendo simplesmente o significado de $(a_n)_n \to \ell$ para o $\ell := +\infty$? (Π6.2 H 0)

▸ **PROBLEMA Π6.3.**
Seja $(a_n)_n$ tal que suas subseqüências $(a_{2n})_n$, $(a_{2n+1})_n$, e $(a_{3n})_n$ são todas convergentes.
(i) Demonstre que as três subseqüências convergem ao mesmo limite ℓ.
(ii) (Meta)demonstre que apagando qualquer uma das três hipoteses o (i) vira indemonstrável.
(iii) Demonstre que $(a_n)_n \to \ell$.

(Π6.3 H 0)

§154. Completude

Agora temos tudo que precisamos para responder à Questão Q6.54. Nossa resposta com palavras de rua é

a linha dos reais não tem "buracos"

mas precisamos formalizar essa proposição.[52] A idéia é exigir que *não falta nenhum supremum*—ou, dualmente, nenhum infimum, pois é a mesma coisa: uma afirmação acaba implicando a outra. Mas o que significa dizer que não falta nenhum supremum? E, nenhum mesmo? Não. Um conjunto que nem é bounded above não tem chances de ter supremum. Um conjunto vazio, também não. Vamos exigir suprema para todos os outros então:

S6.109. Especificação (Os reais (3/3)). Estipulamos um último axioma:

(R-Compl-lub) $\quad (\forall A \subseteq \mathbb{R})[\, A \text{ cotado por cima} \implies A \text{ tem supremum}\,].$

Terminamos com este a lista de todos os axiomas que vamos estipular sobre os números reais. As conseqüências desses axiomas, ou seja, a *teoria dos números reais* é o que estudamos em *calculus* e *análise real*. O resto deste capítulo é um teaserzinho dessa teoria linda; e, como sempre, no fim tenho ponteiros na literatura para mergulhar mais. No Capítulo 17 voltamos nessa investigação de análise real, pois estudamos a teoria dos *espaços métricos*: conjuntos equipados com uma noção de distância, ou seja, uma função binária *com valores reais*, satisfazendo certas leis.

6.110. Corolário. *Seja A conjunto habitado de reais, cotado por baixo. Logo A possui infimum.*

Demonstrarás agora no Exercício x6.128. ∎

▸ **EXERCÍCIO x6.128.**
Demonstre o Corolário 6.110. (x6.128 H 1 2)

6.111. Observação. Assim as operações inf e sup viram totais nos reais estendidos:

$$\inf, \sup : \mathsf{Set\ ExtReal} \to \mathsf{ExtReal}.$$

▸ **EXERCÍCIO x6.129.**
Sejam A, B habitados e cotados. Logo $A \cup B$ também é, e

$$\sup(A \cup B) = \max\{\sup A, \sup B\} \qquad \inf(A \cup B) = \min\{\inf A, \inf B\}.$$

(x6.129 H 0)

▸ **EXERCÍCIO x6.130.**
Sejam A, B habitados e cotados. Logo $A + B$ também é, e

$$\sup(A + B) = \sup A + \sup B \qquad \inf(A + B) = \inf A + \inf B.$$

(x6.130 H 0)

[52] No Capítulo 13 encontraremos uma outra resposta à Questão Q6.54, de natureza diferente. Paciência!

▸ **EXERCÍCIO x6.131.**
E se não são habitados? Ou cotados? (x6.131 H 0)

▸ **EXERCÍCIO x6.132.**
Expresse essas leis usando apenas diagramas comutativos. (x6.132 H 0)

▸ **EXERCÍCIO x6.133.**
Sejam A, B habitados e cotados. Mostre que, em geral, não são garantidas as Demonstre:

$$\sup(A \cdot B) = \sup A \cdot \sup B \qquad\qquad \inf(A \cdot B) = \inf A \cdot \inf B$$

mas, adicionando uma hipotese interessante demonstre que ambas são válidas. (x6.133 H 1)

§155. MCT, NIP, CCC, B–W

Θ6.112. Monotone Convergence Theorem (MCT). *Toda seqüência monótona e cotada é convergente:*

(MCT) monótona & cotada $\implies$ convergente.

Demonstração. Seja $(a_n)_n$ seqüência crescente e sup-cotada. Logo $\{a_n\}_n$ sup-cotado e logo seja s o seu supremum. Vou demonstrar que $(a_n)_n \to s$. Seja $\varepsilon > 0$. Pela escolha de s, $s - \varepsilon$ não pode ser sup-cota da $(a_n)_n$, e logo seja N tal que $a_N > s - \varepsilon$. Temos então $s - \varepsilon < a_N < s$. Como $(a_n)_n$ crescente, temos $s - \varepsilon < (a_n)_{n \geq N} < s$. Logo $(a_n)_{n \geq N} \subseteq \mathcal{B}_\varepsilon(s)$. ∎

▸ **EXERCÍCIO x6.134.**
Seja $0 < \vartheta < 1$. Demonstre que $(\vartheta^n)_n \to 0$ (já demonstrado no Exercício x6.134), mas essa vez construa uma nova demonstração, para obtê-lo como corolário simples do MCT (Θ6.112). (x6.134 H 1 2 3 4)

Θ6.113. Teorema Bolzano–Weierstrass (B–W). *Toda seqüência cotada de reais tem subseqüência convergente:*

(B–W) cotada $\implies$ subseqüência convergente.

Demonstração.

Seja $(a_n)_n$ cotada.
Logo $(a_n)_n$ possui subseqüência monótona (e cotada) $(a_{n_i})_i$. (Teorema Θ6.108)
Logo a subseqüência $(a_{n_i})_i$ é convergente. (MCT (Θ6.112))

∎

Θ6.114. Nested Intervals Property (Cantor) (NIP). *Seja $(I_n)_n$ seqüência aninhada de intervalos fechados, cotados, e habitados, ou seja, tais que*

$$I_0 \supseteq I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

Logo, a interseção deles é um intervalo fechado e habitado. Ainda mais, se $(\operatorname{diam}(I_n))_n \to 0$*, então a interseção é um singleton.*

Demonstração. Sejam, para cada i, a_i, b_i os reais tais que $I_i = [a_i, b_i]$. Como os intervalos da $(I)_n$ são aninhados, temos

$$a_0 \leq a_1 \leq a_2 \leq a_3 \leq \cdots \leq b_3 \leq b_2 \leq b_1 \leq b_0.$$

Considere a seqüência $(a_n)_n$. Ela é crescente e sup-cotada (pelo b_0). Logo seja $a_\omega = \sup_n a_n = \lim_n a_n$. Similarmente, seja $b_\omega = \inf_n b_n = \lim_n b_n$. Graças a ti (que tu vai fechar esses detalhes no Exercício x6.135) temos:

$$(a_n)_n \leq a_\omega \leq b_\omega \leq (b_n)_n \qquad \text{e} \qquad \bigcap_n I_n = [a_\omega, b_\omega]$$

e logo habitado pois $a_\omega \leq b_\omega$. Supondo que $(\operatorname{diam} I_n)_n \to 0$, calculamos:

$$\begin{aligned} d(a_\omega, b_\omega) &= b_\omega - a_\omega \\ &= \lim_n b_n - \lim_n a_n \\ &= \lim_n (b_n - a_n) \\ &= \lim_n d(a_n, b_n) \\ &= \lim_n \operatorname{diam}(I_n) \\ &= 0 \end{aligned}$$

e logo $a_\omega = b_\omega$. Logo $\bigcap_n I_n = [a_\omega, b_\omega]$ é o singleton $\{a_\omega = b_\omega\}$. ∎

▸ **EXERCÍCIO x6.135.**
Feche o que faltou para fechar na demonstração do Θ6.114. (x6.135 H 0)

▸ **EXERCÍCIO x6.136.**
Demonstre que as hipoteses do NIP (Θ6.114) sobre os intervalos serem fechados e cotados são *necessárias*. (x6.136 H 0)

Θ6.115. Cauchy Convergence Criterion (CCC). *Toda seqüência de reais autoconvergente é convergente:*

(CCC) autoconvergente $\implies$ convergente.

Demonstração.

Seja $(a_n)_n$ autoconvergente.	
Logo $(a_n)_n$ cotada.	(Corolário 6.104)
Logo $(a_n)_n$ possui subseqüência convergente.	(B–W (Θ6.113))
Logo $(a_n)_n$ convergente.	(Teorema Θ6.107)

∎

TODO finish

§156. Propriedades arquimedeanas

TODO fix

6.116. Considere as proposições seguintes sobre o conjunto dos reais positivos:

$\mathbb{R}_{\mathbb{N}}$ não é cotado	$(\forall \varepsilon)(\exists n \in \mathbb{R}_{\mathbb{N}})[\,1/n < \varepsilon\,]$	$(\forall s)(\forall b)(\exists n \in \mathbb{R}_{\mathbb{N}})[\,b/n < s\,]$
$(\forall \varepsilon)[\,\varepsilon\mathbb{R}_{\mathbb{N}}$ não é cotado$\,]$	$(\forall \varepsilon)(\exists n \in \mathbb{R}_{\mathbb{N}})[\,n\varepsilon > 1\,]$	$(\forall b)(\forall s)(\exists n \in \mathbb{R}_{\mathbb{N}})[\,ns > b\,]$.

Há diferença entra as duas da última coluna? Como chamarias cada uma no «nível coração»?

D6.117. Definição (infinitamente pequeno ou grande). Sejam u, v reais positivos. Dizemos que:

$$u \text{ alcança subindo o } v \overset{\text{def}}{\iff} (\exists n \in \mathbb{R}_{\mathbb{N}})[\,un > v\,];$$
$$u \text{ alcança descendo o } v \overset{\text{def}}{\iff} (\exists n \in \mathbb{R}_{\mathbb{N}})[\,u/n < v\,].$$

Sejam b, s reais positivos. Chame b de *infinitamente grande* sse existe positivo u que não alcança subindo o b; Chame s de *infinitamente pequeno* sse existe positivo u que não alcança descendo o s.

Com essa terminologia, as últimas duas proposições acima viram pronunciáveis assim:

$$(\forall s)\overbrace{(\forall b)\underbrace{(\exists n \in \mathbb{R}_{\mathbb{N}})[\,b/n < s\,]}_{b \text{ alcança descendo o } s}}^{s \text{ não é infinitamente pequeno}} \qquad (\forall b)\overbrace{(\forall s)\underbrace{(\exists n \in \mathbb{R}_{\mathbb{N}})[\,ns > b\,]}_{s \text{ alcança subindo o } b}}^{b \text{ não é infinitamente grande}}.$$

Θ6.118. Teorema. *O $\mathbb{R}_{\mathbb{N}}$ não é cotado.*

Demonstração. Suponha que $\mathbb{R}_{\mathbb{N}}$ cotado, e logo seja $s = \sup \mathbb{R}_{\mathbb{N}}$ (pelo axioma da completude, pois $\mathbb{R}_{\mathbb{N}}$ habitado também). Considere o $s-1$. Temos $s-1 < s$, e logo $s-1$ não é uma sup-cota do $\mathbb{R}_{\mathbb{N}}$. Logo seja $n \in \mathbb{R}_{\mathbb{N}}$ tal que $s-1 < n$. Como $\mathbb{R}_{\mathbb{N}}$ é $(+1)$-fechado, logo $n+1 \in \mathbb{R}_{\mathbb{N}}$. Mas $s < n+1$, contradizendo que $s > \mathbb{R}_{\mathbb{N}}$. ∎

6.119. Corolário. $(\forall \varepsilon > 0)(\exists N)\big[\,\frac{1}{n} < \varepsilon\,\big]$.

6.120. Corolário. $(\forall \varepsilon > 0)[\,\varepsilon\mathbb{R}_{\mathbb{N}}$ não é cotado por cima$\,]$.

Θ6.121. Teorema. *O $\mathbb{R}$ é arquimedeano, ou seja: para todo $x, y \in \mathbb{R}$,*

$$x > 0 \implies (\exists n \in \mathbb{R}_{\mathbb{N}})[\,xn > y\,].$$

§157. Raizes

Θ6.122. Teorema. *Seja $0 \leq a \leq 1$. Logo a seqüência de reais $(a_n)_n$ definida pelas*

$$\begin{aligned} a_0 &= 0 \\ a_{n+1} &= a_n + \frac{1}{2}(a - a_n^2) \end{aligned}$$

converge ao $\sqrt{a}$.

Demonstração. Primeiramente demonstramos que a $(a_n)_n$ é crescente e sup-cotada (Exercício x6.137). Logo ela é convergente, e logo seja $\ell = \lim_n a_n$. Basta calcular que $\ell^2 = 2$:

$$\begin{aligned} \ell^2 &= (\lim_n a_n)^2 && \text{(escolha de } \ell\text{)} \\ &\vdots && \text{(Exercício x6.137)} \\ &= 2. \end{aligned}$$

∎

▸ **EXERCÍCIO x6.137.**
Feche a demonstração do Θ6.122: (i) $(a_n)_n$ é crescente; (ii) $(a_n)_n$ é sup-cotada; (iii) $\ell^2 = 2$. (x6.137 H 1)

Θ6.123. Teorema. *Existe real h tal que $h^2 = 2$.*

Demonstração. Seja $A = \{ x \mid x^2 < 2 \}$. Como A é habitado (x6.138) e sup-cotado (x6.139), logo seja $h = \sup A$, pelo (R-Compl-lub). Para demonstrar que $h^2 = 2$, basta eliminar os outros dois casos: $h^2 < 2$; $h^2 > 2$.
Caso $h^2 < 2$. Para eliminar este caso, acharemos um membro de A, maior que h, assim contradizendo a escolha de h como sup-cota ($h \geq A$). A esperança é que vamos conseguir aumentar h um tiquinho tão pequeno que seu quadrado vai continuar sendo menor que 2. Vamos apelar tal real de h_+. Teremos então $h_+ > h$ e $h_+^2 < 2$; e isso implicaria $h_+ \in A$ (pela definição de A):

$$h < h_+ \in A$$

e logo $h \not\geq A$, e teremos nossa contradição. Como $h^2 < 2$, logo seja $\vartheta > 0$ tal que

$$h^2 + \vartheta < 2.$$

Basta achar $\varepsilon > 0$ pequeno o suficiente para que $h + \varepsilon$ serve ser nosso desejado h_+:

$$(\underbrace{h + \varepsilon}_{h_+})^2 < h^2 + \vartheta < 2.$$

Seja $\varepsilon = \dfrac{\vartheta}{2h+1}$. Calculamos:

$$\begin{aligned} (h+\varepsilon)^2 &= h^2 + 2h\varepsilon + \varepsilon^2 \\ &< h^2 + 2h\varepsilon + \varepsilon && \text{(pelo Exercício x6.32)} \\ &= h^2 + (2h+1)\varepsilon \\ &= h^2 + (2h+1)\frac{\vartheta}{2h+1} && \text{(pela escolha de } \varepsilon\text{)} \\ &= h^2 + \vartheta \\ &< 2. && \text{(pela escolha de } \vartheta\text{)} \end{aligned}$$

Caso $h^2 > 2$. Para eliminar este caso, vamos achar uma cota superior h_- de A, melhor (menor) que h, assim contradizendo a escolha de h como *melhor* sup-cota. Essa parte é toda tua (x6.140). ∎

▸ **EXERCÍCIO x6.138.**
Mostre que o A da demonstração do Θ6.123 é habitado...

(x6.138 H 1)

▸ **EXERCÍCIO x6.139.**
...e sup-cotado também...

(x6.139 H 1 2)

▸ **EXERCÍCIO x6.140.**
...e mostre que $h^2 \not> 2$, para eliminar o caso que deixei pra tu, fechando assim tudo que ficou aberto na demonstração do Teorema Θ6.123.

(x6.140 H 0)

6.124. Corolário. *Os racionais não satisfazem a especificação dos reais.*

DEMONSTRAÇÃO. Imediato pois já demonstramos que não existe racional q com $q^2 = 2$. ▮

§158. Densidades

Θ6.125. Teorema. *Os racionais são densos nos reais, ou seja: para todo $x, y \in \mathbb{R}$,*

$$x < y \implies (\exists q \in \mathbb{Q})[\, x < q < y \,].$$

Θ6.126. Teorema. *Os irracionais são densos nos reais, ou seja: para todo $x, y \in \mathbb{R}$,*

$$x < y \implies (\exists i \notin \mathbb{Q})[\, x < i < y \,].$$

§159. Cardinalidades infinitas

Θ6.127. Teorema (Cantor). *Existe seqüência $(q_n)_n$ tal que $\{q_n\}_n = [0,1] \cap \mathbb{R}_{\mathbb{Q}}$.*

DEMONSTRAÇÃO. Seja

$$(q_n)_n \overset{\text{“def”}}{=} \frac{0}{1}, \frac{1}{1}, \frac{0}{2}, \frac{1}{2}, \frac{2}{2}, \frac{0}{3}, \frac{1}{3}, \frac{2}{3}, \frac{3}{3}, \frac{0}{4}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \frac{4}{4}, \ldots$$

(Formalmente definir essa seqüência é o Problema Π6.4.) ▮

Θ6.128. Teorema (Cantor). *Não existe seqüência $(t_n)_n$ tal que $\{t_n\}_n = [0,1]$. Equivalentemente: para qualquer seqüência $(t_n)_n$, e quaisquer reais $a < b$, existe $w \in [a,b]$ tal que $w \notin \{t_n\}_n$. Ou seja, nenhuma seqüência consegue “cobrir” um intervalo: tem habitates que nunca serão contados pela seqüência; conseguem escapar dela.*

▸ ESBOÇO. Sejam a, b reais com $a < b$ e $(t_n)_n$ seqüência de reais. Construimos um real $w \in [a,b]$ tal que

$$(\forall n)[\, t_n \neq w \,].$$

Caso que a seqüência $(t_n)_n$ nunca entra no $[a,b]$, seja $w \in [a,b]$ e temos nosso testemunha e acabou. Caso que a seqüência só pega um valor $t \in [a,b]$, seja $w \in [a,b] \setminus \{t\}$, e acabou. Caso contrário, a seqüência pega pelo menos dois distintos valores no $[a,b]$. Chame ℓ_1 o menor deles, e r_1 o maior. Como $\ell_1 < r_1$, seja $I_1 = [\ell_1, r_1]$. Repetimos a mesma idéia no I_1 para obter ou um testemunha w (nos dois primeiros casos), assim acabando com a demonstração; ou dois distintos reais $\ell_2 < r_2$ no $[\ell_1, r_1]$ definindo assim o $I_2 = [\ell_2, r_2]$. Continuando assim acabamos definindo ou N intervalos chegando num último intervalo I_N pois não tem mais dois distintos membros nele contados pela seqüência para continuar, ou uma seqüência de intervalos $(I_n)_n$; e note que são aninhados, fechados, e habitados, e logo sua interseção $\bigcap_n I_n$ é habitada. No primero caso acabamos com

$$a = \ell_0 < \ell_1 < \ell_2 < \cdots < \ell_N \quad < \quad r_N < \cdots < r_2 < r_1 < r_0 = b;$$

no segundo com

$$a = \ell_0 < \ell_1 < \ell_2 < \cdots \qquad\qquad \cdots < r_2 < r_1 < r_0 = b;$$

Note que a $(I_n)_n$ é uma seqüência de intervalos aninhados, fechados, e habitados e logo $\bigcap_n I_n$ é habitada também e qualquer habitante dela serve como testemunha. □

6.129. Observação. A importância desse teorema é assustadora—algo comprovado pelos eventos históricos logo depois de tal descoberta de Cantor. Dedicamos um capítulo inteiro (Capítulo 13) no assunto—onde também encontramos uma outra demonstração (também de Cantor) muito mais elegante—mas por enquanto basta apreciar que temos um primeiro toque de *cardinalidades infinitas distintas e comparáveis: uma estritamente maior que a outra!* Num lado, temos a cardinalidade do $\mathbb{N}$, que é nosso conjunto de índices, e mesmo podendo ter um real para cada tal índice, o intervalo $[a,b]$ é tão populoso que não tem como *contar* todos os seus membros usando nossa seqüência. Tais conjuntos chamamos de *incontáveis*.

§160. Representação geométrica

TODO Expansão como instruções

Intervalo de problemas

▸ **PROBLEMA Π6.4.**
Defina mesmo a seqüência $(q_n)_n$ que eu "pseudodefini" no Teorema Θ6.127. (Π6.4H0)

Θ6.130. Teorema (Ramsey). *Seja* $\wp_n A \stackrel{\text{def}}{=} \{\, S \subseteq A \mid |A| = n \,\}$. *Sejam* A, B, N *tais que* $\wp_2 N = A \cup B$. *Logo existe* $M \subseteq N$ *tal que: (i)* M *é infinito; e (ii)* $M \subseteq A$ *ou* $M \subseteq B$.

▸ **PROBLEMA Π6.5.**
Dado o teorema acima, demonstre o Teorema Θ6.108 como corolário. (Π6.5H0)

§161. Liminf e limsup

D6.131. Definição. Seja $(a_n)_n$ uma seqüência de reais. Definimos

$$\liminf_n a_n \stackrel{\text{def}}{=} \sup_n \inf_{i\geq n} a_i \qquad\qquad \limsup_n a_n \stackrel{\text{def}}{=} \inf_n \sup_{i\geq n} a_i.$$

Usamos também $\underline{\lim}_n$ para o $\liminf_n$ e similarmente $\overline{\lim}_n$ para o $\limsup_n$.

TODO elaborar e adicionar desenhos sobre os $\limsup$ e $\liminf$

6.132. Observação. Seja $(a_n)_n$ seqüência bounded e seja

$$M := \limsup_n a_n = \lim_n \sup\{\, a_k \mid k \geq n \,\}.$$

Logo

$$(\forall \varepsilon > 0)(\exists N \in \mathbb{N})(\forall n \geq N)[\, M - \varepsilon < \sup\{\, a_k \mid k \geq n \,\} < M + \varepsilon \,].$$

6.133. Critérion. *Seja $(a_n)_n$ bounded. Logo*

$$M = \limsup_n a_n \iff (\forall \varepsilon > 0)\begin{bmatrix} a_n < M + \varepsilon \text{ eventualmente para todos os } n\text{'s} \\ a_n > M - \varepsilon \text{ para uma quantidade infinita de } n\text{'s} \end{bmatrix};$$

$$m = \liminf_n a_n \iff (\forall \varepsilon > 0)\begin{bmatrix} a_n > m - \varepsilon \text{ eventualmente para todos os } n\text{'s} \\ a_n < m + \varepsilon \text{ para uma quantidade infinita de } n\text{'s} \end{bmatrix}.$$

TODO demonstrar

TODO elaborar e conectar com os equivalentes operadores em conjuntos

§162. Séries

D6.134. Definição. Seja $(a_n)_n$ uma seqüência de reais. Considere os números

$$\begin{aligned} s_0 &= 0 \\ s_1 &= a_0 \\ s_2 &= a_0 + a_1 \\ s_3 &= a_0 + a_1 + a_2 \\ &\vdots \\ s_n &= \sum_{i=0}^{n-1} a_i \\ &\vdots \end{aligned}$$

dos *somatórios parciais* (ou *iniciais*) da $(a_n)_n$. Escrevemos

$$\sum_{n=0}^{\infty} a_n \qquad \text{como sinônimo de} \qquad \underbrace{\lim_n \left(\sum_{i=0}^{n-1} a_i \right)}_{\lim_n s_n}$$

e naturalmente usamos frases como «a *série* $\sum_n a_n$ *converge*», etc. Dizemos que a série $\sum_n a_n$ *diverge* sse $(s_n)_n$ diverge.

▸ **EXERCÍCIO x6.141 (expansão binária).**
$\sum_{n=1}^{\infty} \frac{1}{2^n} = 1$. (x6.141 H 0)

▸ **EXERCÍCIO x6.142 (série harmônica).**
Oresme, Mengoli (uns 300 anos depois), e Bernoulli (uns 40 anos depois de Mengoli, no ano 1682), independentemente demonstraram que a *série harmônica* ($\sum_{n=1}^{\infty} \frac{1}{n}$) diverge. Entre no clube deles fazendo a mesma coisa (uns poucos séculos depois):

$$\sum_{n=1}^{\infty} \frac{1}{n} = +\infty.$$

(x6.142 H 0)

TODO add hints

▸ **EXERCÍCIO x6.143.**
Bernoulli demonstrou que $\sum_{n=0}^{\infty} \frac{1}{n^2}$ converge. Faça a mesma coisa. (x6.143 H 0)

TODO add hints

6.135. Problema de Basel. Achar uma "forma fechada" para o limite desta série era o famoso *problema de Basel*, enunciado pelo Mengoli no ano 1650. Bernoulli não conseguiu resolver este problema, que acabou ganhando seu apelido pela cidade *Basel*, na Suiça, em qual Bernoulli nasceu. E quem mais nasceu na mesma cidade? Euler, que conseguiu resolver o problema no ano 1734, demonstrando que

$$\sum_{n=0}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Inesperadamente, essa resolução é relacionada à probabilidade que dois aleatórios números grandes são coprimos: escolhendo aleatoriamente inteiros no $\{1, \ldots, n\}$ a seqüência das correspondentes probabilidades tende ao reciproco do limite acima: $6/\pi^2$. Tudo isso é fora do nosso foco aqui, mas confio que tu achou, no mínimo, interessante.

Intervalo de problemas

▸ **PROBLEMA Π6.6 (constante (e)).**
Podemos definir o número e, conhecido como *constante de Euler* (mas introduzido por Bernoulli) por qualquer uma das

$$e \stackrel{\text{def}}{=} \sum_{n=0}^{\infty} \frac{1}{k!} \qquad\qquad e \stackrel{\text{def}}{=} \lim_n \left(1 + \frac{1}{n}\right)^n.$$

(i) Demonstre que a série acima converge; (ii) demonstre que a seqüência acima converge; (iii) mostre que $\sum_{n=0}^{\infty} \frac{1}{k!} = \lim_n \left(1 + \frac{1}{n}\right)^n$; (iv) $(\forall n \geq 1)\big[\, 0 < e - s_n < \frac{1}{n!n} \,\big]$, onde $(s_n)_n$ é a seqüência dos somatórios parciais da série; (v) conclua que e é um número irracional. (Π6.6 H 0)

§163. Funções reais

TODO Elaborar

D6.136. Definição (função real contínua). Sejam $X, Y \subseteq \mathbb{R}$, $f : X \to Y$, e $x_0 \in X$. Chamamos

$$f \text{ contínua no } x_0 \overset{\text{def}}{\iff} (\forall \varepsilon > 0)(\exists \delta > 0) \\ (\forall x \in X)[\, x, x_0 \text{ são } \delta\text{-perto} \implies fx, fx_0 \text{ são } \varepsilon\text{-perto}\,].$$

Dizemos que f é *contínua* sse ela é contínua em cada ponto do seu domínio.

6.137. Continuidade como jogo.

TODO Escrever

Λ6.138. Lema (preservação de sinal). *Seja $f : A \to \mathbb{R}$ contínua no a com $fa \neq 0$. Logo existe $\mathcal{B}_\delta(a)$ tal que f não muda sinal nela.*

▸ Esboço. Caso $fa > 0$. Usamos a continuidade da f no a com $\varepsilon := fa$, assim ganhando um $\delta > 0$ tal que todos os δ-perto de a são mapeados ε-perto de fa. Logo todos são positivos.
Caso $fa < 0$: similar. □

Θ6.139. Teorema (Bolzano). *Seja $f : A \to \mathbb{R}$ contínua em todo ponto dum intervalo $[a, b]$ tal que $(fa), (fb)$ têm sinais opostos. Logo existe $w \in (a, b)$ tal que $fw = 0$.*

▸ Esboço. Caso $fa < 0 < fb$. Observe que podem exisir vários $w \in (a, b)$ com $fw = 0$; a gente precisa achar um tal w. Seja

$$L = \{\, x \in [a, b] \mid fx \leq 0 \,\}.$$

Observe $L \neq \emptyset$ (pois $a \in L$) e ele é bounded above (por b), e logo possui supremum: seja $w := \sup L$. Basta demonstrar que (i) $fw = 0$; (ii) $a < w < b$. (i) Pela tricotomía da ordem basta eliminar as possibilidades $fw > 0$ e $fw < 0$. Fazemos isso usando a continuidade da f e o Lema Λ6.138. supondo a primeira chegamos na contradição de achar um upper bound de L menor que w; supondo a segunda chegamos na contradição que o w não é um upper bound. (ii) Temos $w \in [a, b]$, basta eliminar as possibilidades de $w = a$ e $w = b$: imediato pois $fw = 0$ e $fa, fb \neq 0$.
Caso $fb < 0 < fa$: similar. □

D6.140. Definição (preserva limites). Seja $f : A \to \mathbb{R}$. Dizemos que f *preserva os límites* sse para toda seqüência convergente $(a_n)_n$

$$f(\lim_n a_n) = \lim_n (fa_n).$$

6.141. Critério. *Seja $f : A \to \mathbb{R}$.*

$$f \text{ contínua} \iff f \text{ preserva os limítes.}$$

TODO Demonstrar

§164. Convergência pointwise (ponto a ponto)

D6.142. Definição (pointwise). Seja $(f_n)_n : \mathsf{Seq}\ (\alpha \to \mathsf{Real})$ uma seqüência *de funções* reais. Observe que para cada $x : A$, é determinada uma seqüência *de reais* pelos valores das f_n's nesse ponto: $(f_n\ x)_n$. Se cada uma delas e convergente, definimos o *limite pointwise* da $(f_n)_n$ para ser a função $f : \alpha \to \mathbb{R}$ definida pela

$$f\ x = \lim_n (f_n x).$$

Dizemos que $(f_n)_n$ *converge pointwise* (ou *ponto a ponto*) à f:

$$\begin{aligned}(f_n)_n \to f &\overset{\text{def}}{\iff} (\forall x)[\,(f_n\ x)_n \to f\ x\,] \\ &\iff (\forall x)(\forall \varepsilon > 0)(\exists N)(\forall n \geq N)[\,d(f_n\ x, f\ x) < \varepsilon\,] \\ &\iff (\forall \varepsilon > 0)(\forall x)(\exists N)(\forall n \geq N)[\,d(f_n\ x, f\ x) < \varepsilon\,].\end{aligned}$$

▸ **EXERCÍCIO x6.144.**
Seja $(f_n)_n : \mathsf{Seq}\ ([0,1] \to \mathsf{Real})$ a seqüência definida pelas

$$\begin{aligned}f_n\ &: [0,1] \to \mathsf{Real} \\ f_n\ x &= x^n.\end{aligned}$$

A $(f_n)_n$ converge àlguma função pointwise? (x6.144 H 0)

D6.143. Definição (uniformemente). Sejam $(f_n)_n : \mathsf{Seq}\ (\alpha \to \mathsf{Real})$ e $f : \alpha \to \mathsf{Real}$. Definimos

$$(f_n)_n \rightrightarrows f \overset{\text{def}}{\iff} (\forall \varepsilon > 0)(\exists N)(\forall x)(\forall n \geq N)[\,d(f_n\ x, f\ x) < \varepsilon\,].$$

Dizemos que $(f_n)_n$ *converge uniformemente* à f.

▸ **EXERCÍCIO x6.145.**
Compare as duas noções de convergência: pointwise (D6.142) e uniforme (D6.143). (x6.145 H 0)

▸ **EXERCÍCIO x6.146.**
Defina as noções de *pointwise autoconvergente* e *uniformemente autoconvergente*. (x6.146 H 0)

Intervalo de problemas

TODO Add problems

§165. Os complexos

TODO elaborar

§166. Os surreais

TODO elaborar

Problemas

▸ **PROBLEMA Π6.7.**
Dado que ambos os e, π são transcendentais, mostre que pelo menos um dos $e+\pi$, $e\pi$ é transcendental. (Π6.7H12)

▸ **PROBLEMA Π6.8.**
Na Observação 6.21 afirmei que as duas formalizações são equivalentes. O que isso significa mesmo? Enuncie e demonstre. (Π6.8H0)

▸ **PROBLEMA Π6.9.**
Demonstre que não tem como definir uma ordem no corpo dos complexos em tal forma que ele vira um corpo ordenado. (Π6.9H0)

Leitura complementar

[Abb15], [Spi06], [Apo67], [Tao16], [Har08], [LS14]. [Knu74].

CAPÍTULO 7

TIPOS

§167. Tipos produto

S7.1. Especificação (Produto binário). A partir de quaisquer tipos α e β podemos formar o tipo do seu produto que denotamos por $\alpha \times \beta$:

((×)-Form)
$$\frac{\alpha : \mathsf{Type} \qquad \beta : \mathsf{Type}}{\alpha \times \beta : \mathsf{Type}}$$

Há duas maneiras de utilizar um habitante $w : \alpha \times \beta$, ou seja, duas perguntas que podemos fazer: «qual teu componente esquerdo?» e «qual teu componente direito?». Assim:

((×)-Elim)
$$\frac{w : \alpha \times \beta}{w \,.\, \mathsf{l} : \alpha} \qquad\qquad \frac{w : \alpha \times \beta}{w \,.\, \mathsf{r} : \beta}$$

Para construir um habitante do tipo $\alpha \times \beta$ precisamos fornecer tais duas informações, sendo uma de tipo α e outra de tipo β:

((×)-Intro)
$$\frac{a : \alpha \qquad b : \beta}{\langle a, b\rangle : \alpha \times \beta}$$

Aqui termina a descrição da parte *estática*. A parte *dinâmica* (computacional) é determinada pelas equações abaixo que governam os habitantes deste tipo. Separamos tais equações nas

((×)-β)
$$\langle a, b\rangle \,.\, \mathsf{l} = a \qquad\qquad \langle a, b\rangle \,.\, \mathsf{r} = b$$

que estabelecem o que acontece se tentar introduzir (construir) e logo depois eliminar (usar); e na

((×)-η)
$$\langle w \,.\, \mathsf{l}, w \,.\, \mathsf{r}\rangle = w.$$

que estabelecem o que acontece se construir algo a partir do que obtemos apenas usando uma tal tupla.

7.2. Observação. As equações (β) estão dando uma alma computacional aos habitantes de $\alpha \times \beta$, especialmente quando são lidas de forma direcionada onde as expressões mais complexas (à esquerda) são substituidas pelas expressões mais simples (à direita) durante um cálculo. As equações (η) também, e correspondem em garantias de unicidade e de *ausência de lixo*. Como exemplo, considere a ((×)-η): se o w carregasse mais informação (lixo) além das duas que podemos obter a partir da interface que temos (eliminadores), formando o $\langle w \,.\, \mathsf{l}, w \,.\, \mathsf{r}\rangle$ não seria garantido de criar o próprio w.

? **Q7.3. Questão.** Tendo definido produtos 2-ários, como generalizarias para definir produtos n-ários para qualquer $n \geq 0$?

!! SPOILER ALERT !!

S7.4. Especificação (Produto finito). Precisávamos 2 tipos para formar o tipo de produto binário (deles), agora para o produto n-ário precisamos n tipos: dados $\alpha_1, \ldots, \alpha_n$ podemos formar o tipo do seu produto que denotarei por $\mathsf{Prod}(\alpha_1, \ldots, \alpha_n)$:

(Prod-Form) $$\frac{\alpha_1 : \mathsf{Type} \qquad \cdots \qquad \alpha_n : \mathsf{Type}}{\mathsf{Prod}(\alpha_1, \ldots, \alpha_n) : \mathsf{Type}}$$

Tivemos 2 maneiras de utilizar habitantes do produto 2-ário, logo temos n maneiras de utilizar habitantes do produto n-ário:

(Prod-Elim) $$\frac{w : \mathsf{Prod}(\alpha_1, \ldots, \alpha_n)}{w \,.\, \mathbf{1} : \alpha_1} \qquad \cdots \qquad \frac{w : \mathsf{Prod}(\alpha_1, \ldots, \alpha_n)}{w \,.\, \mathbf{n} : \alpha_n}$$

Precisavamos 2 informações para construir habitantes do produto 2-ário (uma de cada tipo envolvido), logo precisamos n informações para construir habitantes do produto n-ário:

(Prod-Intro) $$\frac{a_1 : \alpha_1 \qquad \cdots \qquad a_n : \alpha_n}{\langle a_1, \ldots, a_n \rangle : \mathsf{Prod}(\alpha_1, \ldots, \alpha_n)}$$

A parte computacional da 2-ária tinha 2 equações-(β), portanto temos n para a n-ária: para cada $i = 1, \ldots, n$, a seguinte:

(Prod-β) $$\langle a_1, \ldots, a_n \rangle \,.\, \mathbf{i} = a_i.$$

E similarmente sobre (η):

(Prod-η) $$\langle w \,.\, \mathbf{1}, \ldots, w \,.\, \mathbf{n} \rangle = w.$$

? **Q7.5. Questão.** Tendo definido produtos n-ários para qualquer $n \geq 0$, como parece o caso especial de produtos 0-ários?

!! SPOILER ALERT !!

7.6. Produto nulário. A partir do nada podemos formar o tipo do produto nulário que denotamos por 1:

(1-Form) $$\frac{}{1 : \mathsf{Type}}$$

Temos 0 (nenhuma) pergunta que podemos fazer aos habitantes de 1:

(1-Elim)

Correspondentemente, precisamos 0 informações para construir um habitante de produto 0-ário:

(1-Intro) $$\frac{}{\langle\rangle : 1}$$

(Nenhuma informação foi incluida nessa construção, e logo nenhuma informação pode ser extraida.) A parte computacional do 2-ário tinha 2 equações-(β), portanto temos 0 para o 0-ário:

(1-β)

Mesmo assim temos algo interessantíssimo parte de (η):

(1-η) $$\langle\rangle = w$$

que garanta que este tipo tem um único habitante, o $\langle\rangle$.

§168. Tipos soma

S7.7. Especificação (Soma binária). A partir de quaisquer tipos α e β podemos formar o tipo da sua soma que denotamos por $\alpha + \beta$:

((+)-Form) $$\frac{\alpha : \mathsf{Type} \qquad \beta : \mathsf{Type}}{\alpha + \beta : \mathsf{Type}}$$

Temos duas maneiras de construir um habitante do tipo $\alpha + \beta$: uma embute nele uma informação do tipo α, e a outra uma do tipo β:

((×)-Intro) $$\frac{a : \alpha}{\mathsf{l}\,.\,a : \alpha + \beta} \qquad\qquad \frac{b : \beta}{\mathsf{r}\,.\,b : \alpha + \beta}$$

Tendo mais que um construtor, o uso de tais habitantes é por um case-analises, e necessita uma função-receita para cada possibilidade:

((+)-Elim) $$\frac{w : \alpha + \beta \qquad f : \alpha \to \gamma \qquad g : \beta \to \gamma}{\mathsf{case}\ w\ \mathsf{of}\ \begin{Bmatrix} \mathsf{l}\,.\,x \mapsto f\ x \\ \mathsf{r}\,.\,y \mapsto g\ y \end{Bmatrix} : \gamma}$$

Aqui termina a parte estática. A parte computacional consiste das equações:

((+)-β) $$\mathsf{case}\ \mathsf{l}\,.\,a\ \mathsf{of}\ \begin{Bmatrix} \mathsf{l}\,.\,x \mapsto f\ x \\ \mathsf{r}\,.\,y \mapsto g\ y \end{Bmatrix} = f\ a \qquad\qquad \mathsf{case}\ \mathsf{r}\,.\,b\ \mathsf{of}\ \begin{Bmatrix} \mathsf{l}\,.\,x \mapsto f\ x \\ \mathsf{r}\,.\,y \mapsto g\ y \end{Bmatrix} = g\ b.$$

((+)-η) $$\mathsf{case}\ w\ \mathsf{of}\ \begin{Bmatrix} \mathsf{l}\,.\,x \mapsto \mathsf{l}\,.\,x \\ \mathsf{r}\,.\,y \mapsto \mathsf{r}\,.\,y \end{Bmatrix} = w$$

S7.8. Especificação (Soma finita). Precisávamos 2 tipos para formar o tipo de soma binária (deles), agora para a soma n-ária precisamos n tipos: dados $\alpha_1, \ldots, \alpha_n$ podemos formar o tipo do sua soma que denotarei por $\mathsf{Sum}(\alpha_1, \ldots, \alpha_n)$:

$$\text{(Sum-Form)} \qquad \frac{\alpha_1 : \mathsf{Type} \qquad \cdots \qquad \alpha_n : \mathsf{Type}}{\mathsf{Sum}(\alpha_1, \ldots, \alpha_n) : \mathsf{Type}}$$

Tivemos 2 maneiras de construir habitantes da soma 2-ária, logo temos n maneiras de construir habitantes da soma n-ária:

$$\text{(Sum-Intro)} \qquad \frac{a_1 : \alpha_1}{\mathbf{1}\,.\,w : \alpha + \beta} \qquad \cdots \qquad \frac{a_n : \alpha_n}{\mathbf{n}\,.\,w : \alpha + \beta}$$

Além do habitante w que queríamos usar precisávamos 2 funções-auxiliares com o mesmo codomínio γ e nosso uso com o case-of teve 2 linhas-casos; agora precisamos n funções-auxiliares e o case-of tem n linhas-casos:

$$\text{(Sum-Elim)} \qquad \frac{w : \mathsf{Sum}(\alpha_1, \ldots, \alpha_n) \qquad f_1 : \alpha_1 \to \gamma \qquad \cdots \qquad f_n : \alpha_n \to \gamma}{\mathsf{case}\ w\ \mathsf{of}\ \left\{\begin{array}{l} \mathbf{1}\,.\,x_1 \mapsto f_1\ x_1 \\ \vdots \\ \mathbf{n}\,.\,x_n \mapsto f_n\ x_n \end{array}\right] : \gamma}$$

A parte computacional da 2-ária tinha 2 equações-(β), portanto temos n para a n-ária: para cada $i = 1, \ldots, n$, a seguinte:

$$\text{(Sum-}\beta\text{)} \qquad \mathsf{case}\ \mathbf{i}\,.\,a_1\ \mathsf{of}\ \left\{\begin{array}{l} \mathbf{1}\,.\,x_1 \mapsto f_1\ x_1 \\ \vdots \\ \mathbf{n}\,.\,x_n \mapsto f_n\ x_n \end{array}\right] = f_i\ a_i.$$

E similarmente sobre (η):

$$\text{(Sum-}\eta\text{)} \qquad \mathsf{case}\ w\ \mathsf{of}\ \left\{\begin{array}{l} \mathbf{1}\,.\,x_1 \mapsto \mathbf{1}\,.\,x_1 \\ \vdots \\ \mathbf{n}\,.\,x_n \mapsto \mathbf{n}\,.\,x_n \end{array}\right] = w.$$

? **Q7.9. Questão.** Tendo definido somatórios n-ários para qualquer $n \geq 0$, como parece o caso especial de produtos 0-ários? Tendo definido o produtório 0-ário, como deveria ser o somatório 0-ário?

!! SPOILER ALERT !!

7.10. Soma nulária. Precisávamos 2 tipos para formar o tipo de soma binária (deles), agora para a soma 0-ária precisamos 0 tipos, ou seja nada: a partir do nada podemos formar o tipo da soma nulária que denotamos por 0:

(0-Form) $$\frac{}{0 : \mathsf{Type}}$$

Tivemos 2 maneiras de construir habitantes da soma 2-ária, logo temos 0 maneiras de construir habitantes da soma 0-ária:

(0-Intro)

Além do habitante w que queríamos usar precisávamos 2 funções-auxiliares com o mesmo codomínio γ e nosso uso com o case-of teve 2 linhas-casos; agora precisamos 0 funções-auxiliares e o case-of tem 0 linhas-casos:

(0-Elim) $$\frac{w : 0}{\mathsf{case}\ w\ \mathsf{of}\ \{\ \} : \gamma}$$

A parte computacional da 2-ária tinha 2 equações-(β), portanto temos 0 para a 0-ária:

(0-β)

Mesmo assim temos algo na parte de (η):

(0-η) $$\mathsf{case}\ w\ \mathsf{of}\ \{\ \} = w$$

§169. O tipo Unit

S7.11. Especificação (Unit). A partir do nada podemos formar o tipo Unit:

(Unit-Form) $$\frac{}{\mathsf{Unit} : \mathsf{Type}}$$

Temos só uma maneira de construir habitantes do tipo Unit:

(Unit-Intro) $$\frac{}{\star : \mathsf{Unit}}$$

Nenhuma informação entrou no processo de construção, e logo não temos nenhuma maneira de extrair informação:

(Unit-Elim)

Sem maneiras de utilizar não temos também equações (β):

(Unit-β)

Finalmente a (η) expressa que $\star$ é o único habitante do Unit:

(Unit-η) $$\star = w.$$

§170. O tipo Empty

S7.12. Especificação (Empty). Empty é um tipo:

(Empty-Form) $$\frac{}{\mathsf{Empty} : \mathsf{Type}}$$

Não há maneiras de construir habitantes do tipo Empty:

(Empty-Intro)

Assim, tendo um habitante de Empty podemos solicitar habitantes de qualquer tipo γ:

(Empty-Elim) $$\frac{w : \mathsf{Empty}}{\mathbf{boom}_\gamma\ w : \gamma}$$

Sem maneiras de utilizar não temos também equações (β):

(Empty-β)

Finalmente a (η) do Empty:

(Empty-η) $$\mathbf{boom}_{\mathsf{Empty}}\ w = w.$$

§171. Tipos função

S7.13. Especificação (Função). A partir de quaisquer tipos α e β podemos formar o tipo de funções de α para β que denotamos por $\alpha \to \beta$:

((→)-Form) $$\frac{\alpha : \mathsf{Type} \qquad \beta : \mathsf{Type}}{\alpha \to \beta : \mathsf{Type}}$$

Este tipo é caraterizado pela sua eliminação. Temos uma única maneira de usar uma função $f : \alpha \to \beta$ para extrair uma informação dela: aplicá-la em algo de tipo α; e o que obtemos é algo de tipo β:

((→)-Elim) $$\frac{f : \alpha \to \beta \qquad a : \alpha}{f\ a : \beta}$$

Chegamos no ponto onde precisamos explicitar a informação dos contextos:

((→)-Intro) $$\frac{\Gamma, x : \alpha \vdash b : \beta}{\Gamma \vdash \lambda x\,.\,b : \alpha \to \beta}$$

Aqui termina a parte estática. A parte computacional consiste do passo computacional chamado (β)-redução:

((→)-β) $$(\lambda x\,.\,b)\ a \ \triangleright_\beta\ b[x := a]$$

e da (η)-conversão:

((→)-η) $$\lambda x\,.\,f\ x \ \triangleright_\eta\ f$$

§172. Implementações de tipos

7.14. Por enquanto aceitamos apenas que nosso sistema de tipos possui (nos permite formar) somas finitas e produtos finitos—note que isso inclui os $\mathsf{0}$ e $\mathsf{1}$ como casos especiais—e também tipos de funções. Nesta secção vamos ver como podemos *implementar* uns tipos desejados, como os booleanos e os $\mathsf{Maybe}\ \alpha$ que conhecemos no Capítulo 4. Começamos com a especificação do tipo dos booleanos:

S7.15. Especificação (Bool). Bool é um tipo:

(Bool-Form) $$\frac{}{\mathsf{Bool} : \mathsf{Type}}$$

Há duas maneiras de construir habitantes de Bool, ambas sem precisar mais informação:

(Bool-Intro) $$\frac{}{\mathsf{ff} : \mathsf{Bool}} \qquad \frac{}{\mathsf{tt} : \mathsf{Bool}}$$

Utilizamos booleans com o *if-then-else*, para qual precisamos fornecer dois valores do mesmo tipo:

(Bool-Elim) $$\frac{b : \mathsf{Bool} \qquad u : \gamma \qquad v : \gamma}{\mathsf{if}\ b\ \mathsf{then}\ u\ \mathsf{else}\ v : \gamma}$$

Computamos com os booleanos assim:

(Bool-β) $\mathsf{if}\ \mathsf{ff}\ \mathsf{then}\ u\ \mathsf{else}\ v = v$ $\mathsf{if}\ \mathsf{tt}\ \mathsf{then}\ u\ \mathsf{else}\ v = u.$

E a (η) do Bool:

(Bool-η) $\mathsf{if}\ b\ \mathsf{then}\ \mathsf{tt}\ \mathsf{else}\ \mathsf{ff} = b.$

D7.16. Implementação (Bool). Definimos:

$$\mathsf{Bool} \stackrel{\mathsf{def}}{=} \mathsf{1} + \mathsf{1}$$

que significa que nossos booleanos serão representados por habitantes do tipo $\mathsf{1}+\mathsf{1}$, mas isso não é suficiente: precisamos definir os ff, tt, que definimos assim:

$$\mathsf{ff} \stackrel{\mathsf{def}}{=} \mathsf{l}\,.\,\star$$
$$\mathsf{tt} \stackrel{\mathsf{def}}{=} \mathsf{r}\,.\,\star$$

mas ainda não terminamos. Falta implementar o if-then-else:

$$\mathsf{if}\ b\ \mathsf{then}\ u\ \mathsf{else}\ v \stackrel{\mathsf{def}}{=} \mathsf{case}\ b\ \mathsf{of}\ \begin{Bmatrix} \mathsf{l}\,.\,x \mapsto v \\ \mathsf{r}\,.\,x \mapsto u \end{Bmatrix}$$

Ainda precisamos mostrar que todas essas construções são de fato factíveis com as mesmas premissas (nenhuma no caso da formação e da introdução, e três no caso da eliminação). Farás isso no Exercício x7.1. E ainda mais, falta verificar que as equações (β) e (η) são satisfeitas (Exercício x7.2).

▸ **EXERCÍCIO x7.1.**
Verifique que as construções envolvidas na Implementação D7.16 são de fato factíveis a partir das premissas de cada uma. (x7.1H0)

▸ **EXERCÍCIO x7.2.**
Verifique que a Implementação D7.16 satisfaz as equações (β) e (η). (x7.2H0)

§173. Tipos têm lógica

§174. Aritmética de tipos

D7.17. Definição (Tipos isomórficos). Sejam α, β tipos. Dizemos que α, β são *isômorfos* ou *isomórficos* sse existem funções

$$\alpha \underset{g}{\overset{f}{\rightleftarrows}} \beta$$

tais que

$$g \circ f = \mathrm{id}_\alpha \qquad\qquad f \circ g = \mathrm{id}_\beta.$$

Escrevemos $\alpha \cong \beta$.

▸ **EXERCÍCIO x7.3.**
(+)-comutatividade (x7.3H0)

▸ **EXERCÍCIO x7.4.**
(+)-identidade. (x7.4H0)

▸ **EXERCÍCIO x7.5.**
(+)-associatividade (x7.5H0)

▸ **EXERCÍCIO x7.6.**
(×)-identidade. (x7.6H0)

▸ **EXERCÍCIO x7.7.**
(×)-associatividade (x7.7H0)

▸ **EXERCÍCIO x7.8.**
(×)-comutatividade (x7.8H0)

► **EXERCÍCIO x7.9.**
distributividade: $\delta(\alpha+\beta) \cong \delta\alpha + \delta\beta$ (x7.9H0)

► **EXERCÍCIO x7.10.**
anulador: $\alpha \cdot 0 \cong 0$ (x7.10H0)

► **EXERCÍCIO x7.11.**
$\alpha^2 \cong \alpha \cdot \alpha$ (x7.11H0)

► **EXERCÍCIO x7.12.**
$0^0 \cong ?$ (x7.12H0)

► **EXERCÍCIO x7.13.**
$0^\alpha \cong ?$ (x7.13H0)

► **EXERCÍCIO x7.14.**
$1^\alpha \cong 1$ (x7.14H0)

► **EXERCÍCIO x7.15.**
$\alpha^1 \cong \alpha$ (x7.15H0)

► **EXERCÍCIO x7.16.**
$\alpha^0 \cong 1$ (x7.16H0)

► **EXERCÍCIO x7.17.**
$(\gamma^\beta)^\alpha \cong \gamma^{\beta\cdot\alpha}$ (x7.17H0)

► **EXERCÍCIO x7.18.**
$\delta^{\alpha+\beta} \cong \delta^\alpha \cdot \delta^\beta$ (x7.18H0)

► **EXERCÍCIO x7.19.**
$(\alpha+\beta)^2 \cong ?$ (x7.19H0)

CAPÍTULO 8

COLEÇÕES

Neste capítulo estudamos uns tipos de dados fundamentais para matemática. Começamos com o *conjunto*, e logo depois encontramos seus tipos-amigos: *tuplas*, *seqüências*, e *famílias indexadas*. Note que já temos encontrado esses tipos de dados, e até trabalhado com eles nos capítulos anteriores mas agora é a sua vez de virar o foco do nosso estudo. Como nós vamos apreciar no Capítulo 16, a linguagem e teoria dos conjuntos oferecem (podem servir como) *fundamentos de matemática*, mas por enquanto nos importa apenas nos acostumar com esses tipos, seus habitantes, suas operações e relações; aprender usá-los e nada mais!

§175. Conceito, notação, igualdade

? **Q8.1. Questão.** O que significa ser conjunto?

Cantor deu a seguinte resposta:

D8.2. "Definição". Um *conjunto* A é a colecção numa totalidade de certos objetos (definidos e separados) da nossa intuição ou mente, que chamamos de *elementos* de A.

▸ **EXERCÍCIO x8.1.**
Qual é o problema principal com a definição acima? (x8.1H0)

8.3. Mudar a pergunta. A Q8.1 é a pergunta errada para perguntar aqui—é uma pergunta para quem quer *implementar* conjuntos responder. As perguntas certas são: (i) o que podemos fazer com um conjunto; (ii) o que precisamos fazer para construir um conjunto; e (iii) o que significa igualdade entre conjuntos. Ou seja, precisamos abordar, como sempre, atravez de uma *especificação*.

8.4. Colleção vs conjunto. O uso da palavra *conjunto* pode variar de contexto para contexto mas destacamos antes de tudo uma propriedade linguística que aplicará sempre estamos falando de um conjunto S: está propriamente referido usando o modo *singular*. A idéia é que ele existe como um (um!) objeto de estudo na nossa mesa, visível no nosso mundo matemático. Tal S da nossa mesa, costuma representar ou corresponder a uma coleção de outros objetos (também visíveis e existentes no nosso mundo). Usaremos aqui a palavra *coleção* sempre na metalinguagem para referir a uma pluraridade de objetos. Nesse caso o uso do modo singular é apenas um modo de falar e sempre deve ser visto como uma abreviação de uma frase em modo plural, referindo aos membros de

tal coleção. Mesmo quando damos um nome (como C, D) para uma coleção, falamos dos seus membros usando esse C mesmo e no plural: «todos os C são legais, mas uns dos D não são». Cuidado pois podemos referir a uma coleção C no singular como no «os membros da C são legais» mas isso não presuponha que existe um objeto C na nossa mesa mesmo, acessível pelo nosso sistema de definições e demonstrações. É apenas uma ferramenta (meta)linguística.

D8.5. Notação. A notação mais simples para denotar um conjunto é usar *chaves* (os símbolos ‘ { ’ e ‘ } ’) e listar todos os seus elementos dentro, os escrevendo numa ordem da nossa escolha. Por exemplo:

$$\begin{aligned} A &= \{0, 1\} & E &= \{2, 3, \{5, 7\}, \{\{2\}\}\} \\ B &= \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\} & F &= \{\text{Thanos}\} \\ C &= \{2\} & G &= \{1, 2, 4, 8, 16, 31, A, B, \mathbb{N}\} \\ D &= \{2, 3, 5, 7\} & H &= \{\text{Thanos}, \text{Natal}, \{E, \{F, G\}\}\} \end{aligned}$$

8.6. Em muitos textos os conjuntos cujos elementos são “do mesmo tipo” são chamados *homogêneos*, e os outros *heterogêneos*. Deixamos sem explicação o que significa “do mesmo tipo”, mas, naturalmente, consideramos os A, B, C, D, F da Notação D8.5 homogêneos e os E, G, H heterogêneos. Até o $\{\{1, 2\}, \{\{2, 3\}, \{3, 4\}\}\}$ acaba heterogêneo se olhar bem: um dos seus membros é conjunto *de números*, mas o outro é conjunto *de conjuntos de números*.

Todos os conjuntos que acabamos de escrever aqui são *finitos*, seus elementos são conhecidos, e ainda mais são poucos e conseguimos listar todos eles. Nenhuma dessas três propriedades é garantida! Se não temos a última fica impráctico listar todos elementos, e quando não temos uma das duas primeiras, é plenamente impossível. Considere por exemplo os conjuntos seguintes:

$$\begin{aligned} X &= \text{o conjunto de todos os números reais entre 0 e 1} \\ Y &= \text{o conjunto dos assassinos do Richard Montague} \\ Z &= \text{o conjunto de todos os números naturais menores que } 2^{256!}. \end{aligned}$$

D8.7. Notação (Set builder). Uma notação diferente e bem útil é chamada notação *set builder* (ou *set comprehension*), onde escrevemos

$$\{\, x : \alpha \mid \ldots x \ldots \} : \mathsf{Set}\ \alpha$$

para denotar «o conjunto de todos os habitantes x do tipo α tais que $\varphi(x)$».[53] Entendemos que no lado direito escrevemos o *filtro*, uma *condição definitiva*, e não algo ambíguo ou algo subjectivo. Por exemplo, não podemos escrever algo do tipo

$$\{\, p : \mathsf{Person} \mid p \text{ é uma pessoa linda} \,\}.$$

Mas como podemos formalizar o que é uma *condição definitiva*? Bem, concordamos escrever apenas algo que podemos (se precisarmos e se quisermos) descrever na linguagem

[53] Na literatura aparecem também os símbolos ‘ : ’ e ‘ ; ’ em vez do ‘ | ’ que usamos aqui.

que temos usado para denotar proposições onde possivelmente aparece a variável x.[54] Tendo qualquer $\varphi : \alpha \to \mathsf{Prop}$ então, podemos formar o conjunto

$$\{\, x : \alpha \mid \varphi(x) \,\}$$

que é o conjunto definido pela

$$a \in \{\, x : \alpha \mid \varphi(x) \,\} \overset{\text{def}}{\iff} \varphi(a).$$

A notação set builder é bem mais poderosa do que acabamos de mostrar, pois nos permite utilizar expressões mais complexas na sua parte esquerda, e não apenas uma variável. Vamos investigar isso e mais variações logo na Secção §180.

8.8. Observação. Na notação

$$\{\, x \mid _\, x \,_ \,\}$$

temos um *ligador de variável*, pois o x no lado esquerdo liga todos os x's que aparecem no lado direito livres (e assim viram ligados). Por exemplo, o conjunto

$$\{\, x \mid x^2 < xy \,\}$$

depende do y (mas não do x).

! **8.9. Cuidado (Capturação de variável).** Podemos trocar o "dummy" x por qualquer variável *que não aparece livre na parte direita*, tomando cuidado para renomear as ligadas também. Por exemplo

$$\{\, x \mid x^2 < xy \,\} \equiv \{\, z \mid z^2 < zy \,\}$$

Mas

$$\{\, x \mid x^2 < xy \,\} \not\equiv \{\, y \mid y^2 < yy \,\}$$

pois o y que tava livre no "filtro" acabou sendo *capturado* pelo ligador no set builder: dentro dos $\{\ldots\}$ perdemos o acesso no objeto denotado por y fora. O $\{\, y \mid y^2 < yy \,\}$ não depende mais do y.

8.10. Sinônimos e fontes. Às vezes usamos os termos *família* e *colecção* como sinónimos da palavra «conjunto»—mas veja a Nota 16.127 também. Seguindo uma práctica comum, quando temos conjuntos de conjuntos dizemos *família de conjuntos*, e depois *colecção de famílias*, etc., pois soam melhor e ajudam raciocinar. Com o mesmo motivo (de agradar ou facilitar nossos olhos, ouvidos, ou cerebros humanos), às vezes mudamos ("elevamos") a fonte que usamos para denotar esses conjuntos: de $A, B, C, \ldots$ para $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ para $\mathscr{A}, \mathscr{B}, \mathscr{C}, \ldots$ por exemplo, dependendo de quantos "níveis de conjuntamentos aninhados" temos. Para ilustrar, imagine que já temos definido uns conjuntos A_1, A_2, A_3, B, C e agora queremos falar sobre os conjuntos $\{A_1, A_2, A_3\}$ e $\{B, C\}$ e dar nomes para eles. Uma escolha razoável seria usar $\mathscr{A}$ e $\mathscr{B}$ para denotá-los:

$$\mathscr{A} = \{A_1, A_2, A_3\} \qquad\qquad \mathscr{B} = \{B, C\}$$

mas isso é apenas questão de costume. Nada profundo aqui.

[54] A situação fica pouco diferente no uso da teoria dos conjuntos como fundamentos de matemática: ela não é sozinha mas vem acompanhando uma lógica (muitas vezes lógica da primeira ordem (FOL)) e nesse caso o que permitimos como filtro varia de acordo com isso (Nota 16.105).

8.11. Observação. Eu vou tentar usar a palavra *colecção* principalmente com seu significado intuitivo e informal que suponho que tu entendes; deixando assim as outras duas (*conjunto* e *família*) para usar na matemática.

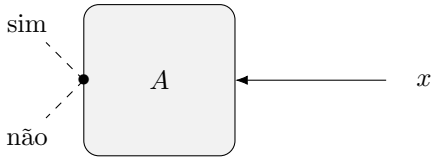
8.12. Teaser. Em geral um conjunto (matemático) realmente representa uma colecção (a dos seus membros), mas como veremos no Capítulo 16 isso não é sempre o caso. Encontramos *colecções que não podem ser representadas por conjunto nenhum* (o motivo mais comum sendo que são grandes demais, algo que deve parecer estranho já que temos *conjuntos infinitos*); mas pode ter outros motivos também!

! **8.13. Aviso.** Mais duas palavras que às vezes são usadas como sinônimos da «conjunto» são as *classe* e *espaço*. Evitarei seu uso aqui por motivos diferentes para cada uma. A primeira (viz. *classe*) é usada em teorias de fundamentos matemáticos, como teorias axiomáticas de conjuntos, (Capítulo 16) e seu papel é exatamente isso: diferenciar o conceito que ela denota por aquele de conjunto! A segunda, (viz. *espaço*) dá a idéia que tal conjunto tem "algo mais" do que *apenas* seus membros: um certo tipo de *estrutura* (Secção §198): talvez alguma relação, e/ou operações, etc.: «...mais que conjuntos: espaços!» Temos espaços: métricos (Capítulo 17), topológicos (18), vetoriais (§269), sóbrios(!), poloneses, projetivos, afim, de Euclides, de Cantor, de Baire, de Borel, de Hibert, de Banach, de Hausdorff, de Fréchet, de Stone, e muitos mais de...muita gente boa! E mesmo assim, não temos uma definição matemática do que significa a palavra (*espaço*) sozinha! Note também que em linguagens naturais *grupo* é mais uma palavra que pode servir como sinônimo de «conjunto» mas em matemática não: no Capítulo 11 definimos o que essa palavra significa «grupo» em matemática e estudamos sua linda teoria: a teoria dos grupos.

8.14. Tipos. Cada vez que introduzimos um novo tipo de objetos, devemos especificar:

(i) Como podemos formar (construir) habitantes desse tipo?
(ii) Como podemos usar (desconstruir) habitantes desse tipo?
(iii) Quando dois objetos desse tipo são *iguais*?

8.15. Black boxes. O conceito de *black box* (ou *caixa preta*) é uma ferramenta muito útil para descrever tipos. A idéia é que queremos descrever o que realmente determina um objeto desse tipo, e *esconder* os detalhes "de implementação", apresentando apenas seu "interface". Podemos então pensar que um conjunto A é um black box que tem apenas uma "entrada" onde podemos botar qualquer objeto x que desejamos, e tem também uma luz que pode piscar "sim" ou "não" (correspondendo nos casos $x \in A$ e $x \notin A$ respectivamente).



Usamos o termo *black* box para enfatizar que não temos como "olhar dentro" desse aparelho, dessa caixa, e ver o que acontece assim que botar uma entrada; nossa única informação será a luz da caixa que vai piscar "sim" ou "não". Quando temos acesso nos "internals" da caixa a gente chama de *white box* ou *transparent box*; mas não vamos precisar o uso desse conceito agora.

A única *estrutura interna* de um conjunto é a capabilidade de *decidir se dois elementos x, y do conjunto são iguais ou não.*

? **Q8.16. Questão.** Quando dois conjuntos são iguais?

!! SPOILER ALERT !!

D8.17. "Definição". Consideramos dois conjuntos A, B *iguais* sse não tem como diferenciar eles como black boxes. Em outras palavras, para cada objeto x que vamos dar como entrada para cada um deles, eles vão concordar: ou ambos vão piscar "sim", ou ambos vão piscar "não". O "slogan" aqui é:

um conjunto é determinado por seus membros.

D8.18. Definição (Igualdade de conjuntos). Dois conjuntos são iguais sse têm exatamente os mesmos membros. Em símbolos,

$$A = B \iff^{\text{def}} (\forall x)[\, x \in A \iff x \in B\,].$$

8.19. Definindo conjuntos. Para determinar então um conjunto A precisamos dizer exatamente o que significa pertencer ao A, ou seja, dizer quando um objeto arbitrário x pertence ao A. As notações que vimos até agora realmente deixam isso claro; mas um outro jeito muito útil para *definir* um certo conjunto A, seria apenas preencher o

$$x \in A \iff^{\text{def}} _____$$

com alguma condição definitiva (veja Notação D8.7).

Concluimos que as duas formas seguintes de definir um conjunto A, são completamente equivalentes:

$$x \in A \iff^{\text{def}} ____ \qquad\qquad A \stackrel{\text{def}}{=} \{\, x \mid ____ \,\}.$$

As duas afirmações tem exatamente o mesmo efeito: definir o mesmo conjunto A. Qual das duas usamos, será mais questão de gosto ou de contexto.

8.20. Observação (O que tá sendo definido mesmo?). Definindo um conjunto A pela

$$x \in A \iff^{\text{def}} _____$$

o que estamos definindo diretamente não é o 'A' mas o '$x \in A$'. Só que: o A, sendo conjunto, ele é *determinado por seus membros* (lembra a "Definição" D8.17) ou seja, sabendo o que $x \in A$ significa para todo x, sabemos *quem é* o A.

8.21. Ordem e multiplicidade. Considere os conjuntos seguintes:

$$A = \{2, 3\}, \qquad B = \{3, 2\}, \qquad C = \{3, 2, 2, 2, 3\}.$$

Observe que $A = B = C$. Ou seja, esses não são três conjuntos, mas apenas *um* conjunto denotado por três jeitos diferentes. O "dispositivo" conjunto não sabe nem de *ordem* nem de *multiplicidade* dos seus membros. Não podemos perguntar a um conjunto «qual é teu *primeiro* elemento?», nem «*quantas vezes* o tal elemento pertence a ti?». Lembre o conjunto como black box! Sua única interface aceita qualquer objeto, e responde apenas com um pleno sim ou não. Logo encontraremos outros tipos de "recipientes", onde as informações de ordem e de multiplicidade são preservadas (e perguntáveis): multisets (§191), tuplas (§186), e seqüências (§190). Bem depois vamos estudar *conjuntos ordenados* (Capítulo 14).

Por enquanto temos apenas duas relações entre conjuntos: igualdade (=)—que sempre temos para qualquer tipo de objetos—e essa "nova" de pertencer ($\in$); Logo vamos definir mais; mas antes disso, bora discutir sobre dois conceitos de igualdade diferentes que mencionei já na Secção §5.[55]

§176. Intensão vs. extensão

8.22. Condidere os conjuntos

$$\begin{aligned} P &= \{\, d \mid d \text{ é um divisor primo de } 2^{256!} \,\} \\ Q &= \{\, p \mid p \text{ é primo e par} \,\} \\ R &= \{\, x \mid x \text{ é raiz real do polinómio } x^3 - 8 \,\} \\ S &= \{2\}. \end{aligned}$$

? **Q8.23. Questão.** Quais são os membros de cada um dos conjuntos acima?

Resposta. *Pensando um pouco* percebemos que esses quatro conjuntos consistem em exatamente os mesmos membros, viz. o número 2 e nada mais. Lembrando na idéia de black box, realmente não temos como diferenciar entre esses black boxes. Começando com o S, é direto que ele responda "sim" apenas no número 2 e "não" em todos os outros objetos. Continuando com o P, realmente temos que o único objeto que satisfaz seu filtro é o número 2. Mesma coisa sobre os Q e R.

8.24. Como comporta o S? Recebendo sua entrada a, ele a compara com o 2 para ver se $a = 2$ ou não, e responde "sim" ou "não" (respectivamente) imediatamente. E o R? Recebendo sua entrada a, ele verifica se a é uma raiz do $x^3 - 8$. Substituindo então o x por a, elevando o a ao 3 e subtraindo 8, se o resultado for 0 responda "sim"; caso contrário, "não". E o Q? Recebendo sua entrada a, ele verifica se a é primo, e se a e par. Se as duas coisa acontecem, ele responda "sim"; caso contrário, "não". E o P? Recebendo sua

[55] Vai que não ficou claro lá, ou que tu pulou o Capítulo 1—mas tu nunca faria isso, né?

entrada a, ele verifica se $a \mid 2^{256!}$ e se a é um número primo. Se as duas coisa acontecem, ele responda "sim"; caso contrário, "não".

Acabamos de descrever a *intensão* de cada conjunto. Mas, sendo black boxes, dados esses conjuntos P, Q, R, S, não conseguimos diferenciá-los, pois a única interação que sua interface permite é botar objetos a como entradas, e ver se pertencem ou não. Falamos então que *extensionalmente* os quatro conjuntos são iguais, mas *intensionalmente*, não. Usamos os termos *igualdade extensional* e *igualdade intensional*. E para abusar a idéia de black box: provavelmente o black box Q demora mais para responder, ou fica mais quente, ou faz mais barulho, etc., do que o S.

Quando definimos um conjunto simplesmente listando todos os seus membros, estamos escrevendo sua *extensão*. E nesse caso, a intensão é a mesma. Quando usamos a notação builder com um filtro, estamos mostrando a *intensão* do conjunto. Nesse caso as duas noções podem ser tão diferentes, que nem sabemos como achar sua extensão!

• **EXEMPLO 8.25.**
Revise a Secção §66 e considere os conjuntos

$$T \stackrel{\text{def}}{=} \{\, p \mid p \text{ e } p+2 \text{ são prímos} \,\}$$

$$L \stackrel{\text{def}}{=} \{\, n \mid n \in \mathbb{N}_{>0} \text{ e não existe primo entre } n^2 \text{ e } (n+1)^2 \,\}$$

$$G \stackrel{\text{def}}{=} \{\, n \mid n \in \mathbb{N}_{>1} \text{ e } 2n = p+q \text{ para alguns primos } p, q \,\}$$

$$C \stackrel{\text{def}}{=} \{\, n \mid n \in \mathbb{N}_{>0} \text{ e a seqüência Collatz começando com } n \text{ nunca pega o valor } 1 \,\}.$$

Sobre o T não sabemos se é finito ou não! Sobre o G, não sabemos se $G = \mathbb{N}_{>1}$ ou não! E, sobre os L e C nem sabemos se eles têm elementos ou não, ou seja, não sabemos nem se $L = \emptyset$ nem se $C = \emptyset$!

Fechando essa secção lembramos que em conjuntos (e em matemática em geral) usamos igualdade '$=$' como igualdade extensional.

§177. Relações entre conjuntos e como defini-las

D8.26. Definição. O conjunto A é um *subconjunto* de B sse todos os membros de A pertencem ao B. Em símbolos:

$$A \subseteq B \iff^{\text{def}} (\forall x \in A)[\, x \in B \,].$$

Se B tem elementos que não pertencem ao A, chamamos o A um *subconjunto próprio* de B, e escrevemos $A \subsetneq B$.

! **8.27. Aviso.** Naturalmente escrevemos $A \not\subseteq B$ para a negação da $A \subseteq B$, que é diferente da afirmação $A \subsetneq B$:

$$A \not\subseteq B \iff A \text{ não é um subconjunto de } B;$$
$$A \subsetneq B \iff A \text{ é um subconjunto próprio de } B.$$

E se quiser dizer que A não é um subconjunto próprio de B? Escreva isso mesmo, ou traduza para seu equivalente («$A \not\subseteq B$ ou $A = B$») pois ninguém merece ler algo do tipo '$A \not\subseteq B$'.

▸ **EXERCÍCIO x8.2.**
$A = B \implies A \subseteq B$. (x8.2H0)

▸ **EXERCÍCIO x8.3.**
$A = B \iff A \subseteq B \ \&\ B \subseteq A$ (x8.3H0)

▸ **EXERCÍCIO x8.4.**
Defina com uma fórmula o $A \subsetneq B$. (x8.4H1)

! **8.28. Cuidado.** O uso dos símbolos $\subseteq$, $\subset$, e $\subsetneq$ não é muito padronizado: encontramos textos onde usam $\subseteq$ e $\subset$ para "subconjunto" e "subconjunto próprio" respectivamente; outros usam $\subset$ e $\subsetneq$. Assim o símbolo $\subset$ é usado com dois significados diferentes. Por isso usamos $\subseteq$ e $\subsetneq$ aqui, evitando completamente o uso do ambíguo $\subset$.

8.29. Notação. Seguindo uma práctica comum que envolve símbolos "direcionais" de relações binárias como os $(\to)$, $(\leq)$, $(\subseteq)$, etc., introduzimos os:

$$A \supseteq B \stackrel{\text{def}}{\iff} B \subseteq A \qquad\qquad A \supsetneq B \stackrel{\text{def}}{\iff} B \subsetneq A.$$

§178. Vazio, universal, singletons

D8.30. Definição (Vazio). Um conjunto é *vazio* sse ele não contem nenhum elemento. Formalmente, definimos o predicado unário

$$\mathsf{Empty}(A) \stackrel{\text{def}}{\iff} (\forall x)[\, x \notin A \,].$$

D8.31. Definição (Singleton). Um conjunto é *singleton* (ou *unitário*) sse ele contem exatamente um elemento. Formulamente,

$$\text{Singleton}(A) \stackrel{\text{def}}{\iff} (\exists! x)[\, x \in A \,].$$

▸ **EXERCÍCIO x8.5.**
Decida se o seguinte pode servir como definição de singleton:

$$\text{Singleton}(A) \stackrel{?}{\iff} (\exists a)[\, a \in A \ \&\ (\forall x)[\, x \in A \to x = a \,]\,].$$

(x8.5H12)

D8.32. Definição. Denotamos o conjunto vazio por $\emptyset$. ↯

▸ **EXERCÍCIO x8.6.**
Na Definição D8.32 roubamos! Resolva o crime. (x8.6H1)

8.33. Para apreciar ainda mais a gravidade do erro acima: se apenas a definição de $\mathsf{Empty}(-)$ fosse suficiente para introduzir a notação $\emptyset$ para denotar "o conjunto vazio", poderiamos também escolher um símbolo para denotar "o conjunto unitário":

$$\begin{aligned} \mathsf{Empty}(-) \text{ definido} &\rightsquigarrow \text{«Denotamos o conjunto vazio por } \emptyset\text{.»} \\ \mathsf{Singleton}(-) \text{ definido} &\rightsquigarrow \text{«Denotamos o conjunto unitário por } 1\text{.»} \end{aligned}$$

Qual de todos—quantos são?—os conjuntos unitários seria o 1? Essa ambigüidade não é permitida em matemática.[56]

▸ **EXERCÍCIO x8.7.**
Quantos são mesmo? (x8.7H0)

Então precisamos demonstrar existência e unicidade. Faça isso agora nos exercícios seguintes.

▸ **EXERCÍCIO x8.8 (Existência do vazio).**
Usando as ferramentas que temos desenvolvido, construa um conjunto vazio. (x8.8H12)

▸ **EXERCÍCIO x8.9 (Unicidade do vazio).**
Supondo que existe pelo menos um conjunto vazio, mostre sua unicidade. Não use reductio ad absurdum. (x8.9H123)

▸ **EXERCÍCIO x8.10.**
Ache uma demonstração diferente, essa vez usando reductio ad absurdum. (x8.10H12)

D8.34. Definição (Universal). Um conjunto é *universal* sse todos os objetos pertencem nele. Formalmente,

$$\mathrm{Universal}(A) \overset{\mathsf{def}}{\iff} \forall x(x \in A).$$

▸ **EXERCÍCIO x8.11 (Existência e unicidade do universal).**
Demonstre a existência e unicidade do conjunto universal. (x8.11H1)

D8.35. Definição. Denotamos o conjunto universal por $\mathcal{U}$.

? **Q8.36. Questão.** Como podemos usar um fato do tipo $D \neq \emptyset$ em nossas demonstrações? O que ganhamos realmente?

[56] Se ainda não tá convencido, bota o artigo definido «o» na frase similar «seja x (um) inteiro». O que significaria se fosse «seja x *o* inteiro»?!

!! SPOILER ALERT !!

Resposta. Ganhamos o direito de escrever "Seja $d \in D$." Em outras palavras: de tomar um elemento arbitrário de D; de declarar uma variável (não usada) para denotar um membro de D.

! **8.37. Aviso.** Quando temos um conjunto A, escrever "seja $x \in A$" seria errado se não sabemos que $A \neq \emptyset$. É um erro parecido quando dividimos uma expressão de aritmética por x, ou apenas escrever uma expressão como a a/x, sem saber que $x \neq 0$. Como em aritmética precisamos separar em casos (caso $x = 0$ e caso $x \neq 0$) e os tratar em formas diferentes, precisamos fazer a mesma coisa trabalhando com conjuntos: caso $A \neq \emptyset$, achamos uma demonstração onde podemos realmente declarar uma variável não-usada para declarar um elemento de A; caso $A = \emptyset$, achamos uma demonstração diferente—e na maioria das vezes esse caso vai ser trivial para demonstrar.

§179. Oito proposições simples

▸ **EXERCÍCIO x8.12.**
Seja A um conjunto. Responda para cada uma das afirmações abaixo com "sim", "não", ou "depende":

$$\emptyset \subseteq \emptyset; \qquad \emptyset \in \emptyset;$$
$$\emptyset \subseteq A; \qquad \emptyset \in A;$$
$$A \subseteq \emptyset; \qquad A \in \emptyset;$$
$$A \subseteq A; \qquad A \in A.$$

(x8.12 H 0)

! **8.38. Cuidado.** Nossa intuição muitas vezes nos engana, e por isso apenas responder no jeito que o Exercício x8.12 pediu não vale muita coisa. Precisamos demonstrar todas essas respostas. Para cada uma das oito afirmações então, precisamos dizer:

- «Sim» e *demonstrar* a afirmação;
- «Não» e *refutar* a afirmação;
- «Depende» e *mostrar* (pelo menos) dois casos: um onde a afirmação é verdadeira, e outro onde ela é falsa.

Idealmente nesse último caso queremos determinar quando a afirmação é verdadeira, achando condições *suficientes* e/ou *necessárias*. Vamos fazer tudo isso agora.

▸ **EXERCÍCIO x8.13.**
Em qual ordem tu escolharia "atacar" essas afirmações? (x8.13 H 0)

8.39. Propriedade. *Para todo conjunto A, $A \notin \emptyset$.*

DEMONSTRAÇÃO. Seja A conjunto. Agora diretamente pala definição de vazio tomando $x := A$, temos $A \notin \emptyset$. ∎

8.40. Corolário. $\emptyset \notin \emptyset$.

DEMONSTRAÇÃO. Essa afirmação é apenas um *caso especial* de Propriedade 8.39: tome $A := \emptyset$. ∎

▸ **EXERCÍCIO x8.14.**
Demonstre o Corolário 8.40 diretamente, sem usar a Propriedade 8.39. (x8.14 H 1)

8.41. Propriedade. *Para todo conjunto A, temos $A \subseteq A$.*

DEMONSTRAÇÃO. Seja A conjunto. Suponha que $a \in A$. Agora precisamos mostrar $a \in A$, algo que já temos. ∎

▸ **EXERCÍCIO x8.15.**
Pode achar uma demonstração com menos passos? (x8.15 H 0)

8.42. Corolário. $\emptyset \subseteq \emptyset$.

DEMONSTRAÇÃO. Caso especial da Propriedade 8.41 tomando $A := \emptyset$, pois $\emptyset$ é um conjunto. ∎

8.43. Propriedade. *Para todo conjunto A, temos $\emptyset \subseteq A$.*

▸ ESBOÇO. Para chegar num absurdo suponha que tem um contraexemplo: um conjunto A tal que $\emptyset \not\subseteq A$. Daí achamos rapidamente o absurdo desejado lembrando a definição de $\not\subseteq$. Sem usar reductio ad absurdum, vamos acabar querendo demonstrar que uma implicação é verdadeira. Mas cuja premissa é falsa, algo que garanta a veracidade da implicação! □

▸ **EXERCÍCIO x8.16.**
Podemos ganhar a Propriedade 8.41 como corolário da 8.43 ou vice-versa? Explique. (x8.16 H 0)

8.44. Proposição. *Existe uma infinidade de conjuntos A que satisfazem a $\emptyset \in A$ e uma infinidade de conjuntos A que não a satisfazem.*

8.45. Propriedade. *O único subconjunto do $\emptyset$ é ele mesmo. Em outras palavras:*

$$A \subseteq \emptyset \iff A = \emptyset.$$

Agora falta apenas uma afirmação para examinar: $A \in A$?

▸ **EXERCÍCIO x8.17.**
Consegues mostrar algum conjunto com a propriedade que ele pertence nele mesmo? Ou seja, podes achar um conjunto A tal que $A \in A$? (x8.17 H 0)

§180. Mais set builder

Já encontramos a versão mais simples de set comprehension (ou notação set builder) que nos permite escrever

$$\{\, x \mid __x__ \,\}$$

onde x é uma variável, e $__x__$ uma afirmação onde pode aparecer essa variável x. Essa notação é bem mais flexível que isso. Por exemplo

$$\{\, p^n + x \mid p \text{ é primo, } n \text{ é ímpar, e } x \in [0,1) \,\}$$

seria o conjunto de todos os números reais que podem ser escritos na forma $p^n + x$ para algum primo p, algum ímpar n, e algum real x com $0 \leq x < 1$.

Finalmente, mais uma extensão dessa notação é que usamos

$$\{\, x \in A \mid __x__ \,\} \stackrel{\text{def}}{=} \{\, x \mid x \in A \;\&\; __x__ \,\}.$$

▸ **EXERCÍCIO x8.18.**
Por que a notação

$$\{\, x \in A \mid __x__ \,\}$$

não é apenas um caso especial da notação que nos permite escrever termos na parte esquerda de set builder? (x8.18 H 1)

▸ **EXERCÍCIO x8.19.**
Usando a notação set builder defina os conjuntos D_{12}, M_{12}, e P_{12} de todos os divisores, todos os múltiplos, e todas as potências de 12. Generalize para um inteiro m. Identifique quais variáveis que aparecem na tua resposta são livres e quais são ligadas. (x8.19 H 0)

▸ **EXERCÍCIO x8.20.**
Seja $T = \{u, v\}$ um conjunto com dois elementos u, v. Definimos um conjunto A pela

$$A \stackrel{\text{def}}{=} \{\, f(n,m) \mid n, m \in T \,\}$$

Quantos elementos tem o A? (x8.20 H 1)

▸ **EXERCÍCIO x8.21.**
Escreva a extensão do conjunto

$$B \stackrel{\text{def}}{=} \left\{\, n^2 + m^2 \mid n, m \in \{1,3\} \,\right\}.$$

(x8.21 H 0)

▸ **EXERCÍCIO x8.22.**
Mostre como a notação "mais rica" de

$$\{\, t(x_1, \ldots, x_n) \mid \varphi(x_1, \ldots, x_n) \,\}$$

pode ser definida como açúcar sintáctico se temos já a notação de comprehensão que permite apénas uma variável no lado esquerdo. Aqui considere que o $t(x_1, \ldots, x_n)$ é um termo que pode ser bem complexo, formado por outros termos complexos, etc., e onde possivelmente aparecem as variáveis $x_1, \ldots, x_n$. (x8.22 H 1 2)

! 8.46. Cuidado. As variáveis que aparecem na parte esquerda de set builder, são *ligadores* que ligam com as correspondentes variáveis livres que aparecem na afirmação na parte direita (filtro). Então cuidado com o uso dessas variáveis pois é fácil escrever algo que mesmo que realmente determina um conjunto, não é o conjunto desejado!

▸ **EXERCÍCIO x8.23.**
Para cada um dos conjuntos abaixo, decida se sua definição realmente é correta. Caso que sim, determina a extensão do conjunto definido. Caso que não, explique qual é o problema com a definição. Em todas elas, considere que nosso universo é o $\mathbb{R}$.

$$\begin{aligned}
A &= \left\{ x \mid \sqrt{x^2+2} \ \&\ x \in \mathbb{R} \right\} \\
B &= \left\{ x \mid \sqrt{x^2+2} \text{ para algum } x \in \mathbb{R} \right\} \\
C &= \left\{ t \mid \sqrt{x^2+2} = t \text{ para algum } x \in \mathbb{R} \right\} \\
D &= \left\{ x \mid \sqrt{x^2+2} = x \text{ para algum } x \in \mathbb{R} \right\} \\
E &= \left\{ x \mid \sqrt{x^2+2} = x \text{ para todo } x \in \mathbb{R} \right\} \\
F &= \left\{ x \mid \sqrt{t^2+2} = x \text{ para todo } t \in \mathbb{R} \right\} \\
G &= \left\{ x \mid \sqrt{t^2+2} = x \text{ para algum } t \in \mathbb{R} \right\}.
\end{aligned}$$

(x8.23 H 0)

§181. Operações entre conjuntos e como defini-las

8.47. Operações. Lembramos que uma operação num tipo de objetos mapeia certos objetos desse tipo (suas entradas) para *exatamente um* objeto desse tipo (sua saída).

8.48. Definindo operações. Então como podemos *definir uma operação* nos conjuntos? O que precisamos deixar claro?

Um operador é determinado por seu comportamento.

Então se a "saída" (ou o "resultado") duma operação é um conjunto, basta determinar esse conjunto para quaisquer entradas aceitáveis pela operação. E como determinamos

um conjunto? Para começar, podemos usar um dos jeitos que já encontramos para definir um conjunto A:

$$A \stackrel{\text{def}}{=} \{\, x \mid __x__ \,\} \qquad\qquad x \in A \stackrel{\text{def}}{\iff} __x__.$$

Bora definir umas operações conhecidas para aquecer.

D8.49. Definição. Sejam A, B conjuntos. Definimos

$$A \cup B \stackrel{\text{def}}{=} \{\, x \mid x \in A \text{ ou } x \in B \,\}$$

Alternativamente, podemos definir a mesma operação na seguinte forma equivalente:

$$x \in A \cup B \stackrel{\text{def}}{\iff} x \in A \text{ ou } x \in B.$$

Chamamos o $A \cup B$ a *união* dos A e B.

8.50. Observação. Primeiramente esquematicamente:

$$x \in A \cup B \stackrel{\text{def}}{\iff} x \in A \text{ ou } x \in B$$
$$x \in A \cup B \stackrel{\text{def}}{\iff} x \in A \text{ ou } x \in B$$
$$x \in A \cup B \stackrel{\text{def}}{\iff} x \in A \text{ ou } x \in B.$$

onde colorifiquei três maneiras de entender o que é que tá sendo definido mesmo.

E agora com palavras: se eu determinar o que significa que um x arbitrário pertence ao $A \cup B$, então eu determinei o $A \cup B$, pois ele é um conjunto e *um conjunto é determinado por seus membros;* e como eu fiz isso para quaisquer conjuntos A, B (arbitrários), então eu determinei o $\cup$, pois ele é um operador e *um operador é determinado por seu comportamento*. Vamos voltar nesse assunto nos capítulos 9 e 16 onde estudamos funções e teoria dos conjuntos respectivamente.

D8.51. Definição. Sejam A, B conjuntos. Definimos

$$x \in A \cap B \stackrel{\text{def}}{\iff} x \in A \;\&\; x \in B.$$

Chamamos o $A \cap B$ a *intersecção* dos A e B.

▸ **EXERCÍCIO x8.24.**
Defina a operação $\cap$ usando a notação set builder. (x8.24H0)

D8.52. Definição. Chamamos dois conjuntos *disjuntos* sse não têm nenhum elemento em comum. Em símbolos,

$$A, B \text{ disjuntos} \stackrel{\text{def}}{\iff} A \cap B = \emptyset.$$

! **8.53. Cuidado (type errors).** Não confunda o uso dos '$\stackrel{\text{def}}{=}$' e '$\stackrel{\text{def}}{\iff}$' (nem dos '$=$' e '$\iff$'). Usamos o '$=$' para denotar *igualdade* entre dois *objetos*, e usamos o '$\iff$' para denotar que as *afirmações* que aparecem nos dois lados são *equivalentes*. No mesmo jeito que não podemos escrever

$$2+3 \iff 5 \qquad \text{nem} \qquad (x \leq y) \;=\; (x+1 \leq y+1)$$

não podemos escrer também

$$A \setminus B \iff A \cap B^{\mathsf{c}} \qquad \text{nem} \qquad (A \subsetneq B) \;=\; (A \subseteq B \;\&\; A \neq B).$$

O que queríamos escrever nesses casos seria:

$$2+3=5 \qquad\qquad x \leq y \iff x+1 \leq y+1$$
$$A \setminus B = A \cap B^{\mathsf{c}} \qquad\qquad A \subsetneq B \iff A \subseteq B \;\&\; A \neq B.$$

Caso que tudo isso não foi óbvio, sugiro revisitar o Capítulo 1: §1, §3, §5).

8.54. Observação (A linguagem rica dos conjuntos). Observe que conseguimos traduzir a frase "os A, B não têm nenhum elemento em comum" como uma igualdade entre dois conjuntos, o $A \cap B$ e o $\emptyset$:

$$\text{«os } A, B \text{ não têm nenhum elemento em comum»} \quad \rightsquigarrow \quad A \cap B = \emptyset.$$

A linguagem de conjuntos é realmente muito expressiva, algo que vamos começar a apreciar ainda mais, na §196.

Continuamos com mais operações, incluindo nossa primeira operação unária.

D8.55. Definição. Seja A conjunto. Definimos

$$A^{\mathsf{c}} \stackrel{\text{def}}{=} \{\, x \mid x \notin A \,\}$$

Chamamos o A^{c} o *complemento* de A.

D8.56. Definição. Sejam A, B conjuntos.

$$A \setminus B \stackrel{\text{def}}{=} \{\, x \in A \mid x \notin B \,\}$$

Chamamos o conjunto $A \setminus B$ o *complemento relativo* de B no A, e pronunciamos o $A \setminus B$ como «A menos B» ou «A fora B».

▸ **EXERCÍCIO x8.25.**
Calcule (a extensão d)os conjuntos:

(1) $\{0,1,2,3,4\} \setminus \{4,1\}$
(2) $\{0,1,2,3,4\} \setminus \{7,6,5,4,3\}$
(3) $\{0,1,2\} \setminus \mathbb{N}$
(4) $\mathbb{N} \setminus \{0,1,2\}$
(5) $\{\{0,1\},\{1,2\},\{0,2\}\} \setminus \{0,1\}$

(6) $\{\{0,1\},\{1,2\},\{0,2\}\} \setminus \{\{0,1,2\}\}$
(7) $\{\{0,1\},\{1,2\},\{0,2\}\} \setminus \{\{1,2\}\}$
(8) $\{\{0,1\},\{1,2\}\} \setminus \{\{1\}\}$
(9) $\{7,\emptyset\} \setminus \emptyset$
(10) $\{7,\emptyset\} \setminus \{\emptyset\}$
(11) $\mathbb{R} \setminus 0$
(12) $\mathbb{R} \setminus \{0\}$
(13) $\{1,\{1\},\{\{1\}\},\{\{\{1\}\}\}\} \setminus 1$
(14) $\{1,\{1\},\{\{1\}\},\{\{\{1\}\}\}\} \setminus \{\{\{1\}\}\}$

Cuidado: um leitor "mal-tipado" daria respostas diferentes em umas dessas. (x8.25 H 1)

▸ **EXERCÍCIO x8.26.**
Sejam A, B conjuntos. Considere as afirmações:

(1)	$\emptyset \setminus \emptyset = \emptyset$	(5)	$A \setminus A = A$	(9)	$A \setminus B = B$
(2)	$A \setminus \emptyset = A$	(6)	$A \setminus A = \emptyset$	(10)	$A \setminus B = B \setminus A$
(3)	$\emptyset \setminus A = \emptyset$	(7)	$A \setminus B = \emptyset$	(11)	$A \setminus \{B\} = A$
(4)	$\{\emptyset\} \setminus A = \emptyset$	(8)	$A \setminus B = A$	(12)	$\{A, B\} \setminus (A \cup B) = \emptyset$

Para cada uma delas: demonstre, se é verdadeira; refuta, se é falsa; mostre um exemplo e um contraexemplo, se sua veracidade depende dos A, B (e tente determinar exatamente quando é verdadeira). (x8.26 H 0)

D8.57. Definição. Sejam A, B conjuntos. Sua *diferença simétrica* é o conjunto de todos os objetos que pertencem a exatamente um dos A, B. O denotamos por $A \triangle B$:

$$x \in A \triangle B \overset{\text{def}}{\iff} x \text{ pertence a exatamente um dos } A, B.$$

• **EXEMPLO 8.58.**
Calculamos (as extensões d)os conjuntos:

- $\{0,1,2,3\} \triangle \{1,2,4,8\} = \{0,3,4,8\}$;
- $\{\{0,1\},\{1,2\}\} \triangle \{0,1,2\} = \{\{0,1\},\{1,2\},0,1,2\}$;
- $\{\{0,1\},\{1,2\}\} \triangle \{\{0,1\},\{0,2\}\} = \{\{0,2\},\{1,2\}\}$;
- $(-2,1) \triangle (-1,2) = (-2,-1] \cup [1,2)$

(Veja a Definição D6.28 caso que não reconheceu a notação de intervalos que aparece no último exemplo.)

▸ **EXERCÍCIO x8.27.**
Dado A conjunto, calcule os conjuntos $A \triangle A$ e $A \triangle \emptyset$. (x8.27 H 0)

? **Q8.59. Questão.** O que interessante (e característico) têm os membros de $A \triangle B$? Como os chamarias com palavras de rua?

!! SPOILER ALERT !!

8.60. Resposta. Pensando pouco nas definições de

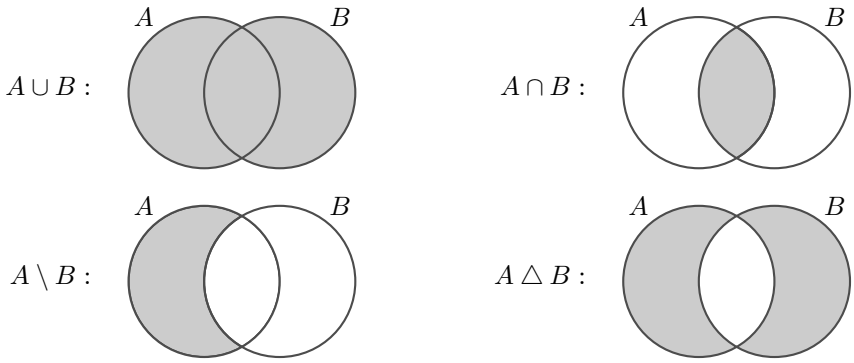
$$A \triangle B \qquad \text{e} \qquad A = B$$

concluimos que a diferença simétrica de dois conjuntos tem exatamente todas as *testemunhas* que mostram que os conjuntos são diferentes:

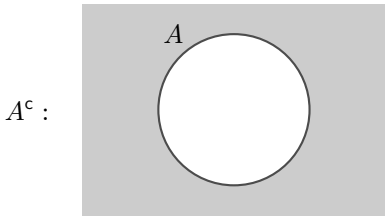
$$x \in A \triangle B \overset{\heartsuit}{\iff} x \text{ é um testemunha que } A, B \text{ são diferentes.}$$

O que podes concluir então assim que souberes que $A \triangle B = \emptyset$? (Isso é o Exercício x8.32, que resolverás logo.)

8.61. Diagramas de Venn. O leitor provavelmente já encontrou os *diagramas de Venn* na sua vida, uma ferramenta muito útil para descrever operações e ajudar em raciocinar sobre relações de conjuntos. Por exemplo, podemos visualizar as quatro operações binárias que definimos até agora assim:

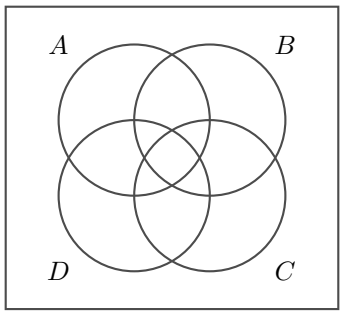


E a única operação unária, o complemento, assim:



! **8.62. Cuidado (Limitações de Venn).** Assim que tiver mais que três conjuntos os diagramas de Venn perdem sua clareza e logo sua utilidade.

▸ **EXERCÍCIO x8.28.**
Um aluno desenhou o seguinte diagrama Venn para representar todas as possíveis maneiras que 4 conjuntos A, B, C, D podem intersectar entre si:



Qual o problema com esse diagrama? (x8.28 H 1)

§182. Demonstrando igualdades e inclusões

▸ **EXERCÍCIO x8.29.**
Demonstre ou refute a afirmação:

$$\text{para todos os conjuntos } A, B, C, \text{ se } A \subseteq B \ \ \& \ \ A \subseteq C \text{ então } A \subseteq B \cap C.$$

(x8.29 H 0)

▸ **EXERCÍCIO x8.30.**
Demonstre ou refute a afirmação:

$$\text{para todos os conjuntos } A, B, C, \text{ se } A \subsetneq B \ \ \& \ \ A \subsetneq C, \text{ então } A \subsetneq B \cap C.$$

(x8.30 H 0)

8.63. Proposição (De Morgan para conjuntos). *Para quaisquer conjuntos A, B, C,*

$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$$
$$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B).$$

Demonstração. Sejam A, B, C conjuntos. Vamos demonstrar a primeira igualdade e deixar a segunda como exercício (x8.31). Mostramos as duas inclusões separadamente:

($\subseteq$): Tome $x \in C \setminus (A \cup B)$. Daí $x \in C$ e $x \notin (A \cup B)$, ou seja $x \notin A$ e $x \notin B$. Como $x \in C$ e $x \notin A$, temos $x \in C \setminus A$, e, similarmente $x \in C \setminus B$. Logo chegamos no desejado $x \in (C \setminus A) \cap (C \setminus B)$.

A inclusão inversa ($\supseteq$) é similar. ∎

▸ **EXERCÍCIO x8.31.**
Demonstre a segunda igualdade da Proposição 8.63. (x8.31 H 0)

! **8.64. Aviso (Não escreva assim!).** Uma outra maneira de demonstrar a Proposição 8.63, é calcular usando fórmulas e leis de lógica:

$$\begin{aligned}
x \in C \setminus (A \cup B) &\iff x \in C \wedge \neg(x \in A \cup B) && \text{(def. } C \setminus (A \cup B)\text{)}\\
&\iff x \in C \wedge \neg(x \in A \vee x \in B) && \text{(def. } \cup\text{)}\\
&\iff x \in C \wedge (x \notin A \wedge x \notin B) && \text{(De Morgan)}\\
&\iff (x \in C \wedge x \notin A) \wedge (x \in C \wedge x \notin B) && \text{(idemp., assoc., comut. de } \wedge\text{)}\\
&\iff (x \in C \setminus A) \wedge (x \in C \setminus B) && \text{(def. } \setminus\text{)}\\
&\iff x \in (C \setminus A) \cap (C \setminus B). && \text{(def. } \cap\text{)}
\end{aligned}$$

Logo $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$ pela definição da igualdade de conjuntos. E a demonstração da outra igualdade é de graça, pois é a sua proposição *dual*: trocamos apenas os $\cup$ com os $\cap$, e os $\vee$ com os $\wedge$! *Mas não fique muito empolgado com essa demonstração–cálculo:* uma demonstração duma proposição é um texto, legível, que um humano consegue seguir, entender, e verificar; exatamente como fizemos na Proposição 8.63.

8.65. Proposição. *Sejam A, B conjuntos. Logo,*

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

▸ Esboço. Antes de começar, traduzimos os dois lados: «em exatamente um dos dois» na esquerda, «no primeiro mas não no segundo ou no segundo mas não no primeiro» na direita. Faz sentido que os dois conjuntos são iguais, pois as duas frases são equivalentes! Mas para demonstrar formalmente a afirmação, mostramos as duas direções

$$A \triangle B \subseteq (A \setminus B) \cup (B \setminus A) \qquad \& \qquad A \triangle B \supseteq (A \setminus B) \cup (B \setminus A)$$

separadamente, usando as definições de $(\subseteq)$ e $(\supseteq)$. □

8.66. Proposição. *Sejam A, B conjuntos. Logo,*

$$A \triangle B = (A \cup B) \setminus (A \cap B).$$

▸ Esboço. Novamente, começamos pensando nos dois lados e suas intensões: «em exatamente um dos dois» na esquerda; «em pelo menos um dos dois, mas não nos dois» na direita. As duas frases são equivalentes, mas vamos mostrar formalmente a igualdade desses conjuntos, mostrando novamente as $(\subseteq)$ e $(\supseteq)$ separadamente. □

8.67. Observação. No D8.57 eu dei uma definição elementária, para determinar o conjunto $A \triangle B$. De fato, seria até melhor *definir* a operação $\triangle$ usando uma das duas expressões que encontramos acima.

▸ **EXERCÍCIO x8.32.**
Demonstre ou refute a afirmação:

para todo conjunto A, B, se $A \triangle B = \emptyset$, então $A = B$.

(x8.32 H 0)

§183. Cardinalidade

D8.68. Definição. Seja A um conjunto. A *cardinalidade* de A é a quantidade de elementos de A. A denotamos por $|A|$:

$$|A| \stackrel{\text{def}}{=} \begin{cases} n, & \text{se } A \text{ é finito com exatamente } n \text{ membros distintos} \\ \infty, & \text{se } A \text{ é infinito.} \end{cases}$$

Às vezes usamos a notação $\#A$ quando o A é finito, mas mesmo nesses casos evitarei essa notação.

Nos capítulos 13 e 16 vamos *refinar* essa notação pois como Cantor percebeu, o segundo caso na Definição D8.68 é *bem*, *bem*, *bem* mais rico do que aparece!

8.69. Propriedade. *Sejam A, B conjuntos finitos. Logo*

$$|A \cup B| \leq |A| + |B| \,.$$

Demonstração. Pelo princípio da inclusão–exclusão (§129) temos

$$|A \cup B| = |A| + |B| - |A \cap B|$$

e como uma cardinalidade não pode ser negativa, segue a desigualdade desejada. ∎

▸ **EXERCÍCIO x8.33.**
Determine quando temos ‘$=$’ na desigualdade da Propriedade 8.69. (x8.33 H 0)

§184. Powerset

D8.70. Definição. Seja A conjunto. Chamamos o *powerset* (ou *conjunto de partes*, ou *conjunto potência*) de A, denotado por $\wp A$, é o conjunto de todos os subconjuntos de A. Formalmente:

$$X \in \wp A \iff^{\text{def}} X \subseteq A.$$

O *powerset finito* de A, que denotamos por $\wp_{\text{f}} A$, é o conjunto de todos os subconjuntos *finitos* de A:

$$X \in \wp_{\text{f}} A \iff^{\text{def}} X \subseteq_{\text{fin}} A.$$

▸ **EXERCÍCIO x8.34 (justificativa do nome).**
Seja A conjunto finito. Qual a cardinalidade do $\wp A$ em termos da cardinalidade do A? (x8.34 H 0)

D8.71. Definição (Mais set builder). Dado conjunto A, introduzimos a notação

$$\{\, X \subseteq A \mid \varphi(X) \,\} \stackrel{\text{def}}{=} \{\, X \in \wp A \mid \varphi(X) \,\}\,.$$

▸ **EXERCÍCIO x8.35.**
Calcule (ache a extensão d)os conjuntos seguintes:

$$\wp\{1,2\} \qquad \wp\{a,b,\{a,b\}\}, \qquad \wp\{\emptyset,\{\emptyset\}\}, \qquad \wp\{\mathbb{N}\}.$$

(x8.35 H 0)

▸ **EXERCÍCIO x8.36.**
Calcule os conjuntos seguintes:

$$\wp\emptyset, \qquad \wp\wp\emptyset, \qquad \wp\wp\wp\emptyset.$$

(x8.36 H 0)

▸ **EXERCÍCIO x8.37.**
Defina usando duas maneiras diferentes um operador unário $\wp_1$ que forma o conjunto de todos os *singletons* feitos por membros da sua entrada. (x8.37 H 0)

§185. União grande; intersecção grande

Generalizamos agora as operações binárias de união e intersecção para suas versões arbitrárias, as operações unitárias $\bigcup -$ e $\bigcap -$. Antes de dar uma definição, mostramos uns exemplos. Esses operadores são mais interessantes e úteis quando são aplicados em conjunto cujos membros são conjuntos também, pois—coloquialmente falando—eles correspondem na união e na intersecção dos seus membros.

• **EXEMPLO 8.72.**
Aplicamos as operações $\bigcup$ e $\bigcap$ nos conjuntos seguintes:

$$\begin{aligned}
\bigcup\{\{1,2,4,8\},\{0,2,4,6\},\{2,10\}\} &= \{0,1,2,4,6,8,10\}\\
\bigcap\{\{1,2,4,8\},\{0,2,4,6\},\{2,10\}\} &= \{2\}\\
\bigcup\{\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}\} &= \mathbb{R}\\
\bigcap\{\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}\} &= \mathbb{N}\\
\bigcup\{2,3,\{4,5\},\{4,6\}\} &= \{4,5,6\}\\
\bigcap\{2,3,\{4,5\},\{4,6\}\} &= \emptyset
\end{aligned}$$

8.73. De conectivos binários para quantificadores. Considere a afirmação:

«Alex comeu manga ou Babis comeu manga.»

Naturalmente essa proposição corresponde numa disjunção:

$$\underbrace{\text{Alex comeu manga}}_{\varphi(\text{Alex})}\ \underbrace{\text{ou}}_{\vee}\ \underbrace{\text{Babis comeu manga}}_{\varphi(\text{Babis})}.$$

Dualmente (trocando o "ou" por "e") chegamos numa conjunção:

$$\underbrace{\text{Alex comeu manga}}_{\varphi(\text{Alex})}\ \underbrace{\text{e}}_{\wedge}\ \underbrace{\text{Babis comeu manga}}_{\varphi(\text{Babis})}.$$

E agora a pergunta:

? **Q8.74. Questão.** Como podemos descrever cada uma das

$$\varphi(A) \vee \varphi(B) \qquad\qquad \varphi(A) \wedge \varphi(B)$$

(que são uma disjunção e uma conjunção) como uma fórmula que começa com quantificador?

!! SPOILER ALERT !!

8.75. Resposta. Assim!:

$$\begin{aligned} \varphi(A) \vee \varphi(B) &\iff (\exists x \in \{A, B\})[\,\varphi(x)\,] \\ \varphi(A) \wedge \varphi(B) &\iff (\forall x \in \{A, B\})[\,\varphi(x)\,]. \end{aligned}$$

Com palavras pouco mais humanas:

«Alguém dos A, B comeu manga.»
«Todos os A, B comeram manga.»

? **Q8.76. Questão.** Como tu definarias as $\bigcup$ e $\bigcap$ formalmente então? Podes adivinhar definições que concordam com todos esses exemplos no 8.72?

!! SPOILER ALERT !!

Observe que pela definição de $\cup$ temos

$$\begin{aligned} x \in A \cup B &\iff x \in A \text{ ou } x \in B \\ &\iff x \text{ pertence àlgum dos } A, B \\ &\iff (\exists X \in \{A, B\})[\, x \in X \,] \end{aligned}$$

e dualmente para a intersecção:

$$\begin{aligned} x \in A \cap B &\iff x \in A \ \&\ x \in B \\ &\iff x \text{ pertence a cada um dos } A, B \\ &\iff (\forall X \in \{A, B\})[\, x \in X \,]. \end{aligned}$$

Chegamos assim na resposta formal:

D8.77. Definição. Seja $\mathscr{A}$ um conjunto.

$$\begin{aligned} x \in \bigcup \mathscr{A} &\overset{\text{def}}{\iff} x \text{ pertence àlgum dos membros do } \mathscr{A} \\ x \in \bigcap \mathscr{A} &\overset{\text{def}}{\iff} x \text{ pertence a todos os membros do } \mathscr{A}. \end{aligned}$$

Equivalentemente com fórmulas,

$$\begin{aligned} x \in \bigcup \mathscr{A} &\overset{\text{def}}{\iff} (\exists A \in \mathscr{A})[\, x \in A \,] \\ x \in \bigcap \mathscr{A} &\overset{\text{def}}{\iff} (\forall A \in \mathscr{A})[\, x \in A \,]. \end{aligned}$$

Chamamos o $\bigcup \mathscr{A}$ a *união* de $\mathscr{A}$, e o $\bigcap \mathscr{A}$ a *intersecção* de $\mathscr{A}$.

▸ **EXERCÍCIO x8.38.**
Defina os operadores binários $\cup$ e $\cap$ como açúcar sintáctico definido pelos operadores unários $\bigcup$ e $\bigcap$ respectivamente. (x8.38 H 0)

▸ **EXERCÍCIO x8.39.**
Calcule os conjuntos: $\bigcup \emptyset$; $\bigcup \bigcup \emptyset$. (x8.39 H 0)

▸ **EXERCÍCIO x8.40.**
Calcule o $\bigcap \emptyset$. (x8.40 H 1)

▸ **EXERCÍCIO x8.41.**
Calcule o $\bigcap \mathcal{U}$. (x8.41 H 1 2)

▸ **EXERCÍCIO x8.42.**
Seja A conjunto. Calcule os $\bigcup \{A\}$ e $\bigcap \{A\}$. (x8.42 H 0)

▸ **EXERCÍCIO x8.43.**
Sejam C conjunto e $\mathscr{A}$ família de conjuntos tais que todos contêm o C (ou seja, C é um subconjunto de cada membro da $\mathscr{A}$). Demonstre que $C \subseteq \bigcap \mathscr{A}$. (x8.43 H 0)

▸ **EXERCÍCIO x8.44.**
Seja $\mathscr{A}$ família não vazia de conjuntos. Demonstre que $\bigcap \mathscr{A}$ está contido em todo membro da $\mathscr{A}$. (x8.44 H 0)

8.78. Bem, bem, bem informalmente podemos dizer que: a operação $\bigcup$ tire o nível mais externo de chaves; a $\bigcap$ também mas jogando fora bem mais elementos (aqueles que não pertencem em todos os membros do seu argumento); e o $\wp$ bote todas as chaves em todas as combinações possíveis para "o nível mais próximo".

▸ **EXERCÍCIO x8.45.**
Sejam A conjunto e $\mathscr{A} \subseteq \wp A$ tal que

$$\bigcup \mathscr{A} = A.$$

A afirmação

$$A \in \mathscr{A}$$

é verdadeira? Se sim, demonstre; se não, refute; se os dados não são suficientes para concluir, mostre um exemplo e um contraexemplo. (x8.45 H 1)

▸ **EXERCÍCIO x8.46.**
Ache conjuntos finitos A, B tais que

$$0 < \left|\bigcap A\right| < |A| < \left|\bigcup A\right| \qquad\qquad 0 < |B| < \left|\bigcap B\right| < \left|\bigcup B\right|.$$

(x8.46 H 0)

▸ **EXERCÍCIO x8.47.**
Sejam $\mathscr{A}, \mathscr{B}$ famílias de conjuntos com $\mathscr{A} \cap \mathscr{B} \neq \emptyset$. Demonstre ou refute a afirmação:

$$\bigcap \mathscr{A} \subseteq \bigcup \mathscr{B}.$$

(x8.47 H 1 2 3 4)

Intervalo de problemas

▸ **PROBLEMA Π8.1.**
Seja $\mathscr{A}$ família de conjuntos tal que

$$\bigcup \mathscr{A} = \bigcap \mathscr{A}.$$

O que podes concluir sobre o $\mathscr{A}$? (Π8.1 H 0)

▸ **PROBLEMA Π8.2.**
Dualize e demonstre o resultado do Exercício x8.43. (Π8.2 H 0)

▸ **PROBLEMA Π8.3.**
Sejam A, B conjuntos. Para cada direcção de

$$\bigcup A \subseteq B \overset{?}{\iff} A \subseteq \wp B$$

demonstre ou refute. (Π8.3 H 0)

▸ **PROBLEMA Π8.4.**
Sejam $n \in \mathbb{N}$ com $n \geq 2$ e n conjuntos $A_1, A_2, \ldots, A_n$. Seja

$$A = A_1 \mathbin{\triangle} A_2 \mathbin{\triangle} \cdots \mathbin{\triangle} A_n.$$

Observe que como a operação $\triangle$ é associativa e comutativa, o A é bem-definido. Demonstre que:

$$A = \{\, a \mid a \text{ pertence a uma quantidade ímpar dos } A_1, \ldots, A_n \,\}.$$

(Π8.4 H 1 2)

▸ **PROBLEMA Π8.5.**
O que devemos mudar (e como) no Problema Π8.4 e sua resolução, se apagar o "$n \geq 2$"? (Π8.5 H 1)

D8.79. Definição. Seja $\mathscr{A}$ uma família de conjuntos. Chamamos a $\mathscr{A}$ de ($\subseteq$)-*chain* sse

$$\text{para todo } A, B \in \mathscr{A}, \text{ temos } A \subseteq B \text{ ou } B \subseteq A.$$

▸ **PROBLEMA Π8.6.**
Seja $\mathscr{C}$ uma ($\subseteq$)-chain e seja $T = \bigcup \mathscr{C}$. A afirmação

$$\mathscr{C} \cup \{T\} \text{ é uma chain}$$

é verdadeira? Se sim, demonstre; se não, refute; se os dados não são suficientes para concluir, mostre um exemplo e um contraexemplo. (Π8.6 H 1)

▸ **PROBLEMA Π8.7.**
Uma chain $\mathscr{C}$ que atende as hipotéses do Problema Π8.6 pode ter a propriedade que

$$\bigcup \mathscr{C} \in \mathscr{C}.$$

Mostre um exemplo duma chain infinita $\mathscr{C}$ cujos membros são todos conjuntos infinitos, e tal que $\bigcup \mathscr{C} \notin \mathscr{C}$. Dá pra garantir (com a mesma $\mathscr{C}$) que $\bigcap \mathscr{C} \notin \mathscr{C}$ também? Demonstre tuas afirmações! (Π8.7 H 1 2)

▸ **PROBLEMA Π8.8.**
No Exercício x8.28 encontramos um desenho errado. Tem como desenhar um correto? (Π8.8 H 1 2)

§186. Tuplas

Até agora temos trabalhado bastante com conjuntos, e sabemos que podemos perguntar um conjunto se qualquer objeto é um membro dele ou não, mas um conjunto não pode nos dar uma informação de ordem (Nota 8.21). Imagine que temos os dois primeiros ganhadores dum campeanato num conjunto W; não temos como saber quem ganhou o ouro e quem o prata. Precisamos um outro tipo nesse caso, cuja interface é perguntar *«quem é teu primeiro objeto?»* e *«quem é teu segundo objeto?»* também. Oi, tuplas!

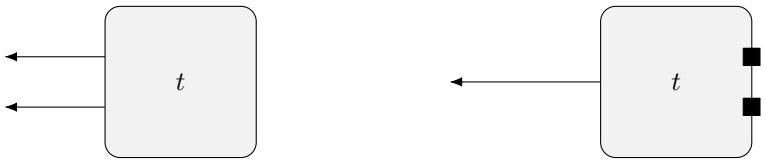
Nessa secção vamos estudar a idéia de *par ordenado*, ou *dupla*, ou 2-*tupla*, ou—por enquanto—apenas *tupla*. O que é? *Dois objetos (não necessariamente distintos) onde um deles é considerado primeiro e o outro segundo.* Só isso mesmo! Vamos denotar o par ordenado dos objetos a e b (nessa ordem) por $\langle a, b\rangle$ ou (a, b).

8.80. Interface, igualdade, notação. Precisamos: descrever qual é o "interface primitivo" desse novo tipo, *em tal forma que deixamos claro o que precisamos definir para determinar uma tupla.* Tendo isso vamos também definir o que significa (=) entre tuplas. Pensando em black boxes ajudou nos conjuntos; que tal tentar agora também?

? **Q8.81. Questão.** Como descreverias um black box de tupla?

!! SPOILER ALERT !!

8.82. Tupla como black box. Aqui duas maneiras equivalentes de visualizar uma tupla como black box:



O da direita, o black box duma tupla $\langle a, b\rangle$ tem dois butões, e uma saida, e cada vez que apertamos um botão cria um objeto: apertando o primeiro sai o objeto a, apertando o segundo sai o b. O da esquerda não tem nenhum botão nem entradas, mas só duas saidas: na primeira sempre sai o a, na segunda o b. Como nos black boxes de conjuntos, os black boxes de tuplas também são deterministas: apertando o mesmo botão sempre sai o mesmo objeto (na primeira versão), e olhando para o mesmo cabo-saida sempre sai o mesmo objeto. Por outro lado, existe uma grande diferença: um black box de conjunto *recebe* um objeto e *vira uma proposição;* um black box de tupla *não recebe nenhum objeto* (apenas escolhemos se queremos extrair o primeiro ou o segundo componente dele, e ele *retorna* mesmo esse *objeto*.

8.83. Interface. As operações primitivas de tuplas são as operações unárias π_0 e π_1, chamadas *projecções*. Nada mais! Para qualquer tupla t, $\pi_0 t$ é seu primeiro componente e $\pi_1 t$ o seu segundo.

8.84. Observação (Notações alternativas). Outros nomes para as projecções π_0 e π_1 são:

$$proj_0,\ proj_1,\ \ldots;\qquad (-)_0,\ (-)_1,\ \ldots;\qquad outl,\ outr;\qquad fst,\ snd.$$

Em vez de decorar os símbolos das projecções com índices começando no 0, às vezes é mais útil começar no 1. Mas não se preocupe tanto com isso pois pelo contexto vai sempre ser claro qual é a notação seguida.

? **Q8.85. Questão.** O que preciso fazer para ter o direito de dizer que eu determinei uma tupla?

Resposta. Preciso ter dois objetos, numa ordem. Querendo ou não, é isto que é uma tupla. Vamos ver isso em mais detalhe.

8.86. Como determinar. A partir da interface de tuplas (8.83), é claro que para determinar uma tupla t precisamos definir como ela comporta, ou seja, isto:

> Seja t a tupla definida pelas
>
> $$\pi_0\, t \stackrel{\text{def}}{=} x \qquad\qquad \pi_1\, t \stackrel{\text{def}}{=} y.$$

Observe que aqui os x e y supostamente já são objetos bem-definidos. Em vez de escrever tudo isso, usamos diretamente a notação-construtor de tuplas:

D8.87. Definição (Construtor de tupla). Sejam x, y objetos. Denotamos por $\langle x, y\rangle$ a tupla definida pelas

$$\pi_0\langle x, y\rangle = x \qquad\qquad \pi_1\langle x, y\rangle = y$$

Consideramos então o $\langle -, -\rangle$ como um *construtor de tuplas*.

! **8.88. Aviso.** Acabamos de *definir* o símbolo $\langle x, y\rangle$ para quaisquer x, y. Não é apenas que «não precisa», ainda mais: é que *não podes* re-definir isso. Se tu tens dois objetos x e y, não tenta justificar nem introduzir para teu leitor o que é o $\langle x, y\rangle$. Ele já sabe, a partir da Definição D8.87. Ele também sabe o que significa somar; tu não escreverias

> Seja $x + y$ inteiro tal que ele é a soma dos x e y.

Certo?

8.89. Equações fundamentais. Considere que temos x, y, dois objetos. Podemos então formar a tupla $\langle x, y\rangle$ deles, e depois usar as projecções π_0 e π_1 nessa tupla. O que cada uma delas vai retornar para nos?

$$\pi_0\,\langle x, y\rangle = x \qquad\qquad \pi_1\,\langle x, y\rangle = y$$

Conversamente agora, considere que temos uma tupla t. E nela usamos as projecções π_0 e π_1, e botamos esses valores (e nessa ordem) para construir uma tupla. Onde chegamos? Olhe isso; e olhe isso bem:

$$t = \langle \pi_0\, t, \pi_1\, t \rangle\,.$$

? **Q8.90. Questão.** Como definarias igualdade entre tuplas?

!! SPOILER ALERT !!

Resposta informal. Duas tuplas são iguais sse "concordam em cada posição".

Sem aspas, chegamos na seguinte

D8.91. Definição (Igualdade). Sejam s, t tuplas. Definimos

$$s = t \iff^{\mathsf{def}} \pi_0 s = \pi_0 t \;\&\; \pi_1 s = \pi_1 t.$$

Com a notação que usamos para tuplas, escrevemos o (talvez) mais amigável:

$$\langle x, y\rangle = \langle x', y'\rangle \iff^{\mathsf{def}} x = x' \;\&\; y = y'.$$

8.92. Precisamos tuplas maiores?. Introduzimos então esse novo *tipo primitivo* de 2-tuplas. E se precisar uma tripla? Precisamos escolher se vamos aceitar mais tipos como primitivos (3-tuplas (triplas), 4-tuplas, (quadruplas), 5-tuplas (quintuplas), etc., etc.) ou não.

Caso que sim, vamos precisar uma n-tupla para cada $n \in \mathbb{N}$. E precisamos definir a igualdade e o intreface para cada um desses tipos, algo que fazemos facilmente:

$$\langle x_1, \ldots, x_n\rangle = \langle x'_1, \ldots, x'_n\rangle \iff^{\mathsf{def}} x_1 = x'_1 \;\&\; \cdots \;\&\; x_n = x'_n$$

e naturalmente dizemos que uma n-tupla t é *determinada por os objetos em cada uma das suas n posições.* Então para definir uma n-tupla basta só definir as

$$\pi^n_0 t, \pi^n_1 t, \ldots, \pi^n_{n-1} t.$$

E caso contrário? Será que podemos utilizar apenas as 2-tuplas para conseguir o que nossos amigos que trabalham com n-tuplas como tipos primitivos conseguem? A resposta é sim; mas vamos primeiro definir uma operação importantíssima entre conjuntos, o produto!

§187. Produto cartesiano

D8.93. Definição. Sejam A, B conjuntos. Definimos o conjunto

$$A \times B \stackrel{\text{def}}{=} \{\, \langle a, b\rangle \;\mid\; a \in A,\; b \in B \,\}$$

que chamamos de *produto cartesiano* (ou simplesmente *produto*) dos A, B. Pronunciamos «A cross B».

▸ **EXERCÍCIO x8.48.**
Justifique a notação $A \times B$, ou seja, ache uma conexão entre o produto cartesiano e o produto de números. Suponha que os A, B são finitos. (x8.48 H 0)

▸ **EXERCÍCIO x8.49.**
Sejam A, B, C conjuntos. Demonstre que:

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$
$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

(x8.49 H 0)

▸ **EXERCÍCIO x8.50.**
Demonstre ou refute: para todos os conjuntos A, B,

$$A \times B = B \times A \implies A = B.$$

(x8.50 H 1)

▸ **EXERCÍCIO x8.51.**
Suponha que $A, B \neq \emptyset$. Escreva uma demonstração direta (sem usar reductio ad absurdum) do $A \times B = B \times A \iff A = B$. (x8.51 H 12)

▸ **EXERCÍCIO x8.52.**
Demonstre usando reductio ad absurdum a direção não-trivial do Exercício x8.51. (x8.52 H 0)

▸ **EXERCÍCIO x8.53.**
Calcule as extensões dos conjuntos:

$$\{\{\emptyset\}\} \times \wp\emptyset; \qquad \{\{\emptyset\}\} \triangle \bigcup \emptyset$$

(x8.53 H 0)

8.94. Observação. Sabemos que para "sejar" algum membro dum conjunto A (sabendo claramente que A não é vazio) escrevemos algo do tipo

> Seja $x \in A$.

onde precisamos tomar cuidado escolhendo um *nome fresco de variável* para denotar esse objeto. Como $A \times B$ também é um conjunto, e também supondo que não é vazio, obviamente faz sentido escrever

Seja $x \in A \times B$.

A partir disso, pela definição do $A \times B$, que tipo de objeto é esse x? Uma tupla cujo primeiro componente pertence a A, e o segundo ao B; pois todos os membros de $A \times B$ são tais tuplas. E o que podemos fazer com esse x então? Bem, é uma 2-tupla, e logo podemos projectar: $\pi_0 x$ e $\pi_1 x$ são objetos já definidos que podemos usar. O que mais podemos fazer? Lembrando a notação de set builder que permite termos (§180), percebemos que a Definição D8.93 do próprio $A \times B$ usou tal set builder:

$$A \times B \stackrel{\text{def}}{=} \{\, \langle a, b\rangle \;\mid\; a \in A,\ b \in B \,\}.$$

A partir da definição dessa notação (Exercício x8.22) temos

$$x \in A \times B \iff (\exists a \in A)(\exists b \in B)[\, x = \langle a, b\rangle \,].$$

Para voltar na nossa pergunta de «o que podemos fazer com esse x» então:

Seja $x \in A \times B$.
Logo sejam $a \in A$ e $b \in B$ tais que $x = \langle a, b\rangle$.

Tudo bem até agora. Mas essa declaração do x parece inútil. Pra que poluir nosso escopo com esse objeto se a único coisa que planejamos fazer com ele é extrair seus componentes para usá-los? Não seria melhor escrever

Seja $\langle a, b\rangle \in A \times B$.

assim ganhando diretamente os a, b sem o bobo x? Seria, mas... já aprendemos que declaramos apenas variáveis (Aviso 2.36), né?

Mas já que $\langle -, -\rangle$ é um *construtor* de tuplas podemos considerar a linha

Seja $\langle a, b\rangle \in A \times B$.

Como abreviação das linhas

Seja $a \in A$. Seja $b \in B$.

E sobre o $\langle a, b\rangle$? Como que vamos introduzí-lo para usá-lo? Nem precisamos nem podemos! Como já temos agora os objetos a, b, querendo ou não a tupla $\langle a, b\rangle$ já é definida e podemos usá la. Isso vai ficar ainda mais claro daqui a pouco (no Observação 8.148) onde discutimos o que significa *tomar um arbitrário membro dum conjunto indexado*.

§188. Implementação de tipo: triplas

Nessa secção temos nosso primeiro contato com a idéia fundamental—literalmente—de *implementação*. Nosso objetivo aqui é só isso: brincar um pouco para entender o conceito. Bem depois, no Capítulo 16 vamos mergulhar mais profundamente.

8.95. Um amigo com triplas. Tudo ótimo até agora neste capítulo (né?): Introduzimos dois *tipos primitivos:* conjuntos e tuplas junto com operações neles, e tudo mais. chega nosso amigo da outra turma que mostra para nos um tipo primitivo deles, a tripla:

«Cara, triplas têm 3 projecções em vez de 2, que denotamos por

$$\pi^3_0, \quad \pi^3_1, \quad \pi^3_2.$$

A própria tupla t com

$$\pi^3_0\, t = x, \quad \pi^3_1\, t = y, \quad \pi^3_2\, t = z$$

denotamos por $\langle x, y, z\rangle$, e definimos igualdade pela

$$\langle x, y, z\rangle = \langle x', y', z'\rangle \iff^{\mathsf{def}} x = x' \;\&\; y = y' \;\&\; z = z'$$

e as equações fundamentais são as óbvias. Lembra da conversa no começo da Secção §186? Com triplas consigo saber quem ganhou o bronze também!»

8.96. Interface. O interface duma tripla, consiste em 3 projecções: π^3_0, π^3_1, π^3_2.

▸ **EXERCÍCIO x8.54.**
Quais são essas «óbvias» equações fundamentais do amigo do Nota 8.95? (x8.54 H 1)

8.97. Implementação de tipo primitivo. Nosso amigo nos apresentou esse tipo primitivo dele: descreveu seu interface, introduziu sua notação, definiu igualdade, e pronto. Podemos copiar essa idéia e fazer a mesma coisa. Em vez disso, vamos tentar algo diferente: *implementar* o tipo de triplas! O que significa mesmo "implementar"? Vamos tratar tudo que ele falou como uma *especificação* dum tipo desejado, que nos vamos *definir* em termos de outros tipos já conhecidos. Cuidado: nossa implementação deve *atender a especificação*.

Então *implementamos*—ou seja, definimos mesmo—as triplas assim:

D8.98. Implementação (Tripla). Sejam x, y, z objetos. Definimos a tripla

$$\langle x, y, z\rangle \stackrel{\mathsf{def}}{=} \langle x, \langle y, z\rangle\rangle\,.$$

Ou seja, a tripla dos objetos x, y, z nessa ordem é a tupla cujo primeiro componente é o x e cujo segundo componente é a tupla $\langle y, z\rangle$. Definimos igualdade entre triplas pela

$$\langle x, y, z\rangle = \langle x', y', z'\rangle \iff^{\mathsf{def}} x = x' \;\&\; y = y' \;\&\; z = z'.$$

↯

? **Q8.99. Questão.** Acabamos de roubar. Como?

!! SPOILER ALERT !!

! 8.100. Cuidado (Não redefinirás). A partir do momento que *definimos* triplas (pra ser certas 2-tuplas) não temos o direito de *redefinir* igualdade entre triplas, pois, simplesmente, agora triplas *são* 2-tuplas, e a igualdade entre 2-tuplas já foi definida, e logo a igualdade

$$\langle x, y, z\rangle = \langle x', y', z'\rangle$$

já tem significado: os objetos nos seus dois lados são 2-tuplas, e logo a igualdade acima *realmente é* a seguinte:

$$\langle x, y, z\rangle = \langle x', y', z'\rangle \iff \langle x, \langle y, z\rangle\rangle = \langle x', \langle y', z'\rangle\rangle\,.$$

8.101. Deveres do implementador. O que *devemos* fazer para implementar mesmo um tipo dada uma especificação? Devemos demonstrar que nossa implementação atende a especificação. E note que nossa implementação não é completa ainda, pois precisamos *definir* o interface também. Para nosso amigo as operações $\pi^3_0, \pi^3_1, \pi^3_2$ são *primitivas*. Ele não as definiu, pelo contrario: determinado seus comportamentos, ele determina uma tripla. Mas aqui queremos implementar as triplas, então devemos definir essas projecções! Bora terminar esses deveres agora.

▸ **EXERCÍCIO x8.55.**
Complete a implementação de triplas: defina as três projecções. (x8.55 H 1 2)

▸ **EXERCÍCIO x8.56.**
Mostre que com a definição de

$$\langle x, y, z\rangle \stackrel{\text{def}}{=} \langle x, \langle y, z\rangle\rangle$$

conseguimos a igualdade *desejada*

$$\langle x, y, z\rangle = \langle x', y', z'\rangle \iff x = x' \;\&\; y = y' \;\&\; z = z'.$$

Mais uma vez, cuidado: é um '$\iff$' acima, não um '$\stackrel{\text{def}}{\iff}$'! Ou seja, definindo as 3-tuplas nessa maneira, querendo ou não, a igualdade entre seus objetos já é definida! Não temos o direito de redefini-la! (x8.56 H 0)

8.102. Produto ternário. Uma das mais interessantes coisas que fizemos assim começamos trabalhar com as duplas foi definir o produto cartesiano duma dupla de conjuntos! Agora que definimos as triplas, naturalmente queremos considerar o produto cartesiano duma tripla de conjuntos. Parece então que temos uma operação ternaria, que para quaisquer conjuntos A, B, C

$$A \times B \times C \stackrel{\text{def}}{=} \{\, \langle a, b, c\rangle \;\mid\; a \in A,\; b \in B,\; c \in C \,\}\,.$$

! 8.103. Cuidado (Implementação agnóstico). *Definimos* o que significa $\langle x, y, z\rangle$, e *definimos* as projecções $\pi^3_0, \pi^3_1, \pi^3_2$. Dada uma tripla $\langle x, y, z\rangle$, podemos chamar a π_1 nela? Intuitivamente, alguém pensaria que não, pois parece ter um "type error" essa aplicação: a projecção π_1 funciona com 2-tuplas, e $\langle x, y, z\rangle$ é uma tripla, então só podemos chamar as

$\pi^3_0, \pi^3_1, \pi^3_2$ nela. Certo? Errado! Podemos sim, pois, pela nossa definição, a tripla $\langle x, y, z\rangle$ *é* a dupla $\langle x, \langle y, z\rangle\rangle$. Ou seja, temos:

$$\begin{aligned} \pi_1 \langle x, y, z\rangle &\equiv \pi_1 \langle x, \langle y, z\rangle\rangle && (\text{def. } \langle x, y, z\rangle) \\ &= \langle y, z\rangle && (\text{def. } \langle x, \langle y, z\rangle\rangle) \end{aligned}$$

O fato que *podemos* não significa que *devemos*. O que estamos fazendo nesse caso é *usar os detalhes da implementação em vez do seu interface*. Tudo que vamos construir a partir desse abuso vale apenas para *nossa* implementação. Nosso amigo que usa triplas como tipo primitivo não pode aproveitar dos nossos cálculos e das nossas teorias. Nem alguém que escolheu implementar triplas em outra maneira. A moral da estória é o seguinte: precisamos ficar *implementação agnósticos*, ou seja, esquecer os detalhes da nossa implementação, usando apenas o interface dos nossos objetos.

Não faz sentido nenhum se limitar em 2-tuplas e 3-tuplas. Partiu n-tuplas para qualquer $n \in \mathbb{N}$!

§189. n-tuplas

8.104. Interface e notação. Nossa única interface dada uma tupla de tamanho n, é que podemos pedir seu i-ésimo elemento, onde $0 \leq i < n$. Conversamente, para definir uma tupla de tamanho n, basta determinar todos os objetos (distintos ou não) nas suas n posições. Usamos as notações $\langle a_0, a_1, \ldots, a_{n-1}\rangle$ e $(a_0, a_1, \ldots, a_{n-1})$ para tuplas de tamanho n. Às vezes é mais legível usar índices começando com 1—tanto faz. Quando queremos enfatizar o tamanho da tupla, falamos de *n-tupla*. Em geral, para tuplas de tamanho n, usamos a notação π^n_i para a i-ésima projecção. Por exemplo:

$$\pi^2_1 \langle x, y\rangle = y; \qquad \pi^3_1 \langle x_1, x_2, x_3\rangle = x_2; \qquad \pi^5_4 \langle x_2, x_3, y_1, x_8, y_0\rangle = y_0; \qquad \text{etc.}$$

Quando o n é implícito pelo contexto, não se preocupamos com ele. Obviamente então π_1 da '$\pi_1 \langle x, y, z\rangle$' denota a π^3_1 mesmo, mas a π_1 da '$\pi_1 \langle x, y\rangle$' denota a π^2_1. Até agora temos chamado de "tupla" o par ordenado. Na verdade, um par ordenado é uma 2-tupla.

Às vezes escolhemos como nome duma tupla uma variável decorada com uma setinha em cima dela, e usando a mesma letra com índices para seus membros, por exemplo $\vec{x} = \langle x_0, x_1, \ldots, x_n\rangle$, $\vec{w} = \langle w_1, w_2\rangle$, etc. Outra convençao comum é usar uma fonte em "negrito", por exemplo $\mathbf{a} = \langle a_1, a_2, a_3\rangle$, $\mathbf{u} = \langle u_0, u_1\rangle$, etc.

D8.105. "Definição". Sejam A conjunto e $n \in \mathbb{N}$ com $n \geq 2$.

$$A^n \overset{\text{"def"}}{=} \{\, \langle a_1, \ldots, a_n\rangle \;\mid\; a_i \in A \text{ para todo } 1 \leq i \leq n \,\}.$$

8.106. Na definição acima aparece a frase «para todo $1 \leq i \leq n$». Qual é a variável ligada com esse «para todo»? Bem, 1 é um constante, e n já foi declarado, então entendemos que a frase corresponde na quantificação:

$$(\forall i \in \mathbb{N})[1 \leq i \leq n \implies a_i \in A].$$

D8.107. Definição. Seja A conjunto. Para $n \in \mathbb{N}$ com $n \geq 1$ definimos as *potências* de A recursivamente pelas:

$$A^1 = A$$
$$A^n = A^{n-1} \times A \qquad (\text{para } n \geq 2).$$

8.108. Comparação com números (I). A semelhança entre a definição de potências de conjuntos e de números é gritante. Vamos investigar. Na Definição D8.107 das duas equações recursivas

$$A^n = A^{n-1} \times A \qquad\qquad A^n = A \times A^{n-1}.$$

escolhemos a primeira. Por quê? Observe que no caso de números, para a equação recursiva, as duas opções óbvias

$$a^n = a^{n-1} \cdot a \qquad\qquad a^n = a \cdot a^{n-1}$$

servem e são equivalentes. Uma explicação disso usa apenas o fato que a multiplicação de números é comutativa, então imediatamente temos $a^{n-1} \cdot a = a \cdot a^{n-1}$. Infelizmente não podemos contar nessa propriedade no caso de conjuntos, pois já sabemos que a $\times$ não é comutativa (Exercício x8.51). Mas as duas equações correspondem nas expressões

$$a^n = ((((\cdots(a \cdot a) \cdot a) \cdot a) \cdots) \cdot a) \qquad\qquad a^n = (a \cdot (\cdots (a \cdot (a \cdot (a \cdot a) \cdots))))$$

que são iguais agora por causa da *associatividade* da operação $(\cdot)$.

? **Q8.109. Questão.** O produto cartesiano é associativo?

!! SPOILER ALERT !!

Resposta. Respondemos nessa pergunta com outra: *as tuplas*

$$\langle a_0, \langle a_1, a_2 \rangle \rangle \qquad \langle \langle a_0, a_1 \rangle, a_2 \rangle \qquad \langle a_0, a_1, a_2 \rangle$$

são iguais? Não, pois já temos uma maneira de observar comportamento diferente usando o interface dessas 2-tuplas. Mas também depende: podemos considerá-las *como se fossem iguais*, pois qualquer uma delas serve para satisfazer a especificação de tuplas: podemos definir as i-ésimas projecções para cada uma, e a especificação vai acabar sendo atendida usando uma delas sse é atendida usando qualquer uma das outras. Pense na idéia sobre a *informação* que uma tupla carrega com ela. Agora tente ler as três tuplas acima:

«Primeiro o objeto a_0, e depois temos: primeiro o a_1 e depois o a_2.»
«Primeiro temos: primeiro o objeto a_0 e depois o a_1; e depois temos o a_2.»
«Primeiro temos o objeto a_0 e depois o a_1 e depois o a_2.»

Mas esse ponto de visto é confundindo implementação com interface. Como enfatisei no Cuidado 8.103, quando queremos referir a uma tripla de objetos, usamos a notação $\langle a_0, a_1, a_2\rangle$, e não alguma que corresponde na nossa implementação peculiar. Assim, se escrever $\langle a_0, \langle a_1, a_2\rangle\rangle$ deve ser porque tu tá considerando a 2-tupla mesmo, cujo primeiro componente é o a_0 e cujo segundo o $\langle a_1, a_2\rangle$. Para resumir: depende do contexto, e do objetivo de cada conversa.

8.110. Comparação com números (II). Uma diferença entre as definições de potências de números e de conjuntos é que no caso de conjuntos definimos o A^n para todo $n \geq 1$, mas no caso de números naturais conseguimos uma definição mais geral, definindo o a^n para todo $n \geq 0$. Nossa base da recursão então foi $a^0 = 1$. Por que 1?

8.111. Unit. Se é para generalizar bem a definição de potências de números para o caso de conjuntos, procuramos nosso 1, ou seja, uma *unidade* (também *identidade*, ou *elemento neutro*) da nossa "multiplicação", $\times$. Essa unidade é chamada *unit*, e muito usada em linguagens de programação. Vamos usar o $\langle\rangle$ para denotá-la. Isso é um abuso notacional, pois $\langle\rangle$ também denota a tupla vazia, que é o único membro da unit; mas o contexto é em geral suficiente para tirar a ambigüidade. Caso contrário, use $\{\langle\rangle\}$, ou introduza alguma outra notação, por exemplo I.

D8.112. Definição (igualdade). Seja $n \in \mathbb{N}$ e sejam s, t n-tuplas. Definimos

$$s = t \iff^{\text{def}} (\forall 1 \leq i \leq n)[\,\pi_i^n s = \pi_i^n t\,],$$

ou, usando a notação $\langle -, \ldots, -\rangle$, temos:

$$\langle s_1, \ldots, s_n\rangle = \langle t_1, \ldots, t_n\rangle \iff^{\text{def}} \text{para todo } i \in \{1, \ldots, n\},\ s_i = t_i.$$

? **Q8.113. Questão.** Como tu definarias os tipos de n-tuplas para $n > 2$, dado um tipo de 2-tuplas?

!! SPOILER ALERT !!

D8.114. "Definição". Seja $n \in \mathbb{N}$ com $n > 2$. Dados n objetos $x_1, x_2, \ldots, x_n$ definimos a n-tupla

$$\langle x_1, x_2, \ldots, x_n\rangle \stackrel{\text{def}}{=} \langle x_1, \langle x_2, \ldots, x_n\rangle\rangle\,.$$

8.115. Tuplas de tamanhos extremos. O que seria uma 1-tupla? E, pior ainda, o que seria uma 0-tupla? E uma tupla infinita? Vamos responder apenas na primeira pergunta agora. Os outros dois casos vamos discutir logo depois: sobre a(s?) 0-tupla(s?) aqui mesmo; e sobre tuplas infinitas nas §190 e §192 onde conhecemos *seqüências* e *famílias indexadas* respectivamente.

D8.116. Definição (Tuplas de tamanho 1). Observe que escolhendo definir a 1-tupla como

$$\langle x \rangle \stackrel{\text{def}}{=} x$$

atendemos nossas exigências:

$$\langle x \rangle = \langle y \rangle \iff x = y$$

que é exatamente a igualdade desejada. Ou seja, para nossos objectivos podemos *identificar os objetos* $\langle x \rangle$ e x. A partir disso, faz sentido considerar que o produto cartesiano dum conjunto só é o próprio conjunto, e logo ter $A^1 = A$

? **Q8.117. Questão.** E sobre 0-tuplas? Faz sentido considerar esse tipo? Teria "habitantes", ou seja, objetos desse tipo? Se sim, quantos, e quais são? Se não, por que não?

!! SPOILER ALERT !!

8.118. A 0-tupla. Seguindo nossa intuição com as tuplas dos outros tamanhos, o que seria uma 0-tupla? Bem, para determinar um objeto $\vec{t}$ desse tipo, precisamos definir suas... 0 projecções. Vamos fazer isso aqui:

Pronto. Acabei de definir as... 0 coisas que precisava definir. Logo existe uma única 0-tupla, que denotamos por $\langle\rangle$ mesmo. E qual seria o produto cartesiano 0-ário, duma—na verdade, da única—0-tupla de conjuntos?

8.119. O produto cartesiano 0-ário. Dados... 0 conjuntos, seu produto cartesiano deve ser o conjunto de todas as 0-tuplas cujo i-ésimo componente pertence ao i-ésimo dos 0 conjuntos. Mas só tem uma 0-tupla e ela satisfaz essa condição, então o produto cartesiano de 0 conjuntos, é o singleton $\{\langle\rangle\}$. Logo devemos definir

$$A^0 \stackrel{\text{def}}{=} \{\langle\rangle\}$$

e consideramos o $\{\langle\rangle\}$ como identidade (elemento neutro) da $\times$, identidicando, por exemplo, as tuplas

$$\langle\langle\rangle, \langle x, y\rangle\rangle \qquad \text{e} \qquad \langle x, y\rangle$$

nesse contexto.

E agora, prontos para tamanho infinito: seqüências.

§190. Seqüências

A generalização de tuplas para seqüências é bem simples. Uma n-tupla $\langle a_0, \ldots, a_{n-1} \rangle$ tem um componente para cada uma das n posições $i = 0, \ldots, n-1$, e nada mais.

P8.120. Noção primitiva (seqüência). Uma *seqüência* tem um componente para cada natural $i \in \mathbb{N}$. Usamos a notação $(a_n)_n$ para denotar a seqüência cujos primeiros termos são

$$a_0, a_1, a_2, a_3, \ldots$$

O interface de seqüências então é uma infinidade de perguntas-projecções, uma para cada natural, que costumamos denotar apenas por índices subscritos mesmo, como fizemos em cima.

8.121. Observação (Ligador de variável). Na notação $(a_n)_n$ o n é um *ligador* da variável n.

8.122. Observação. O que chamamos de seqüência é também conhecido como *seqüência infinita*. Uma *seqüência finita* é apenas uma n-tupla, para algum $n \in \mathbb{N}$.

! **8.123. Aviso (abuso notacional).** Quando escrevemos uma seqüência $(a_n)_n$ onde pelo contexto esperamos ver um conjunto, a entendemos como uma denotação do conjunto $\{\, a_n \mid n \in \mathbb{N} \,\}$. Por exemplo, escrevemos

$$(a_n)_n \subseteq A \overset{\text{abu}}{\iff} \{\, a_n \mid n \in \mathbb{N} \,\} \subseteq A, \qquad \frac{1}{2} \in (a_n)_n \overset{\text{abu}}{\iff} \frac{1}{2} \in \{\, a_n \mid n \in \mathbb{N} \,\},$$

etc.

! **8.124. Cuidado.** Em certos textos aparece a notação a_n ou $\{a_n\}$ para denotar uma inteira seqüência. Aqui não vamos usar nenhuma dessas, pois introduzem ambigüidades possivelmente perigosas:

- Se encontrar a expressão 'a_n', é a seqüência inteira ou apenas o n-ésimo membro dela?
- Se encontrar a expressão '$\{a_n\}$', ele denota a seqüência inteira, o singleton cujo único membro é a seqüência inteira, ou o singleton cujo único membro é o n-ésimo membro da seqüência?

? **Q8.125. Questão.** Como definarias igualdade para seqüências?

!! SPOILER ALERT !!

D8.126. Definição (Igualdade). Sejam $(a_n)_n$, $(b_n)_n$ seqüências. Definimos sua igualdade por

$$(a_n)_n = (b_n)_n \iff^{\text{def}} (\forall n \in \mathbb{N})[\, a_n = b_n \,].$$

8.127. Seqüências e limites. No coração de calculus é o estudo de seqüências de números reais. No Capítulo 6 definimos a noção de *limite* de uma seqüência de reais $(a_n)_n$, e no Capítulo 17 estendemos essa idéia num contexto mais geral e abstrato, onde os membros da seqüência não são necessariamente números reais, mas membros de um *espaço métrico*. Nada mais por enquanto—paciência!

8.128. Seqüências de conjuntos. Mais interessantes para a gente neste momento são *seqüências de conjuntos*.

? **Q8.129. Questão.** Imagina que temos definido, para cada $n \in \mathbb{N}$, um conjunto A_n. Como tu definirias os conjuntos $\bigcup_{n=0}^{\infty} A_n$ e $\bigcap_{n=0}^{\infty} A_n$?

!! SPOILER ALERT !!

D8.130. Definição. Seja $(A_n)_n$ uma seqüência de conjuntos. Definimos os operadores unários $\bigcup_{n=0}^{\infty}$ e $\bigcap_{n=0}^{\infty}$ pelas:

$$x \in \bigcup_{n=0}^{\infty} A_n \iff^{\text{def}} (\exists n \in \mathbb{N})[\, x \in A_n \,]$$
$$x \in \bigcap_{n=0}^{\infty} A_n \iff^{\text{def}} (\forall n \in \mathbb{N})[\, x \in A_n \,].$$

Às vezes usamos as notações mais curtas: $\bigcup_n A_n$ e $\bigcap_n A_n$ respectivamente, mas cuidado: $\bigcup A_n$ é a união (grande) do conjunto A_n, que é o n-ésimo membro da seqüência de conjuntos $(A_n)_n$. Por outro lado, $\bigcup_n A_n$ é a união da seqüência, ou seja o $\bigcup_{n=0}^{\infty} A_n$. Mesmo cuidado sobre intersecções.

▸ **EXERCÍCIO x8.57.**
Sejam $(A_n)_n$ e $(B_n)_n$ duas seqüências de conjuntos tais que

$$\text{para todo } n \in \mathbb{N},\ A_n \subseteq B_{n+1}.$$

Demonstre que:

$$\bigcup_{n=0}^{\infty} A_n \subseteq \bigcup_{n=0}^{\infty} B_n.$$

(x8.57 H 0)

▸ **EXERCÍCIO x8.58.**
Sejam $(A_n)_n$ e $(B_n)_n$ duas seqüências de conjuntos tais que

$$\text{para todo número par } m,\ A_m \subseteq B_{m/2}.$$

Demonstre que:

$$\bigcap_{n=0}^{\infty} A_n \subseteq \bigcap_{n=0}^{\infty} B_n.$$

(x8.58 H 0)

▸ **EXERCÍCIO x8.59.**
Sejam $(A_n)_n$ e $(B_n)_n$ duas seqüências de conjuntos tais que

$$\text{para todo número primo } p,\ A_p \subseteq B_{2p}.$$

Demonstre ou refute:

$$\bigcap_{n=0}^{\infty} A_n \subseteq \bigcup_{n=28}^{\infty} B_n.$$

(x8.59 H 0)

▸ **EXERCÍCIO x8.60.**
Na Definição D8.130 definimos *elementariamente* as operações $\bigcup_{n=0}^{\infty}$ e $\bigcap_{n=0}^{\infty}$. Defina-las usando as operações de $\bigcup$ e $\bigcap$. (x8.60 H 0)

8.131. Proposição. *Para todo conjunto C e cada seqüência de conjuntos $(A_n)_n$,*

$$C \setminus \bigcup_{n=0}^{\infty} A_n = \bigcap_{n=0}^{\infty} (C \setminus A_n)$$
$$C \setminus \bigcap_{n=0}^{\infty} A_n = \bigcup_{n=0}^{\infty} (C \setminus A_n).$$

Demonstração. Sejam C conjunto e $(A_n)_n$ seqüência de conjuntos.

Mostramos as duas inclusões da primeira igualdade separadamente:

($\subseteq$): Seja $x \in C \setminus \bigcup_n A_n$, ou seja, $x \in C$ (1) e $x \notin \bigcup_n A_n$ (2). Vamos demonstrar que $x \in \bigcap_n (C \setminus A_n)$, ou seja, que para todo $u \in \mathbb{N}$, $x \in C \setminus A_u$. Seja $u \in \mathbb{N}$. Basta demonstrar então duas coisas: $x \in C$ e $x \notin A_u$. A primeira já temos (é a (1)). A segunda é direta conseqüência da (2): x não pertence a nenhum dos A's, então nem ao A_u.

($\supseteq$): Deixo pra ti (Exercício x8.61).

Temos mais uma igualdade para demonstrar, novamente em duas partes:

($\subseteq$): Seja $x \in C \setminus \bigcap_n A_n$, ou seja $x \in C$ (1) e $x \notin \bigcap_n A_n$ (2). Vamos demonstrar que $x \in \bigcup_n (C \setminus A_n)$, ou seja procuramos w tal que $x \in C \setminus A_w$, ou seja, tal que $x \in C$ e $x \notin A_w$. Observe que nosso primeiro alvo não tem nada a ver com w, e na verdade já temos: é o (1). Agora usando a (2) achamos o desejado natural: seja $w \in \mathbb{N}$ tal que $x \notin A_w$.

($\supseteq$): Deixo pra ti também (Exercício x8.62). ∎

Bora terminar a demonstração da Proposição 8.131:

▸ **EXERCÍCIO x8.61.**
Demonstre a primeira ($\supseteq$) que deixamos na demonstração da Proposição 8.131. (x8.61 H 0)

▸ **EXERCÍCIO x8.62.**
E a segunda. (x8.62 H 0)

Tu provavelmente adivinhaste: a Proposição 8.131 é uma generalização da 8.63, algo que—que surpresa!—tu demonstrarás no exercício seguinte:

▸ **EXERCÍCIO x8.63.**
O que precisamos fazer para ganhar a Proposição 8.63 como um corolário da Proposição 8.131? (x8.63 H 1)

▸ **EXERCÍCIO x8.64.**
Tente escrever uma demonstração da Proposição 8.131 usando fórmulas como foi visto—e criticado—no Aviso 8.64. (x8.64 H 0)

▸ **EXERCÍCIO x8.65.**
Demonstre ou refute: para todo conjunto A e toda seqüência de conjuntos $(B_n)_n$

$$A \cup \bigcap_{n=0}^{\infty} B_n = \bigcap_{n=0}^{\infty} (A \cup B_n)$$

(x8.65 H 0)

▸ **EXERCÍCIO x8.66.**
Para $n \in \mathbb{N}$, defina os conjuntos de naturais

$$A_n = \{\, i \in \mathbb{N} \mid i \leq n \,\} \qquad\qquad B_n = \mathbb{N} \setminus A_n.$$

Calcule os conjuntos $\bigcup_n A_n$ e $\bigcap_n B_n$. (x8.66 H 1)

▸ **EXERCÍCIO x8.67.**
Seja $(A_n)_n$ uma seqüência (infinita) de conjuntos. A afirmação

$$\bigcap_{n=0}^{\infty} \bigcap_{m=n}^{\infty} A_m = \bigcap_{n=0}^{\infty} A_n$$

é verdadeira? Se sim, demonstre; se não, refute; se os dados não são suficientes para concluir, mostre um exemplo e um contraexemplo. (x8.67 H 1)

! **8.132. Aviso.** Uma diferença importantíssima entre os operadores $\sum$ e $\bigcup$ e seus índices: um "somatório infinito" não é nem associativo nem comutativo! O seguinte teorema de Riemann é bastante impressionante!

Θ8.133. Teorema (Riemann's rearrangement). *Se uma série infinita $\sum a_i$ de reais é condicionalmente convergente,*[57] *então podemos apenas permutando seus termos criar uma nova série infinita que converga em qualquer $x \in [-\infty, \infty]$ que desejamos.*

▸ Esboço. Separe as metas: (i) mostrar como criar uma série que converge num dado número ℓ; (ii) mostrar como criar uma série divergente.

Observe que como $\sum a_i$ é condicionalmente convergente, ela contem uma infinidade de termos positivos, e uma infinidade de termos negativos. Para o (i), fixe um $\ell \in \mathbb{R}$. Fique tomando termos positivos da série a_i até seu somatório supera o ℓ. Agora fique tomando termos negativos da a_i até seu somatório cai embaixo do ℓ. Agora fique tomando termos positivos até superar o ℓ, etc. etc. Continuando assim conseguimos construir uma série feita por termos da $\sum a_i$ que converge no ℓ. Para o (ii), a idéia é similar. □ (Θ8.133P)

8.134. Limites de seqüências de conjuntos. Seja $(A_n)_n$ uma seqüência de conjuntos. Podemos definir a noção $\lim_n A_n$ de *limite* dessa seqüência. Claramente, não todas as seqüências de conjuntos convergem em algum limite. Investigamos isso nos problemas (Problema Π8.12 e Definição D8.168).

§191. Multisets

8.135. Descripção. Coloquialmente falando, um *multiset* (também *bag* ou *sacola*) M é como um conjunto, só que ele não pode responder apenas em perguntas do tipo «o objeto x pertence ao M?», mas também em «*quantas vezes pertence* o x ao M?». Seus membros continuam sem ordem, mas agora tem *multiplicidade*. Usamos a notação $\wr x_0, x_1, \ldots, x_n \wr$ para denotar multisets, ou até $\{x_0, x_1, \ldots, x_n\}$ sobrecarregando a notação $\{\ldots\}$ se é claro pelo contexto que é um multiset e não um conjunto.

8.136. Igualdade. Consideramos os multisets M e M' iguais sse para todo x,

$$x \text{ pertence } n \text{ vezes ao } M \iff x \text{ pertence } n \text{ vezes ao } M'.$$

Multisets têm muitos usos na ciência da computação: acabam sendo a ferramenta ideal para (d)escrever muitos algoritmos, e muitas linguagens de programação já têm esse tipo implementado. Mas seu uso em matemática é menos comum. De qualquer forma, fez sentido introduzí-los agora junto com seus tipos-amigos, pelo menos para saber sobre sua existência na literatura. Voltamos depois para implementá-los (Exercício x9.38, Problema Π16.8); não se preocupe neste momento com eles.

Intervalo de problemas

[57] Uma série $\sum a_i$ é *condicionalmente convergente* sse ela é convergente, mas a $\sum |a_i|$ não é.

▸ **PROBLEMA Π8.9.**
Sejam $(A_n)_n$ e $(B_n)_n$ duas seqüências de conjuntos, tais que para todo $n \in \mathbb{N}$, $A_n \subsetneq B_n$. Podemos concluir alguma das afirmações seguintes?:

$$\bigcup_{n=0}^{\infty} A_n \subsetneq \bigcup_{n=0}^{\infty} B_n \qquad\qquad \bigcap_{n=0}^{\infty} A_n \subsetneq \bigcap_{n=0}^{\infty} B_n$$

(Π8.9 H 1)

▸ **PROBLEMA Π8.10.**
Seja $(A_n)_n$ seqüência (infinita) de conjuntos. Defina recursivamente uma seqüência de conjuntos $(D_n)_n$ tal que (informalmente):

$$\text{para todo } k \in \mathbb{N},\ D_k = A_0 \cup A_1 \cup \cdots \cup A_{k-1}.$$

Em outras palavras, precisas definir formalmente a operação união unária *limitada* $(\bigcup_{i=0}^{k-1} -)$ para qualquer $k \in \mathbb{N}$. Demonstre que para todo $n \in \mathbb{N}$,

$$\underbrace{\bigcup_{i=0}^{n-1} A_i}_{D_n} \subseteq \bigcup_{m=0}^{\infty} A_m.$$

O que muda se trocar de uniões para intersecções? (Π8.10 H 0)

▸ **PROBLEMA Π8.11 (Sanduichando uma seqüência de conjuntos).**
Seja $(A_n)_n$ uma seqüência de conjuntos. Demonstre que para todo $k \in \mathbb{N}$,

$$\bigcap_{i=k}^{\infty} A_i \subseteq A_k \subseteq \bigcup_{i=k}^{\infty} A_i.$$

Ou seja, temos:

$$\begin{array}{rrcccl}
C_0 := A_0 \cap A_1 \cap A_2 \cap A_3 \cap \cdots & \subseteq & A_0 & \subseteq & A_0 \cup A_1 \cup A_2 \cup A_3 \cup \cdots & =: D_0 \\
C_1 := A_1 \cap A_2 \cap A_3 \cap \cdots & \subseteq & A_1 & \subseteq & A_1 \cup A_2 \cup A_3 \cup \cdots & =: D_1 \\
C_2 := A_2 \cap A_3 \cap \cdots & \subseteq & A_2 & \subseteq & A_2 \cup A_3 \cup \cdots & =: D_2 \\
\vdots \quad \ddots \quad \vdots & \vdots & \vdots & \vdots & \ddots \quad \vdots & \vdots
\end{array}$$

(Π8.11 H 0)

§192. Famílias indexadas

Na §190 vimos como nos livrar da restricção de usar um conjunto $\{0, \ldots, n-1\}$ como "rótulos" para indexar os membros duma tupla e, usando o conjunto infinito $\mathbb{N}$, chegamos na idéia de *seqüências*. Agora vamos generalizar os conceitos tanto de tuplas, quanto de seqüências: oi, famílias indexadas!

8.137. Motivação. A idéia que nos motiva é: *por que nos limitar "acessando" os membros de uma tupla apenas usando inteiros como índices (rótulos), enquanto podemos "liberar" qualquer objeto para servir como rótulo?* E é assim que fazemos mesmo.

- **EXEMPLO 8.138.**
Seja $\mathcal{C}$ o conjunto de todos os países do mundo e, para cada $c \in \mathcal{C}$, seja V_c o conjunto de todos os vilarejos do c. Em símbolos,

$$V_c = \{\, v \mid v \text{ é um vilarejo no país } c \,\}.$$

O que acabamos de definir aqui? Para *cada* país $c \in \mathcal{C}$ um novo objeto foi definido: o conjunto de todos os vilarejos de c. Ou seja, acabamos de definir vários objetos, *exatamente um para cada membro do* $\mathcal{C}$. Assim que determinar isso, dizemos que temos uma *família indexada por* $\mathcal{C}$.

D8.139. Definição (família indexada). Chegamos assim na idéia de *família indexada* por algum conjunto $\mathcal{I}$, cuja totalidade denotamos por $(a_i)_{i\in\mathcal{I}}$ ou $(\, a_i \mid i \in \mathcal{I}\,)$, onde a_i é um determinado objeto para cada $i \in \mathcal{I}$. Chamamos o $\mathcal{I}$ o *conjunto de índices* da família, e quando ele é implícito pelo contexto denotamos a família apenas com $(a_i)_i$. Alternativamente usamos como sinônimo o termo $\mathcal{I}$*-tupla*, enfatizando assim que o conceito de família indexada é apenas uma generalização da n-tupla.

Mais uns exemplos de famílias indexadas:

- **EXEMPLO 8.140.**
Seja $\mathcal{P}$ o conjunto de todas as pessoas do mundo. Definimos para cada pessoa $p \in \mathcal{P}$, os conjuntos A_p e C_p de todos os ancestrais e todos os filhos de p, respectivamente. Ou seja, acabamos de definir duas *famílias indexadas* de conjuntos: a $(A_p)_{p\in\mathcal{P}}$ e a $(C_p)_{p\in\mathcal{P}}$.

- **EXEMPLO 8.141.**
Seja $\mathcal{A}$ o conjunto de todos os aeroportos. Para cada aeroporto $a \in \mathcal{A}$, seja

$$D_a \stackrel{\text{def}}{=} \{\, b \in \mathcal{A} \mid \text{existe vôo direto de } a \text{ para } b \,\}.$$

Acabamos de definir uma família de conjuntos $(\, D_a \mid a \in \mathcal{A}\,)$.

- **EXEMPLO 8.142.**
Seja $\mathcal{B}$ o conjunto de todos os livros. Para cada livro $b \in \mathcal{B}$, sejam

$$A_b \stackrel{\text{def}}{=} \{\, a \mid a \text{ é um autor do livro } b \,\}$$
$$W_b \stackrel{\text{def}}{=} \{\, w \mid w \text{ é uma palavra que aparece no texto do livro } b \,\}.$$

Sabendo a definição de igualdade entre tuplas, definir igualdade entre famílias indexadas é fácil.

D8.143. Definição (Igualdade). Sejam $(a_i)_{i\in\mathcal{I}}$, $(b_i)_{i\in\mathcal{I}}$ famílias indexadas por um conjunto de índices $\mathcal{I}$. Chamamo-nas iguais sse

$$(\forall i \in \mathcal{I})[\, a_i = b_i \,].$$

? **Q8.144. Questão.** Como tu definarias as operações (unárias!) de união e de intersecção para famílias?

!! SPOILER ALERT !!

D8.145. Definição. Seja $(A_i)_{i\in\mathcal{I}}$ é uma família de conjuntos indexada por um conjunto de índices $\mathcal{I}$. Definimos

$$x \in \bigcup_{i\in\mathcal{I}} A_i \overset{\text{def}}{\iff} (\exists i \in \mathcal{I})[\, x \in A_i \,] \qquad x \in \bigcap_{i\in\mathcal{I}} A_i \overset{\text{def}}{\iff} (\forall i \in \mathcal{I})[\, x \in A_i \,].$$

Note que em palavras de rua, as definições são igualzíssimas: um objeto pertence à união da família sse ele pertence a pelo menos um dos seus membros; e perence à sua intersecção sse ele pertence a todos os seus membros.

▸ **EXERCÍCIO x8.68.**
Sejam I, J conjuntos de índices e para cada $k \in I \cup J$ seja A_k um conjunto. A afirmação

$$\bigcup_{k\in I\cap J} A_k = \bigcup_{k\in I} A_k \cap \bigcup_{k\in J} A_k$$

é verdadeira? Responda... (1) *sim*, e demonstre; (2) *não*, e refute; ou (3) *depende*, e mostre um exemplo e um contraexemplo. (x8.68 H 1)

Deixando o Exercício x8.68 nos guiar, chegamos numa investigação interessante:

▸ **EXERCÍCIO x8.69.**
Sejam $\mathcal{I}$, $\mathcal{J}$ conjuntos de índices, e suponha que para cada membro $k \in \mathcal{I}\cup\mathcal{J}$ um conjunto A_k é determinado. O que podemos concluir sobre os conjuntos

$$\bigcup_{k\in\mathcal{I}\cup\mathcal{J}} A_k \quad (?) \quad \bigcup_{i\in\mathcal{I}} A_i \cup \bigcup_{j\in\mathcal{J}} A_j \qquad \bigcup_{k\in\mathcal{I}\cap\mathcal{J}} A_k \quad (?) \quad \bigcup_{i\in\mathcal{I}} A_i \cap \bigcup_{j\in\mathcal{J}} A_j$$
$$\bigcap_{k\in\mathcal{I}\cup\mathcal{J}} A_k \quad (?) \quad \bigcap_{i\in\mathcal{I}} A_i \cup \bigcap_{j\in\mathcal{J}} A_j \qquad \bigcap_{k\in\mathcal{I}\cap\mathcal{J}} A_k \quad (?) \quad \bigcap_{i\in\mathcal{I}} A_i \cap \bigcap_{j\in\mathcal{J}} A_j$$

das opções: ‘$=$’, ‘$\subseteq$’, ‘$\supseteq$’, etc. Investigue. (x8.69 H 0)

§193. Conjuntos indexados vs. famílias indexadas

D8.146. Definição (Conjuntos indexados). Quando usamos um conjunto B para "indexar" um conjunto A, chamamos o A um *conjunto indexado por* B. Temos então:

$$A = \{\, \dots b \dots \mid b \in B \,\}.$$

8.147. Observação. Todo conjunto A pode ser indexado por ele mesmo, pois

$$A = \{\, a \mid a \in A \,\}.$$

Em outras palavras, o "conjunto indexado" não é um tipo diferente do tipo "conjunto". Não faz sentido nos perguntar se um conjunto A é indexado ou não, pois todos são (pelo menos por eles mesmo).

8.148. Observação (Tomando elementos de conjuntos indexados). Suponha que temos um conjunto A indexado por um conjunto $B \neq \emptyset$:

$$A = \{\, \mathrm{bla}(b) \mid b \in B \,\}.$$

Como podemos "tomar um arbitrario membro de A"? Claramente podemos dizer: "seja $a \in A$", algo válido para qualquer conjunto $A \neq \emptyset$. Mas nesse caso, "sejando" um $b \in B$, determinamos um membro de A: o $\mathrm{bla}(b)$. Assim, se demonstrarmos algo sobre o $\mathrm{bla}(b)$, isso é suficiente para concluir que todos os elementos de A satisfazem esse algo. Imagine então que queremos demonstrar que

$$A \subseteq C.$$

Podemos seguir o caminho padrão, demonstrando

$$(\forall a \in A)[\, a \in C \,],$$

mas temos um caminho alternativo que podemos seguir nesse caso: demonstrar que

$$(\forall b \in B)[\, \mathrm{bla}(b) \in C \,].$$

8.149. Igualdade entre conjuntos indexados. Para mostrar que dois *conjuntos* indexados pelo mesmo conjunto são iguais, é *suficiente* mostrar que são iguais como famílias—mas não *necessário*: veja Cuidado 8.150.

Por exemplo, sejam A, B conjuntos indexados pelo mesmo conjunto C:

$$A = \{\, \mathrm{bla}(c) \mid c \in C \,\} \qquad\qquad B = \{\, \mathrm{blu}(c) \mid c \in C \,\}.$$

Suponha que queremos demonstrar $A = B$. O caminho orthódoxo seria seguir a definição de igualdade de conjuntos e demonstrar

$$(\forall x)[\, x \in A \iff x \in B \,], \qquad \text{ou seja,} \qquad A \subseteq B \;\&\; A \supseteq B.$$

Mas, vendo eles como *conjuntos indexados por o* C, podemos matar o alvo $A = B$ numa maneira alternativa, aplicando a definição de igualdade de famílias indexadas. No final das contas, parecem famílias indexadas por o mesmo conjunto de índices (o C). Então demonstrando a afirmação

$$(\forall c \in C)[\, \mathrm{bla}(c) = \mathrm{blu}(c) \,]$$

é *suficiente* para demonstrar que $A = B$.

! **8.150. Cuidado (Suficiente mas não necessário!).** Observe que mostramos algo ainda mais forte: não é apenas que $A = B$ como conjuntos, mas como *famílias* indexadas também, ou seja, *concordam em todo índice*. Mas: pode ser que como famílias não são iguais, mas como conjuntos, são, como o exemplo seguinte mostra:

• **EXEMPLO 8.151.**
Considere os

$$A = \{\, x+1 \mid x \in \mathbb{Z} \,\} \qquad\qquad B = \{\, x-1 \mid x \in \mathbb{Z} \,\}.$$

São dois conjuntos indexados pelo mesmo conjunto $\mathbb{Z}$. Obviamente $A = B$, mas para nenhum índice $x \in \mathbb{Z}$ temos $x + 1 = x - 1$.

§194. Disjuntos dois-a-dois

D8.152. Definição. Seja $\mathscr{A}$ uma família de conjuntos. Chamamos seus membros *disjuntos dois-a-dois* sse nenhum deles tem elementos em comum com nenhum outro deles. Em símbolos:

$$\text{os conjuntos da } \mathscr{A} \text{ são disjuntos dois-a-dois} \overset{\text{def}}{\iff} (\forall A, B \in \mathscr{A})[\, A \neq B \implies A \cap B = \emptyset \,].$$

Similarmente para famílias indexadas:

$$\text{os conjuntos da } (A_i)_{i\in\mathcal{I}} \text{ são disjuntos dois-a-dois} \overset{\text{def}}{\iff} (\forall i, j \in \mathcal{I})[\, i \neq j \implies A_i \cap A_j = \emptyset \,].$$

E logo para seqüências também:

$$\text{os conjuntos da } (A_n)_n \text{ são disjuntos dois-a-dois} \overset{\text{def}}{\iff} (\forall i, j \in \mathbb{N})[\, i \neq j \implies A_i \cap A_j = \emptyset \,].$$

▸ **EXERCÍCIO x8.70.**
Ache uma família de conjuntos $\mathscr{A}$ com $\bigcap \mathscr{A} = \emptyset$ mas cujos membros não são disjuntos dois-a-dois. (x8.70 H 0)

§195. Coberturas e partições

TODO Terminar and include figures

D8.153. Definição (cobertura). Seja B conjunto e $\mathscr{A}$ uma família de conjuntos. Dizemos que $\mathscr{A}$ é uma *cobertura* de B sse a união da família contem o B:

$$\mathscr{A} \text{ cobre } B \overset{\text{def}}{\iff} \bigcup \mathscr{A} \supseteq B.$$

D8.154. Definição (partição). Seja B conjunto e $\mathscr{A}$ uma cobertura de B. Dizemos que $\mathscr{A}$ é uma *partição* de B sse todos os membros da $\mathscr{A}$ são subconjuntos habitados de B e disjuntos dois-a-dois.

▸ **EXERCÍCIO x8.71.**
Seja $A = \{0, 1, 2, 3, 4, 5, 6\}$. Quais das colecções seguintes são partições do A?:

$$\mathscr{A}_1 = \{\, \{0,1,3\}, \{2\}, \{4,5\}, \{6\} \,\} \qquad \mathscr{A}_5 = \{\, \{0,1,2\}, \{2,3,4\}, \{4,5,6\} \,\}$$
$$\mathscr{A}_2 = \{\, \{0,1,2,3\}, \emptyset, \{4,5,6\} \,\} \qquad \mathscr{A}_6 = \{\, \{1,2\}, \{0,3\}, \{5\}, \{6\} \,\}$$
$$\mathscr{A}_3 = \{\, \{0,1,2,3,4,5,6\} \,\} \qquad \mathscr{A}_7 = \{\, \{0,1,2\}, \{3\}, \{4,5,6,7\} \,\}$$
$$\mathscr{A}_4 = \{\, \{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\} \,\} \qquad \mathscr{A}_8 = \{\, \{0\}, \{1,2\}, \{6,5,4,3\} \,\}.$$

(x8.71 H 1)

§196. Traduzindo de e para a linguagem de conjuntos

Lembra os exemplos 8.140, 8.141, e 8.142? Bom. Vamos practicar nossa fluência em cojuntos usando esses exemplos agora.

▸ **EXERCÍCIO x8.72.**
Para toda pessoa $p \in \mathcal{P}$ defina A_p e C_p como no Exemplo 8.140. Suponha que p, q, r denotam pessoas. Traduza as afirmações descritas na linguagem de conjuntos para linguagem natural e vice versa.

(a) p e q são irmãos;
(b) $C_p \neq \emptyset$;
(c) p é filho único;
(d) p e q são parentes;
(e) p e q são primos de primeiro grau;
(f) r é filho dos p e q;
(g) $C_p \cap C_q \neq \emptyset$;
(h) $A_p \subseteq A_q$;
(i) $\emptyset \subsetneq C_p \subsetneq C_q$;
(j) $(\exists p \in \mathcal{P})[\, p \in C_p \,]$.

(x8.72 H 0)

§197. Produto cartesiano generalizado

8.155. Vamos começar com *dois objetos* a e b, nessa ordem, ou seja com uma tupla $\langle a, b\rangle$. Já sabemos como generalizar essa idéia para uma *família indexada* por um conjunto abstrato de índices $\mathcal{I}$, chegando assim na $(a_i)_{i\in\mathcal{I}}$.

Agora comece com *dois conjuntos* A e B, nessa ordem, ou seja com uma tupla $\langle A, B\rangle$. Podemos formar o *produto cartesiano* dela, que em vez de escrever $\times\langle A, B\rangle$ escrevemos

com notação comum e infixa $A \times B$.

$$\text{produto de } \langle A, B\rangle = \{\, \langle a, b\rangle \;\mid\; a \in A \;\&\; b \in B \,\}$$

Com mais detalhes: o *produto da tupla de conjuntos* $\langle A, B\rangle$ é *o conjunto de todas as tuplas* $\langle a, b\rangle$ tais que seu *primeiro* membro pertence no *primeiro* membro da nossa tupla de conjuntos $\langle A, B\rangle$, e seu *segundo* membro pertence no *segundo* membro de $\langle A, B\rangle$.

? **Q8.156. Questão.** Como generalizar isso de tuplas para famílias indexadas? Lembre-se que em famílias indexadas não existe mais essa idéia de *primeiro* e *segundo* membro. Em vez disso, temos *membro no índice* i, um para cada $i \in \mathcal{I}$.

!! SPOILER ALERT !!

8.157. Procurando uma generalização. Antes de responder na pergunta, vamos construir nosso caminho numa forma mais metódica.

$$\begin{array}{ccc} \langle A, B\rangle & \rightsquigarrow & A \times B \\ (A_i)_{i\in\mathcal{I}} & \rightsquigarrow & ?? \end{array}$$

Um passo importante é perceber que nessa situação são envolvidos dois processos: um de "formar o produto de coisas", e outro de "generalizar de tuplas para famílias indexadas". Então uma imagem melhor seria o diagrama

$$\begin{array}{ccc} \langle A, B\rangle & \xrightarrow{\text{product}} & A \times B \\ \Big\downarrow{\scriptstyle \text{generalize}} & & \Big\downarrow{\scriptstyle \text{generalize}} \\ (A_i)_{i\in\mathcal{I}} & \xrightarrow{\text{product}} & ?? \end{array}$$

onde idealmente deveria *comutar*, que informalmente quis dizer que os dois caminhos que nos levam de $\langle A, B\rangle$ para o desejado ?? vão chegar na mesma coisa. (Teremos muito mais a falar sobre *diagramas comutativos* nos próximos capítulos.)

Assim fica mais fácil achar o ??:

$$\begin{array}{ccc} \langle A, B\rangle & \longrightarrow & \{\, \langle a, b\rangle \;\mid\; a \in A \;\&\; b \in B \,\} \\ \Big\downarrow & & \Big\downarrow \\ \langle A_0, A_1\rangle & \longrightarrow & \{\, \langle a_0, a_1\rangle \;\mid\; a_0 \in A_0 \;\&\; a_1 \in A_1 \,\} \\ \Big\downarrow & & \Big\downarrow \\ \langle A_0, A_1\rangle & \longrightarrow & \{\, \langle a_0, a_1\rangle \;\mid\; a_i \in A_i \text{ para todo } i \in \{0, 1\} \,\} \\ \Big\downarrow & & \Big\downarrow \\ (A_i)_{i\in\mathcal{I}} & \dashrightarrow & ?? \end{array}$$

A definição correta agora da idéia que estávamos procurando é óbvia:

$$\text{o produto da } (A_i)_{i\in\mathcal{I}} \text{ é o conjunto } \left\{ (a_i)_{i\in\mathcal{I}} \mid a_i \in A_i \text{ para todo } i \in \mathcal{I} \right\}.$$

Só basta achar uma notação legal para esse conjunto, e essa escolha também é fácil.

D8.158. Definição (Produto cartesiano de família). Seja $(A_i)_{i\in\mathcal{I}}$ uma família indexada de conjuntos. Definimos seu *produto cartesiano*

$$\prod_{i\in\mathcal{I}} A_i \stackrel{\text{def}}{=} \left\{ (a_i)_{i\in\mathcal{I}} \mid a_i \in A_i \text{ para todo } i \in \mathcal{I} \right\}.$$

▸ **EXERCÍCIO x8.73.**
Seja $\mathcal{I}$ um conjunto finito de índices e para cada $i \in \mathcal{I}$ seja A_i um conjunto finito. Qual a cardinalidade do $\prod_i A_i$? (x8.73 H 1)

8.159. Escolhedores. Vou tentar dar um ponto de vista "no nível coração" sobre o produto duma família. Vamos começar com o produto cartesiano "normal" (ou seja, aquele que forma n-tuplas mesmo). Como exemplo real, vamos considerar os 3 conjuntos: A, B, C Nesse caso o que seria o $A \times B \times C$? Agora tome um membro t do $A \times B \times C$. O que ele *é*? Uma tripla, certo. Com certeza tem a forma

$$t = \langle a, b, c\rangle$$

para alguns $a \in A$, $b \in B$, e $c \in C$. Mas o que ele é no meu coração? Como a gente o chama no meu bairro? Posso pensar que ele é um *escolhedor*. Ele escolhe *exatamente um membro de cada um dos conjuntos* A, B, C. Pense que os A, B, e C por exemplo são conjuntos de "starter", "main course", e sobremesa respectivamente

$$\begin{aligned} A &= \{\text{salada}, \text{sopa}, \text{tzatziki}\} \\ B &= \{\text{pizza}, \text{carbonara}, \text{pastitsio}\} \\ C &= \{\text{tiramisu}, \text{yogurte}\} \end{aligned}$$

E esse é o menu dum restaurante onde para jantar o cliente (escolhedor) precisa escolher exatamente uma opção de cada. O produto cartesiano $A \times B \times C$ então, que é o

$$\begin{aligned} A \times B \times C = \{&\langle \text{salada}, \text{pizza}, \text{tiramisu}\rangle \\ &, \langle \text{salada}, \text{pizza}, \text{yogurte}\rangle \\ &, \langle \text{salada}, \text{carbonara}, \text{tiramisu}\rangle \\ &\vdots \\ &, \langle \text{tzatziki}, \text{pastitsio}, \text{tiramisu}\rangle \\ &, \langle \text{tzatziki}, \text{pastitsio}, \text{yogurte}\rangle\}. \end{aligned}$$

representa todos os possíveis escolhedores. A tripla

$$\langle \text{tzatziki}, \text{pastitsio}, \text{tiramisu}\rangle$$

então além de ser "apenas uma tripla", pode ser vista como o escolhedor que escolheu:

$$\begin{aligned} \text{tzatziki} &\in A \\ \text{pastitsio} &\in B \\ \text{tiramisu} &\in C. \end{aligned}$$

Observe que a i-ésima escolha do escolhedor, pertence ao i-ésimo argumento do produto $A \times B \times C$, onde aqui $i \in \{0, 1, 2\}$.

Na mesma maneira então, dada família indexada de conjuntos $(A_i)_{i\in\mathcal{I}}$ cada membro do seu produto cartesiano

$$\prod_{i\in\mathcal{I}} A_i = \left\{ (a_i)_{i\in\mathcal{I}} \mid a_i \in A_i \text{ para todo } i \in \mathcal{I} \right\}$$

é uma família indexada

$$(a_i)_{i\in\mathcal{I}} \text{ tal que } a_i \in A_i \text{ para todo } i \in \mathcal{I},$$

ou seja, um escolhedor que escolha um membro de cada um dos membros da família $(A_i)_{i\in\mathcal{I}}$: a i-ésima escolha a_i do escolhedor $(a_i)_{i\in\mathcal{I}}$ pertence ao i-ésimo argumento A_i do produto $\prod_{i\in\mathcal{I}} A_i$. Pense nisso.

TODO Notação: $\amalg_i$ vs. $\amalg$

§198. Conjuntos estruturados

TODO Elaborar

8.160. Conceito, notação, igualdade. Já encontramos a idéia de estrutura (interna) dum conjunto (foi no Nota 8.15).

! **8.161. Aviso (abuso notacional).** Suponha $\mathcal{A} = (A\ ;\ldots)$ é algum conjunto estruturado. Tecnicamente falando, escrever '$a \in \mathcal{A}$' seria errado. Mesmo assim escrevemos sim '$a \in \mathcal{A}$' em vez de '$a \in A$', e similarmente falamos sobre «os elementos de $\mathcal{A}$» quando na verdade estamos se referendo aos elementos de A, etc. Em geral, quando aparece um conjunto estruturado $\mathcal{A}$ num contexto onde deveria aparecer algum conjunto, identificamos o $\mathcal{A}$ com seu *carrier set* A. Às vezes usamos até o mesmo símbolo na sua definição, escrevendo $A = (A\ ;\ldots)$.

8.162. Conjuntos estruturados com constantes.

TODO Escrever

8.163. Conjuntos estruturados com operações.

TODO Escrever

8.164. Conjuntos estruturados com relações.

TODO Escrever

D8.165. Definição. Sejam conjunto A, uma operação binária $*$ no A, e um $g \in A$.

Dizemos que:

$$\begin{aligned}
A \text{ é } *\text{-fechado} &\overset{\text{def}}{\iff} (\forall a, b \in A)[\, a * b \in A \,] \\
* \text{ é associativa} &\overset{\text{def}}{\iff} (\forall a, b, c \in A)[\, (a * b) * c = a * (b * c) \,] \\
* \text{ é comutativa} &\overset{\text{def}}{\iff} (\forall a, b \in A)[\, a * b = b * a \,] \\
u \text{ é uma } *\text{-identidade esquerda} &\overset{\text{def}}{\iff} (\forall a \in A)[\, u * a = a \,] \\
u \text{ é uma } *\text{-identidade direita} &\overset{\text{def}}{\iff} (\forall a \in A)[\, a * u = a \,] \\
u \text{ é uma } *\text{-identidade} &\overset{\text{def}}{\iff} (\forall a \in A)[\, u * a = a = a * u \,] \\
y \text{ é um } *\text{-inverso esquerdo de } g &\overset{\text{def}}{\iff} y * g = e, \text{ onde } e \text{ é uma } *\text{-identidade} \\
y \text{ é um } *\text{-inverso direito de } g &\overset{\text{def}}{\iff} g * y = e, \text{ onde } e \text{ é uma } *\text{-identidade} \\
y \text{ é um } *\text{-inverso de } g &\overset{\text{def}}{\iff} y * g = e = g * y, \text{ onde } e \text{ é uma } *\text{-identidade}
\end{aligned}$$

onde não escrevemos os "$*$-" quando são implícitos pelo contexto.

8.166. Operando numa lista vazia de objetos. Suponha que para algum $k \in \mathbb{N}$ temos uns objetos

$$a_0, a_1, \ldots, a_{k-1}$$

definidos. Ou seja, temos k objetos. O que seria o resultado operando eles entre si? Isso é algo que denotamos por

$$a_0 * a_1 * \cdots * a_{k-1} \qquad \text{ou} \qquad a_0 a_1 \cdots a_{k-1}.$$

Como *a operação associativa*, essa expressão faz sentido, assim sem parênteses, para qualquer $k > 0$. E, se *a operação tem identidade*, então ela é definida até para o caso extremo de $k = 0$. Se $k = 0$ temos uma lista de 0 membros para operar. E realmente definimos esse resultado para ser a identidade da operação.

D8.167. Definição. Seja R uma relação num conjunto A e $X \subseteq A$. Chamamos o X de *R-fechado* sse para todo $x \in X$, e todo $a \in A$ com $x \, R \, a$, temos $a \in X$ também.

Problemas

TODO Maybe have a first contact with σ-rings, σ-fields, topologies, etc.

▸ **PROBLEMA Π8.12.**
Seja $(A_n)_n$ uma seqüência de conjuntos. Definimos os conjuntos

$$A_* = \bigcup_{i=0}^{\infty} \bigcap_{j=i}^{\infty} A_j \qquad\qquad A^* = \bigcap_{i=0}^{\infty} \bigcup_{j=i}^{\infty} A_j.$$

É verdade que um desses conjuntos é subconjunto do outro? São iguais? São disjuntos? (Π8.12H12)

▸ **PROBLEMA Π8.13 (Nível coração).**
Entenda no teu coração o que tu demonstraste no Problema Π8.12. Como descreverias os elementos dos A_* e A^*? Explique com "palavras da rua" justificando o resultado obtenido. (Π8.13H12345678)

▸ **PROBLEMA Π8.14.**
Demonstre que a inclusão conversa não é sempre válida. Ou seja: construa seqüência de conjuntos $(A_n)_n$ tal que

$$A_* \subsetneq A^*.$$

Podes construir uma tal que ambos os A_*, A^* são infinitos e cada um dos A_n's é um subconjunto finito de $\mathbb{N}$? (Π8.14H0)

Os A_* e A^* do Problema Π8.12 merecem seus próprios nomes!

D8.168. Definição. Seja $(A_n)_n$ uma seqüência de conjuntos. Definimos seu *limite inferior* e seu *limite superior* pelas:

$$\liminf_n A_n \stackrel{\text{def}}{=} \bigcup_{i=0}^{\infty} \bigcap_{j=i}^{\infty} A_j \qquad\qquad \limsup_n A_n \stackrel{\text{def}}{=} \bigcap_{i=0}^{\infty} \bigcup_{j=i}^{\infty} A_j.$$

Note que pelo Problema Π8.12 sabemos se um é subconjunto de outro ou não. Mas pode ser que os dois conjuntos são iguais. Digamos que a seqüência de conjuntos $(A_n)_n$ *converge* sse

$$\liminf_n A_n = \limsup_n A_n.$$

Nesse caso, chamamos esse conjunto de *limite* da $(A_n)_n$ e usamos a notação $\lim_n A_n$ para denotá-lo.

D8.169. Definição. Seja $(A_n)_n$ uma seqüência de conjuntos. Dizemos que $(A_n)_n$ é uma *seqüência crescente* sse $A_i \subseteq A_{i+1}$ para todo $i \in \mathbb{N}$. Similarmente, $(A_n)_n$ é uma *seqüência decrescente* sse $A_i \supseteq A_{i+1}$ para todo $i \in \mathbb{N}$. Rascunhamente:

$$(A_n)_n \text{ crescente} \iff A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$$
$$(A_n)_n \text{ decrescente} \iff A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots$$

Uma seqüência é *monótona* (ou *monotônica*) sse ela é crescente ou decrescente.

▸ **PROBLEMA Π8.15.**
Seja $(A_n)_n$ uma seqüência monótona. Demonstre que $(A_n)_n$ tem limite. Qual é? (Π8.15H0)

▸ **PROBLEMA Π8.16 (Os pães do sanduíche são monótonos e ótimos).**
No Problema Π8.11 definimos duas seqüências "sanduichando" a $(A_n)_n$: uma crescente (a $(C_n)_n$) e uma decrescente (a $(D_n)_n$). Pelo Problema Π8.15 então ambas têm limites, e realmente temos

$$\lim_n C_n = \liminf_n A_n \subseteq \limsup_n A_n = \lim_n D_n.$$

Ainda mais é verdade: de todas as seqüências crescentes, $(C_n)_n$ é a maior tal que $C_n \subseteq A_n$ para todo $n \in \mathbb{N}$; e similarmente de todas as decrescentes, $(D_n)_n$ é a menor tal que $A_n \subseteq D_n$ para todo $n \in \mathbb{N}$. Formalize o que significam as palavras "maior" e "menor" na afirmação acima, e demonstre sua veracidade. (Π8.16H0)

Leitura complementar

Podes achar boas explicações, dicas, muitos exemplos resovidos, e exercícios e problemas para resolver no **[Vel06: §1.3 & §2.4]**.

CAPÍTULO 9

FUNÇÕES

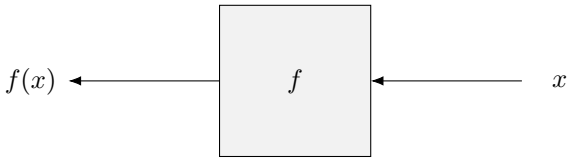
Neste capítulo estudamos mais um *tipo* importantíssimo e fundamental em matemática: a *função*. Nosso objectivo aqui é familiarizar-nos com funções, entender como podemos defini-las, usá-las, combiná-las para criar novas, operar nelas, etc.

Vamos brincar com a poderosa *notação lambda do λ-calculus* (§205), e com funções de *ordem superior* (§207) e apreciar que graças a *currificação* (§208) nem precisamos funções de aridades maiores que 1. Aqui aprendemos também o que são mesmo os *diagramas comutativos* (§216), ferramentas que vamos usar constantemente a partir de agora! Estudamos também o que realmente significa definir funções *recursivamente* (§221), algo que temos feito "sem pensar", baseados na nossa intuição e no nosso insticto muitas vezes até agora. Finalmente (§225) teremos nosso primeiro contato com *categorias*, que oferecem uma abordagem e linguagem unificativa para diversos cantos de matemática (e mais). (O Capítulo 15 e dedicádo na teoria das categorias.)

Bem depois, no Capítulo 16, vamos nos preocupar com a questão de *como implementar* esse tipo (o tipo de funções), *como fundamentar* esse conceito—mas esqueça isso por enquanto. Primeiramente precisamos entender bem o que é uma função e como se comporta. E muitas ferramentas relevantes. Bora!

§199. Conceito, notação, igualdade

9.1. Black boxes. Começamos imaginando funções como black boxes; parecidos mas diferentes daqueles que usamos para conjuntos (8.15), pois essas caixas têm uma entrada mas também uma saída própria:



P9.2. Noção primitiva (função). Sejam A, B conjuntos. Chamamos f uma *função de A para B*, sse para todo $x \in A$, o símbolo $f(x)$ é definido e $f(x) \in B$. O $f(x)$ é o *valor* da f no x. O *domínio* ou *source* da f é o conjunto A, e seu *codomínio* ou *target* é o conjunto B. Consideramos então que a função f associa *para todo* elemento $a \in A$, *exatamente um* elemento $f(a) \in B$.

D9.3. Definição. Escrevemos

$$f : A \to B \qquad \text{e sinonimamente} \qquad A \xrightarrow{f} B$$

para dizer que f *é uma função de* A *para* B, e escrevemos

$$x \xmapsto{f} y$$

para dizer que f *mapeia o* x *para o* y. Definimos também as operações dom e cod que retornam o domínio e o codomínio do seu argumento. Resumindo:

$$f : A \to B \quad \overset{\text{def}}{\iff} \quad f \text{ é uma função} \;\; \& \;\; \operatorname{dom} f = A \;\; \& \;\; \operatorname{cod} f = B.$$

Escrevemos $\operatorname{src}(f)$ e $\operatorname{tgt}(f)$ como sinônimos de $\operatorname{dom}(f)$ e $\operatorname{cod}(f)$ respectivamente. Às vezes o tipo da função aparece olhando para a direção oposta: $f : B \leftarrow A$ em vez de $f : A \to B$. Escrevemos também $f\,x$ em vez de $f(x)$, e em certos casos (mais raros) f_x ou x^f ou até $x\,f$. Podemos referir aos membros do domínio e do codomínio duma função como *pontos* desses conjuntos.

9.4. Observação. Quando escrevemos '$f\,x$' (ou '$f(x)$'), estamos escrevendo algo que representa a *aplicação* da f no x. (E o que estamos denotando é o *valor* da f no x.) O símbolo da aplicação é invisível, ou seja, a aplicação é denotada pela justaposição do nome da função (aqui 'f') e do nome do seu argumento (aqui 'x'). (já discutimos isso no Nota 9.140). Quando precisamos vê-la mesmo na nossa sintaxe podemos usar a notação infixa

$$f \mathbin{@} x \overset{\text{sug}}{\equiv} f(x).$$

9.5. Escrevemos "sejam $f, g : A \to B$" e entendemos como: "sejam funções f e g de A para B", e (abusando) se não temos já declarados os conjuntos A, B, a mesma frase entendemos com um implícito "sejam conjuntos A, B e funções ...". Do mesmo jeito, a frase

$$\text{«Sejam } A \xrightarrow{f} B \xrightarrow{g} C.\text{»}$$

pode ser equivalente à frase

$$\text{«Sejam conjuntos } A, B, C, \text{ e funções } f : A \to B \text{ e } g : B \to C.\text{»}$$

Espero que dá para apreciar a laconicidade dessa notação.

9.6. Função vs. aplicação de função. Em matemática muitas vezes falamos frases como as seguintes:

$$\text{«a função } \sin(x) \text{ é periódica»},$$
$$\text{«a função } f(t) \text{ é monótona»},$$

etc. Literalmente estamos falando algo errado! As funções, nesse exemplo, são as sin e f, não as $\sin(x)$ e $f(t)$. Denotamos por $\sin(x)$ o *valor* da função sin no ponto x, e com $f(t)$ o *valor* da função f no ponto t. Claramente, esse "erro" é algo que não vai confundir nenhum matemático, e com a mínima maturidade matemática não vamos encontrar problema nenhum trabalhando assim. Entendemos então que é apenas um "modo de falar" usado em certos casos. Mas aqui nosso objectivo é estudar e *fundamentar* bem a idéia e a "alma" dos vários tipos matemáticos, e não podemos nos permitir nenhum abuso desse tipo! Essa distinção vai ficar ainda mais crucial, com a notação de λ-calculus e com as funções de ordem superior.

9.7. O tipo duma função. Seja $f : A \to B$. Chamamos o '$A \to B$' o tipo da f, e pronunciamos «função de A para B».

▸ **EXERCÍCIO x9.1.**
Aqui um programa escrito em C:

```
1  int foo(int x)
2  {
3      return x + 1;
4  }
```

Qual é o tipo desse `x` no corpo da `foo`? Qual o tipo da `foo`? Cuidado: programadores de C (e C++, Java, etc.) tendem errar nessa última questão! (x9.1 H 1)

9.8. Um toque de inferência de tipos. Sabendo que $f : A \to B$ e $x : A$, o que podemos inferir? A resposta óbvia aqui é essa:

$$\frac{f : A \to B \qquad x : A}{f\ x : B}\ \textsc{FunApp}$$

Escolhi chamar essa regra de FunApp de "Function Application", talvez dando a impressão errada que é uma regra muito original e nova, que nunca a encontramos antes mas... isso seria mentira:

▸ **EXERCÍCIO x9.2.**
Bem antes de estudar funções, a gente encontrou a "mesma" regra, só que com roupas diferentes, mas nem tanto! De que eu tô falando? (x9.2 H 1)

9.9. Teaser (Curry–Howard). O que tu acabou de descobrir no Exercício x9.2 é uma manifestação duma *conexão muito profunda entre lógica e computação*, conhecida como *correspondência Curry–Howard*, ou também *propositions-as-types and proofs-as-programs interpretation*. A idéia é que podemos ver tipos de funções como proposições e vice versa. E nesse caso *definir uma função* de certo tipo e *demonstrar* a correspondente proposição são ações equivalentes. Com esse ponto de vista as demonstrações são objetos *bem vivos!* Podemos executá-las (pois são programas), observar sua execução e receber a informação que elas retornam. Espero que isso não é *tão* surpresa, pois já tenho dado muitos spoilers e elaborado essa dinámica de demonstrações desde os primeiros capítulos, especialmente no Capítulo 2. Estudando programação funcional, lógica intuicionista, teoria das demonstrações, e teoria dos tipos, tudo isso vai fazer mais sentido, e essa correspondência vai acabar sendo um dos assuntos mais importantes do nosso estudo nesse texto! Por enquanto paciência...

D9.10. Definição. Sejam A, B conjuntos. Denotamos por $(A \to B)$ o conjunto das funções de A para B:

$$f \in (A \to B) \iff^{\text{def}} f : A \to B.$$

O mesmo conjunto denotamos também por B^A.

▸ **EXERCÍCIO x9.3.**
Por quê? Supondo que os A, B são finitos, justifique a notação B^A para o conjunto $(A \to B)$. (Primeiro objetivo desse exercício então é entender o que significa *justificar uma notação* nesse caso.) (x9.3H12)

9.11. Condições de funcionalidade. Na Noção primitiva P9.2 aparece a frase «o símbolo $f(x)$ é definido». Com isso entendemos que não existe ambigüidade, ou seja, para uma entrada x, a f não pode ter mais que uma saída. E graças a outra frase, «para todo $x \in A$», sabemos que tem *exatamente uma* saída. Esta saída é o que denotamos por $f(x)$. Resumindo:
Para todo $x \in \operatorname{dom} f$,

(F-Tot) existe pelo menos um $y \in \operatorname{cod} f$ tal que $x \overset{f}{\longmapsto} y$ (*totalidade*);

(F-Det) existe no máximo um $y \in \operatorname{cod} f$ tal que $x \overset{f}{\longmapsto} y$ (*determinabilidade*).

Quando a 9.11 (F-Tot) acontece dizemos que *a f é definida em todo o seu domínio*. Usamos o termo *univocidade* como sinônimo de determinabilidade.

9.12. Aridade e tuplas. No jeito que "definimos" o que é uma função, ela só pode depender em apenas um objeto, apenas uma entrada. Isso parece bastante limitante, pois estamos já acostumados com funções com aridades diferentes.[58] Caso que uma função precisa mais que um argumento como entrada, usamos a notação $f(x_1, \ldots, x_n)$. Identificamos isso com uma função que recebe "apenas um" objeto como entrada: a n-tupla $\langle x_1, \ldots, x_n \rangle$. Então identificamos as notações

$$f(x_1, \ldots, x_n) = f(\langle x_1, \ldots, x_n \rangle) = f\,\langle x_1, \ldots, x_n \rangle$$
$$f(x) = f(\langle x \rangle) = f\,\langle x \rangle = f\,x$$
$$f() = f(\langle\rangle) = f\,\langle\rangle$$

onde na última linha às vezes identificamos com o próprio f também—quando não existe possibilidade de confusão—mas vamos evitar isso aqui.

Similarmente, se queremos "retornar" mais que um objeto, podemos "empacotar" todos eles numa tupla, e retornar apenas essa tupla, satisfazendo assim a demanda de unicidade de função—cuidado pois isso tem que ser refletido no codomínio da função!

9.13. Sinônimos. Lembra que usamos várias palavras como sinônimos de "conjunto"? (Quais?) Pois é, para funções a situação é parecida. *Dependendo do contexto e da ênfase*, as palavras seguintes podem ser usadas como sinônimos de "função": mapeamento, mapa, map, operação, operador, transformação, etc.

9.14. Intensão vs. extensão. Como nos conjuntos (Secção §176), temos novamente a idéia de *intensão* e *extensão* de uma função. Pensando uma função como uma caixa que dentro dela tem um *programa*, a extensão dela não seria o que ela faz mesmo internalmente (isso seria sua *intensão*), mas o que ela *consegue*. Imaginando duas "caixas pretas" f e g onde podemos apenas observar seus comportamentos usando as suas interfaces e nada mais, faz sentido considerar iguais aquelas que não conseguimos demonstrar nenhum comportamento diferente. Ou seja: qualquer entrada *aceitável* para uma, deve ser *aceitável* para a outra também (pois, se não, isso já seria uma diferença observável); e ainda mais, para a mesma entrada, as funções têm de atribuir o mesmo valor—novamente: se não, isso já seria um comportamento diferente e observável.

[58] Lembra-se que *aridade* é a quantidade de argumentos-entradas.

9.15. Programas vs. funções. Considere as duas funções `f` e `g` implementadas no programa seguinte em Python:

```
1  def f(x):
2      while x > 0:
3          x = x - 1
4      return x
5
6  def g(x):
7      if x > 0:
8          x = 0
9      return x
```

Suponha que queremos considerar ambas definidas nos inteiros. A *extensão* da `f` é a mesma com a extensão da `g`. Ou seja, como funções, temos $f = g$. Suas *intensões* são diferentes. A primeira função, dado um número grande vai fazer bem mais operações até finalmente retornar um valor. Tente calcular as duas no interpretador de Python e também perceberás uma diferença no tempo que cada uma precisa: compare os `f(1000000000)` e `g(1000000000)`. Os *programas* então são diferentes (pois num programa é a intensão que importa) mas as funções são iguais. Note que quando observamos caixas pretas, não podemos nem medir o tempo que cada uma precisa para responder com seu valor, nem podemos tocar elas para ver qual ficou mais quente, nem escutar para possíveis barulhos, etc. Podemos apenas dar uma entrada e observar a saída e nada mais!

9.16. E o codomínio? (I). Em matemática clássica, e especialmente em teoria de conjuntos (Capítulo 16) e análise, em geral não consideramos que o codomínio duma função "faz parte dela". Ou seja, a mesma função sin, por exemplo, pode ser considerada como

$$\sin_1 : \mathbb{R} \to \mathbb{R} \qquad \sin_2 : \mathbb{R} \to [-1, 1] \qquad \sin_3 : \mathbb{R} \to (-\infty, 2).$$

Para esse matemático então, *o codomínio não é algo observável:* como tu vai diferenciar entre as $\sin_1, \sin_2, \sin_3$ acima, se tua única interface é dando objetos para elas, e observando seus valores (saídas)? Pois é, não tem como. Por outro lado, se alterar os domínios isso já é uma diferença demonstrável (observável) com essa mesma única interface.

▸ **EXERCÍCIO x9.4.**
Como? (x9.4 H 1)

9.17. Recuperável ou não?. Com esse ponto de vista, o domínio é um conjunto *recuperável* pela própria função f, pois podemos definir:

$$\operatorname{dom} f \stackrel{\text{def}}{=} \left\{ x \mid (\exists y) \left[x \xmapsto{f} y \right] \right\}.$$

Mas o codomínio não!

▸ **EXERCÍCIO x9.5.**
Qual o problema com essa suposta definição de codomínio de uma função f?:

$$\operatorname{cod} f \stackrel{\text{def}}{=} \left\{ y \;\middle|\; (\exists x)\left[x \xmapsto{f} y \right] \right\}.$$

(x9.5 H 1)

O conjunto definido no Exercício x9.5 realmente é interessante e importante, só que ele não é (necessariamente) o codomínio da função, mas o que chamamos de range:

D9.18. Definição. Seja $f : A \to B$ função. Seu *range* é o conjunto

$$\operatorname{range}(f) \stackrel{\text{def}}{=} \left\{ y \;\middle|\; (\exists x)\left[x \xmapsto{f} y \right] \right\}.$$

Observe que $\operatorname{range}(f) \subseteq B$.

! **9.19. Cuidado.** O conjunto que acabamos de definir na Definição D9.18 é também chamado de *imagem* da f, e a notação $\operatorname{im} f$ também é usada para denotá-lo. Esse conjunto é a imagem *duma função*. Não confunda isso com a imagem *dum conjunto* (*através* duma função), algo que estudamos na Secção §213.

▸ **EXERCÍCIO x9.6.**
Podemos considerar a função sin como uma função com os tipos seguintes?:

$$\sin_4 : \mathbb{Q} \to \mathbb{R} \qquad \sin_5 : \mathbb{R} \setminus \mathbb{Q} \to \mathbb{R} \setminus \mathbb{Q} \qquad \sin_6 : \mathbb{Q} \to \mathbb{Q} \qquad \sin_7 : \{\pi\} \to \{0\}$$

(x9.6 H 0)

9.20. Observação. Seguindo o ponto de vista do 9.16, tendo uma função $f : A \to B$, podemos considerar ela como uma função com codomínio qualquer superconjunto de B, sem mudar nada observável. Em símbolos:

$$f : A \to B \;\;\&\;\; \operatorname{range}(f) \subseteq B' \implies f : A \to B'.$$

Esse ponto de vista, identifica funções com gráficos iguais, mas nem definimos ainda o que é um gráfico de função. É o seguinte.

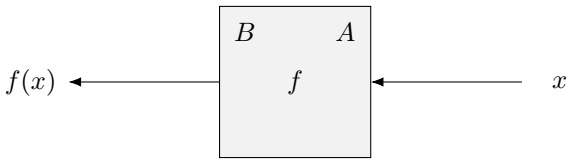
D9.21. Definição. Dado função $f : X \to Y$, o *gráfico da* f, é o conjunto

$$\operatorname{graph} f \stackrel{\text{def}}{=} \{\, \langle x, f(x)\rangle \;\mid\; x \in X \,\}.$$

Observe que $\operatorname{graph} f \subseteq X \times Y$.

9.22. E o codomínio? (II). Em outras partes de matemática, especialmente em teoria das categorias (Capítulo 15), teoria dos tipos (Capítulo 19), e álgebra, consideramos que o codomínio duma função faz parte dela sim! Pensando em funções como black boxes então, com essa visão, temos que imaginar que as caixas pretas tem dois rótulos impressos: um na sua entrada com o domínio escrito nele, e um na sua saída com o codomínio. Assim, a diferença do codomínio vira uma coisa imediatamente observável: é só olhar no rótulo da saída!

9.23. Funções como black boxes com rótulos. Com a idéia (II) de função visualizamos uma função $f : A \to B$ assim:



9.24. Igualdade de funções. Dependendo qual ponto de vista de função seguimos, a definição de igualdade para o tipo de função vai ser diferente! Mostramos primeiramente as definições corretas para o ponto de vista (I) e o ponto de vista (II) (explicados nos 9.16 e 9.22). Depois, escrevendo num jeito diferente, chegamos numa definição que vamos realmente usar e que é aplicável independente do ponto de vista. Nesse texto vamos sempre deixar claro para cada função encontrada qual conjunto consideramos como seu domínio e qual como seu codomínio.[59] Assim, a escolha de ponto de vista de função não vai nos afetar.

D9.25. Definição (Igualdade (I): "Conjuntista"). Sejam f, g funções. Digamos que $f = g$ sse *quaisquer duas* das afirmações seguintes são válidas:

(1) $\operatorname{dom} f = \operatorname{dom} g$;
(2) para todo $x \in \operatorname{dom} f$, $f(x) = g(x)$;
(3) para todo $x \in \operatorname{dom} g$, $f(x) = g(x)$.

Equivalentemente,

$$f = g \overset{\text{def}}{\iff} \operatorname{graph} f = \operatorname{graph} g.$$

D9.26. Definição (Igualdade (II): "Categorista"). Sejam f, g funções. Dizemos que $f = g$ sse

(1) $\operatorname{dom} f = \operatorname{dom} g$;
(2) $\operatorname{cod} f = \operatorname{cod} g$;
(3) para todo $x \in \operatorname{dom} f$, $f(x) = g(x)$.

9.27. Duas religiões. Podemos pensar então que tem duas religiões, que vamos chamar aqui de Conjuntista e de Categorista. Cada um tem sua idéia do que se trata uma função. Note que cada um vai ler as notações $f : A \to B$ e $A \xrightarrow{f} B$ numa maneira diferente:

Conjuntista: «f é uma função com domínio A, e $\operatorname{range}(f) \subseteq B$»
Categorista: «f é uma função com domínio A, e codomínio B».

Vamos escrever agora uma definição de igualdade flexível para satisfazer os dois:

D9.28. Definição (Igualdade (agnóstica)). Sejam $f, g : A \to B$ funções. Definimos

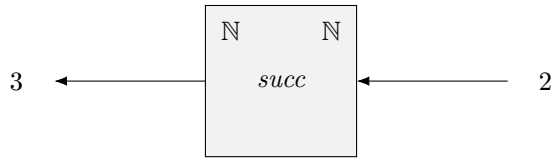
$$f = g \overset{\text{def}}{\iff} \text{para todo } x \in A,\ f(x) = g(x).$$

[59] Exceto numas partes onde esclarecemos qual a noção de função que utilizamos.

9.29. Observação. Assuma a fé do Conjuntista e leia a Definição D9.28: ela é equivalente à D9.25. Agora assuma a fé do Categorista e leia a D9.28 novamente: ela é equivalente à D9.26.

D9.30. Definição. Uma função f é um *endomapa* no A sse $\operatorname{dom} f = \operatorname{cod} f = A$.

- **EXEMPLO 9.31.**
A função $succ : \mathbb{N} \to \mathbb{N}$ que retorna para cada natural n seu sucessor $n+1$. Dando por exemplo 2 como entrada nela, observamos o valor $succ(2) = 3$:



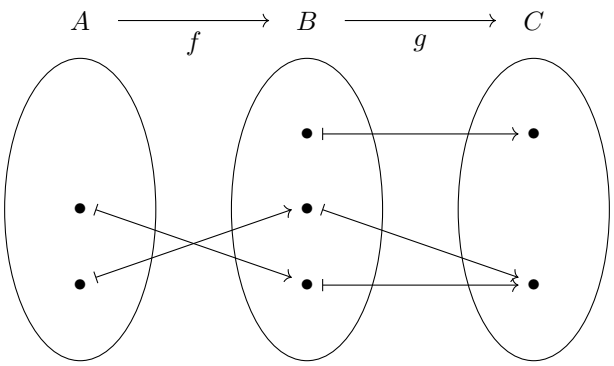
O *succ* é um exemplo de endomapa.

9.32. Observação. Observe que a noção de "ser endomapa" não faz sentido para quem escolher definir *função* pela Definição D9.25 (ou seja, para o "Conjuntista") pois ele nem sabe dizer qual é o codomínio duma função. Logo vamos encontrar mais noções que também não fazem sentido pra ele—fique alerto!

§200. Diagramas internos e externos

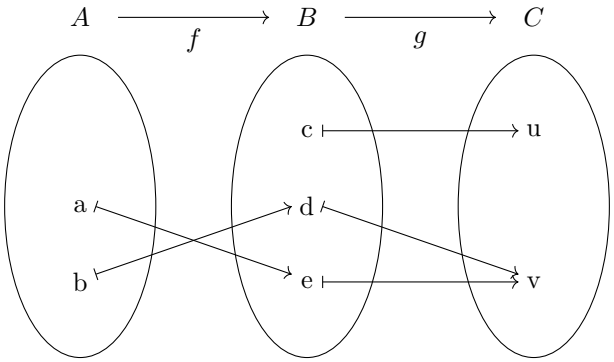
9.33. Diagramas internos. Em certos casos podemos representar toda a informação numa função usando *diagramas internos*, ou seja, diagramas que mostram o interno do domínio e codomínio duma função, e como ela comporta nele.

- **EXEMPLO 9.34.**
Aqui um diagrama interno de duas funções $A \xrightarrow{f} B \xrightarrow{g} C$:



Aqui o conjunto A tem 2 membros—não importa quais são, ou seja, os nomes deles—o B tem 3, e o C tem 2 também.

9.35. Nomes de elementos. É muito comum desenhar esse tipo de diagramas para construir exemplos e contraexemplos que envolvem funções, e quando os *quais são* os membros não é importante desenhamos apenas um • para representar os membros, com o entendimento que pontos distintos representam membros distintos. Note que *se* quisermos definir formalmente um exemplo baseado num desenho, nossa tarefa é trivial: é só escolher nomes para os • e pronto. Por exemplo, dando esses nomes nos pontos do Exemplo 9.34 chegamos no seguinte:



E agora para definir isso formalmente na escrita podemos apenas dizer: Sejam os conjuntos

$$A = \{\mathrm{a}, \mathrm{b}\} \qquad B = \{\mathrm{c}, \mathrm{d}, \mathrm{e}\} \qquad C = \{\mathrm{u}, \mathrm{v}\}$$

e as funções $f : A \to B$ e $g : B \to C$ definidas pelas:

$$\begin{array}{ll} f(\mathrm{a}) = \mathrm{e} & g(\mathrm{c}) = \mathrm{u} \\ f(\mathrm{b}) = \mathrm{d} & g(\mathrm{d}) = \mathrm{v} \\ & g(\mathrm{e}) = \mathrm{v}. \end{array}$$

Observe que os $\mathrm{a}, \mathrm{b}, \mathrm{c}$, etc. *não são variáveis*, mas as próprias letras ‘ a ’, ‘ b ’, ‘ c ’, etc. Naturalmente escolhemos nomes bem conhecidos, como números, letras, etc.

9.36. Observação. Então em que corresponde cada uma das setinhas barradas do diagrama interno? Numa das *equações* que definam a correspondente função, ou seja, num par da forma $\langle x, f(x)\rangle$.

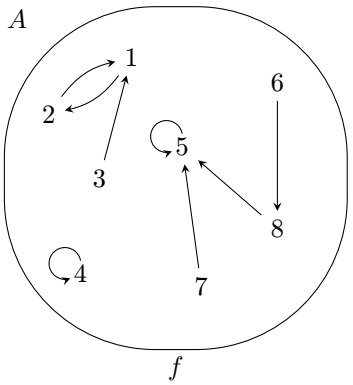
9.37. Diagramas externos. Muitas vezes queremos olhar para a “big picture” e os detalhes “internos” da configuração não nos importam. Pelo contrário, nos atrapalham: *perdemos a floresta pelas árvores*. Nesse caso usamos *diagramas externos*.

• **EXEMPLO 9.38.**
O diagrama externo da configuração do Exemplo 9.34 é o seguinte:

$$A \xrightarrow{\ f\ } B \xrightarrow{\ g\ } C.$$

9.39. Diagramas de endomapas. No caso especial que temos um endomapa $f : A \to A$, podemos desenhar seu diagrama interno sem usar duas cópias de A, mas apenas mostrando os mapeamentos assim como o exemplo seguinte sugere.

- **EXEMPLO 9.40.**
Considere o diagrama interno:



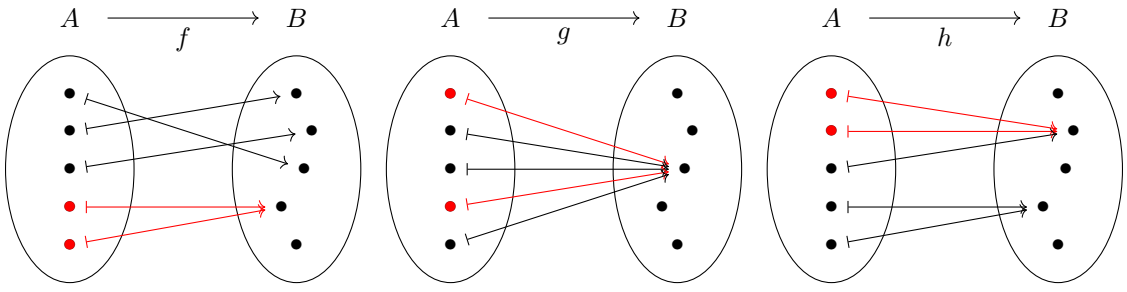
Esse é o diagrama interno da função $f : A \to A$ definida pelas

$$f(1) = 2; \quad f(2) = 1; \quad f(3) = 1; \quad f(4) = 4; \quad f(5) = 5; \quad f(6) = 8; \quad f(7) = 5; \quad f(8) = 5;$$

onde $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Tecnicamente as setinhas deveriam ter bundas, mas já que é um diagrama interno só tem esse tipo de setas (as '$\mapsto$') então não dá pra confundir e o diagrama fica mais fácil de desenhar sem tanta bunda.

§201. Jecções: injecções, sobrejecções, bijecções

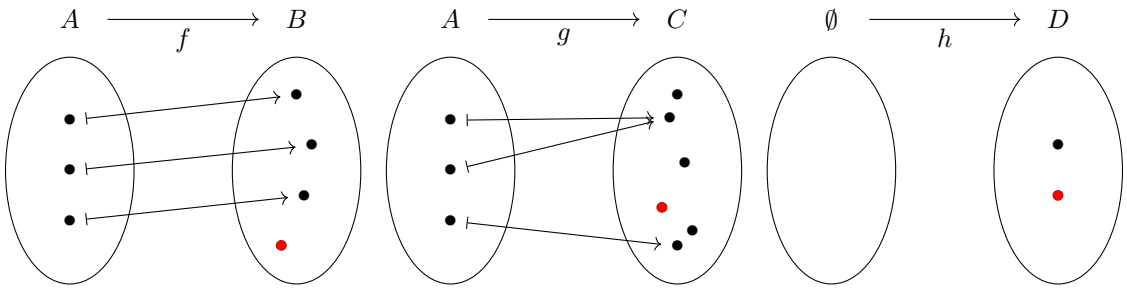
- **NÃOEXEMPLO 9.41.**
Nenhuma dessas funções é injetora:



Em cada caso *uma* razão é enfatizada com cor.

- **NÃOEXEMPLO 9.42.**

E aqui nenhuma dessas funções é sobrejetora:



Novamente em cada caso *uma* razão é enfatizada com cor.

? **Q9.43. Questão.** Como tu definirias os conceitos de função injetora e sobrejetora?

!! SPOILER ALERT !!

D9.44. Definição. Seja $f : A \to B$. Chamamos a f *injectiva* (ou *injetora*) sse

$$\text{para todo } x, y \in A, \text{ se } f(x) = f(y) \text{ então } x = y.$$

Chamamos a f *sobrejectiva* (ou *sobrejetora*) sse

$$\text{para todo } b \in B, \text{ existe } a \in A \text{ tal que } f(a) = b.$$

Chamamos a f *bijectiva* (ou *bijetora*, ou *correspondência*), sse f é injectiva e sobrejectiva. Formulamente,

$$\begin{aligned} f \text{ injectiva} &\overset{\text{def}}{\iff} (\forall x, y \in A)[\, f(x) = f(y) \implies x = y \,]; \\ f \text{ sobrejectiva} &\overset{\text{def}}{\iff} (\forall b \in B)(\exists a \in A)[\, f(a) = b \,]; \\ f \text{ bijectiva} &\overset{\text{def}}{\iff} f \text{ injetora } \& \ f \text{ sobrejetora}. \end{aligned}$$

Usamos as notações

$$\begin{aligned} f : A \rightarrowtail B &\overset{\text{def}}{\iff} f : A \to B \text{ injectiva}; \\ f : A \twoheadrightarrow B &\overset{\text{def}}{\iff} f : A \to B \text{ sobrejectiva}; \\ f : A \rightarrowtail B &\overset{\text{def}}{\iff} f : A \to B \text{ bijectiva}. \end{aligned}$$

As palavras “injectiva”, “sobrejectiva”, e “bijectiva” são adjectivos. Os substantivos correspondentes são os: *injecção*, *sobrejecção*, *bijecção*. Dizemos por exemplo que «f é uma bijecção», que significa que «f é uma função bijectiva».

9.45. Observação. A seguinte afirmação equivalente de $f : A \rightarrowtail B$ é muito útil:

$$\text{para todo } x, y \in A, \text{ se } x \neq y \text{ então } f(x) \neq f(y).$$

(É a sua contrapositiva.) Vamos traduzir essa afirmação mais perto "no nível coração":

$$\text{«}f \textit{ preserva} \text{ as distincções do seu domínio.»}$$

Também digamos que f *respeita* as distincções. Assim podemos pensar que uma função injetora embute seu domínio no seu codomínio, criando uma *cópia fiel* dele, só que com nomes diferentes para seus membros.

9.46. Observação (Conjuntista vs. Categorista). Observe que o conjuntista pode realmente se perguntar se uma função é injetora ou não, pois a definição de ser injetora não mexe com o codomínio da função. Mas pra ele, ser sobrejetora ou não, não é uma propriedade da função "sozinha"; ele afirma que «a função f é *sobre* o B», e é isso que ele quis dizer quando ele afirma «a função $f : A \to B$ é sobrejetora». Pense na diferença que suas caixas pretas têm: como decidir se uma caixa preta dum conjuntista é sobrejetora ou não? Mas tem como decidir se ela é injetora sim. Então o "ser injetora" é um predicado de aridade 1 para ambos, mas o predicado "ser sobrejetora" já difere dependendo da fé: para o categorista tem aridade 1; para o conjuntista tem aridade 2, o segundo argumento sendo o conjunto B nesse caso.

▸ **EXERCÍCIO x9.7.**
Seja S o conjunto de todos os strings *não vazios* dum alfabeto Σ, com $|\Sigma| \geq 2$. Considere a função $f : S \times \{0, 1\} \to S$ definida pela:

$$f(w, i) = \begin{cases} ww, & \text{se } i = 0 \\ w', & \text{se } i = 1 \end{cases}$$

onde w' é o string reverso de w, e onde denotamos a concatenação de strings por justaposição. (1) A f é injetora? (2) A f é sobrejetora? (x9.7H1)

▸ **EXERCÍCIO x9.8.**
Considere as $f, g, h : \mathbb{N}^2 \to \mathbb{N}$ definidas pelas

$$f(x, y) = 2^x 3^y \qquad g(x, y) = 2^x 6^y \qquad h(x, y) = 12^x 18^y.$$

Para cada uma, decida se é injetora, e se é sobrejetora. (x9.8H12)

D9.47. Definição. Sejam A, B conjuntos. Definimos os conjuntos:

$$(A \rightarrowtail B) \stackrel{\text{def}}{=} \{\, f : A \to B \mid f \text{ injetora} \,\}$$
$$(A \twoheadrightarrow B) \stackrel{\text{def}}{=} \{\, f : A \to B \mid f \text{ sobrejetora} \,\}$$
$$(A \rightarrowtail\!\!\!\!\twoheadrightarrow B) \stackrel{\text{def}}{=} \{\, f : A \to B \mid f \text{ bijetora} \,\}$$

▸ **EXERCÍCIO x9.9.**
Ache a cardinalidade dos conjuntos da Definição D9.47 em termos das cardinalidades dos A e B, supondo que ambas são finitas. (x9.9H0)

▸ **EXERCÍCIO x9.10.**
Sejam A um conjunto habitado e $f : A \to \wp A$ definida pela equação

$$f(a) = \{a\}\,.$$

Investigue: (i) A f é injetora? (ii) A f é sobrejetora? (x9.10 H 0)

▸ **EXERCÍCIO x9.11.**
No Exercício x9.10, a hipotese sobre o A é necessária? (x9.11 H 0)

§202. Como definir e como não definir funções

? **Q9.48. Questão.** O que precisamos fazer para definir corretamente uma função?

9.49. Resposta. Precisamos deixar claro qual é o seu domínio e o seu valor para cada ponto no seu domínio (totalidade e determinabilidade). Se consideramos que o codomínio da função faz parte dela também (veja conversa na §199), precisamos deixar claro seu codomínio também—aqui sempre faremos isso.

9.50. Definição por expressão. Uma das maneiras mais comuns para definir funções, é escrever algo do tipo: *Seja $f : A \to B$ a função definida pela* __

9.51. Observação. Literalmente, o que estamos definindo assim é o "$f(x)$" para todo $x \in A$, e não o próprio f. Mas, a f sendo função, realmente é determinada para seu comportamento (seus valores) das todas as entradas possíveis do seu domínio, então isso realmente defina a própria função f—graças a definição de igualdade de funções. (Veja também a Observação 8.50.)

• **EXEMPLO 9.52.**
Seja $f : \mathbb{R} \to \mathbb{R}$ definida pela

$$f(x) = x^2 + 2x + 1, \qquad \text{para todo } x \in \mathbb{R}.$$

Em geral, cada polinómio de n variáveis, pode ser visto como uma função de aridade n.

! **9.53. Cuidado (depender de nome de parametro).** Quando definimos uma função vale a pena pensar como programador que está tentando programar essa função, ou até assumir o papel da própria função que vai receber seus argumentos e vai precisar decidir qual seria o seu valor. Imagine alguém programando uma função `foo` de `int` para `int` numa linguagem de programação. O programador e sua função não têm como saber o *nome* que o chamador da função vai usar quando chamando-la. Em algum ponto ela pode ser chamada pelo `foo(42)` passando assim diretamente o *literal* `42`, ou, depois de umas atribuições como `int a = 42; int num = 42;`, chamá-la `foo(a)` ou `foo(num)`. Não tem como programar a função depender nesses nomes. Por exemplo: «se for chamada com nome que começa com vogal, retorna o inteiro 0; caso contrário, retorna o inteiro 1»; ou «retorna o tamanho do nome do teu argumento» (querendo retornar `1` caso que for chamada pelo `foo(a)`, e `3` caso que for chamada pelo `foo(num)`).

• **NÃOEXEMPLO 9.54.**
Seja $f : \mathbb{Z} \to \mathbb{Z}$ definida pela

$$f(x+y) = y.$$

! **9.55. Cuidado (depender de escolhas).** Por que o Nãoexemplo 9.54 é um nãœxemplo mesmo? Imagine que definimos uma "função" f pela

$$f(x+y) = y.$$

O que seria o $f(2+3)$? 3? Por que não 0? No final das contas (literalmente)

$$2+3 \;=\; 5+0 \;=\; 4+1 \;=\; 12+(-7) \;=\; \dots$$

e f não tem como saber o jeito que tu imaginou "quebrar" sua entrada em dois somantes! A f está olhando ao seu argumento (aqui o 5) e está tentando decidir qual seria o seu valor nesse ponto! E não tem como saber pois, consultando a sua "definição" o resultado vai depender da escolha desses x e y.

9.56. Descripção definitiva. Podemos definir uma função $f : A \to B$ dando uma *descripção definitiva* do seu valor num ponto x do seu domínio:

$$f(x) = \text{aquele } b \in B \text{ que } _____.$$

Cuidado pois nesse caso precisamos verificar que realmente para cada $x \in A$, existe exatamente um $b \in B$ que satisfaz a afirmação no $_____$.

9.57. Observação (Descritor definitivo). Existe uma notação especial para a frase «aquele b que $_____$»: o *descritor definitivo* ι:

$$\text{«aquele } b \text{ que } _____\text{»} \quad \rightsquigarrow \quad \iota b\,.\; _____.$$

Essa notação parece bastante com a λ-notação que encontramos logo na Secção §205, mas é diferente pois na $__$ aqui precisamos algo que denota uma afirmação; na notação lambda algo que denota um objeto. Aqui não vamos usar o descritor definitivo ι, mas a λ-notação é importantíssima e ficaremos a usando o tempo todo. Paciência até §205 então.

• **EXEMPLO 9.58.**
Queremos definir as funções $m, s : \mathcal{P} \to \mathcal{P}$ pelas equações

$$\begin{aligned} m(p) &= \text{a mãe de } p \\ s(p) &= \text{o filho de } p \end{aligned}$$

(onde "mãe" significa "mãe biológica"). Mas...

▸ **EXERCÍCIO x9.12.**
Ache o problema no Exemplo 9.58 acima. (x9.12 H 1)

▸ **EXERCÍCIO x9.13.**
Considere o problema do Exemplo 9.58 que achaste no Exercício x9.12. Vamos tentar resolvê-lo restringindo o $\mathcal{P}$: em vez do conjunto de todas as pessoas, $\mathcal{P}'$ denota o conjunto de todas as pessoas que possuem exatamente um filho. Assim garantimos que $s(p)$ é bem definido, pois $s(p)$ é a única pessoa y tal que y é filho de p: e sabemos que tal y existe, e que é único, pela definição de $\mathcal{P}'$. Então para esse conjunto as m, s do x9.12 realmente definam funções. (x9.13 H 1)

▸ **EXERCÍCIO x9.14.**
Tua resposta dependeu da tua religião? (x9.14 H 1)

9.59. Definição por casos (branching). Às vezes os valores $f(x)$ duma função f não seguem o mesmo "padrão", a mesma "regra" para todos os $x \in \operatorname{dom} f$.

• **EXEMPLO 9.60.**
Seja $f : \mathbb{R} \to \mathbb{R}$ definida pela

$$f(x) = \begin{cases} x^2, & \text{se } x \in \mathbb{Q}; \\ 0, & \text{se } x = \sqrt{p} \text{ para algum primo } p; \\ 2x+1, & \text{caso contrário.} \end{cases}$$

! **9.61. Cuidado.** Cada vez que definimos uma função por casos, precisamos verificar que:

(1) contamos para todos os casos possíveis da entrada;
(2) não existe sobreposição inconsistente em nossos casos.

Seguem uns exemplos que demonstram esses erros.

• **EXEMPLO 9.62.**
Definimos a função $f : \mathbb{N} \to \mathbb{N}$, pela

$$f(n) = \begin{cases} 0, & \text{se } n \text{ pode ser escrito como } 3k \text{ para algum } k \in \mathbb{N}; \\ k, & \text{se } n \text{ pode ser escrito como } 3k+1 \text{ para algum } k \in \mathbb{N}. \end{cases}$$

Aqui o problema é que f não foi definida para todo o seu domínio, pois existem números (por exemplo o 2) que não satisfazem nenhum dos casos da definição da f.

9.63. Observação. Para ter certeza que tomamos cuidado de todos os casos possíveis, podemos descrever o último caso com um "otherwise" (ou "caso contrário"). Observe que as funções $f_1, f_2 : \mathbb{N} \to \mathbb{N}$ definidas pelas

$$f_1(n) = \begin{cases} 0, & \text{se } n \text{ pode ser escrito como } 3k \text{ para algum } k \in \mathbb{N}; \\ n, & \text{se } n \text{ pode ser escrito como } 3k+1 \text{ para algum } k \in \mathbb{N}; \\ 2, & \text{otherwise.} \end{cases}$$

$$f_2(n) = \begin{cases} 0, & \text{se } n \text{ pode ser escrito como } 3k \text{ para algum } k \in \mathbb{N}; \\ n, & \text{otherwise.} \end{cases}$$

são realmente duas funções bem-definidas e diferentes.

▸ **EXERCÍCIO x9.15.**
Demonstre que são diferentes! (x9.15 H 0)

• **EXEMPLO 9.64.**
Definimos a função $g : \mathbb{N} \to \mathbb{N}$, pela

$$g(n) = \begin{cases} 0, & \text{se } n \text{ é primo;} \\ 1, & \text{se } n \text{ é par;} \\ 12, & \text{caso contrário.} \end{cases}$$

Aqui o problema é que não determinamos um único valor para cada membro do domínio da g. Por exemplo o 2, satisfaz os dois primeiros casos da definição acima. Então $g(2) = 0$, pois 2 é primo, e também $g(2) = 1$, pois 2 é par! Por isso essa g é mal-definida, e não uma função.

▸ **EXERCÍCIO x9.16.**
A $h : \mathbb{N} \to \mathbb{N}$, definida pela

$$h(n) = \begin{cases} n+2, & \text{se } n \text{ é primo;} \\ n^2, & \text{se } n \text{ é par;} \\ 12, & \text{caso contrário.} \end{cases}$$

é uma função bem-definida? (x9.16 H 1)

9.65. Observação. Quando dois casos diferentes duma definição de função atribuem os mesmos valores para as mesmas entradas da sua sobreposição comum, dizemos que são *compatíveis*, ou que *concordam*.

9.66. Else-if. Programadores são bastante acostumados com o uso do "else-if", e isso é algo que podemos usar definindo funções por casos. Alterando a definição da função do Exemplo 9.64 podemos realmente (bem) definir uma função $g : \mathbb{N} \to \mathbb{N}$ pela

$$g(n) = \begin{cases} 0, & \text{se } n \text{ é primo;} \\ 1, & \text{se não; e se } n \text{ é par;} \\ 12, & \text{caso contrário.} \end{cases}$$

Assim, cada caso é necessariamente separado de todos os casos anteriores. Em programação o múltiplo uso de "else-if", é chamado uma *if-else-if ladder*.

9.67. Por fórmula. Outro jeito para definir uma função $f : A \to B$, é determinar completamente quando é que $f(x) = v$, para todo $x \in A$ e $v \in B$:

$$f(x) = v \overset{\text{def}}{\iff} \underbrace{\varphi(x, v)}_{\text{function-like}} .$$

Onde a fórmula (ou a afirmação) $\varphi(x, v)$ deve ser *function-like* no A, ou seja, φ é tal que para todo $x \in A$, exatamente um $v \in B$ satisfaz a $\varphi(x, v)$.[60]

[60] Pode olhar também na definição formal disso, D16.76.

▸ **EXERCÍCIO x9.17.**
As "funções" abaixo são bem-definidas?

$$\begin{aligned}
f : \mathbb{R}_{\geq 0} \to \mathbb{R} \qquad & f(x) = y \overset{\text{def}}{\iff} y^2 = x \\
g : \mathbb{N} \to \mathbb{N} \qquad & g(x) = y \overset{\text{def}}{\iff} y^2 = x \\
h : \mathbb{R} \to \mathbb{R} \qquad & h(x) = y \overset{\text{def}}{\iff} y \text{ é o maior inteiro que satisfaz } y \leq x \\
u : \mathbb{Z}^2 \to \mathbb{Z} \qquad & u(x,y) = z \overset{\text{def}}{\iff} z \text{ é primo } \& \ z \mid x+y; \\
v : \mathbb{Z}^2 \to \mathbb{Z} \qquad & v(x,y) = z \overset{\text{def}}{\iff} z \text{ é o menor primo tal que } z \mid x+y.
\end{aligned}$$

Justifique tuas refutações. (x9.17 H 0)

9.68. Por gráfico. Podemos definir uma função $f : A \to B$ se definir qual é o seu gráfico $\operatorname{graph} f$. Observe que do gráfico já podemos recuperar o domínio mas o codomínio não (veja 9.17). Então basta so deixar isso claro e pronto. Claro que precisamos tomar cuidado: o gráfico tem que satisfazer as condições de ser função: totalidade e determinabilidade (Nota 9.11). Olhando apenas para o gráfico, só a determinabilidade pode ser quebrada. Mas se o domínio foi especificado separadamente, precisamos verificar a totalidade também. (Aqui vamos sempre deixar claro o domínio e o codomínio.) Seguem uns exemplos.

• **EXEMPLO 9.69.**
Sejam $A = \{0,1,2,3\}$ e $f : A \to \mathbb{N}$ a função com gráfico

$$\operatorname{graph} f = \{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,4\rangle, \langle 3,2\rangle\}.$$

Temos, por exemplo, $f(0) = 0$ e $f(2) = 4$.

▸ **EXERCÍCIO x9.18.**
Quais dos gráficos abaixo podem ser usados para definir funções com codomínio o $\mathbb{N}$? Quais os seus domínios recuperados por seus gráficos?

$$\begin{aligned}
\operatorname{graph}(f) &= \{\langle 0,1\rangle, \langle 2,4\rangle, \langle 3,8\rangle, \langle 1,2\rangle\} \\
\operatorname{graph}(g) &= \{\langle 0, 12^{12}\rangle\} \\
\operatorname{graph}(h) &= \{\langle 0,1\rangle, \langle 1,1\rangle, \langle 0,1\rangle, \langle 8,1\rangle, \langle 3,2\rangle\} \\
\operatorname{graph}(k) &= \{\langle \mathbb{N},0\rangle, \langle \mathbb{Z},0\rangle, \langle \mathbb{Q},0\rangle, \langle \mathbb{R},1\rangle\} \\
\operatorname{graph}(r) &= \emptyset \\
\operatorname{graph}(s) &= \{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,2^3\rangle, \langle 3,3^{-1}\rangle\} \\
\operatorname{graph}(t) &= \{\langle 3,0\rangle, \langle 2,0\rangle, \langle 2,1\rangle, \langle 2,7\rangle\} \\
\operatorname{graph}(w) &= \{\langle 0,0\rangle, \langle\langle 1,2\rangle, 2\rangle, \langle\langle 12,12\rangle, 2\rangle, \langle\langle 0,1,0,0\rangle, 1\rangle\}
\end{aligned}$$

(x9.18 H 0)

9.70. Por desenho. Conhecemos no Secção §200 dois tipos de diagramas relacionados a funções: internos e externos. Lá observamos que desenhando o diagrama *interno* já temos determinado tudo que precisamos determinar para definir uma função (Nota 9.35). O que deve te deixar surpreso é que usando certos diagramas *externos* podemos *definir* sim funções muito interessantes e importantes em muitos casos! (Faremos isso bastante

no Capítulo 15.) Isso *deve* mesmo ser algo dificilmente aceitável neste momento: se tu estiveres com dúvidas estás no caminho certo: «Como assim determinou uma função pelo diagrama externo? Lá só tem domínio e codomínio! Qual o comportamento da tua função?» Calma: é porque não conhecemos ainda o poder—nem a beleza, nem a elegância—dos diagramas comutativos, que encontraremos logo na Secção §216.

Ainda não encontramos a notação mais interessante para definir funções. Vamos estudá-la logo; ela merece uma secção própria (Secção §205). Antes disso, vamos ver mais uma maneira de definir funções: com buracos!

§203. (Co)domínios vazios

▸ **EXERCÍCIO x9.19.**
Seja $f : A \to \emptyset$. O que podemos concluir sobre o A? Quantas funções têm esse tipo? (x9.19 H 1)

▸ **EXERCÍCIO x9.20.**
Seja $f : \emptyset \to A$. O que podemos concluir sobre o A? Quantas funções têm esse tipo? (x9.20 H 0)

D9.71. Definição (Função vazia). Uma função f com $\operatorname{dom} f = \emptyset$ é chamada *função vazia*.

▸ **EXERCÍCIO x9.21.**
«Uma» ou «a»? (x9.21 H 0)

9.72. Observação. Com tudo que o leitor tem visto até agora a Definição D9.71 não deve aparecer nada estranha. Caso contrário—talvez tu pulou diretamente pra cá?—pense na maneira seguinte: Já determinamos o domínio da função: é o $\emptyset$. O que falta fazer para ter o direito de falar que definimos uma função? Sendo conjuntista, basta determinar para cada um dos membros do domínio seu valor. Se o domínio tivesse três membros, por exemplo se fosse o $\{1, 2, 3\}$, bastaria definir as

$$f(1) = \ldots ?\ldots$$
$$f(2) = \ldots ?\ldots$$
$$f(3) = \ldots ?\ldots$$

Mas agora o domínio tem zero membros, então temos zero valores para determinar, e vamos fazer isso com uma equação para cada um deles mesmo. Aqui, então, minhas zero equações:

Pronto, defini minha função. (Lembrou da 0-tupla (8.118), né?) E se eu fosse categorista, teria mais um trabalho para fazer: determinar o seu codomínio (x9.21).

§204. Expressões com buracos

9.73. O que é uma expressão com buraco?. Podemos criar uma função através duma expressão, escolhendo um dos objetos que aparecem nela e o substituindo por um *buraco*. Criamos assim *aquela função* que, recebendo um argumento, retorna o valor criado botando sua entrada no buraco da expressão. Usamos $\bullet$, $-$, e $_$, para denotar esses buracos.

- **EXEMPLO 9.74.**
Considere a expressão

$$\cos(1+5\sqrt[3]{2})^{2a}+\sin(5).$$

Qual o tipo dela? Ela denota um número real, ou seja,

$$\cos(1+5\sqrt[3]{2})^{2a}+\sin(5):\mathbb{R}.$$

Escolhemos um objeto nela e botamos um buraco no seu lugar:

$$\cos(\bullet+5\sqrt[3]{2})^{2a}+\sin(5).$$

Assim criamos uma função. Qual o tipo dela? Para decidir o domínio dela, olhamos para o tipo do objeto substituido por esse buraco. Nesse caso, consideramos $1:\mathbb{R}$, então temos

$$\cos(\bullet+5\sqrt[3]{2})^{2a}+\sin(5):\mathbb{R}\to\mathbb{R}$$

Uma outra opção seria escolher o 2 no $5\sqrt[3]{2}$, ou até o próprio $5\sqrt[3]{2}$, criando assim a função

$$\cos(1+\bullet)^{2a}+\sin(5):\mathbb{R}\to\mathbb{R}$$

do mesmo tipo.

Podemos botar mais que um buraco na mesma expressão, assim criando funções de aridades maiores. Seguimos a convenção que os seus argumentos são botados nos buracos que aparecem na ordem de esquerda para direita, e de cima pra baixo.

- **EXEMPLO 9.75.**
Considere de novo a expressão

$$\cos(1+5\sqrt[3]{2})^{2a}+\sin(5):\mathbb{R},$$

mas agora bote os buracos

$$\cos(\bullet+5\sqrt[3]{2})^{2\bullet}+\sin(\bullet).$$

Qual o tipo dessa função? Cada um dos buracos está esperando receber um real, ou seja:

$$\cos(\bullet+5\sqrt[3]{2})^{2\bullet}+\sin(\bullet):\mathbb{R}^3\to\mathbb{R}$$

Uma outra opção seria criar a função

$$\cos(1+\bullet\sqrt[3]{\bullet})^{\bullet a}+\sin(\bullet):\mathbb{R}^4\to\mathbb{R},$$

etc.

► **EXERCÍCIO x9.22.**
Calcule:

(a) $(2+\bullet)(40)$;
(b) $(\bullet+2\bullet)(2,4)$;
(c) $(-\cdot 2^{-})(3,0)$;
(d) $(\{1,2,3\}\cup -)(\{2,8\})$.

(x9.22 H 0)

9.76. Observação. Da expressão

$$\frac{1}{2} : \mathbb{Q}$$

podemos criar as funções

$$\frac{\bullet}{2} : \mathbb{Z} \to \mathbb{Q} \qquad \frac{1}{\bullet} : \mathbb{Z}_{\neq 0} \to \mathbb{Q} \qquad \frac{\bullet}{\bullet} : \mathbb{Z} \times \mathbb{Z}_{\neq 0} \to \mathbb{Q}$$

Agora o símbolo ÷ da operação binária de divisão que aparece nos calculadores talvez faz mas sentido, né?

9.77. Limitações. Para um uso simples e rápido as expressões com buracos oferecem uma ferramenta muito útil. Mas, temos umas limitações importantes:

(a) Não podemos "ligar" dois ou mais buracos para representar a idéia que o mesmo argumento vai ser copiado em todos eles.
(b) Não podemos escolher a ordem que os argumentos da função criada vão preencher os buracos.

Finalmente vamos estudar a notação lambda e com ela vamos superar essas limitações facilmente!

§205. Um toque de lambda

9.78. Nomeamentos inúteis. Imagine que precisamos identificar uma certa função dum conjunto A prum conjunto B, e depois de muitos cálculos e usando várias outras funções e objetos dados pelo nosso problema, concluimos com a frase: *«. . . a função desejada é aquela função que recebendo como entrada um número x, ela retorna o $2x+5$.»*. Vamos isolar esta subfrase:

$$\text{aquela função que recebendo como entrada um } x\text{, retorna o } __\, x \,__ .$$

O que ela denota? Claramente uma função. Mas qual é o *nome* dessa função? Pois é, ela não tem. É uma função *anônima*. Isso talvez parece estranho, mas acontece o tempo todo com outros tipos de objetos matemáticos, por exemplo com números. Suponha que temos um triângulo com base b e altura h. Falamos

$$\text{«a área do triângulo é } bh/2\text{»}$$

sem nenhuma obrigação de nomear essa área com um nome para usá-la; e ninguém reclama. Se tivessimos essa obrigação deveriamos falar:

$$\text{«. . . seja } a = bh/2\text{. A área do triângulo é } a\text{.»}$$

Claramente isso é inútil. Introduzimos um novo nome apenas para usá-lo logo após e nunca mais. Em nossa última frase "a área do triângulo é a", a informação nem é mais visível. O leitor vai ter que lembrar qual foi a definição desse a, ou ir procurar achá-la. Obviamente a abordagem anterior é melhor. Com ela podemos enunciar nossa proposição numa maneira melhor:

$$\text{«a área dum triângulo com base } b \text{ e altura } h \text{ é } bh/2\text{»}$$

em vez de falar algo do tipo

$$\text{«a área dum triângulo com base } b \text{ e altura } h \text{ é } a\text{, onde } a = bh/2.\text{»}$$

Para usar um exemplo de "nomeamento inútil" em programação, considere as funções seguintes em Python cada uma programada por um programador diferente:

```
1  def f(x):
2      return 2 * x + 1;
3
4  def g(x):
5      r = 2 * x + 1
6      return r
```

Como funções são iguais, mas o programador que programou `g`, fez algo estranho. Decidiu nomear a expressão `2 * x + 1` com o nome `r`, e a única coisa que ele fez com esse `r`, foi returnar seu valor. Pra quê isso, programador?

9.79. De palavras para lambda. Voltamos na frase

$$\text{"aquela função que recebendo como entrada um } x\text{, retorna o } __\,x\,__\text{"}$$

onde '$__\,x\,__$' é uma expressão que determina um único objeto e que, possivelmente depende (refere) no x, como aconteceu por exemplo com o $2x + 5$ acima. Se essa frase realmente determina uma função, então podemos também definir uma função *epônima* ("com nome") quando desejamos, escrevendo:

$$\text{«Seja } f : A \to B \text{ tal que}$$
$$f \stackrel{\text{def}}{=} \text{aquela função que recebendo...»}.$$

Mas escrever tudo isso toda vez que queremos construir uma função anônima é muito chato. Bem vindo λ (lambda) da notação de λ-calculus! Escrevemos apenas

$$\lambda x\,.\,2x + 5$$

para a frase:

$$\overbrace{\text{aquela função que recebendo como entrada um}}^{\lambda}\ \overbrace{x}^{x}\ \overbrace{\text{retorna o}}^{.}\ \overbrace{2x+5}^{2x+5}.$$

D9.80. Definição (lambda abstracção). A expressão

$$\lambda x\,.\,__\,x\,__$$

é chamada λ-*abstracção* e *denota uma função*:

"aquela função que recebendo x como entrada, retorna o $__\,x\,__$"

Supomos aqui que o domínio e codomínio são claros pelo contexto. Chamamos a parte "$__\,x\,__$" o *corpo* da abstracção.

D9.81. Definição. Uma notação diferente usada em matemática para criar funções anônimas utiliza a *setinha barrada* '$\mapsto$':

$$\text{escrevemos} \qquad (x \mapsto __) \qquad \text{como sinônimo de} \qquad \lambda x\,.\,__\,.$$

9.82. Observação. Não vamos usar muito a notação $(x \mapsto __)$. Pois a notação $\lambda x\,.\,__$ serve bem melhor para a maioria dos nossos usos.

9.83. Observação. O λ é um *ligador de variável*. Todos os x que aparecem livres no $__\,x\,__$ viram ligados com o x do λx. Naturalmente consideramos funções que são diferentes apenas nos nomes das variáveis ligadas como iguais. Por exemplo:

$$\lambda x\,.\,x = \lambda y\,.\,y.$$

Compare com programação onde uma troca *com cuidado* de variáveis resulta em programas e procedimentos equivalêntes. Precisamos tomar os mesmos cuidados aqui, e deixamos os detalhes formais para o Capítulo 20.

9.84. Observação (Comparação com set builder). Num certo sentido o papel de $\lambda x\,.\,__$ é parecido com o papel do $\{\,x \mid __\,\}$. O set builder constrói conjuntos (anônimos), e o λ parece então um "function builder" que constrói funções (anônimas).

! **9.85. Aviso (Construimos funções mesmo?).** É "forte demais" afirmar que a expressão $\lambda x\,.\,x^2$ determina uma função. Qual é o seu domínio? E o categorista vai perguntar também sobre seu codomínio. Sem essa informação faz mais sentido considerar que um termo como o $\lambda x\,.\,x^2$ corresponde numa *alma*, ou seja, *um comportamento* que em geral pode "animar o corpo" de várias funções.[61] Se as informações de domínio (e codomínio dependendo da fé) não estão claras pelo contexto escrevemos o tipo logo após da λ-expressão para realmente determinar uma função. Podemos "tipar" o termo $\lambda x\,.\,x^2$ então

$$\lambda x\,.\,x^2 \;:\; \mathbb{R} \to \mathbb{R} \qquad\qquad \lambda x\,.\,x^2 \;:\; \mathbb{N} \to \mathbb{N} \qquad\qquad \lambda x\,.\,x^2 \;:\; \{0\} \to \mathbb{N}$$

etc., e agora sim cada uma dessas determina mesmo uma função.

[61] Aqui tô usando a palavra «corpo» numa maneira mais antropomórfica, e nesse caso corresponde num *tipo* de função, que tá esperando uma *alma para habitá-lo*. Quando pegamos emprestada a terminologia de programação a mesma palavra «corpo» acaba significando algo diferente: aí, o corpo duma "função" seria o código que determina o seu comportamento.

Então: o λ nos permite criar funções anônimas numa maneira simples e útil. E o que podemos fazer com uma expressão dessas? *Tudo* que podemos fazer com uma função!

• **EXEMPLO 9.86.**
Calculamos:

$$(\lambda x\,.\,2x+5)(4) = 2\cdot 4+5 = 13$$
$$(\lambda x\,.\,x)(2) = 2.$$

Em geral omitimos as parenteses no argumento, escrevendo:

$$(\lambda x\,.\,2x+5)\ 4, \qquad (\lambda x\,.\,x)\ 2, \qquad \text{etc.},$$

algo que acontece com funções epônimas também (veja Definição D9.3).

9.87. Convenção. Para evitar uso excessivo de parenteses, acordamos que o corpo duma λ-abstracção estende o maior possível, por exemplo:

$$(\lambda x\,.\,x+y+z) \qquad \text{significa} \qquad (\lambda x\,.\,(x+y+z)).$$

9.88. A alma da λ-computação. Assim que aparecer uma coisa ♡ no lado duma λ-abstracção $(\lambda x\ldots x\ldots x\ldots)$ temos uma expressão *reductível* (chamada *β-redex*)

$$(\lambda x\,.\,\underbrace{\ldots x\ldots x\ldots}_{\tau(x)})\ \heartsuit$$

ou seja, podemos fazer um passo computacional: *substituir o redex inteiro por uma nova expressão criada substituindo todas as ocorrências livres de x no $\tau(x)$ por ♡, chegando assim no $\tau(\heartsuit)$*. Denotando esse passo com um ' $\triangleright_\beta$ ', temos então

$$(\lambda x\,.\,\underbrace{\ldots x\ldots x\ldots}_{\tau(x)})\ \heartsuit\ \triangleright_\beta\ \underbrace{\ldots\heartsuit\ldots\heartsuit\ldots}_{\tau(\heartsuit)}.$$

• **EXEMPLO 9.89.**
Calcule a expressão:

$$(\lambda x\,.\,2+(\lambda y\,.\,x-y)\ 8)\ 50.$$

Resolução. Procuramos achar *redexes* e achamos dois:

$$\underline{(\lambda x\,.\,2+(\lambda y\,.\,x-y)\ 8)\ 50} \qquad\qquad (\lambda x\,.\,2+\underline{(\lambda y\,.\,x-y)\ 8})\ 50.$$

Então temos dois caminhos diferentes para seguir. Vamos tentar ambos:

$$\begin{aligned}\underline{(\lambda x\,.\,2+(\lambda y\,.\,x-y)\ 8)\ 50} &\triangleright_\lambda\ 2+\underline{(\lambda y\,.\,50-y)\ 8}\\ &\triangleright_\lambda\ 2+(50-8)\\ &=\ 44.\end{aligned}$$

Escolhendo o outro caminho, talvez chegamos em algum valor diferente. Vamos ver:

$$\begin{aligned}(\lambda x\,.\,2+\underline{(\lambda y\,.\,x-y)\ 8})\ 50 &\triangleright_\lambda\ \underline{(\lambda x\,.\,2+(x-8))\ 50}\\ &\triangleright_\lambda\ 2+(50-8)\\ &=\ 44.\end{aligned}$$

Interessante. Chegamos no mesmo valor. Mas talvez foi coincidência.

9.90. Church–Rosser: «Foi não». Graças ao teorema Church–Rosser que vamos estudar no Capítulo 20 sabemos que se existem dois caminhos que chegam em dois valores "finais", não podem ser valores diferentes. Isso não quis dizer que as escolhas não importam, pois pode ser que um caminho nem termine! Mas se dois caminhos realmente chegarem em valores finais mesmo, então chegaram no mesmo valor![62]

▸ **EXERCÍCIO x9.23.**
Calcule os seguintes:

(a) $(\lambda x\,.\,x)\ 5$;
(b) $(\lambda y\,.\,42)\ 5$;
(c) $(\lambda z\,.\,x)\ 5$;
(d) $(\lambda x\,.\,x+1)\ 41$;
(e) $(\lambda x\,.\,2+(\lambda y\,.\,3y)\ 5)\ 3$;
(f) $(\lambda x\,.\,2+(\lambda y\,.\,3y)\ (x^2))\ 3$;
(g) $(\lambda x\,.\,2+(\lambda y\,.\,xy)\ 4)\ 3$;
(h) $\lambda x\,.\,(\lambda x\,.\,x+1)\ 1\cdot(\lambda y\,.\,xy)\ 4$.

Em cada passo, sublinhe o redex que tu escolheu para reduzir. Não se preocupe se uns deles parecem errados ou bizarros, nem se tu errar calculando uns deles; mas verifique tuas respostas. (x9.23 H 0)

▸ **EXERCÍCIO x9.24.**
Quando puder, escreva λ-expressões que podem ser tipadas com os tipos seguintes:

$$
\begin{array}{ll}
: A \to A & : A \times B \to B \times A \\
: A \times B \to A & : A \cup B \to A \\
: A \times B \to B & : A \to A \cup B \\
: A \times A \to A & : A \times B \to A \cup B \\
: A \to A \times A & : A \cup B \to A \times B \\
: A \to A \times B & : ((A \times B) \cup (C \times D)) \to ((A \cup C) \times (B \cup D)).
\end{array}
$$

Observe que sobre os A, B tu não tens nenhuma informação. Pode achar mais que uma resolução para algum desses desafios? (x9.24 H 0)

▸ **EXERCÍCIO x9.25.**
Escreva λ-expressões que podem ser tipadas com os tipos seguintes:

$$
\begin{array}{l}
: \mathbb{N} \to \mathbb{N} \\
: \mathbb{N}^2 \to \mathbb{N} \\
: \mathbb{N} \to \mathbb{N}^2 \\
: \wp\mathbb{N} \setminus \{\emptyset\} \to \mathbb{N} \\
: \wp\mathbb{N} \to \mathbb{N} \\
: \wp_{\mathrm{f}}\mathbb{N} \to \mathbb{N}.
\end{array}
$$

Tente usar o argumento no corpo dos teus λ-termos se puder. (x9.25 H 0)

[62] Essa é uma grande hipersimplificação do teorema de Church–Rosser; para a versão "raiz", paciência até o Capítulo 20.

▸ **EXERCÍCIO x9.26.**
Seja $f : A \to B$. Qual nome tu daria para a função $\lambda x \,.\, f\, x$? Lembre-se que graças as convenções notacionais essa expressão é a mesma com a $\lambda x \,.\, (f(x))$. (x9.26 H 1)

9.91. β-reducção. O nome real desse passo computacional de λ-cálculo que encontramos aqui é *β-reducção*, e o redex é formalmente chamado um *β-redex*. Para enfatizar quando for necessário escrevemos ‘ $\triangleright_\beta$ ’ para denotar um passo de β-reducção.

Tem mais duas regras de λ-computação: α-renomeamento e η-conversão.

9.92. α-renomeamento. O princípio que nos permite identificar como equivalentes as λ-expressões que diferem apenas nas escolhas das suas variáveis ligadas é chamado *α-renomeamento* ou *α-conversão* ou *α-equivalência*. Podemos considerar cada λ-abstracção um *α-redex*; denotamos por ‘ $\triangleright_\alpha$ ’ um passo onde aconteceu um α-renomeamento.

• **EXEMPLO 9.93 (em programação).**
Considere o código seguinte:

```
1  def f(x):
2      return x * z
```

Aqui parece que o `z` é uma variável já declarada e definida no escopo exterior. Deve ser óbvio que podemos trocar a variável `x` por qualquer variável que não aparece livre no corpo da `f`. Escolhendo trocá-la por `y`, por exemplo, chegamos na função equivalente:

```
1  def f(y):
2      return y * z
```

onde semanticamente nada mudou no nosso programa. Mas seria errado ter escolhido a `z`, pois ela capturaria a antes-livre `z` do corpo da `f`:

```
1  def f(z):
2      return z * z
```

Isso não é mais o mesmo programa. Antes a função `f` poderia ser descrita como

«a função que retorna o produto da sua entrada com z»;

uma descripção que serve para qualquer um dos dois primeiros programas. Observe que não usei nem ‘ x ’ nem ‘ y ’ nessa frase, mas não teria como descrevé-la sem usar a ‘ z ’. Já a terceira função seria

«a função que retorna o quadrado da sua entrada»;

algo claramente diferente.

• **EXEMPLO 9.94 (em conjuntos).**
Considere o conjunto seguinte:

$$\{\, x \mid x < z^2 \,\}.$$

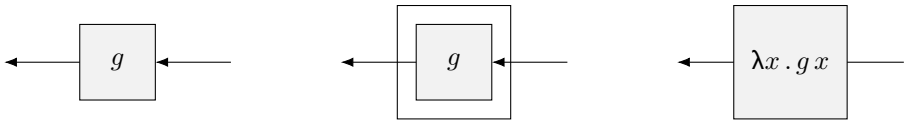
Obviamente podemos trocar o 'x' por qualquer variável que não aparece livre no filtro '$x < z^2$', por exemplo por 'y':

$$\{\, x \mid x < z^2 \,\} \equiv \{\, y \mid y < z^2 \,\};$$

mas não poderiamos ter escolhido substituir o 'x' por 'z', pois assim aconteceria *captura de variável* (já discutimos isso no Cuidado 8.9).

9.95. η-conversão. Essa é a idéia de *extensionalidade* para o sistema: se duas expressões comportam na mesma maneira, as consideramos equivalentes. Qualquer expressão da forma $\lambda x\,.\,f\,x$ é um *η-redex*, e denotamos por '$\triangleright_\eta$' o passo onde o substituimos por f.

9.96. η-wrapping desenhado. Começa com uma função g; agora pega um embrulho preto e embrulhe; e pronto, tu criou uma "nova" função. Só que não é tão nova né? Talvez tu vai rotulá-la como f ou talvez vai escolher um rótulo mais honesto, como $\lambda x\,.\,g\,x$.



A η-conversão nos permite identificar as duas caixas acima.

• **EXEMPLO 9.97 (em programação).**
Considere o código seguinte, que corresponde no desenho acima:

```
1  def f(x):
2      return g(x)
```

Deve ser óbvio que essa `f`, como função, comporta na mesma maneira que a `g`.

‣ **EXERCÍCIO x9.27 (em conjuntos).**
Qual seria o equivalente de η-conversão para os conjuntos? (x9.27 H 0)

• **EXEMPLO 9.98.**
Computamos a mesma expressão usando dois caminhos diferentes:

$$\begin{aligned} \underline{(\lambda x\,.\,(\lambda y\,.\,y^2)\;x)}\;3 &\triangleright_\eta \underline{(\lambda y\,.\,y^2)}\;3 \\ &\triangleright_\alpha \underline{(\lambda x\,.\,x^2)\;3} \\ &\triangleright_\beta 3^2. \end{aligned} \qquad \begin{aligned} \underline{(\lambda x\,.\,(\lambda y\,.\,y^2)\;x)}\;3 &\triangleright_\alpha \underline{(\lambda y\,.\,(\lambda y\,.\,y^2)\;y)}\;3 \\ &\triangleright_\eta \underline{(\lambda y\,.\,y^2)\;3} \\ &\triangleright_\beta 3^2. \end{aligned}$$

Observe que provavelmente nenhum humano sano escolheria esse α-renomeamento no segundo caminho, pois a expressão piorou para nossos olhos humanos; aqui escolhi proceder assim para enfatizar que não tem nada (literalmente) errado nisso.

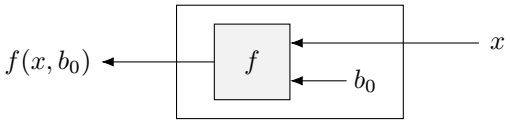
§206. Aplicação parcial

9.99. Aplicação parcial com black boxes. Suponha que temos uma função de aridade 2:

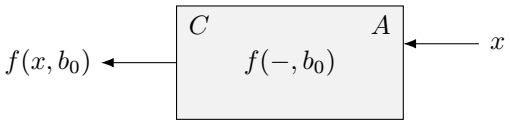
$$f : (A \times B) \to C.$$

Ou seja, nossa função, "para funcionar", precisa receber exatamente dois argumentos: algum $a \in A$ e algum $b \in B$ para "produzir" o valor $f(a, b) \in C$:

Queremos utilizar essa função de aridade 2, para criar duas outras, cada uma de aridade 1. A idéia é a seguinte: vamos "fixar" uma das suas entradas com um valor, e deixar a outra como entrada mesmo. Imagine que fixamos um certo $b_0 \in B$ no segundo "cabo" de entrada, puxamos o outro cabo, e criamos uma nova caixa assim:



E agora pintamos preta nossa caixa, escrevemos seus rótulos (seu tipo), e pronto, construimos uma nova função de aridade 1:



Observe que temos $f(-, b_0) : A \to C$. Vamos agora ver a mesma idéia usando buracos, sem black boxes.

9.100. Aplicação parcial usando buracos. Considere uma função f de aridade 3:

$$A \times B \times C \xrightarrow{\quad f \quad} D.$$

Lembre-se que

$$f(-, -, -) : A \times B \times C \to D$$

e ainda mais $f(-, -, -)$ é a própria f! Queremos preencher uns desses buracos, mas não todos. E nada especial sobre esse 3. Em geral, dada uma função f de aridade n, podemos *fixar* k dos seus argumentos com certos valores, botar buracos nos ouros, e criar assim uma função de aridade $n - k$. Uns exemplos vão esclarecer esse processo.

- **EXEMPLO 9.101.**
Considere a função $f : \mathbb{R}^3 \to \mathbb{R}$, definida pela

$$f(x, y, z) = x + y^2 + z^3.$$

Temos então

$$f(-,-,-) : \mathbb{R}^3 \to \mathbb{R}.$$

Com aplicação parcial, fixando uns dos seus argumentos, criamos então as funções seguintes:

$$\begin{aligned} f(2,-,-) &: \mathbb{R}^2 \to \mathbb{R} \\ f(2,-,\sin(2)) &: \mathbb{R} \to \mathbb{R} \\ f(-,\sqrt{2},\sqrt[3]{2}) &: \mathbb{R} \to \mathbb{R} \\ f(-,0,0) &: \mathbb{R} \to \mathbb{R}. \end{aligned}$$

A última, por exemplo, é a $\mathrm{id}_{\mathbb{R}}$; a penúltima é a $\lambda x \,.\, x + 4$.

- **EXEMPLO 9.102.**
Aplicando a função de adição $+ : \mathbb{N}^2 \to \mathbb{N}$ parcialmente fixando seu segundo argumento no número 1, criamos a função

$$(\bullet + 1) : \mathbb{N} \to \mathbb{N}$$

que é a função *succ* de sucessor; e fixando seu primeiro argumento no 0 criamos a

$$(0 + \bullet) : \mathbb{N} \to \mathbb{N}$$

que é a $\mathrm{id}_{\mathbb{N}}$.

9.103. Teaser. Já que entendeu a relação entre expressões que envovlem buracos e abstracções lambda com variáveis, espero que nem preciso explicar que podemos denotar a aplicação parcial $f(2,-)$ por $\lambda x \,.\, f(2, x)$. Mas trabalhando com lambdas é mais comum tratar funções de aridades maiores que 1 numa outra maneira, chamada currificação (§208). E a aplicação parcial brilha ainda mais nesse caso: não precisa nem buracos, nem variáveis (Nota 9.129)!

§207. Funções de ordem superior

9.104. Buracos de novo. Já encontramos a idéia de *abstrair* certas partes de uma expressão, botando *buracos*, criando assim funções de várias aridades. Além de buracos, trabalhamos com *λ-abstracção* que nos permitiu dar nomes para esses buracos, ligar (identificar) certos buracos, etc. Considere novamente uma expressão como a

$$\cos(1 + 5\sqrt[3]{2})^{2a} + \sin(5)$$

onde $\cos : \mathbb{R} \to \mathbb{R}$, $\sin : \mathbb{R} \to \mathbb{R}$, e $a \in \mathbb{R}$. Botando uns buracos ou abstraindo com lambdas, criamos, por exemplo, as funções:

$$\begin{aligned}
f_1 &= \cos(1 + 5\sqrt[3]{2})^{\bullet a} + \sin(5) && : \mathbb{R} \to \mathbb{R} \\
f_2 &= \cos(\bullet + 5\sqrt[3]{\bullet})^{2a} + \sin(\bullet) && : \mathbb{R}^3 \to \mathbb{R} \\
f_3 &= \cos(\bullet + \bullet\sqrt[3]{2})^{2\bullet} + \sin(5) && : \mathbb{R}^3 \to \mathbb{R} \\
f_4 &= \cos(\bullet + \bullet)^{\bullet} + \sin(5) && : \mathbb{R}^3 \to \mathbb{R} \\
f_5 &= \bullet + \sin(\bullet) && : \mathbb{R}^2 \to \mathbb{R} \\
f_6 &= \lambda x \,.\, \cos(1 + 5\sqrt[3]{2})^{2x} + \sin(5) && : \mathbb{R} \to \mathbb{R} \\
f_7 &= \lambda x, y \,.\, \cos(1 + y\sqrt[3]{x})^{2a} + \sin(y) && : \mathbb{R}^2 \to \mathbb{R}.
\end{aligned}$$

▸ **EXERCÍCIO x9.28.**
Para quais entradas cada uma dessas funções retorna o valor da expressão inicial? (x9.28 H 1)

9.105. Buracos de ordem superior. Em todos os exemplos acima, botamos os buracos para substituir apenas termos cujos valores seriam números (reais). Expressões tanto como as 2, 1, 5, e a, quanto como as $5\sqrt[3]{2}$, $2a$, e $\cos(1 + 5\sqrt[3]{2})^{2a}$, denotam, no final das contas, números reais. Que tal botar um buraco assim:

$$\cos(1 + 5\sqrt[3]{2})^{2a} + \bullet(5)$$

O que substituimos aqui? O próprio sin! Por que não? E o que tipo de objetos podemos botar nesse buraco? Um real, não serve: a expressão

$$\cos(1 + 5\sqrt[3]{2})^{2a} + 7(5)$$

não faz sentido: *ela é mal-tipada*. O 7 não pode receber um argumento como se fosse uma função, pois não é. Que tipo de coisas então cabem nesse buraco? Funções! E não funções quaisquer, mas precisam ter um tipo compatível, com a aridade certa, etc. Esses buracos são *de ordem superior*. E com buracos de ordem superior, vêm funções de ordem superior.

D9.106. "Definição". Dizemos que uma função $f : A \to B$ é de *ordem superior* se ela recebe ou retorna funções.

▸ **EXERCÍCIO x9.29.**
Escreva os tipos das funções seguintes:

$$\begin{aligned}
F_1 &= \cos(1 + 5\sqrt[3]{2})^{2a} + \bullet(5) \\
F_2 &= \bullet(1 + 5\sqrt[3]{2})^{2a} + \sin(5) \\
F_3 &= \bullet(1 + 5\sqrt[3]{2})^{2a} + \bullet(5) \\
F_4 &= \cos(\bullet(1, 5\sqrt[3]{2})^{2a} + \sin(5) \\
F_5 &= \cos(\bullet(1, 5\sqrt[3]{2})^{2a} + \bullet(\bullet) \\
F_6 &= \lambda r, t, u \,.\, \cos(1 + r(u, \sqrt[3]{2}))^{r(t,a)} + \sin(u)
\end{aligned}$$

(x9.29 H 0)

9.107. Retornando funções. Até agora encontramos exemplos onde funções recebem como argumentos outras funções, mas ainda não conhecemos alguma função que *retorna função*. Ou será que conhecemos? Se tu resolveu o Exercício x9.23, tu já encontrou esse caso, na sua última expressão. Seguem uns exemplos de operadores de ordem superior que você talvez já encontrou e até usou na tua vida.

- **EXEMPLO 9.108 (Definindo uma função de ordem superior).**
Considere a função $F : \mathbb{N} \to (\mathbb{N} \to \mathbb{N})$ definida pela

$$F(w) = \text{aquela função } g : \mathbb{N} \to \mathbb{N} \text{ que recebendo um } x, \text{ retorna } w + x.$$

Ou, equivalentemente:

$$F(w) = \text{aquela função } g : \mathbb{N} \to \mathbb{N} \text{ definida pela } g(x) = w + x.$$

Que tipo de objetos a função F retorna? Funções! Nesse caso determinamos exatamente para qualquer entrada dela, qual seria a função que vai ser retornada. Observe que na definição de $F(w)$, apareceu a frase «aquela função $g \ldots$ ». Assim baptizamos temporariamente essa função com um nome ("g") à toa: apenas para referir a ela e retorná-la. Usando a λ-notação, essa definição fica mais direta, mais elegante, e (logo) mais legível:

$$F(w) = \lambda x \,.\, w + x \ : \mathbb{N} \to \mathbb{N}.$$

Observe que no lado direito aparece uma função anônima.

- **EXEMPLO 9.109 (em Python).**
Em Python podemos (ainda bem...) por exemplo escrever:

```
1  def F(w):
2
3      # define the function that will be returned
4      def g(x):
5          return w + x
6
7      # at this point a function g has been defined
8
9      # return it
10     return g
```

que corresponde na primeira maneira de definir a F, criando e nomeando a função para ser retornada. Podemos com λ também:

```
1  def F(w):
2      return (lambda x: w + x)
```

Não ficou melhor?

? **Q9.110. Questão.** Que tipo de coisa é o $F(25)$?

!! SPOILER ALERT !!

9.111. Antes de responder nessa pergunta, vamos responder numa outra, ainda mais específica: quem *é* o $F(25)$? Ou seja:

$$F(25) = \ldots ?\ldots$$

Não precisamos pensar nada profundo! Vamos apenas *copiar fielmente* sua definição (no lado depois do '='), substituindo cada ocorrência de w, por 25:

$F(25) =$ aquela função $g : \mathbb{N} \to \mathbb{N}$ que recebendo um $x \in \mathbb{N}$, retorna o número $25 + x$.

Ou seja,

$$F(25) : \mathbb{N} \to \mathbb{N}.$$

Sendo função, podemos chamá-la com um argumento do certo tipo, por exemplo como o $3 \in \mathbb{N}$, e evaluá-la:

$$(F(25))(3) = 28.$$

▸ **EXERCÍCIO x9.30.**
De onde chegou esse 28? (x9.30 H 0)

▸ **EXERCÍCIO x9.31.**
Escreva λ-expressões que podem ser consideradas como funções com os tipos seguintes:

$$\begin{aligned} F_1 &: \mathbb{R} \to \mathbb{R} \\ F_2 &: \mathbb{R} \to (\mathbb{R} \to \mathbb{R}) \\ F_3 &: (\mathbb{R} \to \mathbb{R}) \to \mathbb{R} \\ F_4 &: (\mathbb{R} \to \mathbb{R}) \to (\mathbb{R} \to \mathbb{R}) \\ F_5 &: (\mathbb{R}^2 \to \mathbb{R}) \to \mathbb{R} \\ F_6 &: (\mathbb{R}^2 \to \mathbb{R}) \to (\mathbb{R} \to (\mathbb{R} \to \mathbb{R})). \end{aligned}$$

(x9.31 H 0)

▸ **EXERCÍCIO x9.32.**
Escreva λ-expressões que podem ser consideradas como funções com os tipos seguintes, onde A, B, C são conjuntos sobre quais tu não podes supor absolutamente nada mais! Para cada um dos tipos, tente escrever as mais λ-expressões realmente diferentes que tu

consegues. Cuidado: para uns deles não é possível achar nenhuma!

$$
\begin{aligned}
&: A \to B \\
&: A \to (B \to A) \\
&: A \to (B \to B) \\
&: (A \to A) \to A \\
&: A \to (A \to A) \\
&: A \to \big(B \to ((A \to B) \times (A \cup C) \times \mathbb{N})\big) \\
&: (A \to (B \to C) \to ((A \times B) \to C)) \\
&: ((A \times B) \to C) \to (A \to (B \to C))
\end{aligned}
$$

(x9.32 H 0)

9.112. First-class citizens. O slogan aqui é que funções são *first-class citizens*. Trabalhando no Exercício x9.23, o último cálculo chega no valor seguinte:

$$
\begin{aligned}
(\lambda x\,.\,(\lambda x\,.\,x+1)\;1\cdot\underline{(\lambda y\,.\,xy)\;4}) &\;\triangleright_\lambda\; (\lambda x\,.\,\underline{(\lambda x\,.\,x+1)\;1}\cdot x\cdot 4) \\
&\;\triangleright_\lambda\; (\lambda x\,.\,(1+1)\cdot x\cdot 4)) \\
&\;=\; (\lambda x\,.\,8x).
\end{aligned}
$$

Como falei na resolução, se esse "resultado" (valor final) não parece satisfatório, é por causa de um preconceito teu que favorece os objetos de tipo "número" contra os objetos de tipo "função". Os números têm o direito de ser valores finais; e as funções também têm! Esse "preconceito" é bastante alimentado por causa de varias linguagens de programação que realmente não tratam as funções em termos iguais com os outros tipos. Em C, C++, ou Java, por exemplo, não é possível passar como argumentos funções, nem retorná-las; mas claramente números podem ser argumentos e também podem ser retornados como saída de funções. Por outro lado, linguagens como Haskell, Agda, Idris, PureScript, Racket, Clojure, Scala, Python, etc., adoptam o slogan

«functions are first-class citizens»

ou seja, lá temos funções de ordem superior—e logo, felicidade.

Funções de ordem superior não é algo tão desconhecido como talvez parece. O leitor já está acostumado com os operadores nos exemplos seguintes:

- **EXEMPLO 9.113 (Composição).**
  Sejam conjuntos A, B, C. O operador da composição $\circ$ (cuja notação decoramos aqui para especificar o domínio e codomínio dele e dos seus argumentos) é o seguinte:

  $$- \circ_{A\to B\to C} - : \big((B \to C) \times (A \to B)\big) \to (A \to C).$$

  Observe que ele é um operador de ordem superior, pois seus (dois) argumentos são funcões, e também pois sua saída também é uma função.

  Definimos agora a função *eval* que faz algo bem simples: aplica seu primeiro argumento (que deve ser uma função) no seu segundo (que deve ser um ponto do domínio do primeiro argumento).

D9.114. Definição (eval). Dados conjuntos A, B definimos a função

$$\begin{aligned} \mathit{eval} &: \big((A \to B) \times A\big) \to B \\ \mathit{eval}(f, a) &= f(a). \end{aligned}$$

Chamamos essa função de *evaluação* ou *avaliação*. Como fizemos na composição, decoramos essa operação escrevendo $\mathit{eval}_{A\to B}$ para esclarecer os conjuntos envolvidos, mas escrevemos simplesmente eval quando os A, B são implícitos pelo contexto.

• **EXEMPLO 9.115.**
Dados conjuntos A, B, a $\mathit{eval}_{A\to B}$ é claramente uma operação de ordem superior.

‣ **EXERCÍCIO x9.33.**
Sejam $f : A \to B$ e $X \subseteq A$. Ache o tipo dos:

$$\begin{aligned} f \restriction - &: ? \\ (- \restriction X) \restriction (A \to B) &: ? \end{aligned}$$

(x9.33 H 0)

• **EXEMPLO 9.116 (Derivação).**
Considere o operador da derivação D. Por exemplo, se $f(x) = x^3 + 5x$, temos

$$\mathrm{D}(f) = g, \quad \text{onde } g(x) = 3x^2 + 5.$$

Cuidado, não escrevemos aqui $\mathrm{D}(f) = 3x^2 + 5$, mas podemos escrever

$$\mathrm{D}(f) = \lambda x \,.\, 3x^2 + 5$$

sim. Qual o tipo da própria D? Ela recebe e retorna funções de reais para reais, mas não podemos tipá-la

$$\mathrm{D}(-) : (\mathbb{R} \to \mathbb{R}) \to (\mathbb{R} \to \mathbb{R})$$

pois estaríamos perdendo a totalidade da D: tem funções no $(\mathbb{R} \to \mathbb{R})$ que não são deriváveis. Ainda mais, seria legal poder iterar o D (Definição D9.150) à vontade. Logo tipamos assim:

$$\mathrm{D}(-) : \mathrm{C}^\infty \to \mathrm{C}^\infty$$

onde C^∞ é o conjunto de todas as funções infinitamente deriváveis: são deriváveis, e suas derivadas também são, e suas derivadas também, etc.

9.117. Teaser (funções parciais). Mas talvez queremos mesmo considerar a D como uma operação que opera no conjunto $(\mathbb{R} \to \mathbb{R})$ *sacrificando* a totalidade. Chegamos assim no conceito de *função parcial*, que voltamos a investigar na Secção §219.

• **EXEMPLO 9.118 (Integração).**
Sejam $a, b \in \mathbb{R}$ com $a < b$ e seja

$$\mathrm{R}[a,b] \stackrel{\mathsf{def}}{=} \{\, f : [a,b] \to \mathbb{R} \mid f \text{ é Riemann-integrável} \,\}.$$

Observe que $\mathrm{R}[a,b]$ é um conjunto de funções. Definimos o operador

$$\lambda f \,.\, \lambda x \,.\, \int_a^x f : \mathrm{R}[a,b] \to ([a,b] \to \mathbb{R})$$

cujo argumento é uma função—e ainda mais, sua saída também é uma função—e logo ele é um operador de ordem superior também. Para a integração "indefinita" (antiderivadas), seja

$$R \stackrel{\mathsf{def}}{=} \{\, f : \mathbb{R} \to \mathbb{R} \mid f \text{ é Riemann-integrável} \,\}$$

e defina o operador

$$\int - : R \to \wp(\mathbb{R} \to \mathbb{R})$$

onde $\int f$ é o conjunto das antiderivadas da F:

$$\int f = \{\, F : \mathbb{R} \to \mathbb{R} \mid \mathrm{D}\,(F) = f \,\}.$$

Observe que a notação comum em análise é diferente: usamos por exemplo $\int_a^x f(t)\,dt$, e o $\int f$ é visto como uma antiderivada (que depende duma constante) e não como o conjunto de todas essas antiderivadas como definimos aqui.

§208. Currificação

9.119. Ha-ha! Minha linguagem é melhor que a tua. Imagine que um amigo definiu uma função $f : \mathbb{Z}^2 \to \mathbb{Z}$ trabalhando numa linguagem de programação que não permite definições de funções de ordem superior. Queremos escrever um programa equivalente ao programa do nosso amigo numa outra linguagem que permite sim definir funções de ordem superior mas não funções de aridade maior que 1. Mesmo assim nossas funções podem *chamar* a função f do nosso amigo nos seus corpos.

? **Q9.120. Questão.** Como fazer isso?

!! SPOILER ALERT !!

9.121. Resposta em Python. Aqui uma resposta, escrita em Python.

```
# assume that f is given
def f(x,y):
    pass

# without lambdas
def F(x):
    def tmp(y):
        return f(x,y)
    return tmp

# with lambdas
def F(x):
    return lambda y: f(x,y)
```

Para computar a `f(x,y)` usando a `F`, usamos a `F(x)(y)`, ou seja, `(F(x))(y)`.

TODO Explicar o que acontece

▸ **EXERCÍCIO x9.34.**
Resolva o problema converso: começando com a função de ordem superior F, defina sua versão f (de aridade 2). (x9.34H0)

9.122. Currificação. A maneira que conseguimos utilizar funções de ordem superior mas de aridade 1, para "emular" funções de aridades maiores é chamada *currificação*, em homenagem ao Haskell Curry.[63] No exemplo acima dizemos que *F é a currificação da da f*, ou *sua versão currificada*.

? **Q9.123. Questão.** Usando a λ-notação como podemos definir funções *curry*, *uncurry* para a situação mais genérica onde a função de dois argumentos é do tipo $(A \times B) \to C$?

!! SPOILER ALERT !!

9.124. Resposta. Primeiramente vamos nos preocupar com os tipos dessas funções. São assim:

$$((A \times B) \to C) \underset{uncurry}{\overset{curry}{\rightleftarrows}} (A \to (B \to C))$$

Temos então

$$curry : ((A \times B) \to C) \longrightarrow (A \to (B \to C))$$

definida pela

$$curry(\ldots?$$

[63] O próprio Curry atribuiu o conceito ao Schönfinkel, mas Frege já tinha usado isso antes.

Como denotar o arbitrário membro do seu domínio ($(A \times B) \to C$)? Sendo uma função, vou escolher denotá-lo por f. Ajuda. Voltamos então:

$$curry(f) = \ldots?$$

Que tipo de coisa estamos tentando *construir* no lado direito? Pelo tipo da *curry*, deve ser uma função de A para $(B \to C)$. E o que tenho na minha disposição? Neste ponto apenas a f. Facilita escrever claramente todas as coisas disponíveis e seus tipos. Então por enquanto tenho apenas

$$f : (A \times B) \to C.$$

E eu quero construir uma função de tipo $A \to (B \to C)$. Para defini-la preciso deixar claro o seu comportamento então:

$$curry(f) = \lambda \ldots?$$

Como denotar a arbitrária entrada dessa função? Bem, sendo uma função com domínio A, vou escolher denotar seu argumento por a:

$$curry(f) = \lambda a \,.\, \ldots?$$

A mesma pergunta: o que eu ganhei e o que tipo de coisa preciso construir agora? Ganhei um $a : A$, e preciso construir algo do tipo $B \to C$, ou seja, uma função (então vou começar com um $\lambda \ldots$) que recebe B's (então $\lambda b \,.\, \ldots$) e retorna C's:

$$curry(f) = \lambda a \,.\, \lambda b \,.\, \ldots?$$

Aqui preciso construir um C'zinho e eu tenho:

$$\begin{aligned} f &: (A \times B) \to C \\ a &: A \\ b &: B \end{aligned}$$

Fácil! Pois eu tenho um fornecedor de C's, e ele só precisa de um par de um A'zinho e um B'zinho para funcionar—pun intended—e felizmente eu tenho ambos, e logo

$$f(a, b) : C$$

Com isso consigo finalmente terminar:

$$curry(f) = \lambda a \,.\, \lambda b \,.\, f(a, b).$$

Deixo a definição da *uncurry* pra ti:

▸ **EXERCÍCIO x9.35.**
Defina a *uncurry*. (x9.35H12345)

9.125. Árvore de inferência de tipo. A última parte da argumentação acima corresponde na árvore de inferência seguinte:

$$\dfrac{f : A \times B \to C \qquad \dfrac{x : A \qquad y : B}{(x, y) : A \times B}}{f(x, y) : C}$$

Verifique cada passo, e acostume-se com essa forma!

▸ **EXERCÍCIO x9.36 (Acostume-se mesmo).**
Construa a árvore que corresponde na última parte da tua resolução do Exercício x9.35 caso que tu não fez isso já enquanto o resolvendo. (x9.36 H 0)

9.126. Associatividade sintáctica. Considere que temos uma operação binária ♡. A frase

«♡ é associativa»

é uma *afirmação matemática:*

$$\text{para todo } x, y, z, \quad (x \heartsuit y) \heartsuit z = x \heartsuit (y \heartsuit z).$$

Isso é algo que pode ser demonstrado, suposto, refutado, etc. Por outro lado, considere as frases seguintes:

«♡ é associativa na esquerda»	«♡ é associativa na direita»
«♡ associa na esquerda»	«♡ associa na direita»
«♡ é L-associativa»	«♡ é R-associativa»

Nenhuma dessas frases é algo que podemos demonstrar, refutar, ou supor! O que significam então? Apenas uma convenção sintáctica, que dá significado às expressões como a '$x \heartsuit y \heartsuit z$' que sem uma associatividade sintáctica não denotam absolutamente nada (pois têm um erro de aridade). As frases acima então correspondem respectivamente nas:

$$x \heartsuit y \heartsuit z \stackrel{\text{def}}{\equiv} (x \heartsuit y) \heartsuit z \qquad\qquad x \heartsuit y \heartsuit z \stackrel{\text{def}}{\equiv} x \heartsuit (y \heartsuit z).$$

! **9.127. Aviso.** Às vezes abusarei essa idéia e escrever o nome duma função currificada mas usá-la como se ela não fosse; e vice-versa. Por exemplo, defini (D9.114) a $eval_{A\to B}$ como uma função

$$eval_{A\to B} : ((A \to B) \times A) \to B.$$

Ou seja, para chamá-la escrevemos

$$eval_{A\to B}(f, a).$$

Mas (abusando a notação!) posso considerar o mesmo símbolo $eval_{A\to B}$ para denotar sua currificação

$$eval_{A\to B} : (A \to B) \to A \to B$$

que *é uma função diferente sim*, nesse caso escrevendo

$$eval_{A\to B}\ f\ a.$$

Tudo isso apenas no caso que pelo contexto tá claríssimo qual das duas funções tá sendo denotada.

TODO notação de "aridades maiores" currificada

9.128. Olhos humanos e os tipos higher-order.

TODO Escrever

9.129. Aplicação parcial e currificação.

TODO Escrever

- **EXEMPLO 9.130 (powTwo).**
Definimos a função $powTwo : \mathbb{N} \to \mathbb{R}$ pela

$$powTwo = exp\, 2.$$

Assim $powTwo\, 0 = 1$, $powTwo\, 10 = 1024$, etc.

9.131. Observação (Parece cancelamento).

TODO Escrever

§209. Novas implementações: seqüências e famílias

? **Q9.132. Questão.** Suponha que alguém robou de ti os tipos (primitivos) de seqüências e de famílias indexadas. Dá para se virar sem esses? Ou seja, tem como defini-los em termos dos outros tipos que tu (ainda) tens?

!! SPOILER ALERT !!

Resposta. Agora que temos funções, podemos apreciar que qualquer seqüência $(a_n)_n$ *pode ser representada por uma função* com domínio $\mathbb{N}$ e codomínio o conjunto de todos os membros da $(a_n)_n$. Similarmente, uma família $(\, a_i \mid i \in \mathcal{I}\,)$ indexada por um conjunto $\mathcal{I}$ *pode ser representada por uma função* com domínio $\mathcal{I}$ e codomínio o conjunto de todos os membros da $(a_i)_i$.

D9.133. Implementação (Seqüências como funções). Chamamos qualquer função $a : \mathbb{N} \to A$ de *seqüência de A*. Introduzimos como açúcar sintáctico o

$$a_n \overset{\text{sug}}{\equiv} a(n).$$

Com essa definição, quando duas seqüências de A são iguais? Elas precisam concordar em cada $n \in \operatorname{dom} a$; e essa implementação atende a especificação pois concorda com a definição de igualdade do tipo que estamos implementando (Definição D8.126).

D9.134. Implementação (Famílias indexadas como funções). Chamamos qualquer função $a : \mathcal{I} \to A$. de *família de A indexada por* $\mathcal{I}$. Introduzimos como açúcar sintáctico o

$$a_i \overset{\text{sug}}{\equiv} a(i).$$

Com essa definição, quando duas tais famílias são iguais? Os conjuntos de índices precisam ser iguais, e as famílias precisam concordar em cada índice. Essa implementação atende a especificação pois concorda com a definição de igualdade do tipo que estamos implementando (Definição D8.143).

▸ **EXERCÍCIO x9.37.**
Implemente as tuplas; tome cuidado para deixar claro como usá-las; lembre-se o que elaboramos nas secções §186, §187, §188, e §189. (x9.37 H 0)

▸ **EXERCÍCIO x9.38.**
Implemente os multiset (§191); tome cuidado para deixar claro como usá-las; lembre-se o 8.136. (x9.38 H 0)

D9.135. Definição (Conjuntos indexados: versão adulta). Já conhecemos o que significa que um conjunto A é indexado por um conjunto B (Definição D8.146). Isso praticamente quis dizer que o A pode ser escrito na forma

$$A = \{\, \ldots b \ldots \mid b \in B \,\},$$

ou, mais "adultamente" e plenamente:

$$A \text{ é indexado por } B \overset{\text{def}}{\iff} \text{existe função sobrejetora } f : B \twoheadrightarrow A.$$

Intervalo de problemas

▸ **PROBLEMA Π9.1 (iniciais e terminais teaser).**
(1) Quais conjuntos S (se algum) têm a propriedade seguinte?:

$$\text{para todo conjunto } A, \text{ existe única função } f : S \to A.$$

(2) Quais conjuntos T (se algum) têm a propriedade seguinte?:

$$\text{para todo conjunto } A, \text{ existe única função } f : A \to T.$$

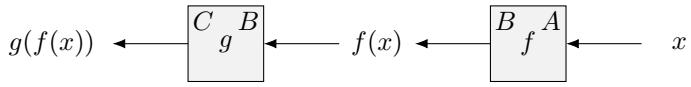
(Π9.1 H 0)

§210. Composição

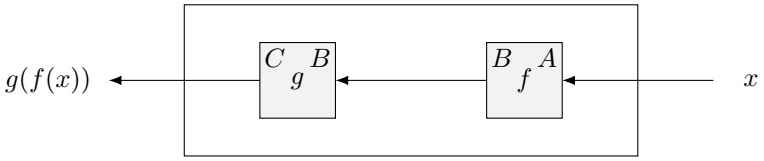
9.136. Composição com black boxes. Suponha que temos uma configuração de conjuntos e funções assim:

$$A \xrightarrow{f} B \xrightarrow{g} C.$$

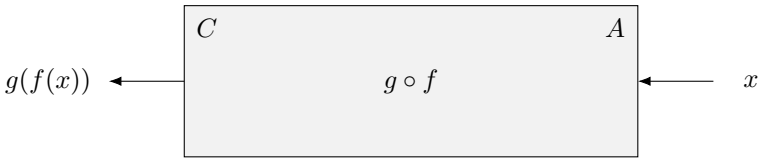
Note então que a saída da f pode ser usada como entrada para a g:



Podemos criar um novo black box, conectando os "cabos" assim:



Pintamos preta essa construção, botando os rótulos certos de domínio e codomínio, e pronto:



Criamos assim a composição $g \circ f$ das funções f e g. Formalmente, chegamos na definição seguinte.

D9.137. Definição. Sejam $A \xrightarrow{f} B \xrightarrow{g} C$. Definimos a função $g \circ f : A \to C$ pela

$$(g \circ f)(x) \stackrel{\text{def}}{=} g(f(x)).$$

Assim temos

$$\operatorname{dom}(g \circ f) = \operatorname{dom} f \qquad\qquad \operatorname{cod}(g \circ f) = \operatorname{cod} g.$$

Chamamos a $g \circ f$ a *composição* da g com f. Pronunciamos a $g \circ f$ também como: «g seguindo f», «g after f», ou até «g de f».

! **9.138. Cuidado.** Escrevemos $g \circ f$ e não $f \circ g$ para a composição na Definição D9.137! Então quando temos $A \xrightarrow{f} B \xrightarrow{g} C$, a composição é $A \xrightarrow{g \circ f} C$, que parece o oposto da ordem das setinhas. Definimos a notação alternativa

$$f \,;\, g \stackrel{\text{sug}}{=} g \circ f,$$

chamada *notação diagramática* pois concorda com a posição das setinhas do diagrama:

$$A \xrightarrow{f;g} C.$$

Mas vamos principalmente usar a notação $g \circ f$ mesmo.

▸ **EXERCÍCIO x9.39.**
Sejam $A \xrightarrow{f} B \xrightarrow{g} C$. Qual função é a $f \circ g$? (x9.39 H 0)

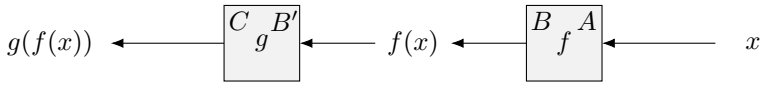
9.139. Por que não compor mais?. Sejam $f : A \to B$ e $g : B' \to C$, e suponha que $B \subsetneq B'$. É tentador definir uma função de composição $g \circ f : A \to C$ pela

$$(g \circ f)(x) = g\big(f(x)\big) \quad \text{para todo } x \in A.$$

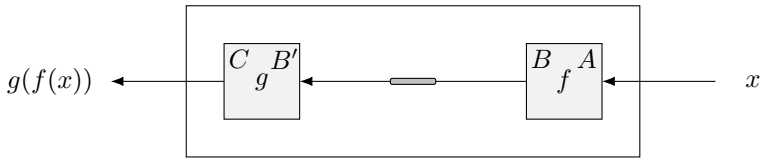
No final das contas, para qualquer $x \in A$ temos $f(x) \in B$ e como $B \subsetneq B'$, também temos $f(x) \in B'$. Então $g(f(x))$ é definido! Então por que não relaxar pouco a restricção que temos na definição da composição

$$\text{de} \quad \operatorname{cod} f = \operatorname{dom} g \quad \text{para} \quad \operatorname{cod} f \subseteq \operatorname{dom} g \quad ?$$

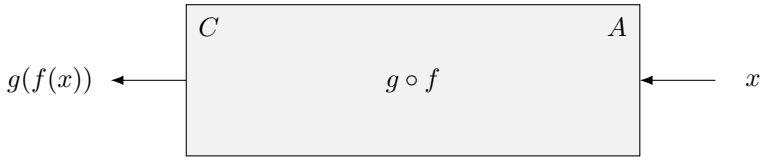
Usando black boxes, temos as funções



e queremos "conectar os cabos" para criar um novo black box



pintar ele preto e considerar como a $g \circ f$ de A para C mesmo:



Qual o problema com isso? «Nenhum», disse o Conjuntista orgulhoso. E realmente muitos matemáticos responderiam a mesma coisa—até uns irreligiosos—e ficariam usando esse tipo de composição "mais geral". Mas para a gente aqui, vamos supor que para motivos que não importam—talvez religiosos, ou um TOC mesmo—*não podemos* conectar esse cabo no meio quando os conjuntos são diferentes:

$$\textit{«Não comporás funções } g \textit{ e } f \textit{ se } \operatorname{cod} f \neq \operatorname{dom} g\textit{!»}$$

Essa suposta restricção, na verdade não nos restringe—pelo contrário: nos ajuda criar composições "limpas" sem gambiarras como essa "fita durex" no cabo conectando o B com o B'! Trabalhe agora no exercício seguinte para demonstrar exatamente isso!

▸ **EXERCÍCIO x9.40.**
Mostre como construir a função criada no Nota 9.139 como composição de black boxes que contenha as f e g mas sem nenhuma conexão "proibida". (x9.40 H 1 2)

9.140. Preguiça (clareza!) na notação funcional. Como tu já se acostumou—eu espero—às vezes denotamos a aplicação duma função no seu argumento silenciosamente, ou seja, por *justaposição:* escrevemos fx em vez do (mais comum em matemática clássica) $f(x)$. Agora que temos *uma operação padrão* entre funções queremos pegar emprestada a mesma preguiça e denotar por justaposição a composição também:

$$\text{`}fg\text{'} \qquad \text{quis dizer} \qquad \text{`}f \circ g\text{'}.$$

Com essa convenção, o que seria o 'fgx'? Acontece que ambas as interpretações

$$\text{`}(fg)x\text{'} \qquad \text{ou} \qquad \text{`}f(gx)\text{'}$$

são iguais nesse caso (deu sorte *extensional*), mas *intensionalmente* falando elas correspondem nas notações tradicionais

$$\text{`}(f \circ g)(x)\text{'} \qquad \text{e} \qquad \text{`}f(g(x))\text{'}$$

respectivamente. E até pior—nossa preguiça não tem fim—entre números também temos uma operação padrão que denotamos por justaposição:

$$xy \qquad \text{é o produto} \qquad x \cdot y.$$

E supondo que $f, g : \mathbb{R} \to \mathbb{R}$ e $x, y \in \mathbb{R}$, a expressão '$gfxy$' denota o quê? Sem parenteses, nada, por isso vamos escrever

$$\text{`}g\ f\ (xy)\text{'} \qquad \text{ou} \qquad \text{`}(gf)(xy)\text{'}$$

que (ambas!) denotam o

$$(g \circ f)(x \cdot y)$$

que é igual ao $g(f(x \cdot y))$ pela definição da $\circ$. Eu vou ficar misturando a notação mais tradicional e a notação mais "funcional" dependendo do contexto e assim vamos se acostumar com ambas.

Bora ver uns exemplos para resumir:

- **EXEMPLO 9.141.**
Sejam $f, g, h : \mathbb{R} \to \mathbb{R}$ e $x, y \in \mathbb{R}$. Usando '$\equiv$' para igualdade sintáctica e '$=$' para igualdade semántica (veja Secção §14) temos:

$$\begin{aligned}
fx &\equiv f(x) \\
(fg)x &\equiv (f \circ g)(x) = f(g(x)) \\
f(gx) &\equiv f(g(x)) \\
fgh &\equiv (f \circ g \circ h) \\
f(ghx) &\equiv f((g \circ h)(x)) = f(g(h(x))) \\
(fg)h(xy) &\equiv ((f \circ g) \circ h)(x \cdot y) = (f \circ g)(h(x \cdot y)) = f(g(h(x \cdot y))).
\end{aligned}$$

Espero que ficou claro.

▸ **EXERCÍCIO x9.41 (Composição respeita "-jectividade").**
Sejam $f : A \to B$ e $g : B \to C$. Demonstre:
(1) Se f e g são injetoras, então $g \circ f$ também é;
(2) Se f e g são sobrejetoras, então $g \circ f$ também é;
(3) Se f e g são bijetoras, então $g \circ f$ também é. (x9.41 H 0)

▸ **EXERCÍCIO x9.42.**
Se $g \circ f$ é bijetora, o que podemos concluir sobre as f, g? Justifique. (x9.42 H 0)

▸ **EXERCÍCIO x9.43.**
Se f é injetora e g sobrejetora, a $g \circ f$ é necessariamente bijetora? (x9.43 H 0)

§211. Funções de graça

Investigamos aqui umas funções garantidas de existir assim que tivermos alguns outros objetos: conjuntos, funções, etc.

D9.142. Definição (Identidade). Seja A conjunto. A função $\lambda x \,.\, x : A \to A$ é chamada *identidade do A*. Denotamos a identidade do conjunto A por $\mathrm{id}_A : A \to A$ ou $1_A : A \to A$.

! **9.143. Cuidado («uma» ou «a»).** Podemos falar *da* função identidade? Não, pois para usar o artigo definido precisamos *unicidade* e não existe uma única «função identidade». Pelo contrário: para cada conjunto A, temos uma função identidade: a identidade *do A*.

D9.144. Definição (Inclusão). Sejam A, B conjuntos com $A \subseteq B$. A função $\lambda x \,.\, x : A \to B$ é chamada *inclusão do A no B*. Usamos o $\imath$ para denotar uma inclusão e escrevemos

$$\imath : A \hookrightarrow B \qquad \text{ou} \qquad \imath : A \xhookrightarrow{\subseteq} B \qquad \text{ou até} \qquad \imath : A \subseteq B$$

para enfatizar que é uma inclusão mesmo. Decoramos a notação escrevendo $\imath_{A \hookrightarrow B}$ quando essa informação não é implícita pelo contexto. Todos os $i, \imath, \iota$ são símbolos freqüentemente usados para denotar inclusões.

9.145. Observação. Note que seguindo o ponto de vista categorial (D9.26), se $A \subsetneq B$ então $\imath_{A \hookrightarrow B} \neq \mathrm{id}_A$, mas seguindo o ponto de vista conjuntista (D9.25), temos $\imath_{A \hookrightarrow B} = \mathrm{id}_A$.

▸ **EXERCÍCIO x9.44.**
O Cuidado 9.143 afirmou que para conjuntos distintos temos identidades distintas. Isso é válido para o Conjuntista também? Ou é como o que descobrimos resolvendo o Exercício x9.21 sobre as funções vazias?: que para o Categorista tem muitas funções vazias (uma para cada conjunto) mas para o Conjuntista tem apenas uma única. Compare! (x9.44 H 1)

▸ **EXERCÍCIO x9.45.**
Verifique que composição de inclusões é inclusão. (x9.45 H 1)

! **9.146. Cuidado.** A notação $A \hookrightarrow B$ não sempre denota a própria inclusão; pode ser usada para denotar uma *injecção* diferente dependendo do contexto. A idéia é que mesmo sem ter $A \subseteq B$ pensamos que uma injecção determina uma cópia fiel do A dentro do B. Isso vai fazer muito mais sentido na §201, pois per enquanto nem sabemos o que significa «injecção»!

D9.147. Definição (constante; invariável). Dados conjuntos A, B, e $b \in B$, definimos a função $\mathrm{k}_b : A \to B$ pela

$$\mathrm{k}_b(x) = b.$$

A k_b é chamada *função constante (do A para B) com valor b*. Aqui tanto seu domínio quanto se codomínio estavam claros pelo contexto então não precisamos sobrecarregar nossa notação com muitas decorações. Quando não são e quando importam escrevemos k_b^A ou até $\mathrm{k}_b^{A,B}$. Dizemos que uma função $f : A \to B$ é *constante* sse ela é constante com valor b para algum $b \in B$:

$$f : A \to B \text{ constante} \overset{\text{def}}{\iff} (\exists b \in B)[\, f = \mathrm{k}_b \,].$$

Chamamos uma função de *invariável* (ou *steady*) sse ela mapeia todos os membros do seu domínio para o mesmo objeto. Formulamente,

$$f : A \to B \text{ invariável} \overset{\text{def}}{\iff} (\forall x, y \in A)[\, f(x) = f(y) \,].$$

! **9.148. Cuidado (O termo "constante").** Muitos textos usam o termo "constante" para descrever o que chamamos de "invariável" (ou "steady"). Na maioria dos casos não existe confusão, pois as duas definições concordam. Mas precisamos tomar cuidado, como tu vai descobrir agora fazendo o Exercício x9.46.

▸ **EXERCÍCIO x9.46.**
Às vezes aparece como definição de constante a seguinte: *«A função $f : A \to B$ é constante sse mapeia todos os membros do seu domínio para o mesmo objeto.»* Essa definição é equivalente com a Definição D9.147? Ou seja, com nossa terminologia aqui:

$$f \text{ invariável} \overset{?}{\iff} f \text{ constante}.$$

(Verifique ambas as direcções.) (x9.46 H 1)

▸ **EXERCÍCIO x9.47.**
Uma função $f : A \to B$ pode ser constante com valor b e com valor b' também, com $b \neq b'$? (x9.47 H 1)

▸ **EXERCÍCIO x9.48.**
Sejam $A \xrightarrow{f} B$ com $A \neq \emptyset$. Demonstre que:

$$f \text{ constante} \iff (\exists b \in B)(\forall x \in A)[\, f(x) = b \,].$$

(x9.48 H 0)

▸ **EXERCÍCIO x9.49.**
No caso geral, alguma das direções da Exercício x9.48 é válida ainda? (x9.49 H 0)

▸ **EXERCÍCIO x9.50.**
Demonstre ou refute a afirmação seguinte: *se* $(g \circ f)$ *é constante, então pelo menos uma das* f, g *também é.* (x9.50 H 1)

▸ **EXERCÍCIO x9.51.**
O que é errado na definição seguinte de função constante?

$$f : A \to B \text{ constante} \overset{\text{def}}{\iff} (\forall a \in A)(\exists b \in B)[\, f(a) = b\,].$$

Será que substituindo o $\exists$ por $\exists!$ o problema tá resolvido? Sugira uma outra resolução simples. (x9.51 H 1)

9.149. Definindo funções como composições. Como $(\circ)$ é uma operação de funções, ganhamos então mais uma maneira de definir funções. Dadas componíveis funções $A \xrightarrow{f} B \xrightarrow{g} C$ podemos definir uma função $h : A \to C$ apenas escrevendo:

$$\text{«Seja } h = g \circ f.\text{»}$$

Claramente (e seguindo a discussão no 9.78) não precisamos dar um nome para essa função. Podemos apenas falar sobre a $g \circ f$, exatamente no mesmo jeito que falamos do número $2 \cdot 8$ sem precisar dar um nome pra ele!

D9.150. Definição (iterações). Seja $f : A \to A$. Definimos as *iterações* de f pela recursão

$$\begin{aligned} f^0 &= \mathrm{id}_A \\ f^{n+1} &= f \circ f^n. \end{aligned}$$

• **EXEMPLO 9.151.**
Seja $f : A \to A$. Calculamos:

$$\begin{aligned} f^3(x) &= (f \circ f^2)(x) && \text{(def. } f^3\text{)} \\ &= (f \circ (f \circ f^1))(x) && \text{(def. } f^2\text{)} \\ &= (f \circ (f \circ (f \circ f^0)))(x) && \text{(def. } f^1\text{)} \\ &= (f \circ (f \circ (f \circ \mathrm{id}_A)))(x) && \text{(def. } f^0\text{)} \\ &\overset{\cdots}{=} (f \circ f \circ f)(x) && \text{(ass. } \circ\text{; lei da } \mathrm{id}_A\text{)} \\ &\overset{\cdots}{=} f(f(f(x))) && \text{(def. } \circ\text{)} \end{aligned}$$

Em geral omitimos parenteses quando a expressão envolve apenas uma operação associativa; botamos aqui para enfatizar cada aplicação de definição nesse cálculo.

▸ **EXERCÍCIO x9.52.**
Como definarias numa maneira simples a função $succ^3$ para alguém que não sabe (e sequer quer saber) o que são as iterações duma função? (x9.52 H 0)

! **9.152. Cuidado.** Em certos textos de matemática, aparece a notação $f^n(x)$ como sinónimo de $(f(x))^n$. Por exemplo:

quem escreveu...	$\sin^2 x + \cos^2 x$	...quis dizer...	$(\sin x)^2 + (\cos x)^2$
		...mas aqui seria...	$\sin(\sin x) + \cos(\cos x)$.

9.153. Observação. Poderiamos ter escolhido definir as potências de f pelas:

$$f^0 = \mathrm{id}_A$$
$$f^{n+1} = f^n \circ f$$

em vez da recursão que usamos na Definição D9.150. As duas definições são equivalentes, ou seja, as duas operações de exponenciação definidas são iguais. Por enquanto pode aceitar isso como um fato que vamos demonstrar depois (Teorema Θ11.73), ou esquecer completamente essa definição alternativa.

Θ9.154. Teorema. *A operação de iteração que definimos no Definição D9.150 nos endomapas dum conjunto A satisfaz as leis:*

(1) $(\forall n, m \in \mathbb{N})(\forall f : A \to A)[\, a^{m+n} = a^m \circ a^n \,]$;
(2) $(\forall n, m \in \mathbb{N})(\forall f : A \to A)[\, a^{m\cdot n} = (a^m)^n \,]$;
(3) $(\forall n \in \mathbb{N})[\, \mathrm{id}^n = \mathrm{id} \,]$.

JÁ DEMONSTRADO. Demonstramos por indução as três leis nos exercícios x4.19, x4.20, e x4.21—se tu não resolveu, volte a resolver! Verifique que nossas demonstrações precisaram apenas a *associatividade* e a *identidade* da multiplicação e *nada da sua definição*, então podemos substituir a multiplicação por nossa $\circ$. Sobre a outra operação envolvida nas demonstrações, a adição, não precisamos verificar nada, pois nos dois casos é a mesma operação: a adição nos naturais. ∎

D9.155. Definição (Idempotente). Seja $f : A \to A$ um endomapa. Chamamos a f *idempotente* sse

$$f \circ f = f.$$

▸ **EXERCÍCIO x9.53.**
Seja A conjunto com $|A| = 3$. Quantas funções idempotentes podemos definir no A? (x9.53H123)

▸ **EXERCÍCIO x9.54.**
Seja $f : A \to A$. Demonstre ou refute a implicação:

$$f \text{ constante} \implies f \text{ idempotente}.$$

(x9.54H1)

D9.156. Definição (Característica). Sejam A conjunto e $C \subseteq A$. A *função característica do C no A* é a função $\chi_C^A : A \to \{0, 1\}$ definida pela

$$\chi_C^A(x) = \begin{cases} 1, & \text{se } x \in C; \\ 0, & \text{se } x \notin C. \end{cases}$$

Escrevemos apenas χ_C quando o domínio A é implícito pelo contexto—e na práctica esse é quase sempre o caso!

! **9.157. Aviso.** O uso de 1 para representar "true" e o 0 para o "false" é aleatório. De fato, dependendo de caso, às vezes definimos a função característica com esses valores invertidos! Isso é muito comum em teoria de recursão (veja **[Kle52]** por exemplo), mas não só: nos shells de Unix, também o valor 0 representa o "true" (ou "deu certo") e cada valor positivo o "false" (ou "deu errado").[64]

A moral da estória: sempre verifique a definição da função característica usada—e se quiseres usar num texto teu, sempre bota sua definição junto! Nesse texto, quando aparece a notação χ_C sem definição, denota a função que definimos acima na Definição D9.156.

▸ **EXERCÍCIO x9.55 (Para os Unixeiros).**
Num shell de Unix (cujo "prompt" denoto aqui por '`#`') escrevemos:

```
# cmd1 && cmd2
# cmd1 || cmd2
```

onde `cmd1` e `cmd2` são dois comandos. Explique o comportamento sabendo que `&&` e `||` denotam os operadores lógicos da conjunção e disjunção (respectivamente). Conclua que o shell de Unix é "apenas" um calculador de valores de verdade nesse sentido. Todas as coisas que vão acontecer executando isso "no mundo real" são nada mais que *side-effects* enquanto calculando os seus comandos, para achar seus valores de verdade. Como posso dar para o shell a ordem «executa o `cmd1` e depois o `cmd2`»? (x9.55 H 0)

9.158. Observação. Um dos usos comuns de funções características é definir funções num jeito mais curto, aproveitando os fato que $0x = 0$ e $1x = x$ para todo $x \in \mathbb{R}$. Esse uso lembra das expressões *if-then-else* que usamos em linguagens de programação.

• **EXEMPLO 9.159.**
Considere a $f : \mathbb{R} \to \mathbb{R}$ definida pela

$$f(x) = \begin{cases} 2\sqrt[3]{x + \log_2 |x+1|} + x^2, & \text{se } x \in \mathbb{Q} \\ 2\sqrt[3]{x + \log_2 |x+1|} + e^x, & \text{caso contrário.} \end{cases}$$

Usando as funções características de $\mathbb{Q}$ e $\mathbb{R} \setminus \mathbb{Q}$ podemos definir a f com uma equação só, e "sem repetição":

$$f(x) = 2\sqrt[3]{x + \log_2 |x+1|} + x^2 \chi_{\mathbb{Q}}(x) + e^x \chi_{\mathbb{R}\setminus\mathbb{Q}}(x).$$

Isso lembra um

$$f(x) = 2\sqrt[3]{x + \log_2 |x+1|} + \big(\textbf{if } x \in \mathbb{Q} \textbf{ then } x^2 \textbf{ else } e^x\big).$$

usado em linguagens de programação que suportam *if-then-else expressions*.

---

64 Nesse caso essa escolha é obviamente melhor, pois sabendo que "deu certo", em geral não perguntamos «por que deu certo?»; mas se der errado, queremos saber mais sobre o motivo que deu errado: talvez um arquivo não existe, talvez uma conexão não pode ser feita, talvez faltou uma permissão, etc., e cada um desses casos pode retornar um valor positivo diferente.

Esse "retornar" que eu tô me referindo aqui é o proprio `return` que muitas vezes estudando programação o aluno acaba memorizando como "regrinha" que sua `main` precisa terminar com um "`return 0`". Por quê? E pra quem que ta retornando isso? Para o próprio sistema operacional. No final das contas, foi ele que chamou essa `main`.

! **9.160. Cuidado (expressions vs. statements).** Uma *if-then-else expression* não é a mesma coisa com um *if-branching statement* encontrado em muitas linguagens de programação imperativas. A idéia é que uma expressão denota um valor; um statement é apenas uma ordem para ser executada. A linguagem C por exemplo tem ambas mas o que escrevemos em C com "`if...`" corresponde no branching *statement*. Nunca faria sentido em C, por exemplo, multiplicar um *if statement* por um número. A *expressão* if-then-else de C corresponde no seu único operador ternário, com a sintaxe (bizarra)

$$\texttt{(__?__:__)}.$$

Em Haskell, por outro lado, escrevemos mesmo

$$\texttt{if __ then __ else __}.$$

▸ **EXERCÍCIO x9.56.**
Sejam A, X conjuntos com $A \subseteq X$. Suponha que $\chi_A^X \circ \chi_A^X$ é definida. O que podes concluir sobre o X? Podemos concluir que a $\chi_A \circ \chi_A$ é constante ou a identidade? (x9.56 H 1)

D9.161. Definição (Restricção). Sejam $f : A \to B$ e $X \subseteq A$. A *restricção da f no X*, denotada por $f \restriction X$ é a função de X para B definida pela

$$(f \restriction X)\ x = f\ x.$$

Também é usada a notação $f|_X$.

▸ **EXERCÍCIO x9.57.**
Sejam $f : A \to B$ e $X \subseteq A$. Ache o tipo de $f \restriction X$. (x9.57 H 0)

▸ **EXERCÍCIO x9.58 (restrição sem pontos).**
Sejam A, B conjuntos e $X \subseteq A$. Defina a função $f \restriction X$ sem usar nenhuma referência aos membros desses conjuntos. Na Definição D9.161, por exemplo, usamos esse x para representar um mebro de A. (Esqueça o "sem pontos" no rótulo desse exercício; vai fazer sentido depois: §214.) (x9.58 H 1 2)

§212. Funções inversas

Informalmente, para construir a inversa duma função pegamos o seu diagrama interno, e viramos todas as setinhas barradas para a direção oposta. Vamos estudar essa idéia formalmente agora.

D9.162. Definição (função inversa). Seja função bijetora $f : A \rightarrowtail B$. Definimos a função $f^{-1} : B \to A$ pela

$$f^{-1}(y) \stackrel{\text{def}}{=} \text{aquele } x \in A \text{ que } x \overset{f}{\longmapsto} y.$$

Ou, *equivalentemente*, pela

$$f^{-1}(y) = x \iff^{\text{def}} f(x) = y.$$

Com outra notação:

$$y \overset{f^{-1}}{\longmapsto} x \overset{\text{def}}{\iff} x \overset{f}{\longmapsto} y.$$

Chamamos a f^{-1} a *função inversa* da f.

9.163. Observação (Os olhos humanos não são simétricos). Às vezes a direção em que a gente olha para uma igualdade faz diferença:

$$\alpha = \beta \iff \beta = \alpha$$

sim, ou seja, '$=$' é simétrica, mas nossos olhos humanos conseguem enxergar certas informações melhor na forma $\alpha = \beta$, e outras na forma $\beta = \alpha$! (Talvez nossos olhos não são tão simétricos.) A mesma coisa é sobre relações "direcionadas" como por exemplo:

$$\alpha \leq \beta \iff \beta \geq \alpha$$

que também são afirmações equivalentes, mas muitas vezes a gente enxerga uma numa maneira diferente da outra!

Na Definição D9.162 acima, por exemplo, reescrevendo a igualdade na outra direção temos:

$$f^{-1}(y) = x \overset{\text{def}}{\iff} y = f(x)$$

que possivelmente nos permite enxergar a situação numa maneira diferente. Similarmente, usando a notação das setinhas barradas podemos enxergar a equivalência assim:

$$x \overset{f^{-1}}{\longmapsto} y \overset{\text{def}}{\iff} x \overset{f}{\longmapsto} y.$$

▸ **EXERCÍCIO x9.59 (A inversa é bem-definida).**
Demonstre que a função f^{-1} foi bem-definida. O que precisas demonstrar? (x9.59 H 0)

▸ **EXERCÍCIO x9.60 (A inversa é bijetora).**
Demonstre que quando a função inversa f^{-1} é definida, ela é bijetora. (x9.60 H 1 2)

▸ **EXERCÍCIO x9.61 (Inversa da inversa).**
Demonstre que se a função inversa f^{-1} é definida, então a sua inversa $\left(f^{-1}\right)^{-1}$ também é e temos $\left(f^{-1}\right)^{-1} = f$. (x9.61 H 1 2)

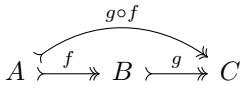
▸ **EXERCÍCIO x9.62 (Leis da inversa (com pontos)).**
Seja $f : A \rightarrowtail B$. Para todo $a \in A$ e todo $b \in B$, temos:

$$\text{(L)} \qquad f^{-1}(fa) = a \qquad\qquad f(f^{-1}b) = b. \qquad \text{(R)}$$

(x9.62 H 0)

▸ **EXERCÍCIO x9.63 (Inversa da identidade).**
Para todo conjunto A, ${\mathrm{id}_A}^{-1} = \mathrm{id}_A$. (x9.63 H 0)

? **Q9.164. Questão.** Queremos descrever a inversa duma composição de bijecções em termos das inversas dessas bijecções. Ou seja, temos a configuração seguinte:



Agora, já que $g \circ f$ é bijetora, sabemos que possui inversa. O desafio é descrevê-la em termos das f^{-1} e g^{-1}. Como o farias?

!! SPOILER ALERT !!

! **9.165. Cuidado.** Um erro comum é afirmar que $(g \circ f)^{-1} = g^{-1} \circ f^{-1}$. Por que isso não faz sentido? Pense em funções como "processos" e na $g \circ f$ como o processo «faça f e depois faça g». Como exemplo, considere f o «botar cueca» e g o «botar shorts». Logo $g \circ f$ é o processo «botar a cueca e depois botar os shorts». Assim, qual processo seria o $g^{-1} \circ f^{-1}$? «Tirar a cueca e depois tirar os shorts.» O erro é óbvio: esquecemos de invertar a ordem das acções (Mais um exemplo para enfatizar: tu tá usando teu editor de texto, tu fez várias alterações, uma depois de outra, e agora quer desfazer tudo que tu fez. Começando fazer "undo" qual a primeira alteração que vai ser "undoada"? Voltando: se eu quero desfazer o $g \circ f$ mesmo, o que preciso fazer? Praticamente já te dei a resposta para o exercício seguinte (x9.64)—sorry. Ainda bem que tem uma parte mais interessante: demonstrar.

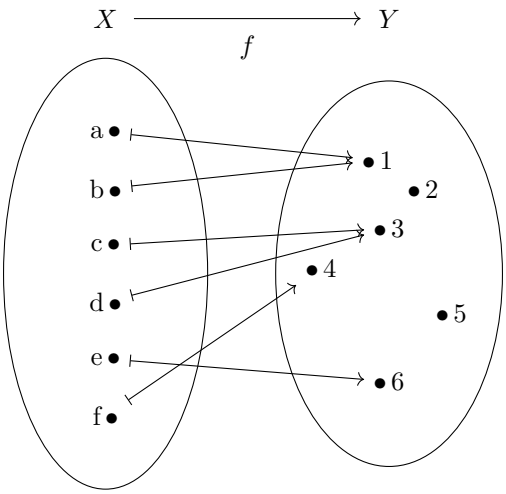
▸ **EXERCÍCIO x9.64 (Inversa da composição).**
Sejam $A \overset{f}{\rightarrowtail\!\!\!\!\twoheadrightarrow} B \overset{g}{\rightarrowtail\!\!\!\!\twoheadrightarrow} C$. Descreva a $(g \circ f)^{-1}$ em termos das f^{-1} e g^{-1} e demonstre tua afirmação. (x9.64 H 1 2 3)

▸ **EXERCÍCIO x9.65 (Basta uma lei).**
Seja $f : A \rightarrowtail B$. Se uma $f' : B \to A$ satisfaz pelo menos uma das duas leis do Exercício x9.62, então f' é a própria f^{-1}. (x9.65 H 0)

É chato, né?. Mergulhar nos domínios e codomínios das funções, mexendo com os bichinhos que tem lá, tanto para enunciar teoremas quanto para demonstrá-los espero que foi uma experiência não exatamente divertida. Logo vamos ver uma outra maneira para enunciar e demonstrar essas propriedades, "de longe", sem olhar os detalhes internos.

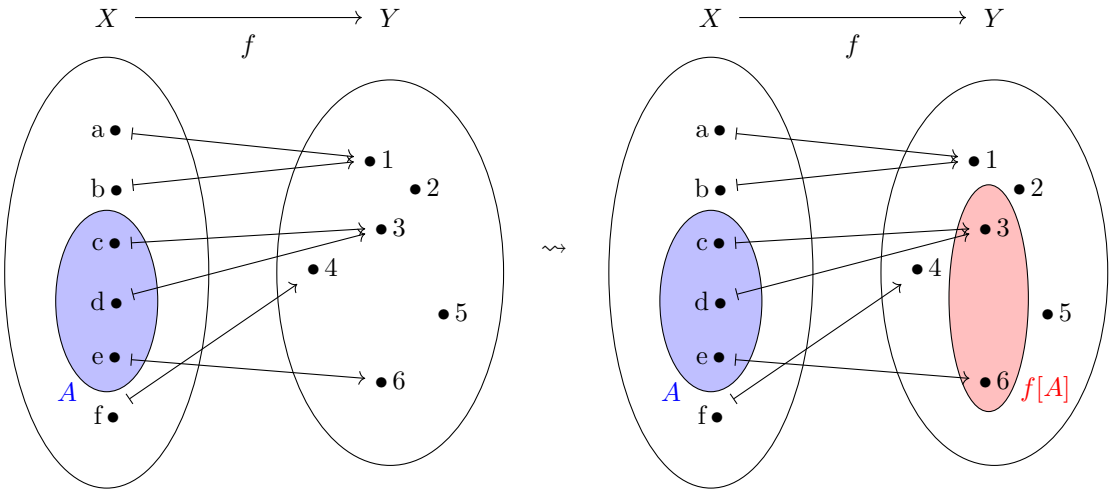
§213. Imagens, preimagens

9.166. Dois subconjuntos importantes. Sejam X, Y conjuntos e $f : X \to Y$.



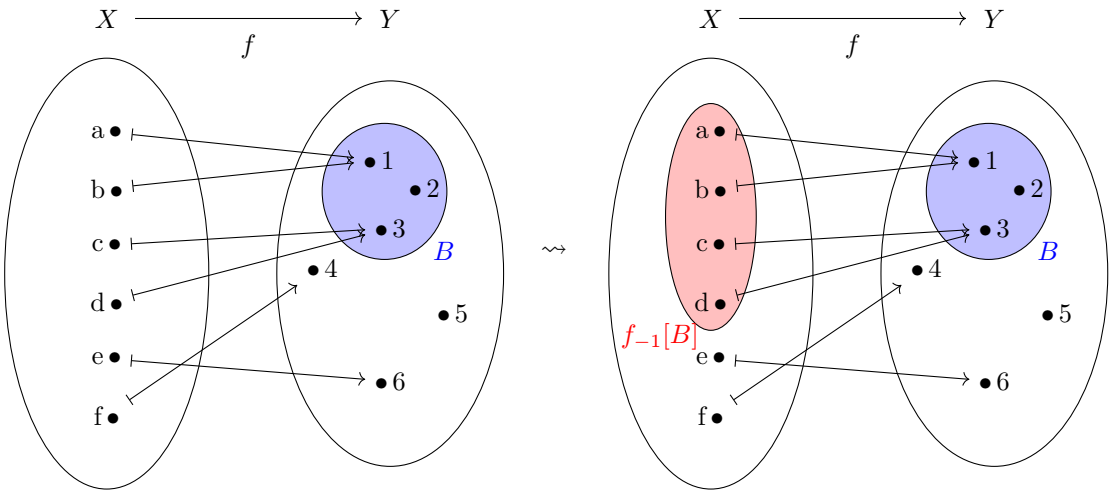
Vamos associar, com qualquer subconjunto A de X, um certo subconjunto de Y, que vamos chamá-lo a *imagem* de X através da f. Similarmente, com qualquer subconjunto B de Y, vamos associar um certo subconjunto de X, que vamos chamá-lo a *preimagem* de B através da f. Parece que estamos "elevando" a função f do nível *membros* para para o nível *subconjuntos*. Vamos ver como.

- **EXEMPLO 9.167.**
Nas figuras seguintes mostramos com azul o subconjunto com que começamos, e com vermelho o subconjunto que associamos com ele. Considere o $A \subseteq X$ como aparece no desenho abaixo, e veja qual é o subconjunto $f[A]$ de Y que vamos associar com o A:



Na direção oposta, comece por exemplo com esse $B \subseteq Y$ e observe qual é o subconjunto

$f_{-1}[B]$ de X que queremos associar com o B:



9.168. Observação. Observe que na discussão acima não supusemos *nada mais* além da existência de uma função f dum conjunto X para um conjunto Y.

? **Q9.169. Questão.** Como podemos definir formalmente os conjuntos indicados nos desenhos acima?

!! SPOILER ALERT !!

D9.170. Definição. Seja $f : X \to Y$, e sejam subconjuntos $A \subseteq X$ e $B \subseteq Y$. Definimos:

$$f[A] \stackrel{\text{def}}{=} \{\, f(a) \mid a \in A \,\}$$
$$f_{-1}[B] \stackrel{\text{def}}{=} \{\, x \in X \mid f(x) \in B \,\}.$$

Lembrando a notação set builder (Notação D8.7), temos as definições:

$$y \in f[A] \iff^{\text{def}} (\exists a \in A)[\, f(a) = y \,]$$
$$x \in f_{-1}[B] \iff^{\text{def}} f(x) \in B.$$

Chamamos o conjunto $f[A]$ *imagem* do A através da f ou, mais curtamente, a *f-imagem* do A. O conjunto $f_{-1}[B]$ é a *preimagem* do B através da f; ou a *f-preimagem* do B. ↯

! **9.171. Aviso.** Todas as notações seguintes são freqüentemente usadas para a denotar f-imagem de A:

$$f[A], \quad f_*A, \quad \vec{\wp}fA, \quad \vec{\wp}_f A, \quad f\text{ “ }A, \quad \exists_f A;$$

e todas essas para a f-preimagem de B:

$$f_{-1}[B], \quad f^*B, \quad \overleftarrow{\wp}fB, \quad \overleftarrow{\wp}_f B.$$

▸ **EXERCÍCIO x9.66.**
Quais os tipos das $f[-]$ e $f_{-1}[-]$? (x9.66 H 0)

▸ **EXERCÍCIO x9.67.**
Seja $f : X \to Y$. Verifique:

$$f[\emptyset] = \emptyset \qquad \text{e} \qquad f_{-1}[\emptyset] = \emptyset.$$

(x9.67 H 0)

9.172. Observação. Se $f : X \to Y$ então, temos que:

(i) $\operatorname{range} f = f[X]$;

(ii) $f[X] = Y \iff f$ é sobrejetora.

As duas afirmações são conseqüências imediatas das definições envolvidas.

▸ **EXERCÍCIO x9.68 (Nossa notação é melhor).**
Em matemática, às vezes aparece a notação $f(X)$ para denotar a imagem do $X \subseteq \operatorname{dom} f$ através da função f. Aqui usamos a notação $f[X]$. *Sem usar o conjunto vazio em lugar nenhum na tua resposta*, dê um exemplo (completo) que mostra que a notação $f(X)$ pode ser problemática (e logo nossa notação $f[X]$ é melhor). Explique curtamente. (x9.68 H 1 2)

9.173. Só que não. Então no Exercício x9.68 descobrimos que “nossa” notação é melhor. Né? Para o mundo não cuidosamente tipado, sim, ela é melhor. Mas num mundo onde tipamos com carinho nossos objetos, tendo assim tipos distintos

$$\mathsf{Set}(\mathsf{Int}), \qquad \mathsf{Set}(\mathsf{Set}(\mathsf{Int})), \qquad \mathsf{Set}(\mathsf{Set}(\mathsf{Set}(\mathsf{Int}))), \qquad \dots$$

será que podemos realmente nos livrar da complicação de ter notações distintas para essa infinidade de “elevações” de f? Considere:

$$5 : \mathsf{Int}$$
$$\{3, 8, 12\} : \mathsf{Set}(\mathsf{Int})$$
$$\{\{1, 4\}, \{3\}, \mathbb{Z}\} : \mathsf{Set}(\mathsf{Set}(\mathsf{Int}))$$

Vamos usar a $f = \lambda x \,.\, x + 2 : \mathsf{Int} \to \mathsf{Int}$. Se eu escrever ‘ $f\,5$ ’ só pode ser a f “original”, pois $5 : \mathsf{Int}$. E se eu escrever ‘ $f\ \{3, 8, 12\}$ ’ só pode ser a $\vec{\wp}f$ sendo aplicada mesmo, e escrevendo ‘ $f\,\{\{1, 4\}, \{3\}, \mathbb{Z}\}$ ’ só pode ser a $\vec{\wp}\vec{\wp}f$. Calculamos:

$$\begin{aligned}
f\,5 &= 7 \\
f\ \{3, 8, 12\} &= \{f\,3, f\,8, f\,12\} \\
&= \{5, 10, 14\} \\
f\,\{\{1, 4\}, \{3\}, \mathbb{Z}\} &= \{f\ \{1, 4\}, f\ \{3\}, f\,\mathbb{Z}\} \\
&= \{\{f\,1, f\,4\}, \{f\,3\}, \{\, x + 2 \mid x \in \mathbb{Z}\,\}\} \\
&= \{\{3, 6\}, \{5\}, \mathbb{Z}\}.
\end{aligned}$$

9.174. Observação. O perigo descrito no Exercício x9.68 não existe quando trabalhamos com conjuntos *homogêneos* (8.6). Em tal mundo podemos usar a notação $f(X)$ para o $f[X]$ sem problema: um conjunto como o $\{1, 7, \{1, 7\}\}$ seria considerado: inconstrutível, mal-tipado, não definido, sem significado, blasfêmico, etc. ↯

▸ **EXERCÍCIO x9.69.**
Podemos definir a f-preimagem de Y assim?:

$$f_{-1}[Y] \stackrel{\text{def}}{=} \{\, f^{-1}(y) \mid y \in Y \,\}$$

(x9.69 H 0)

▸ **EXERCÍCIO x9.70.**
Sejam $f : A \rightarrowtail B$, e $Y \subseteq B$. Mostre que

$$f_{-1}[Y] = \{\, f^{-1}(y) \mid y \in Y \,\}.$$

(x9.70 H 1)

▸ **EXERCÍCIO x9.71.**
Qual o problema com a Definição D9.170? (x9.71 H 1 2)

▸ **EXERCÍCIO x9.72.**
Depois de resolver o Exercício x9.71, justifique a corretude da Definição D9.170: explique o que precisas demonstrar, e demonstre! (x9.72 H 1 2)

▸ **EXERCÍCIO x9.73.**
Verdadeiro ou falso?: para toda função f e todo x no seu domínio temos

$$f[\{x\}] = \{f(x)\}.$$

(x9.73 H 0)

▸ **EXERCÍCIO x9.74.**
É alguma das $f[-]$, $f_{-1}[-]$ garantidamente injetora ou sobrejetora? (x9.74 H 0)

▸ **EXERCÍCIO x9.75.**
Seja $f : A \to B$. Demonstre que

$$f \text{ bijetora} \iff \text{para todo } b \in B,\ f_{-1}[\{b\}] \text{ é um conjunto unitário.}$$

(x9.75 H 1 2)

▸ **EXERCÍCIO x9.76.**
Sejam conjuntos X e Y, $f : X \to Y$, e $A \subseteq X$ e $B \subseteq Y$. Demonstre as afirmações:

$$A \subseteq f_{-1}[f[A]]$$
$$B \supseteq f[f_{-1}[B]].$$

(x9.76 H 0)

▸ **EXERCÍCIO x9.77.**
Sejam conjuntos X e Y, $f : X \to Y$, e $A \subseteq X$ e $B \subseteq Y$. Considere as afirmações:

$$A \stackrel{?}{=} f_{-1}[f[A]]$$
$$B \stackrel{?}{=} f[f_{-1}[B]].$$

Para cada uma delas: se podemos concluí-la, demonstre; e caso contrário, mostre um contraexemplo. (x9.77 H 1 2)

? **Q9.175. Questão.** O que muda no Exercício x9.77 se f é injetora? Se é sobrejetora?

!! SPOILER ALERT !!

Θ9.176. Teorema. *Seja $f : X \to Y$. Temos:*

(1) f injetora $\iff$ para todo $A \subseteq X$, $A = f_{-1}[f[A]]$

(2) f sobrejetora $\iff$ para todo $B \subseteq Y$, $B = f[f_{-1}[B]]$.

Demonstração. As duas idas tu demonstrarás (agora!) no x9.78; as voltas no Problema Π9.8 (pode ser depois). ∎

▸ **EXERCÍCIO x9.78.**
Demonstre as idas do Teorema Θ9.176. (x9.78 H 0)

Vamos ver agora como essas operações comportam em combinação com as operações de conjuntos.

▸ **EXERCÍCIO x9.79.**
Sejam $f : X \to Y$, $A, B \subseteq X$. Mostre que:

$$f[A \cup B] = f[A] \cup f[B]$$
$$f[A \cap B] \stackrel{?}{=} f[A] \cap f[B]$$
$$f[A \setminus B] \stackrel{?}{=} f[A] \setminus f[B]$$

onde nas $\stackrel{?}{=}$ demonstre que a igualdade em geral não é válida, mas uma das $(\subseteq)$ e $(\supseteq)$, é. (x9.79 H 1)

▸ **EXERCÍCIO x9.80.**
Sejam $f : X \rightarrowtail Y$ injetora, e $A, B \subseteq X$. Mostre que:

$$f[A \cap B] = f[A] \cap f[B]$$
$$f[A \setminus B] = f[A] \setminus f[B].$$

(x9.80 H 1)

A preimagem comporta bem melhor que a imagem: ela respeita todas essas operações mesmo quando f não é injetora, algo que tu demonstrarás agora.

▸ **EXERCÍCIO x9.81.**
Sejam $f : X \to Y$, $A, B \subseteq Y$. Mostre que:

$$f_{-1}[A \cup B] = f_{-1}[A] \cup f_{-1}[B]$$
$$f_{-1}[A \cap B] = f_{-1}[A] \cap f_{-1}[B]$$
$$f_{-1}[A \setminus B] = f_{-1}[A] \setminus f_{-1}[B]$$

(x9.81 H 0)

Essas propriedades generalizam naturalmente para uniões e intersecções de seqüências e famílias de conjuntos; veja por exemplo o Problema Π9.9.

§214. Definições estilo point-free (tácito)

9.177. Pointful vs. pointfree. Olhe para a definicão seguinte duma função $f : \mathbb{N} \to \mathbb{N}$:

$$f\ n = 2 \cdot (n^2 + 1).$$

Literalmente estamos definindo o que significa $f\ n$, e não o que significa f. Mas, já que temos igualdade extensional entre funções, e já que n é um natural arbitrário natural aqui, definindo $f\ n$ é suficiente para determinar a f. A situação deve te lembrar algo (Nota 8.19) por justa causa.

Agora olhe novamente na definição acima. Para entender *quem é f* precisamos *entrar na floresta do seu domínio*, pegar uma árvore n, *entrar na floresta do seu codomínio* e procurar passo por passo o que aconteceu com ela. Lendo o início da definição, «$2 \cdot \ldots$» sabemos que alguém foi multiplicado por 2, talvez não tem algo a ver como nossa árvore, precisamos andar ainda mais, e depois de muitas trilhas descubrir o que aconteceu.

Compare com a definição seguinte que define a mesma função f sem sequer mencionar "árvores":

$$f = \mathrm{double} \circ \mathit{succ} \circ \mathrm{square} \qquad \text{ou} \qquad f = \mathrm{square}\ ;\ \mathit{succ}\ ;\ \mathrm{double}.$$

Ela é claríssima e sucinta, define *diretamente* a própria f (sem enrolar fazendo trilhas nas florestas), e dá pra ler e entender tanto da esquerda para a direita, quanto da direita para a esquerda.

• **EXEMPLO 9.178.**
Seja $f : \mathbb{Z} \to \mathbb{Z}$ a função definida pela

$$f(x) = -(x^2 + 3).$$

Mostre como definir a f como composição de três funções $g, h, k : \mathbb{Z} \to \mathbb{Z}$ sem nenhuma das g, h, k ser a $\lambda x\,.\,x$. Sim, use lambdas (só pra praticá-los mais).
Resolução. Idéia: vamos tentar descrever o processo do que acontece na entrada x passo por passo até chegar na saida $-(x^2+3)$. Primeiramente acontece um quadramento,

depois um incremento por 3, e depois uma negação. Vamo lá então: sejam as $g, h, k : \mathbb{Z} \to \mathbb{Z}$ definidas pelas

$$g = \lambda x \,.\, x^2 \qquad h = \lambda x \,.\, x + 3 \qquad k = \lambda x \,.\, -x.$$

Assim definimos a f como

$$f = k \circ h \circ g.$$

Sem ambigüidade podemos omitir os '$\circ$' pois já estamos em modo "de longe" (sem mexer com pontinhos):

$$f = khg.$$

Simplíssimo!

9.179. Conselho (to name or not to name). Observe que nem precisamos nomes para as funções "intermediárias" do Exemplo 9.178. Poderiamos simplesmente definir a função $f : \mathbb{Z} \to \mathbb{Z}$ assim:

$$f = (\lambda x \,.\, -x) \circ (\lambda x \,.\, x + 3) \circ (\lambda x \,.\, x^2).$$

(Nesse caso não vamos omitir os '$\circ$' pois aparecem os pontinhos (os 'x') e poderia confundir entre composição e aplicação.) Então: usamos funções anônimas ou epônimas? Depende! E a escolha não é nada de boba. Pelo contrário, é muito importante elaborar uma intuição boa sobre:

(i) *se* vamos nomear algo (lembra do 9.78);
(ii) *qual* vai ser o seu nome, caso que decidirmos dar um.

Isso tanto em programação quanto em matemática! Vamos voltar no nosso Exemplo 9.178 onde temos três "componentes intermediários" e precisamos decidir para cada um deles se vamos nomeá-lo e como. Uns fatores importantes para considerar:

- esse componente é algo já bem conhecido? já possui um nome?
- esse componente vai ser reutilizado?

Com essa guia, faria sentido definir a f assim:

$$f = \mathrm{negate} \circ (\lambda x \,.\, x + 3) \circ \mathrm{square}$$

onde

$$\begin{aligned} \mathrm{negate} &: \mathbb{Z} \to \mathbb{Z} & \qquad \mathrm{square} &: \mathbb{Z} \to \mathbb{Z} \\ \mathrm{negate}(x) &= -x & \qquad \mathrm{square}(x) &= x^2. \end{aligned}$$

Aqui não me pareceu tão útil ter um nome para a operação $\lambda x \,.\, x + 3$ e logo escolhi deixá-la anônima. Se fosse $\lambda x \,.\, x + 1$ teria escolhido usar o *succ*. Não existe maneira correta ou errada aqui: nomeá-las por g, h, k também não foi bizarro não, nem deixá-las todas anônimas! Depende da situação, do contexto, da intenção, do uso, das estrelas, etc.

▸ **EXERCÍCIO x9.82.**
Fatore as funções seguintes na maneira mais legal que tu consegues:

$$\begin{aligned} f &: \mathbb{Q} \to \mathbb{Q} & \qquad f(x) &= \frac{1}{\sqrt{(x+1)^2 + 1}} \\ g &: \mathbb{N} \times \mathbb{N} \to \mathbb{N} & \qquad g(x, y) &= y^2 + 1 \\ h &: \mathbb{N} \times \mathbb{N} \to \mathbb{N} & \qquad h(x, y) &= 2(x + y) + 1 \\ k &: \mathbb{N} \times \mathbb{N} \to \mathbb{N} & \qquad k(x, y) &= 2(x + 2y) + 1. \end{aligned}$$

(x9.82 H 1 2)

• **EXEMPLO 9.180.**
Defina a função $f = \lambda x \,.\, 2x + 1 : \mathbb{N} \to \mathbb{N}$ diretamente como composição de funções sem usar λ-notação. Desenhe o diagrama externo da configuração e confirme tua resolução.
RESOLUÇÃO. Temos as funções

$$\mathbb{N} \xrightarrow{\Delta} \mathbb{N} \times \mathbb{N} \xrightarrow{+} \mathbb{N} \xrightarrow{succ} \mathbb{N}.$$

Assim defino

$$f = (succ \circ + \circ \Delta_{\mathbb{N}}) : \mathbb{N} \to \mathbb{N}$$

e tomando um $x \in \mathbb{N}$ calculo:

$$\begin{aligned} f(x) &= (succ \circ + \circ \Delta)(x) && \text{(def. } f\text{)} \\ &= succ(+(\Delta(x))) && \text{(def. } \circ\text{)} \\ &= succ(+(x, x)) && \text{(def. } \Delta\text{)} \\ &= succ(2x) \\ &= 2x + 1 && \text{(def. } succ\text{)} \end{aligned}$$

confirmando assim que minha definição foi correta.

▸ **EXERCÍCIO x9.83.**
Faça a mesma coisa para a função $f = \lambda x \,.\, 2x^2 : \mathbb{N} \to \mathbb{N}$. (x9.83 H 0)

▸ **EXERCÍCIO x9.84 (Leis da inversa (sem pontos)).**
Como podemos expressar as leis da inversa (F-Inv) sem pontos? (x9.84 H 0)

Intervalo de problemas

▸ **PROBLEMA Π9.2.**
Supondo que teu leitor não sabe o que são as iterações duma função (Definição D9.150) e que *sequer quer saber*, defina a função $succ^n$ numa maneira simples. Demonstre tua afirmação, que a $succ^n$ (oficial) realmente é igual à função que tu escreveste para teu leitor. (Π9.2 H 1 2 3)

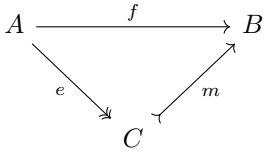
▸ **PROBLEMA Π9.3.**
Na definição do Exercício x9.46 não escrevemos "existe único", mas apenas "existe". O que mudaria com esse "único"? Demonstre tua afirmação. (Π9.3 H 1)

▸ **PROBLEMA Π9.4.**
Seja $\mathbb{N}^\star = \bigcup_n \mathbb{N}^n$ o conjunto de todos os strings finitos feitos por naturais. Considere a $f : \mathbb{N}^\star \to \mathbb{N}_{>0}$ definida pela

$$f(x_0, \ldots, x_{n-1}) = \prod_{i=0}^{n-1} p_i^{x_i}$$

onde $(p_n)_n$ é a seqüência dos números primos ($p_0 = 2$, $p_1 = 3$, $p_2 = 5$, …). (1) Explique por que f não é injetora. (2) Demonstre que f é sobrejetora. (3) O que acontece se substituir os exponentes x_i por $x_i + 1$? (Π9.4 H 0)

▸ **PROBLEMA Π9.5.**
Sejam $A \xrightarrow{f} B$. Então existem: injecção m, surjecção e, e conjunto C tais que o diagrama seguinte comuta:



Em outras palavras, mostre que qualquer função $f : A \to B$ pode ser "decomposta" em

$$f = m \circ e$$

onde e é uma função sobrejetora e m uma função injetora. (Π9.5 H 1)

▸ **PROBLEMA Π9.6.**
Seja A um conjunto habitado. Defina funções f, g com os tipos seguintes:

$$f : A \rightarrowtail \wp A$$
$$g : \wp A \twoheadrightarrow A.$$

Demonstre que: (i) a f é injetora; (ii) a f não é sobrejetora; (iii) a g é sobrejetora; (iv) a g não é sobrejetora. Como eu posso pedir pra tu demonstrar tudo isso (as (ii) e (iv)) sem sequer saber quais são as f, g que tu escolheu definir? (Essa pergunta não é retórica.) (Π9.6 H 1 2 3 4 5)

▸ **PROBLEMA Π9.7.**
Sejam $A \neq \emptyset$ conjunto, $n \in \mathbb{N}_{>0}$, e $I = \{\, i \in \mathbb{N} \mid i < n \,\}$. Considere a função $\pi : I \times A^n \to A$ definida por

$$\pi(i, \alpha) = \pi_i(\alpha) \qquad \Big(= \text{o } i\text{-ésimo membro da tupla } \alpha\Big)$$

onde consideramos o primeiro membro duma tupla seu "0-ésimo" membro, etc. Investigue a injectividade e a sobrejectividade da π. (Π9.7 H 1)

▸ **PROBLEMA Π9.8.**
Demonstre o Teorema Θ9.176. (Π9.8 H 0)

▸ **PROBLEMA Π9.9.**
Sejam $f : A \to B$, e duas famílias indexadas de conjuntos: $(A_i)_{i \in \mathcal{I}}$ feita por subconjuntos de A, e $(B_j)_{j \in \mathcal{J}}$ feita por subconjuntos de B. Ou seja, par todo $i \in \mathcal{I}$, e todo $j \in \mathcal{J}$, temos $A_i \subseteq A$ e $B_j \subseteq B$. Mostre que:

(1) $$f\Big[\bigcup_{i \in \mathcal{I}} A_i\Big] = \bigcup_{i \in \mathcal{I}} f[A_i]$$

(2) $$f\Big[\bigcap_{i \in \mathcal{I}} A_i\Big] \stackrel{?}{=} \bigcap_{i \in \mathcal{I}} f[A_i]$$

(3) $$f_{-1}\Big[\bigcup_{j \in \mathcal{J}} B_j\Big] = \bigcup_{j \in \mathcal{J}} f_{-1}[B_j]$$

(4) $$f_{-1}\Big[\bigcap_{j \in \mathcal{J}} B_j\Big] = \bigcap_{j \in \mathcal{J}} f_{-1}[B_j]$$

onde na $\stackrel{?}{=}$ demonstre que a igualdade em geral não é válida, mas uma das $(\subseteq)$ e $(\supseteq)$ é. A demonstre, e, supondo que f é injetora, demonstre a outra também. (Π9.9 H 0)

▸ **PROBLEMA Π9.10.**
Um aluno "demonstrou" que se $f : A \to B$ e $(A_n)_n$ é uma seqüência de subconjuntos de A, então

$$f\Big[\bigcap_{n=0}^{\infty} A_n\Big] = \bigcap_{n=0}^{\infty} f[A_n].$$

Sua "demonstração" foi a seguinte:

> «Calculamos:
>
> $$\begin{aligned}
> b \in f\Big[\bigcap_{n=0}^{\infty} A_n\Big] &\overset{1}{\iff} \Big(\exists a \in \bigcap_{n=0}^{\infty} A_n\Big)[\, f(a) = b\,] && \text{(def. } f[-]\text{)}\\
> &\overset{2}{\iff} \exists a\Big(a \in \bigcap_{n=0}^{\infty} A_n \wedge f(a) = b\Big) && \text{(lógica)}\\
> &\overset{3}{\iff} \exists a(\forall n(a \in A_n) \wedge f(a) = b) && \text{(def. } \textstyle\bigcap_{n=0}^{\infty}\text{)}\\
> &\overset{4}{\iff} \exists a(\forall n(a \in A_n \wedge f(a) = b)) && \text{(lógica)}\\
> &\overset{5}{\iff} \exists a \forall n(a \in A_n \wedge f(a) = b) && \text{(lógica)}\\
> &\overset{6}{\iff} \forall n \exists a(a \in A_n \wedge f(a) = b) && \text{(lógica)}\\
> &\overset{7}{\iff} \forall n(\exists a \in A_n)[\, f(a) = b\,] && \text{(lógica)}\\
> &\overset{8}{\iff} \forall n(b \in f[A_n]) && \text{(def. } f[-]\text{)}\\
> &\overset{9}{\iff} b \in \bigcap_{n=0}^{\infty} f[A_n] && \text{(def. } \textstyle\bigcap_{n=0}^{\infty}\text{)}
> \end{aligned}$$
>
> Logo temos $f[\bigcap_{n=0}^{\infty} A_n] = \bigcap_{n=0}^{\infty} f[A_n]$ pela definição de igualdade de conjuntos.»

Ache os seus erros. (Π9.10 H 1 2)

▸ **PROBLEMA Π9.11.**
Seja $f : A \to B$. Considere a afirmação seguinte:

$$f(-) \text{ sobrejetora} \overset{?}{\iff} f_{-1}[-] \text{ injetora.}$$

Para cada uma das direções responda... (1) "sim", e demonstre; (2) "não", e refute; ou (3) "depende", e mostre dois exemplos: um onde a implicação é válida, e outro onde não é. (Π9.11 H 1)

▸ **PROBLEMA Π9.12 (Don't just read it; fight it).**
Ache a coisa mais óbvia para se perguntar depois do Problema Π9.11; pergunte-se; responda (demonstra ou refuta). (Π9.12 H 1)

▸ **PROBLEMA Π9.13.**
(Continuação do Problema Π9.2.) Qual é (a extensão d)o conjunto

$$\bigcap_{n=0}^{\infty} succ^n[\mathbb{N}]\,?$$

Demonstre tua afirmação. (Π9.13 H 1 2)

▸ **PROBLEMA Π9.14.**
A Observação 9.174 tem um probleminha. Mesmo trabalhando apenas com uma funções homogêneas podemos cair em ambigüidade! Bem depois, no Capítulo 19, vamos entender a situação melhor; e tenho um teaser na resolução. Mas por enquanto só resolva esse problema, ou seja, ache um exemplo problemático para essa notação, usando apenas conjuntos homogêneos. (Π9.14 H 1 2)

▸ **PROBLEMA Π9.15 (flip).**
No Exemplo 9.130 da §208 definimos a função *powTwo* diretamente como aplicação parcial da função *exp*

$$powTwo = exp\ 2$$

evitando o uso de pontos ou lambdas:

$$powTwo\ n = exp\ 2\ n; \qquad\qquad powTwo = \lambda n\ .\ exp\ 2\ n.$$

Similarmente podemos definir a função que corresponde seqüência das potências de qualquer outro número real. Mas parece que não podemos criar com a mesma laconicidade (apenas como aplicação parcial) uma função *square* ou *cube*, pois os argumentos da *exp* estão "na ordem errada". O objectivo desse problema é fazer exatamente isso.

Defina uma função de ordem superior *flip*, que recebe qualquer função binária currificada, e retorna a função binária currificada que comporta no mesmo jeito mas recebendo seus argumentos na ordem oposta. Por exemplo:

$$exp\ 2\ 3 = 8; \qquad\qquad (flip\ exp)\ 2\ 3 = 9$$

Começa escrevendo o tipo da *flip* e o lendo com as duas maneiras diferentes que discutimos na Nota 9.128. (Π9.15 H 0)

§215. Leis de composição

9.181. Composição como operação. No mesmo jeito que o produto $3 \cdot 2$ denota um número, a composição $g \circ f$ de certas funções f e g denota uma função. A $\circ$ então realmente é uma operação (binária) nas funções, e agora vamos investigar as leis que ela satisfaz, fazendo uma comparação com a multiplicação nos números, procurando similaridades e diferências. Note que já começamos com uma ambigüidade com esse "nos números", pois as leis satisfeitas pela $(\cdot)$ dependem de *qual multiplicação* estamos considerando: a multiplicação nos reais, por exemplo, satisfaz a uma lei de inversos (viz. «cada número diferente de zero tem um inverso multiplicativo») mas nos inteiros não. Mais sobre isso depois.

9.182. Fatoração de função. Num certo sentido muito interessante, e fortalecendo nossa metáfora entre composição e multiplicação, o que fizemos no Exemplo 9.178 pode ser visto como uma *fatoração de função*: escrevemos a f como "produto" dos "fatores" g, h, k. Sabendo como fatorar funções é importaníssimo em programação, algo que apreciamos extensivamente no no Capítulo 4.

9.183. Totalidade. Primeiramente observe uma grande diferença entre composição e multiplicação: a multiplicação é uma operação *total*, ou seja, para todo número x, y, seu produto $x \cdot y$ é definido. Mas como vimos na Definição D9.137, para formar a composição $g \circ f$ de duas funções f e g elas precisam satisfazer a condição $\operatorname{cod} f = \operatorname{dom} g$. Caso contrário, o $g \circ f$ nem tem significado! Continuamos investigando mais propriedades.

9.184. Intuição com tarefas. Vamos agora imaginar funções como tarefas para ser feitas em algo, e a composição como a idéia de "seqüenciar as tarefas". Ou seja $g \circ f$ seria a tarefa de *fazer a tarefa f e depois a g*. Com essa intuição, parecem óbvias estas duas afirmações:

(i) a composição é associativa;
(ii) a composição não é comutativa.

Mas intuição nunca demonstrou nada sozinha, então bora demonstrar essas afirmações!

9.185. Associatividade. Suponha que temos funções

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D.$$

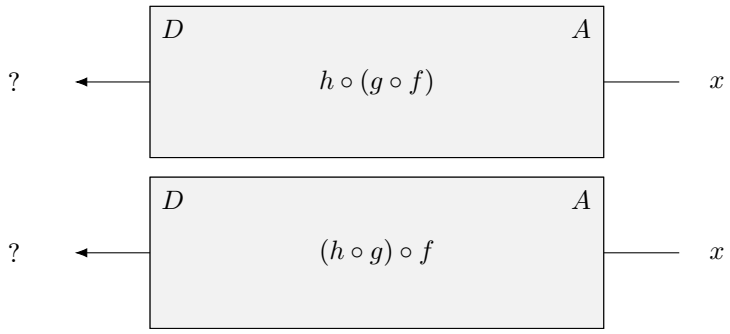
Podemos então formar as composições $g \circ f$ e $h \circ g$. Temos então:

$$A \xrightarrow{g \circ f} C \xrightarrow{h} D \qquad A \xrightarrow{f} B \xrightarrow{h \circ g} D.$$

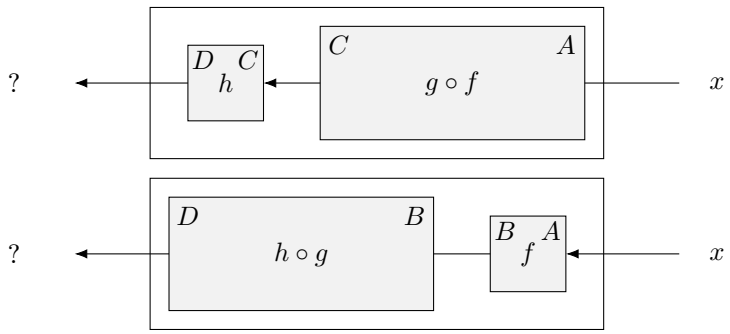
Compondo as funções do primeiro diagrama criamos a função $h \circ (g \circ f)$, e compondo aquelas do segundo criamos a $(h \circ g) \circ f$:

$$A \xrightarrow{h \circ (g \circ f)} D \qquad A \xrightarrow{(h \circ g) \circ f} D.$$

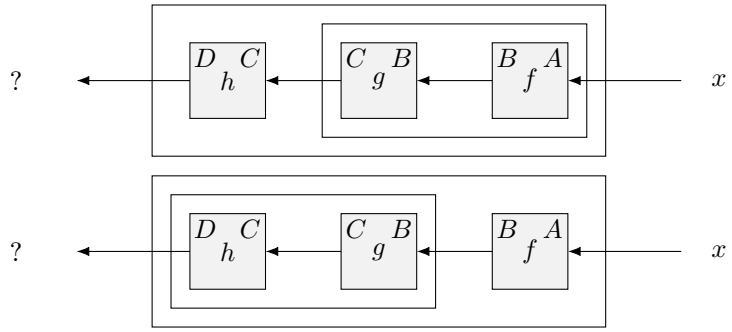
Queremos saber se as duas funções são iguais. Vamos pensar sobre isso usando black boxes.



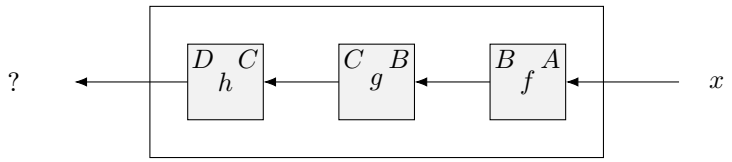
Primeiramente observe que os tipos delas são iguais. Então basta verificar que concordam para todo ponto $x \in A$. Pela definição de composição sabemos que "internalmente" elas funcionam assim:



Agora pelas definições das $g \circ f$ e $h \circ g$, o que precisamos comparar na verdade são as:



Agora que tá tudo transparente parece óbvio que as duas funções são iguais, e comportam como a seguinte:



Mas para demonstrar que as duas construções resultam na mesma função, vamos precisar calcular os «?» do desenho acima, e seguir fielmente as definições.

Θ9.186. Teorema (Lei de associatividade). *Sejam*

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D.$$

Então

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

▸ Esboço. Mostramos que as duas funções são iguais seguindo a definição de igualdade D9.28: mostrando que elas têm o mesmo domínio A, e que comportam igualmente para o arbitrário $a \in A$. Observe que seus codomínios também são iguais, satisfazendo assim a definição de igualdade D9.26 também. Pegando cada lado da igualdade e aplicando a definição de $\circ$ chegamos no mesmo valor. □ (Θ9.186P)

9.187. Comutatividade. É fácil demonstrar que a composição de funções *não é comutativa*. Faça isso agora no exercício seguinte!

▸ **EXERCÍCIO x9.85.**
Existem funções f, g entre conjuntos A, B tais que $f \circ g$ e $g \circ f$ são ambas definidas, mas mesmo assim

$$f \circ g \neq g \circ f.$$

Mostre pelo menos dois exemplos diferentes: um com $A \neq B$; outro com $A = B$. (x9.85H0)

9.188. Identidades. Investigamos agora se a operação de composição possui *identidade* mas primeiramente vamos lembrar o que isso significa. Por enquanto não demonstramos nada a respeito disso, então trate as funções que chamamos de identidades na D9.142 como uma coincidência.

? **Q9.189. Questão.** Chamamos o 1 a *identidade* da operação $(\cdot)$ nos reais, pois:

$$1 \cdot x = x = x \cdot 1, \qquad \text{para todo } x \in \mathbb{R}.$$

Tentando achar uma similaridade entre funções e números num lado, e composição e multiplicação no outro, qual seria nosso 1 aqui? Ou seja, procuramos objeto ? tal que

$$? \circ f = f = f \circ ?$$

para toda função f.

!! SPOILER ALERT !!

▸ **EXERCÍCIO x9.86.**
Sejam A, B conjuntos diferentes, e $f : A \to B$. Para cada uma das igualdades abaixo, decida se ela é válida ou não, justificando tua resposta.

(1) $f = f \circ \mathrm{id}_A$; (2) $f = f \circ \mathrm{id}_B$; (3) $f = \mathrm{id}_A \circ f$; (4) $f = \mathrm{id}_B \circ f$.

(x9.86H0)

Θ9.190. Teorema (Leis de identidade). *Para todo conjunto A, existe unica função $\mathrm{id}_A : A \to A$ tal que:*

$$\begin{aligned} &\text{para toda } f : A \to B, \quad f \circ \mathrm{id}_A = f; \\ &\text{para toda } f : B \to A, \quad \mathrm{id}_A \circ f = f. \end{aligned}$$

▸ Esboço. Primeiramente verificamos que a identidade do A (Definição D9.142) que "coincidentemente" denotamos por id_A realmente satisfaz tudo isso. Depois mostramos que qualquer outra possível função id'_A com essas propriedades deve ser (igual) à própria id_A. □ (Θ9.190P)

9.191. Leis de funções. As configurações na esquerda implicam as equações na direita:

(F-Ass) $$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \implies (h \circ g) \circ f = h \circ (g \circ f)$$

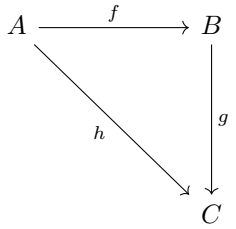
$$A \xrightarrow{f} B \implies \begin{cases} f \circ \mathrm{id}_A = f \\ \mathrm{id}_B \circ f = f \end{cases}$$

§216. Diagramas comutativos

Começamos com uma definição complicada; leia agora, mas veja logo os exemplos seguintes.

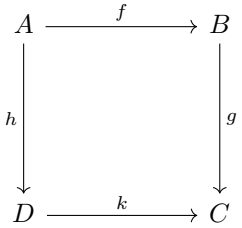
D9.192. "Definição" (diagrama comutativo). Digamos que um diagrama externo de funções *comuta* ou que é um *diagrama comutativo* sse: para todo par de "caminhos" feitos por seguindo setas, *se pelo menos um dos dois caminhos tem tamanho maior que* 1, então os dois caminhos são iguais.

- **EXEMPLO 9.193.**
O que significa que o diagrama seguinte comuta?



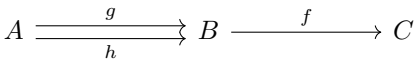
Significa que $h = g \circ f$.

- **EXEMPLO 9.194.**
O que significa que o diagrama seguinte comuta?



Significa que $g \circ f = k \circ h$

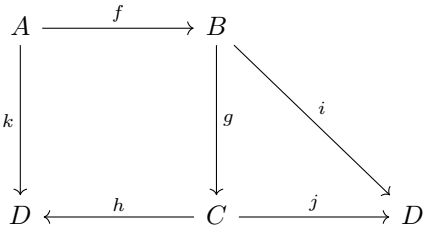
- **EXEMPLO 9.195.**
O que significa que o diagrama seguinte comuta?



Significa que $f \circ g = f \circ h$.

! 9.196. Cuidado. Graças à parte enfatizada na "Definição" D9.192, *não podemos* concluir no Exemplo 9.195 que $g = h$, pois mesmo que existem esses dois caminhos de A para B (um seguindo a seta g, outro seguindo a seta h), nenhum deles tem tamanho maior que 1.

• **EXEMPLO 9.197.**
O que significa que o rectângulo no diagrama seguinte comuta?

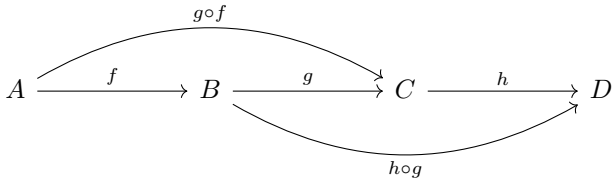


Apenas que $h \circ g \circ f = k$. Observe que isso não nos permite concluir nada especial sobre as setas i e j do triângulo. Se soubéssemos que o diagrama comuta (e não apénas seu rectângulo), poderiamos concluir que $i = j \circ g$ também.

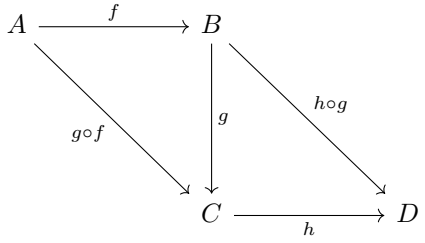
Afirmando a comutatividade de certos diagramas vira uma maneira curta de afirmar proposições, como por exemplo essas duas leis que já encontramos na §215.

• **EXEMPLO 9.198.**
Afirme a lei da associatividade da §215 usando a comutatividade dum diagrama.

RESOLUÇÃO. Sejam $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$. Basta desenhar um diagrama cuja comutatividade quis dizer $h \circ (g \circ f) = (h \circ g) \circ f$. É o seguinte:



Outra maneira para desenhar o mesmo diagrama seria a seguinte:

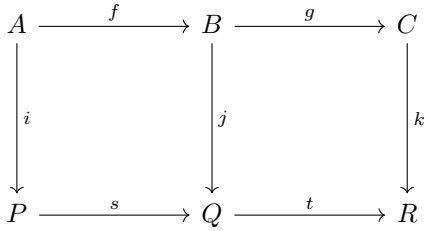


Questão de gosto.

▸ **EXERCÍCIO x9.87.**
Como podemos expressar as leis da identidade (Secção §215) usando apenas a comutatividade dum diagrama? (x9.87 H 1)

▸ **EXERCÍCIO x9.88 (Leis da inversa (com diagrama comutativo)).**
Como podemos expressar as leis da inversa (F-Inv) usando apenas a comutatividade dum diagrama? (x9.88 H 1)

▸ **EXERCÍCIO x9.89.**
Suponha que os quadrados no diagrama seguinte comutam:



Demonstre que o rectângulo grande também comuta. (x9.89 H 0)

§217. Produtos e demais construções

D9.199. Definição (cross). Sejam

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & C \\ B & \xrightarrow{\ g\ } & D \end{array}$$

Chamamos *função-produto das* f, g, que denotamos por $f \times g$, a função

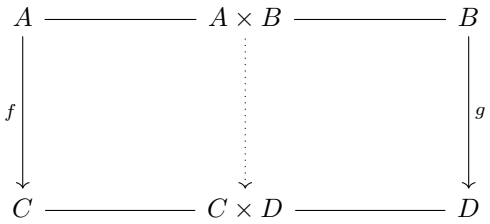
$$A \times B \xrightarrow{\ f\times g\ } C \times D$$

definida pela

$$(f \times g)(x, y) = \langle f(x), g(y) \rangle .$$

Pronunciamos «f cross g».

▸ **EXERCÍCIO x9.90.**
Bote nomes e direcções onde faltam e demonstre que o diagrama comuta:



(x9.90 H 0)

9.200. Observação (Um puzzle). Vamos fazer um "rewind" no momento exatamente antes de definir nossa função de $A \times B$ para $C \times D$. O diagrama parece como no Exercício x9.90, exceto sem a setinha pontilhada no meio. E esse é o "missing piece" do nosso puzzle. Procuramos então achar uma *seta* que é *legal*. O que significa "legal" aqui? *Uma seta que faz o diagrama comutar!*

▸ **EXERCÍCIO x9.91.**
Para cada uma das expressões seguintes, calcule seu valor quando tiver.

$$(\sin \times \cos)(\pi) = \qquad (\mathit{outl} \times \mathit{succ})(5,6) =$$
$$(\sin \times \cos)(\pi/2, \pi) = \qquad (\mathrm{id}_{\mathbb{N}} \times \mathit{succ})(0,1) =$$

Pode ser que umas delas tem type errors, e logo nenhum valor. (x9.91 H 0)

▸ **EXERCÍCIO x9.92.**
O operador binário $(- \times -)$ nas funções que definimos no Definição D9.199, é um operador total? (x9.92 H 0)

D9.201. Definição (pairing). Sejam

$$A \xleftarrow{\ f\ } D \xrightarrow{\ g\ } B$$

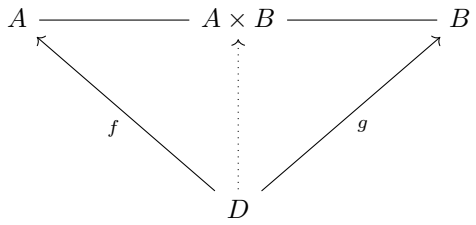
Chamamos *função-pareamento da f "pairing" g*, que denotamos por $\langle f, g \rangle$, a função

$$D \xrightarrow{\ \langle f,g \rangle\ } A \times B$$

definida pela

$$\langle f, g \rangle(x) = \langle f(x), g(x) \rangle \,.$$

▸ **EXERCÍCIO x9.93.**
Bote nomes e direcções onde faltam e demonstre que o diagrama comuta:



(x9.93 H 0)

? **Q9.202. Questão.** Dadas $f, g : A \to B$, e sabendo que no B é definida uma operação binária $* : B^2 \to B$, qual função interessante tu podes definir de A para B? Qual notação tu gostaria de usar pra ela?

!! SPOILER ALERT !!

D9.203. Definição (pointwise). Sejam A, B conjuntos e $*$ uma operação binária no B. Dadas funções $f, g : A \to B$, definimos a função $f * g : A \to B$ pela

$$(f * g)(x) = f(x) * g(x), \qquad \text{para todo } x \in A.$$

Chamamos a $(- * -)$ a *operação pointwise* da $*$ no conjunto $(A \to B)$.

9.204. Uma outra maneira de se inspirar. Se tu realmente tentou responder na pergunta acima, provavelmente tu chegou nessa mesma definição. Uma maneira de chegar nela é realmente "entrar na floresta", e começar brincar com as árvores, ate achar o que tu ta procurando. Uma outra abordagem seria observar a floresta de longe, por fora. Desenhar as setas que tu tens, e ver o que tu podes fazer interessante com elas; pra onde elas te guiam. Nesse caso temos $f, g : A \to B$, e também a $* : B^2 \to B$. Nosso desafio é definir uma função *interessante* do tipo $A \to B$.[65] Desenhamos então:

$$A \times A \xrightarrow{f \times g} B \times B \xrightarrow{*} B.$$

O que *interessante* podemos definir agora? Com certeza uma composição tem chances boas de ser interessante, só que aqui a

$$* \circ (f \times g) : A \times A \longrightarrow B$$

não tem o tipo desejado $A \to B$. Agora podemos desistir dessa abordagem e entrar na floresta mesmo para brincar com as árvores; *ou podemos perceber que talvez falta apenas uma setinha para nos ajudar*. Se a gente tivesse uma setinha interessante assim:

$$A \xrightarrow{?} A \times A \xrightarrow{f \times g} B \times B \xrightarrow{*} B,$$

a gente teria um candidato ótimo para algo interessante, pois assim a composição de todas essas setinhas tem o tipo desejado. Basta definir uma função interessante então de A para $A \times A$ e assim ganhar a

$$A \xrightarrow{* \circ (f \times g) \circ ?} B.$$

▸ **EXERCÍCIO x9.94.**
Dado conjunto A, define uma função interessante de A para $A \times A$. Começa descrevendo sua alma com um λ; consegue defini-la sem descrever explicitamente o seu comportamento? (x9.94 H 0)

▸ **EXERCÍCIO x9.95.**
Verifique se as duas funções definidas na Definição D9.203 e no fim do Nota 9.204 (com o Exercício x9.94) são as mesmas. (x9.95 H 0)

A função que tu definiu no Exercício x9.94 é muito útil e freqüentemente usada e sim, tem seu próprio nome e sua própria notação:

[65] Claramente não é o desafio mais claro que tu já viu na vida, mas isso faz parte do próprio desafio!

D9.205. Definição (Função diagonal). Seja A conjunto. Definimos sua *função diagonal* $\Delta_A : A \to A \times A$ pela

$$\Delta_A(x) = \langle x, x \rangle .$$

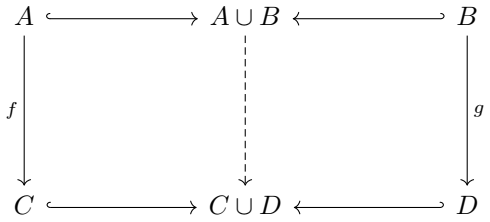
Equivalentemente:

$$\Delta_A \stackrel{\text{def}}{=} \langle \mathrm{id}_A, \mathrm{id}_A \rangle.$$

Quando o conjunto A é implícito pelo contexto escrevemos apenas Δ.

Com o que já temos na nossa disposição podemos definir umas funções interessantes apenas usando composições, e *diretamente* definindo a função (sem utilizar um ponto do seu domínio nem a λ-notação). Vamos investigar isso agora no Secção §214.

▸ **PROBLEMA Π9.16 (união de funções).**
Sejam $f : A \to C$ e $g : B \to D$. Queremos definir a $f \cup g : A \cup B \to C \cup D$, consultando as f e g, numa maneira parecida com aquela da definição de $f \times g$ (D9.199). Uma definição razoável deve fazer o diagrama seguinte comutar:



Explique quais são as condições necessárias para definir a $f \cup g$, e defina-a. (Π9.16 H 0)

§218. Coproduto; união disjunta

Vamos voltar no Problema Π9.16. (Se tu não resolveu ainda, volte a resolver agora, antes de continuar.) Definimos o $f \cup g$ a partir de duas funções f e g mas a situação não foi tão agradável como esperamos (cf. $f \times g$): necessitamos restrições adicionais.

? **Q9.206. Questão.** Quem é o culpado?

!! SPOILER ALERT !!

9.207. Resposta. A união! O conjunto que $\cup$ construiu, o $A \cup B$, não é útil aqui. Nem se compara com o $A \times B$, em questão de utilidade e elegância. Além disso—caso que os conjuntos são finitos por enquanto—com o produto tivemos a lei bacana

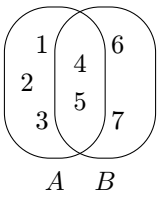
$$|A \times B| = |A| \cdot |B| .$$

A união não é tão legal, pois não consegue garantir igualdade mas apenas

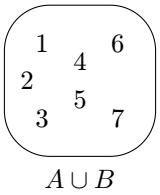
$$|A \cup B| \leq |A| + |B| .$$

Decepção de novo! Será que podemos descobrir um outro operador binário que comportaria numa maneira tão legal como o $\times$?

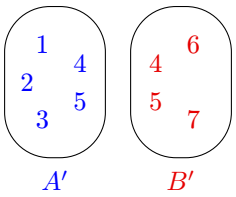
9.208. Contruindo o coproduto.



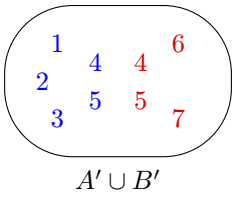
unindo:



Em vez disso, vamos criar cópias A', B' dos A, B numa maneira que garanta que os A', B' são disjuntos. Por exemplo, pintamos todos os membros de A azuis e de B vermelhos:[66]



Os conjuntos agora são disjuntos (observe que $4 \neq 4$ e $5 \neq 5$) então vamos simplesmente uni-los:



[66] Leitores sem acesso nessas cores neste texto vão ficar confusos aqui; mas paciência pois uma definição formal tá chegando já já; uma que não necessita telas e impressoras (e olhos?) chiques.

e nesse caso vamos tomar $A \uplus B := A' \cup B'$. Observe que esse processo descrito aqui garanta mesmo que

$$\begin{aligned} |A \uplus B| &= |A' \cup B'| && (\text{def. } A \uplus B) \\ &= |A'| + |B'| && (A', B' \text{ disjuntos}) \\ &= |A| + |B|\,. && (|A| = |A|' \text{ e } |B| = |B|') \end{aligned}$$

Parece então que conseguimos definir o operador de união disjunta.

9.209. "O" ou "um"?. A descripção acima envolve um passo bem ambiguo: a *contruição das cópias* A', B'. Com certeza existem muitas maneiras diferentes de conseguir essas cópias e a gente so descreveu uma—inclusive nem formalmente, mas dá pra fazer (Exercício x9.96). Precisamos escolher uma pra realmente definir nosso operador.

▸ **EXERCÍCIO x9.96.**
Ache algo matematicamente formal que podes usar em vez do informal «pintar os membros do A de azul e do B de vermelho». (x9.96 H 0)

D9.210. Definição (união disjunta ou coproduto). Sejam A, B conjuntos. Definimos o *coproduto*

$$A \amalg B \stackrel{\text{def}}{=} (\{0\} \times A) \cup (\{1\} \times B).$$

Generalizmos para qualquer família indexada $(A_i)_{i\in\mathcal{I}}$:

$$\coprod_i A_i \stackrel{\text{def}}{=} \bigcup_i (\{i\} \times A_i).$$

Também usamos o termo *união disjunta*; e a notações correspondente $A \uplus B$ para o caso binário; e a $\biguplus_i A_i$ para famílias.

9.211. Observação. No contexto de teoria dos tipos (Capítulo 19) o tipo correspondente é chamado *sum type* e usamos as notações $A + B$ e $\sum_i A_i$.

9.212. Nível coração: escolhedores. Seja $(A_i)_{i\in\mathcal{I}}$ família de conjuntos. Lembre-se que enxergamos (8.159) cada membro do produto $\prod_i A_i$ como um escolhedor: ele escolhe exatamente um membro *de cada* A_i. Podemos enxergar um membro do coproduto como um escolhedor também. Mas antes disso, vamos ver se podemos enxergar o arbitrário membro do $\bigcup_i A_i$ como escolhedor. Sim: o $a \in \bigcup_i A_i$ representa o escolhedor que escolha o a, entre todos os membros que pertencem a qualquer um dos A_i's. No coproduto a situação é mais informativa e interessante: o arbitrário membro do $\coprod_i A_i$ parece assim: (j, a), onde $j \in \mathcal{I}$ e $a \in A_j$. Ou seja, parece uma escolha rotulada, que selecionou um membro do conjunto com seu rótulo e nada mais. Vamos comparar três escolhedores P, C, U então:

$$P \in \prod_i A_i \qquad C \in \coprod_i A_i \qquad U \in \bigcup_i A_i.$$

Podemos perguntar ao P:

- Qual foi tua escolha para o $i \in \mathcal{I}$?
- Do A_i escolhi o $u \in A_i$.
- E para o $j \in \mathcal{I}$?

– Do A_j escolhi o $v \in A_j$.
– E para o $k \in \mathcal{I}$?
– Do A_k escolhi o $w \in A_k$.

etc., e vamos ter uma resposta para cada um dos i's. Ao C perguntamos:

– Quem tu escolheu?
– Escolhi o x por dentro do w-esimo: $x \in A_w$.

E ao U perguntamos:

– Quem tu escolheu?
– Escolhi o x.
– Donde?
– Como assim?
– Onde tu achou esse x, em qual dos A_i's?
– Sei-lá! Foi num deles. Não lembro. Não quero dizer.

▸ **EXERCÍCIO x9.97.**
Imite a idéia da construcção do $\langle f, g\rangle$ (Definição D9.201) que baseamos no $\times$ para definir duas novas construcções parecidas: uma baseada no $\cup$, e outra no $\amalg$. Qual das duas parece comportar melhor? (Nossa referência de comportamento aqui é a construcção baseada no $\times$.) (x9.97 H 0)

▸ **EXERCÍCIO x9.98.**
O que tu percebes sobre os diagramas comutativos do $\times$ (Definição D9.201) e do $\amalg$ (que tu desenhou no Exercício x9.97)? (x9.98 H 1)

Intervalo de problemas

▸ **PROBLEMA Π9.17.**
Generalize o Exercício x9.53 para um arbitrário conjunto finito A. (Π9.17 H 1)

§219. Funções parciais

A restricção que uma função $f : A \to B$ precisa ser *totalmente* definida no A, não nos permite considerer naturalmente situações onde um certo programa, por exemplo, retorna valores para certas entradas aceitáveis, e para as outras não: talvez ele fica num *loop infinito*; ou ele faz a máquina explodir; ou simplesmente não termina com uma saída—não importa o porquê. Definimos então o conceito de *função parcial*, que é exatamente isso: funções que para certas entradas aceitáveis delas, possivelmente *divergem*.

D9.213. Definição. Sejam A, B conjuntos. Chamamos a f uma *função parcial* de A para B sse:

para todo $x \in A$, se $f(x)$ é definido, então $f(x) \in B$.

Nesse caso, chamamos *domínio de convergência* o conjunto

$$\operatorname{domain} f \stackrel{\text{def}}{=} \{\, x \in A \mid f(x) \text{ é definido} \,\}$$

e *codomínio* o B mesmo. Preferimos usar os sinônimos *source* e *target* para o A e B para não ter o conflito entre domínio e domínio de convergência, escrevendo $\operatorname{src} f$ e $\operatorname{tgt} f$ respectivamente.

Naturalmente não podemos usar o símbolo fx em expressões matemáticas quando o $x \notin \operatorname{domain} f$, já que fx é indefinido nesse caso. Mesmo assim, abrimos uma exceção, introduzindo a notação

$$f\,x\uparrow \stackrel{\text{def}}{\iff} x \in A \;\&\; x \notin \operatorname{domain} f$$

que lemos assim: f *diverge* no x. Dizemos que f *converge* no x, e escrevemos $f\,x\downarrow$ quando $x \in \operatorname{domain} f$.

Escrevemos $f : A \rightharpoonup B$ para «f é uma função parcial de A para B». Naturalmente denotamos o conjunto de todas as funções parciais de A para B por

$$(A \rightharpoonup B) \stackrel{\text{def}}{=} \{\, f \mid f : A \rightharpoonup B \,\}.$$

▸ **EXERCÍCIO x9.99.**
Se A, B são finitos, qual a cardinalidade do $(A \rightharpoonup B)$? (x9.99 H 1 2)

9.214. Observação. Com essas definições cada função total é uma função parcial. Escrevemos esse «total» quando queremos enfatizar, mas normalmente «função» sem o adjectivo «parcial» significa «função total». Claramente, quando trabalhamos principalmente com funções parciais, seguimos a convenção oposta.

▸ **EXERCÍCIO x9.100.**
Sejam $A \xrightarrow{f} B \xrightarrow{g} C$. Como definarias a composição $g \circ f$? (x9.100 H 0)

9.215. Observação (Condições). Encontramos então aqui o que acontece se apagar a primeira das condições 9.11:

(1) ~~totalidade~~;
(2) determinabilidade.

e ficar só com a (2). No Problema Π9.19 implementarás funções *não-deterministicas*, onde apagamos a (2), ficando apenas com a totalidade. E se apagar as duas? Esse conceito podemos facilmente implementar assim que conhecer melhor relações (Capítulo 10).

§220. Fixpoints

D9.216. Definição (Fixpoint). Seja $f : A \to A$ um endomapa num conjunto A. Chamamos *fixpoint* da f qualquer $x \in A$ tal que $f(x) = x$. Com palavras de rua,

$$x \text{ é um fixpoint de } f \stackrel{\heartsuit}{\iff} f \text{ deixa } x \text{ em paz.}$$

• **EXEMPLO 9.217.**
Para qualquer conjunto A, todos os seus membros são pontos fixos da id_A.

• **NÃOEXEMPLO 9.218.**
No outro extremo, nem a $succ : \mathbb{N} \to \mathbb{N}$ possui fixpoints, nem a $mother : \mathsf{Person} \to \mathsf{Person}$—o que seria um fixpoint da *mother*?

• **EXEMPLO 9.219 (trigonometria).**
0 é um fixpoint da sin—tem outros? E a cos?

• **EXEMPLO 9.220.**
A $\mathrm{square} = \lambda x \,.\, x^2 : \mathbb{Z} \to \mathbb{Z}$ possui dois fixpoints: o 0 e o 1.

9.221. Observação. Olhando para o diagrama interno dum endomapa (9.39) os fixpoints são os "redemoinhos" .

▸ **EXERCÍCIO x9.101.**
Seja $d \in \mathbb{N}$. Defina uma função $f : \mathbb{N} \to \mathbb{N}$ com exatamente d fixpoints. (x9.101 H 1)

9.222. Teaser. OK, eu sei: parece estranho dedicar uma secção só pra isso. Mas os fixpoints vão fazer um papel importantíssimo depois, e queria destacá-los desde já. (Mentira: não um. Muitos!)

TODO Adicionar refs para secções específicas

§221. Definições recursivas

Já encontramos várias definições recursivas. Agora vamos analisar com que precisamos tomar cuidado para garantir que nossas "funções" realmente são funções bem-definidas. Vamos começar lembrando como exemplo duas funções recursivas famosas demais.

• **EXEMPLO 9.223.**
Sejam $a : \mathbb{N} \to \mathbb{N}$ definida pelas

$$\begin{aligned} a(0) &= 1 \\ a(n) &= n \cdot a(n-1), \quad \text{para todo } n > 0; \end{aligned}$$

e $b : \mathbb{N} \to \mathbb{N}$ definida pelas

$$\begin{aligned} b(0) &= 1 \\ b(1) &= 1 \\ b(n) &= b(n-1) + b(n-2), \quad \text{para todo } n > 1. \end{aligned}$$

Muitas vezes deixamos as frases "para todo $n > 0$" como implícitas pelo contexto—mas entenda que elas precisam estar lá, e *estão* lá mesmo quando escolhemos omiti-las.

Agora, assuma que tu aceita ambas as $a, b : \mathbb{N} \to \mathbb{N}$ do exemplo assima como funções *bem-definidas*, e continue lendo.

9.224. Recursão mutual. Podemos definir duas ou mais funções, cada uma chamando recursivamente outras, tomando certos cuidados como sempre para garantir que realmente todas as funções vão ser definidas mesmo para todas as entradas aceitas pelos domínios delas.

• **EXEMPLO 9.225.**
Vamos definir as funções $even, odd : \mathbb{N} \to \{0, 1\}$ pelas

$$\begin{aligned} even(0) &= 1 & odd(0) &= 0 \\ even(n+1) &= odd(n) & odd(n+1) &= even(n) \end{aligned}$$

Calculamos, por exemplo:

$$\begin{aligned} even(3) = odd(2) = even(1) = odd(0) = 0 \\ odd(3) = even(2) = odd(1) = even(0) = 1 \end{aligned}$$

9.226. Recursão segura. Na maioria das vezes que definimos funções recursivamente existe "algo"—muitas vezes esse "algo" é o próprio argumento da função (como no Exemplo 9.223) mas não sempre—que com cada "chamada recursiva" da função fica menor e menor, até cair num valor que garanta uma "saída da recursão". (Essa descripção é bem vaga sim.)

• **EXEMPLO 9.227.**
Seja $p : \mathbb{N} \to \mathbb{N}$ a função definida pela:

$$p(x) = \begin{cases} \log_2(x), & \text{se } x \text{ é uma potência de 2;} \\ p(x+1), & \text{se não.} \end{cases}$$

Aqui nas chamadas recursivas não é o próprio argumento que é "cada vez menor"—pelo contrário: as chamadas recursivas estão sendo cada vez com argumento maior! Mesmo assim, a recursão "sempre termina", e a f realmente é bem-definida. Calculamos como exemplo uns valores:

$$\begin{aligned} p(0) = p(1) &= \log_2(1) = 0 \\ p(4) &= \log_2(4) = 2 \\ p(5) = p(6) = p(7) = p(8) &= \log_2(8) = 3 \\ p(1020) = p(1021) = p(1022) = p(1023) = p(1024) &= \log_2(1024) = 10. \end{aligned}$$

▸ **EXERCÍCIO x9.102.**
Ache um "algo" que fica cada vez menor com cada chamada recursiva da p do Exemplo 9.227. (x9.102 H 1)

9.228. Recursão perigosa. Não é cada equação recursiva que realmente defina uma função! Vamos ver agora uns exemplos que mostram exatamente isso.

• **EXEMPLO 9.229.**
Seja $f : \mathbb{N} \to \mathbb{N}$ a função definida pela

$$f(n) = f(n), \quad \text{para todo } n \in \mathbb{N}.$$

É óbvio que isso não *determina* uma função. Mas por quê?

• **EXEMPLO 9.230.**
Seja $g : \mathbb{N} \to \mathbb{N}$ a função definida pela

$$\begin{aligned} g(0) &= 1 \\ g(n) &= g(n) + 1, \quad \text{para todo } n > 0. \end{aligned}$$

Isso também não *determina* uma função. Por quê?

• **EXEMPLO 9.231.**
Seja $h : \mathbb{N} \to \mathbb{N}$ a função definida pela

$$h(n) = h(n+1), \quad \text{para todo } n \in \mathbb{N}.$$

Isso também não *determina* uma função—mas por quê?

‣ **EXERCÍCIO x9.103.**
As perguntas sobre as f, g, h acima não foram rhetóricas! (x9.103 H 0)

• **EXEMPLO 9.232.**
Considere a função $k : \mathbb{N} \to \mathbb{N}$ definida pela recursão

$$\begin{aligned} k(0) &= 1 \\ k(1) &= 1 \\ k(n) &= \begin{cases} k(n/2), & \text{se } n \text{ é potência de 2} \\ k(n+1), & \text{caso contrário} \end{cases} \quad (\text{para todo } n > 1). \end{aligned}$$

Aceitaria isso como uma definição duma função $k : \mathbb{N} \to \mathbb{N}$?

• **EXEMPLO 9.233.**
Considere a função $d : \mathbb{N} \to \mathbb{N}$ definida pela recursão

$$\begin{aligned} d(0) &= 1 \\ d(1) &= 1 \\ d(n) &= \begin{cases} d(n/2), & \text{se } n \text{ é potência de 2} \\ d(n+3), & \text{caso contrário} \end{cases} \quad (\text{para todo } n > 1). \end{aligned}$$

Aceitaria isso como uma definição duma função $d : \mathbb{N} \to \mathbb{N}$?

‣ **EXERCÍCIO x9.104.**
Responda nas perguntas dos exemplos acima (9.232 e 9.233). (x9.104 H 0)

▸ **EXERCÍCIO x9.105.**
Usando as $k, d : \mathbb{N} \to \mathbb{N}$ dos exemplos 9.232 e 9.232 acima calcule os:

$$k(6); \quad k(9); \quad d(5); \quad d(11); \quad d(6).$$

(Confira teus resultados com minha dica e minha resolução!) (x9.105 H 1)

▸ **EXERCÍCIO x9.106.**
Qual é a função k do Exemplo 9.232? (Tu deves saber um nome dela bem simples.) (x9.106 H 0)

• **EXEMPLO 9.234.**
Considere a função $c : \mathsf{Nat} \to \mathsf{Nat}$ definida pela recursão

$$\begin{aligned} c(0) &= 1 \\ c(1) &= 1 \\ c(n) &= \begin{cases} c(n/2), & \text{se } n \text{ é par} \\ c(3n+1), & \text{caso contrário} \end{cases} \qquad (\text{para } n > 1). \end{aligned}$$

E a mesma pergunta: aceita?

▸ **EXERCÍCIO x9.107.**
Calcule os valores $c(8), c(3), c(7)$ da função c acima. (x9.107 H 0)

9.235. O que tá acontecendo?. Já deve ser claro que apenas escrevendo umas equações que envolvem a função que queremos definir não é uma maneira segura que garanta que realmente nossas equações *determinam* (definam) uma função. Umas vezes deu certo, outras não. Mas em todos os casos, a "definição" da função foi apenas uma *lista de equações.*[67] Estamos procurando entender melhor essa situação: um cara chega com um um bocado de equações como uma suposta definição recursiva duma função, e a gente da uma olhada nelas, e aceita isso como definição mesmo; outro cara chega com *o mesmo tipo de coisa* (um bocado de equações) e no caso dele a gente falou "desculpa mas isso não serve como definição de função". O que tá acontecendo?

9.236. Lembra da "matemática" na escola?. Lembra os *sistemas de equações* em um ou mais *incógnitos* que tu precisava *resolver* estudando matemática básica?[68] Por exemplo, um exercício pode pedir para o aluno: *resolva o sistema* seguinte nos reais ($x \in \mathbb{R}$):

$$\begin{aligned} x^2 &= 64 \\ 10 + 2x &= 2 + x \end{aligned}$$

O aluno vai responder que

$$\text{«o sistema tem uma resolução única: } x = -8\text{»}$$

e vai ganhar um biscoito. Esses sistemas são mais comuns em espaços de dimenções superiores ($\mathbb{R}^2$, $\mathbb{R}^n$, $\mathbb{C}^n$, etc.). Mas no final das contas, qual é o objectivo? O que significa resolver um sistema deles? Bem, significa dar uma das seguintes respostas:

[67] Foi mesmo? Não exatamente: mas deixe isso para depois (Observação 9.240).

[68] Presumo aqui que o leitor já teve contato com esse tipo de exercícios desde criança; mas caso contrário, espero que a conversa vai continuar fazendo sentido.

(i) O sistema é impossível;
(ii) O sistema é possível e indeterminado;
(iii) O sistema é possível e determinado;

e nos dois últimos casos, queremos descrever todas as resoluções se for indeterminado, ou achar sua única resolução caso que é determinado. Uns sistemas no $\mathbb{R}^2$ por exemplo são os:

$$\text{(A)}\begin{cases} x^2+y^2=1 \\ y=2x \end{cases} \qquad \text{(B)}\begin{cases} y=x^2+8 \\ x=y+1 \end{cases} \qquad \text{(C)}\begin{cases} x=2y+1 \\ 3x-6y=3 \end{cases} \qquad \text{(D)}\begin{cases} x=y^2 \\ y=\sin(x). \end{cases}$$

Aqui o aluno deu umas respostas interessantes. (A) O sistema é possível mas indeterminado: tem duas resoluções: $(x,y)=\big(\sqrt{3}/2,1/2\big)$ e $(x,y)=\big(1/2,\sqrt{3}/2\big)$. (B) O sistema é impossível: nenhum par $(x,y)\in\mathbb{R}^2$ satisfaz ambas as equações. (C) O sistema é possível mas indeterminado: todos os membros do conjunto $\{\,(t,2t+1)\in\mathbb{R}^2 \mid t\in\mathbb{R}\,\}$ satisfazem o sistema (e tem pelo menos dois membros nesse conjunto—na verdade tem uma infinidade deles). (D) O sistema é possível e determinado: tem resolução única, o $(x,y)=(0,0)$.

9.237. Observação. O fato que um sistema tem uma infinidade de resoluções, não significa que *todos* os possíveis candidatos são resoluções. Por exemplo o sistema (3) acima tem uma infinidade de resoluções, mas não são todos os membros do $\mathbb{R}^2$ que servem: considere o $(x,y):=(1,1)$ por exemplo.

9.238. Definições recursivas como sistemas para resolver. O que isso tem a ver com as definições recursivas? No primeiro sistema acima estamos procurando *números reais*, ou seja, estamos procurando determinar o incógnito $x\in\mathbb{R}$ que consegue satisfazer todas as suas equações.

$$\begin{aligned} x^2 &= 64 \\ 10+2x &= 2+x \end{aligned}$$

Podemos pensar então que todos os reais são candidatos consideráveis aqui, e nosso trabalho é achar quem serve para o sistema (se é possível) e quem não. Testando então para o $x:=8$ temos:

$$\begin{aligned} x^2 &= 64 \\ 10+2\cdot x &= 2+x \end{aligned} \quad\rightsquigarrow\quad \begin{aligned} 8^2 &= 64 \\ 10+2\cdot 8 &= 2+8 \end{aligned}$$

e assim percebemos que o 8 *não* serve pois tem pelo menos uma equação que ele não satisfaz. E a situação é similar resolvendo sistemas com incógnitos membros de $\mathbb{R}^2$ ou $\mathbb{C}^n$, etc., onde procuramos um par de números reais no primeiro caso, ou n números complexos no segundo, etc. Testamos então o $(\sqrt{2},0)$ nos sistemas

$$\text{(A)}\begin{cases} x^2+y^2=1 \\ y=2x \end{cases} \qquad \text{(B)}\begin{cases} y=x^2+8 \\ x=y+1 \end{cases} \qquad \text{(C)}\begin{cases} x=2y+1 \\ 3x-6y=3 \end{cases} \qquad \text{(D)}\begin{cases} x=y^2 \\ y=\sin(x). \end{cases}$$

etc., etc.

Agora te convido olhar para todas as definições recursivas que a gente encontrou aqui com uma maneira similar: *como sistemas*, onde agora *o incógnito não é um número real mas uma função no* $(\mathbb{N}\to\mathbb{N})$.

• **EXEMPLO 9.239.**
Considere o sistema que usamos para definir a função b do Exemplo 9.223.

$$\begin{aligned} b(0) &= 0 \\ b(1) &= 1 \\ b(n) &= b(n-1) + b(n-2), \quad \text{para todo } n > 1. \end{aligned}$$

Agora o incógnito é uma função $b : \mathbb{N} \to \mathbb{N}$. Vamos testar uns candidatos consideráveis: tome $b := \mathrm{id}_{\mathbb{N}}$:

$$\left.\begin{aligned} \mathrm{id}_{\mathbb{N}}(0) &= 0 \\ \mathrm{id}_{\mathbb{N}}(1) &= 1 \\ \mathrm{id}_{\mathbb{N}}(n) &= \mathrm{id}_{\mathbb{N}}(n-1) + \mathrm{id}_{\mathbb{N}}(n-2) \end{aligned}\right\} \iff \begin{cases} 0 = 0 \\ 1 = 1 \\ n = (n-1) + (n-2), \quad \text{para todo } n > 1. \end{cases}$$

Legal! As duas primeiras linhas do sistema são satisfeitas. Para a terceira, testando com o $n := 3$ dá certo, pois realmente $3 = 2 + 1$ mas é muito fácil perceber que essa igualdade não é satisfeita em geral. Tome $n := 4$ e já temos problema, pois $4 \neq 3 + 2$. O candidato $\mathrm{id}_{\mathbb{N}}$ então não satisfaz o sistema. Próximo! Vamos tentar com $b := succ$, essa vez divulgando a notação mais econômica, sem parenteses:

$$\left.\begin{aligned} succ\ 0 &= 0 \\ succ\ 1 &= 1 \\ succ\ n &= succ\ (n-1) + succ\ (n-2) \end{aligned}\right\} \iff \begin{cases} 1 = 0 \\ 2 = 1 \\ n + 1 = n + (n-1), \quad \text{para todo } n > 1. \end{cases}$$

Fuen-fuen-fuen! Bem, então nem a $\mathrm{id}_{\mathbb{N}}$ nem a $succ$ satisfazem esse sistema.

9.240. Observação. No Nota 9.235 afirmei que cada suposta definição de função foi "apenas uma lista de equações". São realmente listas de *equações?* Umas dessas afirmações não são equações não; pois em vez de ter a forma "____ = ____" elas têm a forma "$\forall n$ ____". Ou seja, correspondem em proposições universais (quantificadas universalmente) e não em proposições (atômicas) de equações. Mas não seria errado considerar que essas são listas de equações sim, com o acordo que... são listas infinitas! Pois sim, podemos ver cada uma dessas como um *esquema* de equações que fornece uma equação para cada escolha de $n \in \mathbb{N}$.

9.241. Quando um sistema serve para definir. Quando um sistema cujos incógnitos são números tem resolução única isso quis dizer que o sistema *determina* um certo número. Ou seja, *podemos usar o próprio sistema para definir um número real* como a resolução dele. Por exemplo, escrevemos «seja $r \in \mathbb{R}$ *a* resolução do sistema tal», etc. Observe o artigo definido! Por outro lado, se o sistema tem várias resoluções, *não pode servir como definição;* mas pelo menos sabendo que o conjunto das suas resoluções não é vazio podemos escrever, por exemplo, «seja $t \in \mathbb{R}$ *uma* resolução do sistema tal». E nada muda com sistemas cujos incognitos são funções! E por que mudaria? No final das contas é a existência e unicidade de algo que nos permite defini-lo!

Voltamos agora para o sistema que usamos para definir as funções a, b do Exemplo 9.223.

? **Q9.242. Questão.** Tu conhece alguma função que satisfaz o sistema da a? Alguma que satisfaz o sistema da b?

!! SPOILER ALERT !!

Resposta comum. *Possivelmente* o leitor respondeu

«Sim: o factorial para o primeiro, e a função fibonacci para o segundo.»

ou algo similar. Só que: eu esqueci quais são essas funções. Pode lembrar pra mim, por exemplo, qual é essa função "fibonacci" que tu tá afirmando que é uma resolução do sistema da b?

«Claro. Vou escrever esse poeminho mágico para dar a sua definição:»

D9.243. Definição. Seja $\mathit{fib} : \mathbb{N} \to \mathbb{N}$ definida pelas

$$\text{(FIB)} \quad \begin{cases} \mathit{fib}\, 0 = 0 \\ \mathit{fib}\, 1 = 1 \\ \mathit{fib}\, n = \mathit{fib}\,(n-1) + \mathit{fib}\,(n-2), & \text{para todo } n > 1. \end{cases}$$

↯

? **Q9.244. Questão.** Tem problema?

!! SPOILER ALERT !!

Resposta. Usamos a própria coisa que queremos definir (a função fibonacci) para justificar sua própria definição (ou seja, para argumentar que o sistema (FIB) tem resolução única)! (E sobre o factorial seria a mesma coisa.) Como a fib foi definida pelas equações recursivas do (FIB), sua definição *depende da existência e unicidade da resolução do sistema*, então não podemos usá-la antes de demonstrar isso!

9.245. Infelizmente, caro Fibonacci, não estamos prontos neste momento para demonstrar que esse sistema tem *pelo menos* uma resolução![69] Atrás desse fato fica o poderoso Teorema de Recursão Θ16.92. Mas pelo menos deve ser fácil demonstrar que tem *no máximo* uma resolução:

[69] Mas calma, daqui uns capítulos estaremos!

▸ **EXERCÍCIO x9.108.**
Demonstre que se o sistema (FIB) da Definição D9.243 tem resolução, então ela é única. (x9.108 H 1 2 3 4)

▸ **EXERCÍCIO x9.109.**
Com esse novo ponto de vista, para cada uma das supostas definições das funções $f, g, h : \mathbb{N} \to \mathbb{N}$ (dos exemplos 9.229, 9.230, e 9.231) responda na pergunta: por que não deu certo?

$$(1)\ \{ f(n) = f(n) \qquad (2)\ \begin{cases} g(0) = 1 \\ g(n) = g(n) + 1 \end{cases} \qquad (3)\ \{ h(n) = h(n+1)$$

Foi porque o sistema não tem resoluções? Ou porque tem várias? Tem infinítas? Tem todas? (x9.109 H 0)

▸ **EXERCÍCIO x9.110.**
Quais são exatamente as funções que satisfazem a "definição" da h acima? (x9.110 H 1)

▸ **EXERCÍCIO x9.111.**
Qual o problema com a definição da função c do Exemplo 9.234? (x9.111 H 1)

Deixamos esse assunto por enquanto (até o Capítulo 4), supondo que temos já um entendimento de como definições recursivas funcionam.

Intervalo de problemas

▸ **PROBLEMA Π9.18 (Implementação: funções parciais).**
Pense numa maneira de *implementar* o tipo das *funções parciais* (Secção §219) usando conceitos (tipos) que encontramos até agora: conjuntos, tuplas, seqüências, famílias indexadas, funções, etc.

Para implementar um conceito não basta apenas definir o que são os objetos desse tipo em termos de já conhecidos. Precisamos implementar também a interface desejada, em termos de operações e relações que já temos em nossa disposição. (Π9.18 H 1 2 3)

▸ **PROBLEMA Π9.19 (Implementação: funções não-determinísticas).**
Na Secção §219 definimos um conceito mais geral de "função": as *funções parciais*, onde apagamos a primeira das condições 9.11:

~~(1) totalidade~~;
(2) determinabilidade.

Neste problema, encontramos *funções não-determinísticas*, ou seja, "funções" que não respeitam necessariamente a determinabilidade; apenas a totalidade. Ou seja, agora apagamos a outra condição:

(1) totalidade;
~~(2) determinabilidade~~.

O objectivo desse problema é *implementar o tipo de função não-determinística*.

Como definarias a composição $g \cdot f$ de duas funções não-determinísticas? Use a notação $f : A \rightsquigarrow B$ para «f é uma função não-determinística de A para B». Que mais tu poderias fazer para tua implementação ser uma implementação boa? (Π9.19 H 0)

▸ **PROBLEMA Π9.20.**
Tem como mudar o $\mathbb{Z}$ do Exemplo 9.220 para outro conjunto X de números, tal que tua $\mathrm{square} : X \to X$ terá mais que dois fixpoints? (Π9.20 H 1 2 3)

▸ **PROBLEMA Π9.21.**
Seja $f : A \to A$. Demonstre a afirmação:

$$x \text{ é um fixpoint da } f \iff \text{para todo } n \in \mathbb{N},\ x \text{ é um fixpoint da } f^n.$$

(Π9.21 H 1)

▸ **PROBLEMA Π9.22.**
Seja $F \subseteq (A \to A)$ e seja $a \in A$. Demonstre ou refute a afirmação:

$$a \text{ é um fixpoint de toda } f \in F \iff \left\{ \begin{array}{c} \text{para todo } d \in \mathbb{N} \text{ e toda } \vec{f} \in F^d \\ a \text{ é um fixpoint da } f_1 \circ f_2 \circ \cdots \circ f_d. \end{array} \right\}$$

Como isso se compara com o Problema Π9.21? (Π9.22 H 0)

▸ **PROBLEMA Π9.23.**
Seja $f : A \to A$, e seja F o conjunto de todos os fixpoints da f.

$$F = \{\, x \in A \mid x \text{ é um fixpoint da } f \,\}$$

Quais das igualdades seguintes podemos concluir?:

$$f[F] = F \qquad\qquad f_{-1}[F] = F$$

Demonstre aquelas que sim; mostre um contraexemplo daquelas que não, mas verifique se alguma das duas inclusões ($\subseteq$) ou ($\supseteq$) é válida. O que muda se f é injetora? (Π9.23 H 0)

§222. Uma viagem épica

9.246. Algo irritante?. Seria bom desenvolver um certo "TOC" matemático: ganhar certas frescuras matemáticas úteis, e sentir *matematicamente irritados* quando sentir algo bizarro. E algo bizarro já aconteceu recentemente: tá bem ali na Definição D9.44 de injetora e sobrejetora:

$$\begin{array}{lll} f \text{ injetora} & \overset{\text{def}}{\iff} & (\forall x \in A)\,(\forall y \in A)\,[\, f\,x = f\,y \implies x = y\,]; \\ f \text{ sobrejetora} & \overset{\text{def}}{\iff} & (\forall b \in B)\,(\exists a \in A)\,[\, f\,a = b\,]. \end{array}$$

Consegues ver algo irritante?

!! SPOILER ALERT !!

Injectividade e sobrejectividade têm cara de conceitos que deveriam ser intimamente relacionados. Simétricos, duais, espelhados, sei lá o que, algo que com certeza não parece olhando para suas definições! A primeira começa com dois quantificadores do mesmo tipo, universais, ambos no domínio, e acaba com uma implicação; a segunda começa com dois quantificadores de tipos diferentes: um existencial, agora no codomínio, o outro universal no domínio, e acaba com uma igualdade! *Nada a ver*, pelo jeito![70] Isso deveria te dar pelo menos uns arrepeios; e no pior—melhor?—dos casos te deixar acordado até encontrar definições desses dois conceitos que realmente são intimamente relacionadas. Agora calma—podes dormir tranqüilamente—pois vamos chegar nessa satisfacção logo.

9.247. Bora viajar. Começamos na Secção §215 procurar conexões entre a composição e a multiplicação e realmente achamos muitas similaridades e essa influência já se tornou muito útil. Vamos começar dando uma olhada novamente numa propriedade de funções, a injectividade. Pela sua definição, f é injetora exatamente quando

$$\text{para todo } x, y, \quad f\,x = f\,y \implies x = y.$$

Isso até parece pouco com cancelamento:

$$\not{f}\,x = \not{f}\,y \implies x = y.$$

Queremos investigar se e quando podemos cancelar uma função quando operada com composições:

$$f \circ g = f \circ h \overset{?}{\implies} g = h$$

e como nossa operação já sabemos que não é comutativa precisamos tratar essa questões similares separadamente:

$$g \circ f = h \circ f \overset{?}{\implies} g = h$$
$$g \circ f = f \circ h \overset{?}{\implies} g = h.$$

Vamos voltar no

$$\not{f}\,x = \not{f}\,y \implies x = y$$

mas agora vamos fingir que os f, x, y são números reais! E logo as expressões fx e fy denotam apenas os produtos $f \cdot x$ e $f \cdot y$. Bem. O que podemos concluir sabendo que

$$f\,x = f\,y?$$

Caso $f \neq 0$, podemos cancelá-lo:

$$\not{f}\,x = \not{f}\,y$$

chegando assim na

$$x = y.$$

[70] Existe uma justificativa muito boa sobre isso: na própria idéia do que é uma função, não tratamos seu domínio e seu codomínio numa maneira parecida: a função foi "total no seu domínio" mas não no seu codomínio, e foi "univoca", ou seja, do mesmo ponto do seu domínio não podem sair duas setinhas (barradas), mas estamos de boas se nuns pontos do seu codomínio chegam mais que uma setinhas. Esqueça esse ponto de vista para viajar comigo aqui; prometo que no Capítulo 10 tu pode voltar a repensar nesse assunto.

Caso $f = 0$, a f não é cancelável.[71]

Parece ótimo: exatamente o tipo da coisa que estamos procurando! Será que podemos já trazer essa sabedoria da $(\cdot)$ nos números para a $\circ$ nas funções? O que seria nosso "zero" nas funções? Uma resposta boba seria «a função constante 0». Com certeza para funções numéricas a função constante $\mathrm{k}_0 = \lambda x\,.\,0$ não é nada de cancelável. (Veja Exercício x9.112.) Por que boba então? Pois dizendo isso já perdemos a generalidade: *queremos algo descrevível para qualquer função e não algo que serve apenas para funções cujos codomínios tem o* 0 *como membro.* Mas peraí. Talvez não é o "ser zero" que é importante nesse ponto de cancelamento! Realmente: por que esse «se $f \neq 0$» acima? *«É que se $f = 0$ então f não é cancelável.»* Mas essa resposta não é exatamente iluminante. O que nos permite cancelar números na multiplicação? Vamos tentar algo mais cuidadoso e formal:[72]

$$\begin{aligned} fx = fy &\implies f^{-1}(fx) = f^{-1}(fy) && \text{(multiplicando por } f^{-1}\text{)} \\ &\implies (f^{-1}f)x = (f^{-1}f)y && \text{(pela associatividade da } (\cdot)\text{)} \\ &\implies 1x = 1y && \text{(pela def. da } f^{-1}\text{)} \\ &\implies x = y. && \text{(pela def. de 1)} \end{aligned}$$

O único passo duvidoso seria o primeiro: como sabemos que existe esse inverso? *Não sabemos.* Então talvez é isso que estamos procurando! Talvez

$$f \text{ tem inversa} \overset{?}{\iff} f \text{ é cancelável!}$$

Para demonstrar essa afirmação precisamos saber o que "cancelável" significa formalmente aqui. Qual das três implicações que consideramos acima vamos escolher?:

$$f \text{ é cancelável} \overset{?}{\iff} \begin{cases} f \circ g = f \circ h \implies g = h \\ g \circ f = h \circ f \implies g = h \\ g \circ f = f \circ h \implies g = h. \end{cases}$$

A $(\cdot)$ nos números, sendo uma operação *comutativa*, não consegue diferenciar entre essas afirmações. Ou seja, por causa da riquesa das leis que temos na multiplicação nos números, certas distinções desaparecem, "se desabam"—algo que podemos pensar como pobresa também! E vice versa: com menos leis ganhamos mais distinções—riquesa! No mundo dos reais, um certo x ou tem inverso ou não. De qual lado inverso? Não faz sentido perguntar isso nos números pois o lado não importa. Quando importa, não vamos falar apenas sobre "inverso" mas sim sobre *inverso esquerdo* e *inverso direito*. Similarmente, nos números só tem uma 1 para considerar; nas funções, cada conjunto A chega com sua própria 1_A! *O mundo das funções é suficientemente rico para enxergar essas noções inenxergáveis no mundo dos números!*

▸ **EXERCÍCIO x9.112.**
Demonstre que a função constante $\mathrm{k}_0 : \mathbb{R} \to \mathbb{R}$ em geral não é cancelável nem pela direita nem pela esquerda. (x9.112 H 0)

[71] Por que não? Se tu aprendeu numa maneira religiosa algum poeminha do tipo "não cancelarás 0 nas multiplicações", esqueça; ninguém se importa com que teu padre falou. A gente vai voltar nessa questão mais tarde (Capítulo 12 (§263); Capítulo 6).

[72] Mesmo sendo cedo neste momento para essa abordagem creio que o leitor vai conseguir acompanhar a idéia. Estudando algebra abstrata nos capítulos 11 e 12 tudo isso vai aparecer bem tranqüilo e natural. Prometo.

9.248. Olhe de novo na implicação que tem na definição da injetora:

(L-canc) $$f\,x = f\,y \implies x = y.$$

Ela lembra muito do que acabamos de demonstrar, mas nosso objectivo foi investigar a composição $\circ$ usando a multiplicação $(\cdot)$. Quando escrevi a (L-canc) em números, a justaposição denotou a $(\cdot)$ mesmo; mas na definição da injetora que temos, a justaposição não denota a $\circ$, mas a *eval*! Então vamos ver o que acontece se mudar para a $\circ$, obviamente tomando cuidado para usar objetos dos certos tipos:

$$f \circ g = f \circ h \overset{?}{\implies} g = h$$

que escrevemos por justaposição sem confusão:

$$fg = fh \overset{?}{\implies} g = h.$$

Vamos tentar imitar a demonstração anterior:

$$\begin{aligned} fg = fh &\implies f^{-1}(fg) = f^{-1}(fh) && \text{(??)} \\ &\implies (f^{-1}f)g = (f^{-1}f)h && \text{((F-Ass))} \\ &\implies 1_A g = 1_A h && \text{((F-Inv))} \\ &\implies g = h && \text{((F-Id))} \end{aligned}$$

O que precisamos no '??' acima?

!! SPOILER ALERT !!

9.249. Uma resposta "de preguiça" seria "preciso f bijetora". Claro que isso é *suficiente*, mas é *necessário* também? Começamos pensando que "f injetora" é algo que corresponde nesse cancelamento aí, então será que basta só isso? Mas parece que precisei a existência de f^{-1}, ou seja, precisamos que f seja invertível. Ou não? Lembre que o inverso f^{-1} de f é um objeto que satisfaz *ambas* as

(LInv) $$f^{-1}f = 1_A; \qquad ff^{-1} = 1_B$$ (RInv)

mas, olhando de novo para nosso caminho, a gente precisou apenas a (LInv). Então não necessitamos mesmo que f tem um inverso f^{-1}; basta ter um inverso-esquerdo f_{L} e a demonstração rola:

$$\begin{aligned} fg = fh &\implies f_{\mathrm{L}}(fg) = f_{\mathrm{L}}(fh) && (f \text{ é L-invertível}) \\ &\implies (f_{\mathrm{L}}f)g = (f_{\mathrm{L}}f)h && \text{((F-Ass))} \\ &\implies 1_A g = 1_A h && \text{((F-LInv))} \\ &\implies g = h. && \text{((F-Id))} \end{aligned}$$

Já temos descoberto umas idéias interessantes: L-cancelável e L-invertível, e obviamente temos as noções laterais de R-cancelável e R-invertível.

Influenciados por toda essa viagem, podemos chegar nuns resultados muito importantes e interessantes sobre as "jectividades" ('in-' e 'sobre-'); as invertibilidades laterais; e as cancelabilidades laterais das funções.

? **Q9.250. Questão.** Quais resultados tu acha que vamos demonstrar? Consegues demonstrá-los?

!! SPOILER ALERT !!

Resposta. Um chute bom é o seguinte:

$$\begin{aligned} f \text{ mono} &\overset{\text{def}}{\iff} f \text{ L-cancelável} \overset{?}{\iff} f \text{ L-invertível} \overset{?}{\iff} f \text{ injetora} \\ f \text{ epí} &\overset{\text{def}}{\iff} f \text{ R-cancelável} \overset{?}{\iff} f \text{ R-invertível} \overset{?}{\iff} f \text{ sobrejetora.} \end{aligned}$$

E sim, tem esses nomes chique mesmo.

D9.251. Definição (mono, epi). Seja $f : A \to B$. Dizemos que f é uma função *mônica* (ou simplesmente que f é uma *mono*) sse f é $\circ$-cancelável pela esquerda. Dizemos que f é uma função *épica* (ou simplesmente que f é uma *epí*) sse f é $\circ$-cancelável pela direita.

Bora investigar então!

Θ9.252. Teorema. *Sejam $B \xrightarrow{f} C$. A f é injetora sse ela é $\circ$-cancelável pela esquerda:*

$$f \circ g = f \circ h \implies g = h$$

para todas as g, h tais que as composições acima são definidas.

▸ Esboço. A direção ($\Rightarrow$) é o Exercício x9.113. Para a direção ($\Leftarrow$), tome $b, b' \in B$ tais que $f(b) = f(b')$. Basta demonstrar que $b = b'$. Tome $A := \{0\}$ e defina g, h no diagrama

$$\{0\} \underset{h}{\overset{g}{\rightrightarrows}} B \xrightarrow{f} C$$

em tal maneira que o diagrama comuta (tem que definir mesmo as g, h). Usamos agora a hipótese para concluir que $b = b'$. □ (Θ9.252P)

▸ **EXERCÍCIO x9.113.**
Demonstre a direção ($\Rightarrow$) do Teorema Θ9.252. (x9.113H0)

Θ9.253. Teorema. *Sejam* $B \xrightarrow{f} C$. *A* f *é sobrejetora sse ela é* $\circ$*-cancelável pela direita:*

$$g \circ f = h \circ f \implies g = h$$

para todas as g, h *tais que as composições acima são definidas. Digamos então que* f *é* $\circ$*-cancelável pela direita.*

▸ Esboço. A direção ($\Rightarrow$) é o Exercício x9.114. Para a direção ($\Leftarrow$), tomamos $c \in C$ e procuramos achar $b \in B$ tal que $f(b) = c$. Defina o D (cuidado: aqui não ajuda tomar $D = \{0\}$) e as g, h no diagrama

$$B \xrightarrow{\quad f \quad} C \underset{h}{\overset{g}{\rightrightarrows}} D$$

em tal maneira que $g \neq h$, mas mesmo assim *concordam em todo o* C *exceto no ponto* c. Usando a contrapositiva da hipótese ganhamos $g \circ f \neq h \circ f$, mas isso só pode acontecer se a f mandou pelo menos um ponto do domínio dela para o c. □ (Θ9.253P)

▸ **EXERCÍCIO x9.114.**
Demonstre a direção ($\Rightarrow$) do Teorema Θ9.253. (x9.114H0)

▸ **EXERCÍCIO x9.115 (Mono e epí com diagramas comutativos).**
Descreva as propriedades das definições de mono e epi (D9.251) usando diagramas comutativos. (x9.115H0)

D9.254. Definição (conjuntos isómorfos). Sejam A, B conjuntos. Chamamos os A, B *conjuntos isómorfos* (ou *isomórficos*) sse existe bijecção $f : A \rightarrowtail B$. Nesse caso chamamos a f um *isomorfismo de conjuntos*. Escrevemos $A \cong B$, e também $f : A \cong B$ ou $f : A \xrightarrow{\cong} B$ para denotar que f é um isomorfismo do conjunto A para o conjunto B.

9.255. Observação (etimologia). As palavras vêm do grego *ίσο* que significa "igual" e *μορφή* que significa "forma". Isómorfos então são aqueles que têm a mesma forma; "a mesma cara". Mas o que significa forma, cara? Depende do contexto! Aqui nos conjuntos, podemos pensar que $A \cong B$ quis dizer que os A e B só podem variar nos *nomes* usados para seus membros e em nada mais: um isomorfismo seria um renomeamento, uma tradução *fiel* de A para B. Podemos considerar então o B como uma *cópia* do A onde apenas re-rotulámos seus membros. Começando no Capítulo 11 vamos estudar tipos de coisas onde sua forma é bem mais rica que isso, e lá "isómorfos" vai acabar sendo uma noção bem mais forte.

Já tivemos definido os conceitos de inversa e de identidade antes de fazer essa viagem que fizemos aqui. Mas com essa experiência podemos voltar e repensar em mais motivações e influências para chegar nesses conceitos, e mais idéias para demonstrar nossos teoremas. Pode viajar à vontade! Graças a tudo isso, já podemos dormir tranqüilamente pois encontramos finalmente umas definições para satisfazer nossas frescuras.

§223. Retracções e secções

D9.256. Definição (Retracções, secções). Seja $f : A \to B$. Se $r : B \to A$ satisfaz a

$$r \circ f = \mathrm{id}_A$$

dizemos que r é uma *retracção* ou uma $\circ$-*inversa esquerda* da f. Se $s : B \to A$ satisfaz a

$$f \circ s = \mathrm{id}_B$$

dizemos que s é uma *secção* ou uma $\circ$-*inversa direita* da f. Observe que no primeiro caso, f é uma secção da r; e no segundo caso f é uma retracção da s.

Ganhamos imediatamente dois corolários fáceis dos teoremas Θ9.252–Θ9.253:

9.257. Corolário. *Se $f : A \to B$ tem retracção, então f é injetora.*

Demonstração. Seja r uma retracção da f. Temos

$$f \circ g = f \circ h \implies r \circ f \circ g = r \circ f \circ h \implies \mathrm{id}_A \circ g = \mathrm{id}_A \circ h \implies g = h$$

e logo f é injetora pelo Teorema Θ9.252. ∎

9.258. Corolário. *Se $f : A \to B$ tem secção, então f é sobrejetora.*

Demonstração. Seja s uma secção da f. Temos

$$g \circ f = h \circ f \implies g \circ f \circ s = h \circ f \circ s \implies g \circ \mathrm{id}_B = h \circ \mathrm{id}_B \implies g = h$$

e logo f é sobrejetora pelo Teorema Θ9.253. ∎

▸ **EXERCÍCIO x9.116.**
Demonstre o Corolário 9.257 elementariamente (sem o Θ9.252). (x9.116H0)

▸ **EXERCÍCIO x9.117.**
Demonstre o Corolário 9.258 elementariamente (sem o Θ9.253). (x9.117H0)

TODO Como chegar na definição alternativa

▸ **EXERCÍCIO x9.118.**
O que mais falta demonstrar? Apenas enuncie o que é, sem demonstrar. (x9.118H1)

Θ9.259. Teorema (Basta uma lei: agora sem pontos). *Seja $f : A \rightarrowtail B$. Se uma $f' : B \to A$ satisfaz pelo menos uma das duas leis da inversa (Nota 9.191), então $f' = f^{-1}$.*

Demonstração. Caso que f' satisfaz a (L):

$$\begin{aligned}
f' &= f' \circ \mathrm{id}_B && \text{(lei da } \mathrm{id}_B\text{)} \\
&= f' \circ (f \circ f^{-1}) && \text{((R) da } f^{-1}\text{)} \\
&= (f' \circ f) \circ f^{-1} && \text{(assoc.)} \\
&= \mathrm{id}_A \circ f^{-1} && \text{((L) da } f'\text{)} \\
&= f^{-1}. && \text{(lei da } \mathrm{id}_A\text{)}
\end{aligned}$$

E caso que f' satisfaz a (R):

$$\begin{aligned} f' &= \mathrm{id}_A \circ f' && \text{(lei da } \mathrm{id}_A\text{)} \\ &= (f^{-1} \circ f) \circ f' && \text{((L) da } f^{-1}\text{)} \\ &= f^{-1} \circ (f \circ f') && \text{(assoc.)} \\ &= f^{-1} \circ \mathrm{id}_B && \text{((R) da } f'\text{)} \\ &= f^{-1}. && \text{(lei da } \mathrm{id}_B\text{)} \end{aligned}$$

∎

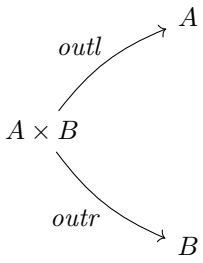
▸ **EXERCÍCIO x9.119.**
Seja $f : A \to B$ tal que $r, s : A \leftarrow B$ são retracção e secção da f respectivamente. Podemos concluir a afirmação seguinte?:

$$f \text{ é bijetora} \quad \& \quad r = f^{-1} = s.$$

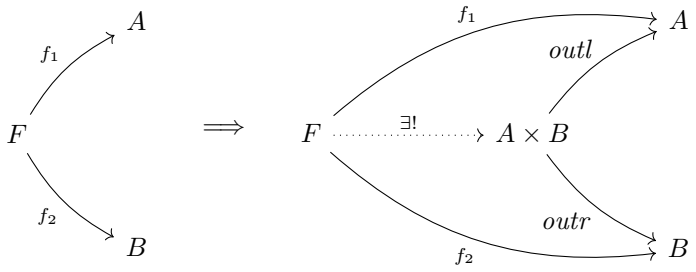
Se sim, demonstre; se não, refute. (x9.119 H 1)

§224. Duma resolução para um problema para uma teoria

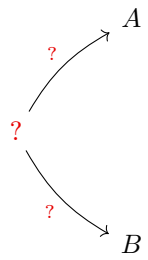
9.260. Duma resolução para o problema. Aqui o produto cartesiano $A \times B$ que chega junto com suas projecções $outl : A \times B \to A$ e $outr : A \times B \to B$:



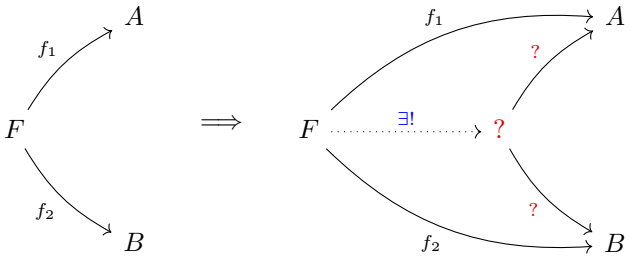
Esse bicho junto com suas duas setinhas, $(outl, A \times B, outr)$ tem uma propriedade *muito interessante:* para cada *impostor* (f_1, F, f_2):



A partir dessa *resolução*, vamos descobrir um *problema:* determine os ? no



tais que para todo (f_1, F, f_2),



Observe que realmente o $(\mathit{outl}, A \times B, \mathit{outr})$ é uma resolução desse problema.

TODO Escrever

§225. Pouco de cats—um primeiro toque de categorias

Podemos *finalmente* introduzir pouca da linguagem e das idéias principais das *categorias* para ter na nossa disposição antes de chegar no Capítulo 15 onde vamos fazer mesmo nossos primeiros passos na sua teoria. Mas o que é uma categoria?

D9.261. Definição (categoria). Uma *categoria* $\mathbb{C}$ é composta por duas colecções de coisas:

- $\mathrm{Obj}\,(\mathbb{C})$: os *objetos* da $\mathbb{C}$, que denotamos por $A, B, C, \ldots$;
- $\mathrm{Arr}\,(\mathbb{C})$: as *setas* da $\mathbb{C}$, que denotamos por $f, g, h, \ldots$;

tais que:

(i) Para toda seta f do $\mathrm{Arr}\,(\mathbb{C})$, são determinados dois objetos: o *source* da f e o *target* da f, denotados por $\mathrm{src}\, f$ e $\mathrm{tgt}\, f$ respectivamente. Escrevemos $f : A \to B$ para afirmar que f é uma seta, e que $\mathrm{src}\, f = A$ e $\mathrm{tgt}\, f = B$. Denotamos por $\mathrm{Hom}(A, B)$ a colecção de todas as setas de A para B.

(ii) Para cada objeto A da $\mathbb{C}$ é determinada uma seta $1_A : A \to A$ chamada a *identidade do* A.

(iii) Dados objetos A, B, C e setas $A \xrightarrow{f} B \xrightarrow{g} C$ é determinada uma seta $g \circ f : A \to C$ chamada a *composição da* g *com* f (ou *"g de f"*; ou *"g seguindo f"*) que freqüentemente denotamos por gf ou $f\,;g$. Ou seja, dados quaisquer objetos A, B, C temos um operador de composição

$$\circ_{A\to B\to C} : \mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C).$$

Tudo isso é o que temos numa categoria. Mas apenas *ter* tudo isso não é suficiente. Essas coisas todas devem satisfazer as *leis de categoria:*

(C-Ass) Para todas as setas $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ temos:

$$(hg)f = h(gf).$$

(C-Unit) Para toda seta $A \xrightarrow{f} B$ temos:

$$f1_A = f = 1_B f.$$

9.262. Observação. Observe que a Definição D9.261 está nos dando operações:

$$\operatorname{Arr}(\mathbb{C}) \underset{\text{tgt}}{\overset{\text{src}}{\rightrightarrows}} \operatorname{Obj}(\mathbb{C}).$$

E também

$$\operatorname{Obj}(\mathbb{C}) \xrightarrow{\text{id}} \operatorname{Arr}(\mathbb{C}) \qquad \operatorname{Hom}(B,C) \times \operatorname{Hom}(A,B) \xrightarrow{\circ} \operatorname{Hom}(A,C)$$

$$A \xmapsto{\text{id}} 1_A \qquad \langle g, f\rangle \xmapsto{\circ} gf$$

- **EXEMPLO 9.263 (conjuntos).**
A Set com objetos os conjuntos e setas as funções entre conjuntos é uma categoria.

▸ **EXERCÍCIO x9.120.**
Verifique. (x9.120 H 0)

- **EXEMPLO 9.264 (inteiros com ordem).**
Denotamos por $\mathsf{Int}_{(\leq)}$ a categoria cujos objetos são os inteiros e entre dois objetos A, B existe seta f sse $A \leq B$. Observe que o que são mesmo as setas não importa, mas caso que insista para defini-las podemos considerar a única seta de A para B pra ser o par $\langle A, B\rangle$.

▸ **EXERCÍCIO x9.121.**
Demonstre que a suposta categoria do Exemplo 9.264 realmente é uma categoria mesmo. Deixe claro o que precisas demonstrar mesmo; e demonstre. (x9.121 H 0)

- **EXEMPLO 9.265 (inteiros com divide).**
Similarmente definimos a $\mathsf{Int}_{(|)}$: aqui temos seta $f : A \to B$ sse $A \mid B$.

▸ **EXERCÍCIO x9.122.**
Demonstre que a suposta categoria do Exemplo 9.265 realmente é uma categoria. (x9.122 H 0)

Queremos trazer o conceito de isomorfismo pra cá, pra ser aplicável em qualquer categoria. Observe que não podemos usá-lo mesmo, pois na Set definimos o isomorfismo pra ser sinônimo de bijecção. E não temos como falar "bijecção" no contexto abstrato de categorias.

▸ **EXERCÍCIO x9.123.**
Por que não? (x9.123 H 0)

Mesmo assim, podemos definir o que significa que uma seta é *iso*, numa maneira que acaba sendo equivalente a ser bijectiva quando aplicada na **Set**:

D9.266. Definição (iso). Seja $\mathbb{C}$ uma categoria e $f : A \to B$ uma das suas setas. Chamamos a f de *iso* sse f é invertível:

$$f \text{ iso} \overset{\text{def}}{\iff} (\exists f' : B \to A)[\, f'f = 1_A \;\&\; ff' = 1_B \,].$$

Nesse caso chamamos os objetos A, B *isómorfos* ou *isomórficos*, algo que denotamos por $A \cong B$. Como encontramos na Definição D9.254, às vezes escrevemos $f : A \xrightarrow{\cong} B$ ou até $f : A \cong B$ para enfatizar que f é um isomorfismo de A para B.

D9.267. Definição (iniciais, terminais). Numa categoria $\mathbb{C}$, um objeto S é *inicial* sse para todo objeto X, existe única seta $S \xrightarrow{!} X$. Similarmente, um objeto T é *terminal* sse para todo objeto X, existe única seta $X \xrightarrow{!} T$. Sinônimos de terminal: *universal*, *final*, *terminador*; sinônimos de inicial: *couniversal*, *coterminal*, *coterminador*. Um objeto inicial e terminal é chamado *nulo*.

▸ **EXERCÍCIO x9.124.**
Todos os objetos nulos duma categoria $\mathbb{C}$ são isómorfos. Em outras palavras, se $\mathbb{C}$ tem objeto nulo, ele é *único a menos de isomorfismos*. (x9.124 H 0)

▸ **EXERCÍCIO x9.125 (seta zero).**
Seja Z um objeto nulo duma categoria $\mathbb{C}$. Dados quaisquer objetos A, B existe uma única seta que *passa pelo* Z:

$$A \xrightarrow{!} Z \xrightarrow{!} B$$

(a composição das setas acima) onde entendemos que os ! nas setas indicam que essa seta é *a única seta* desse objeto para aquele objeto. (x9.125 H 0)

! **9.268. Cuidado.** Na literatura às vezes aparece o termo "terminal" para significar tanto "inicial" quanto "final". Se o contexto deixa claro qual dos dois é, procure a definição.

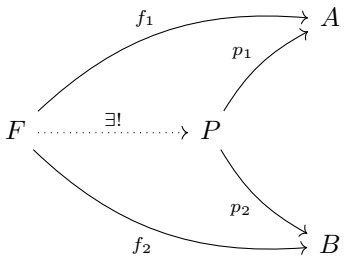
• **EXEMPLO 9.269.**
A categoria **Set** possui iniciais? Terminais? Quais?
Resolução. Sim e sim. Demonstraste isso no Problema Π9.1: $\emptyset$ é seu único objeto inicial; e cada singleton é um terminal.

▸ **EXERCÍCIO x9.126.**
A categoria $\mathsf{Int}_{(\leq)}$ tem iniciais? Terminais? Se sim, quais são? (x9.126 H 0)

▸ **EXERCÍCIO x9.127.**
A $\mathsf{Int}_{(|)}$? (x9.127 H 0)

D9.270. Definição (produto). Sejam A, B objetos numa categoria $\mathbb{C}$. Uma tripla (p_1, P, p_2) é um *produto* dos A, B, sse:

- $A \xleftarrow{p_1} P \xrightarrow{p_2} B$;
- para toda tripla (f_1, F, f_2) com $A \xleftarrow{f_1} F \xrightarrow{f_2} B$, existe única seta ! que faz o diagrama



comutar.

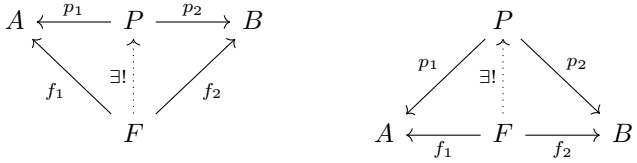
Quando as setas são óbvias usamos apenas o objeto P para representar a tripla (p_1, P, p_2).

▸ **EXERCÍCIO x9.128 (o produto é um produto).**
Dados conjuntos A, B na Set, demonstre que $A \times B$ é um produto. Entenda que literalmente o produto não é o $A \times B$, mas a tripla $(\mathit{outl}, A \times B, \mathit{outr})$. (x9.128 H 0)

▸ **EXERCÍCIO x9.129 (produtos não são únicos).**
Dados conjuntos A, B na Set, ache um outro conjunto, além do $A \times B$ que também é produto dos A, B. Pode achar mais? (x9.129 H 0)

▸ **EXERCÍCIO x9.130 (são únicos a menos de isomorfismo).**
Demonstre que em qualquer categoria, dois produtos dos mesmos objetos são necessariamente isómorfos. (x9.130 H 0)

9.271. Observação. Outras maneira para desenhar o diagrama acima são as seguintes:



Obviamente é a mesma coisa. Use qualquer delas, ou qualquer outra equivalente.

▸ **EXERCÍCIO x9.131.**
A categoria $\mathsf{Int}_{(\leq)}$ do Exemplo 9.264 tem produtos? Se sim, dados dois objetos nela A, B, qual seria o seu produto $A \times B$? (x9.131 H 0)

▸ **EXERCÍCIO x9.132.**
A categoria $\mathsf{Int}_{(|)}$ do Exemplo 9.265 tem produtos? Se sim, dados dois objetos nela A, B, qual seria o seu produto $A \times B$? (x9.132 H 0)

TODO Escrever

Problemas

▸ **PROBLEMA Π9.24.**
Sabemos que bijecções tem inversa e logo são canceláveis pela esquerda, e também canceláveis pela direita. Mas no 9.247 da viagem da §222 encontramos mais uma versão de cancelável: "cancelável stereo", que—para motivos óbvios—desconsideramos na discussão. Então: existe bijecção f e funções g, h tais que

$$f \circ g = h \circ f \implies g = h\,?$$

Se sim mostre um exemplo; se não, refute mesmo a afirmação. (Π9.24 H 0)

▸ **PROBLEMA Π9.25.**
Demonstre que a composição respeita injectividade e sobrejectividade num estilo point-free (Exercício x9.41). Ou seja, tu vai ter que usar as "versões point-free" dessas noções.
(Π9.25 H 0)

▸ **PROBLEMA Π9.26.**
Descreva a afirmação «f é constante» numa maneira point-free. (Π9.26 H 1)

▸ **PROBLEMA Π9.27 (Definição: coproduto em categoria).**
Defina formalmente o que significa *coproduto* numa categoria. (Π9.27 H 0)

▸ **PROBLEMA Π9.28 (o coproduto é um coproduto ué).**
Demonstre que a *união disjunta* $A \uplus B$ que encontramos na Definição D9.210, conhecida por seus amigos algebristas e categoristas como *coproduto* e denotado por $A \amalg B$ e $A + B$, merece seu apelido: "ele" realmente é um coproduto dos A, B na Set. Por que o "ele" está em aspas? (Π9.28 H 0)

▸ **PROBLEMA Π9.29 (mais coprodutos).**
As $\mathsf{Int}_{(\leq)}$ e $\mathsf{Int}_{(|)}$ têm coprodutos? Quais são? (Π9.29 H 0)

▸ **PROBLEMA Π9.30.**
Calculando para resolver o Exercício x9.105 pareceu que o cálculo do $d(6)$ não ia terminar. Demonstre que realmente não termina. (Π9.30 H 1 2 3 4 5 6 7)

Leitura complementar

O **[Vel06:** Cap. 5**]** defina e trata funções como casos especiais de relações (veja Capítulo 10), algo que não fazemos nesse texto. Muitos livros seguem essa abordagem, então o leitor é conselhado tomar o cuidado necessário enquanto estudando esses assuntos.

Um livro excelente para auto-estudo é o **[LS09]**. *Não pule seus exercícios e problemas!*

CAPÍTULO 10

RELAÇÕES

Neste capítulo estudamos então mais um *tipo* importante para matemática: a *relação*. Se pensamos em funções como construtores (ou "apontadores") de objetos, então as relações são *construtores de afirmações*. Podemos pensar que uma relação é como um *verbo*, ou um *predicado* duma afirmação. Como no Capítulo 9, nosso objectivo é entender *o que são* as coisas desse tipo (relações) e não como defini-las formalmente como objetos matemáticos—sobre isso, paciência até o Capítulo 16.

§226. Conceito, notação, igualdade

- **EXEMPLO 10.1.**
Nos números, estamos bem acostumados com as relações de ordem: $(\leq)$, $(\geq)$, $(<)$, $(>)$. Nos inteiros já estudamos bastante a relação binária de «divide» $(- \mid -)$ e a relação ternária de «congruência modular» $(- \equiv - \pmod{-})$.

- **EXEMPLO 10.2.**
No nossa vida, conhecemos várias relações também:

$$\begin{aligned} \text{Mother}(x,y) &\overset{\text{def}}{\iff} x \text{ é a mãe de } y \\ \text{Parents}(x,y,z) &\overset{\text{def}}{\iff} x \text{ e } y \text{ são os pais de } z \\ \text{Love}(x,y) &\overset{\text{def}}{\iff} x \text{ ama } y. \end{aligned}$$

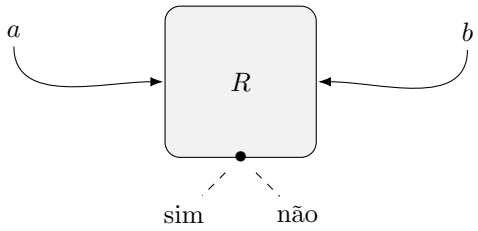
10.3. Black boxes. Visualizamos uma relação R de aridade n como um black box com n entradas e uma lâmpada que pisca sim ou não (como o black box dum conjunto), dependendo de se os objetos-entradas $x_1, \ldots, x_n$ são relacionados pela R. Nesse caso dizemos que os $x_1, \ldots, x_n$ *satisfazem* a R e escrevemos

$$R(x_1, \ldots, x_n)$$

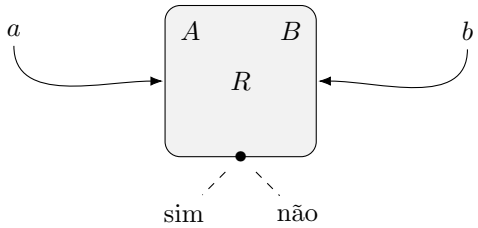
para denotar isso e, quando R é binária, em vez de escrever $R(x,y)$ preferimos usar o R com notação *infixa*:

$$x \; R \; y \overset{\text{def}}{\iff} R(x,y).$$

Podemos então visualizar uma relação binária assim:



Como nas funções, se suas entradas são rotuladas ou não é questão de religião: para o Conjuntista o black box parece como esse acima, e para o Categorista como este abaixo:



Ele escreveria $R : \mathrm{Rel}\,(A, B)$ para deixar claro o tipo dessa relação.

Relações podem relacionar tipos diferentes:

- **EXEMPLO 10.4.**
Considere as relações seguintes, cujos argumentos não têm o mesmo tipo.

$$\mathrm{Born}(x, w) \overset{\text{def}}{\iff} x \text{ nasceu no ano } w$$
$$\mathrm{Author}(x, k) \overset{\text{def}}{\iff} x \text{ escreveu o livro } k$$
$$\mathrm{Read}(x, k) \overset{\text{def}}{\iff} x \text{ leu o livro } k$$

O primeiro argumento da primeira relação é uma pessoa mas o segundo é um ano; e as relações Author e Read são ambas entre pessoas e livros.

- **EXEMPLO 10.5 (Igualdades).**
Para cada tipo, sua igualdade é uma relação, de aridade 2. Nos números naturais por exemplo, se $n, m \in \mathbb{N}$, $n = m$ é uma afirmação:

$$n = m \overset{\text{"def"}}{\iff} \text{os } n \text{ e } m \text{ denotam o mesmo número natural.}$$

Similarmente nos conjuntos: se A, B são conjuntos, $A = B$ é a afimação seguinte:

$$A = B \overset{\text{"def"}}{\iff} \text{os } A \text{ e } B \text{ denotam o mesmo conjunto.}$$

Etc., etc. Observe que podemos fazer uma *aplicação parcial*, nas relações como fazemos nas funções. Fixando um objeto de nosso tipo, por exemplo o natural $0 \in \mathbb{N}$ em qualquer um dos dois lados da igualdade (vamos fixar na direita nesse exemplo), chegamos numa relação de aridade 1:

$$- = 0$$

onde ' $-$ ' é um buraco e aplicando a relação para qualquer $x \in \mathbb{N}$ chegamos na afirmação

$$x = 0.$$

D10.6. Definição (O tipo duma relação). Com cada relação associamos o seu *tipo* (pedimos emprestada aqui a terminologia usada em funções) que é apenas a informação de qual é o tipo de cada uma das suas entradas. Escrevemos

$$R : \mathrm{Rel}\,(A_1, \ldots, A_n)$$

para afirmar que R é uma relação n-ária entre os conjuntos $A_1, \ldots, A_n$. As relações dos exemplos 10.2 e 10.4 têm os tipos seguintes:

$$\begin{aligned} \mathrm{Mother} &: \mathrm{Rel}\,(\mathcal{P}, \mathcal{P}) & \qquad \mathrm{Born} &: \mathrm{Rel}\,(\mathcal{P}, \mathcal{Y}) \\ \mathrm{Parents} &: \mathrm{Rel}\,(\mathcal{P}, \mathcal{P}, \mathcal{P}) & \qquad \mathrm{Author} &: \mathrm{Rel}\,(\mathcal{P}, \mathcal{B}) \\ \mathrm{Love} &: \mathrm{Rel}\,(\mathcal{P}, \mathcal{P}) & \qquad \mathrm{Read} &: \mathrm{Rel}\,(\mathcal{P}, \mathcal{B}) \end{aligned}$$

onde $\mathcal{P}, \mathcal{Y}, \mathcal{B}$ são os conjuntos de pessoas, anos, livros (respectivamente).

D10.7. Notação (funcionista). Relações de aridade 2 são as mais comuns, e usamos certa notação e terminologia especialmente só para elas. Nesse caso, podemos ver o conceito de relação como uma generalização de função, onde nos livramos das duas condições do 9.11. Por isso, quando temos uma relação no $\mathrm{Rel}\,(A, B)$ usamos a frase «relação *de* A *para* B». Vamos criar uma notação parecida com aquala das funções para dizer que R é uma relação do conjunto A para o conjunto B. Escrevemos, equivalentemente:

$$R : A \twoheadrightarrow B \qquad R : B \twoheadleftarrow A \qquad A \xrightarrow{R} B \qquad B \xleftarrow{R} A.$$

Tudo isso quis dizer apenas que R é uma relação binária entre A e B. Ou seja, tudo isso é sinónimo com o $R : \mathrm{Rel}\,(A, B)$.

! 10.8. Cuidado. A notação "$\twoheadrightarrow$" definida no D10.7 *não* é padrão.

D10.9. Notação (conjuntista). Vestindo nosso chapéu de conjuntista, abusamos a notação e escrevemos também $(x, y) \in R$ para dizer que $R(x, y)$. E para afirmar que $R : \mathrm{Rel}\,(A, B)$, escrevemos até $R \subseteq A \times B$. É importante entender bem neste momento que essas são apenas *notações*. Uma relação R *não é* um conjunto, então nada pertence a ela, e conseqüentemente ela não é subconjunto de ninguém! Mesmo assim escrevemos coisas como

$$\mathrm{Author} \subseteq \mathcal{P} \times \mathcal{B} \qquad \mathrm{Parents} \subseteq \mathcal{P}^3$$

entendendo como:

$$\mathrm{Author} \ : \mathrm{Rel}\,(\mathcal{P}, \mathcal{B}) \qquad \mathrm{Parents} \ : \mathrm{Rel}\,(\mathcal{P}, \mathcal{P}, \mathcal{P}).$$

É muito conveniente tratar relações *como se fossem* conjuntos —mas mais uma vez: relações *não são* conjuntos.

▸ **EXERCÍCIO x10.1.**
Repita! (x10.1 H 1)

Cada vez que introduzimos um tipo novo, precisamos definir quando dois objetos desse tipo são iguais. Vamos fazer isso agora. Novamente, vamos optar para identificar relações cujos comportamentos são indistinguíveis usando apenas as suas interfaces.

D10.10. Definição (igualdade). Sejam R, S relações binárias num conjunto A. Definimos

$$R = S \iff^{\text{def}} (\forall x, y \in A)[\, x \mathrel{R} y \iff x \mathrel{S} y \,].$$

Principalmente vamos trabalhar com relações binárias definidas num conjunto só, então a definição de igualdade D10.10 que acabamos de ver nos serve bem. No Exercício x10.2 e no Exercício x10.3 tu vai estender essa definição para os casos mais gerais.

▸ **EXERCÍCIO x10.2 (igualdade).**
Como tu estenderia a Definição D10.10 para o caso que as R, S não são relações num conjunto só? Ou seja, tendo relações binárias R, S, a R de A para B, e a S de C para D, como tu definirias a igualdade $R = S$ nesse caso? (x10.2 H 0)

▸ **EXERCÍCIO x10.3 (igualdade (agnóstica)).**
Defina a igualdade para o caso mais geral de relações, numa maneira "agnóstica" como fizemos nas funções (Definição D9.28). (x10.3 H 0)

10.11. Intensão vs. extensão. Com nossa experiência com *intensão* e *extensão* de conjuntos (§176) e de funções (9.14 e 9.15), não precisamos esclarecer muita coisa sobre relações, pois a idéia continua a mesma.

• **EXEMPLO 10.12.**
Considere as relações no $\mathbb{N}$:

$$R(n) \iff^{\text{def}} \text{Prime}(n) \;\&\; \text{Even}(n)$$
$$T(n) \iff^{\text{def}} n = 2.$$

As *intensões* das relações R e T são diferentes, mas a *extensão* é comum:

$$(\forall n \in \mathbb{N})[\, R(n) \iff T(n) \,].$$

Para capturar a extensão duma relação, definimos o seu gráfico, na mesma forma que definimos no caso de funções (Definição D9.21).

D10.13. Definição (gráfico). Dado relação $R : \text{Rel}(A_1, \ldots, A_n)$, o *gráfico da* R é o conjunto

$$\text{graph}\, R \stackrel{\text{def}}{=} \{\, \vec{a} \in A_1 \times \cdots \times A_n \mid R(\vec{a}) \,\},$$

também conhecido como *truth set* da R.

10.14. Observação. Agora temos uma maneira formal para afirmar que R e T tem a mesma extensão: $\text{graph}\, R = \text{graph}\, T$. E agora a notação conjuntista do D10.9 vira literalmente até correta se substituir as relações por seus gráficos.

§227. Definindo relações

10.15. Com buracos. Começando com uma expressão que denota um *objeto* e botando n buracos em certas subexpressões dela, criamos uma *função* de aridade n. Se fizer a mesma coisa numa expressão que denota uma *afirmação*, então criamos uma *relação* de aridade n.

- **EXEMPLO 10.16.**
Considere a frase «João ama Maria». Criamos assim as relações:

$$L \stackrel{\text{def}}{=} \text{«__ ama __»}$$
$$J \stackrel{\text{def}}{=} \text{«João ama __»}$$
$$M \stackrel{\text{def}}{=} \text{«__ ama Maria».}$$

A primeira é uma relação binária no $\mathcal{P}$ e as outras duas unárias. Usando variáveis em vez de buracos, escrevemos:

$$L(x,y) \iff \text{«}x \text{ ama } y\text{»}$$
$$J(x) \iff \text{«João ama } x\text{»}$$
$$M(x) \iff \text{«}x \text{ ama Maria».}$$

10.17. Outras maneiras de definir relações. Em vez de explicar todas as maneiras seguintes em detalhe, eu acho que um exemplo é suficiente para cada caso, pois todas essas maneiras são já bem conhecidas graças à nossa experiência com funções no Capítulo 9.

- **EXEMPLO 10.18 (formulamente).**
Considere os conjuntos $\mathcal{P}$ de todas as pessoas e $\mathcal{B}$ de todos os livros. Sejam as relações

$$P : \text{Rel}\,(\mathbb{Z}), \qquad R : \text{Rel}\,(\mathbb{Z},\mathbb{Z}), \qquad Q : \text{Rel}\,(\mathcal{P}\times\mathcal{B}), \qquad M : \text{Rel}\,(\mathbb{Z},\mathbb{Z},\mathbb{Z}),$$

definidas pelas fórmulas:

$$P(n) \iff (\forall x,y\in\mathbb{Z})[\,xy = n \to (|x|=1 \vee |y|=1)\,]$$
$$R(n,m) \iff \neg(\exists k\in\mathbb{Z})[\,\text{Prime}(k) \wedge 2^n < k < 3^m\,];$$
$$Q(p,b) \iff (\exists b'\in\mathcal{B})[\,b\neq b' \wedge \text{Read}(p,b') \wedge (\exists a\in\mathcal{P})[\,\text{Author}(a,b)\wedge\text{Author}(a,b')\,]\,]$$
$$C(a,b,m) \iff (\exists k\in\mathbb{Z})[\,mk = a-b\,]$$

Tente expressar cada uma delas em lingua natural.

- **EXEMPLO 10.19 (Com texto).**
Sejam as relações Coauthors (binária, entre pessoas) e SameCard (unária, nos conjuntos), definidas pelas:

$$\text{Coauthors}(x,y) \iff x \text{ e } y \text{ já escreveram algum livro juntos;}$$
$$\text{SameCard}(x) \iff \text{todos os membros de } x \text{ são conjuntos com a mesma cardinalidade.}$$

Por exempo: $\text{Coauthors}(\text{Birkhoff}, \text{Mac Lane})$ e $\text{SameCard}(\{\{0,1\},\{\mathbb{N},\{42\}\},\{\emptyset,\{\emptyset\}\}\})$.

! **10.20. Cuidado.** Como sempre, tomamos cuidado quando definimos coisas com texto: tem que ser uma afirmação definitiva, sem ambigüidades, etc.

▸ **EXERCÍCIO x10.4.**
Com a definição de SameCard do Exemplo 10.19, SameCard($\{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$)? Responda com "sim" ou "não", com uma curtíssima explicação (sem demonstração). (x10.4H1)

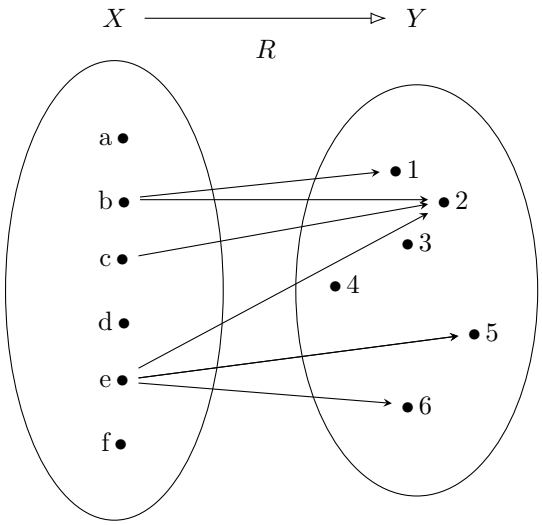
• **EXEMPLO 10.21 (Aplicação parcial).**
Sejam as relações EqParity (binária entre inteiros), B (unária em pessoas), e Neg (unária em inteiros), definidas pelas:

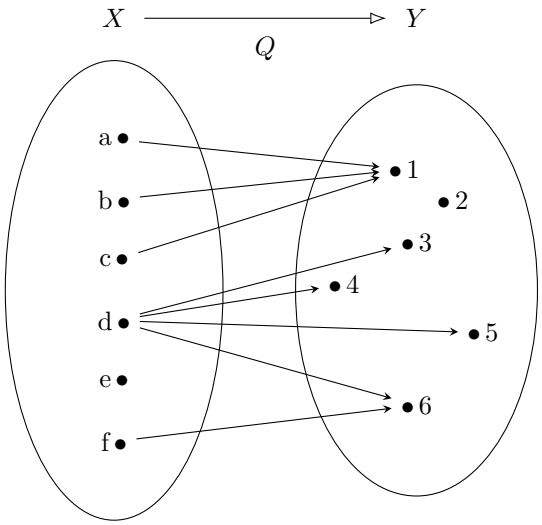
$$\begin{aligned} \text{EqParity}(a,b) &\stackrel{\text{def}}{\iff} a \equiv b \pmod 2 \\ B(y) &\stackrel{\text{def}}{\iff} \text{Coauthors}(\text{Birkhoff}, y) \\ \text{Neg}(x) &\stackrel{\text{def}}{\iff} x < 0. \end{aligned}$$

Assim temos por exemplo: EqParity$(103, 11)$ mas não EqParity$(21, 42)$; B(Mac Lane) mas não B(Thanos); Neg(-23) mas não Neg(0).

§228. Diagramas internos

10.22. Relação como uma generalização de função. Um jeito de olhar para uma relação é como uma "função" sem as restricções de totalidade e de determinabilidade que encontramos no 9.11. Então: lembra dos conjuntos A, B que encontramos na Secção §213? Aqui são duas relações R, Q de A para B, determinadas por seus diagramas internos:

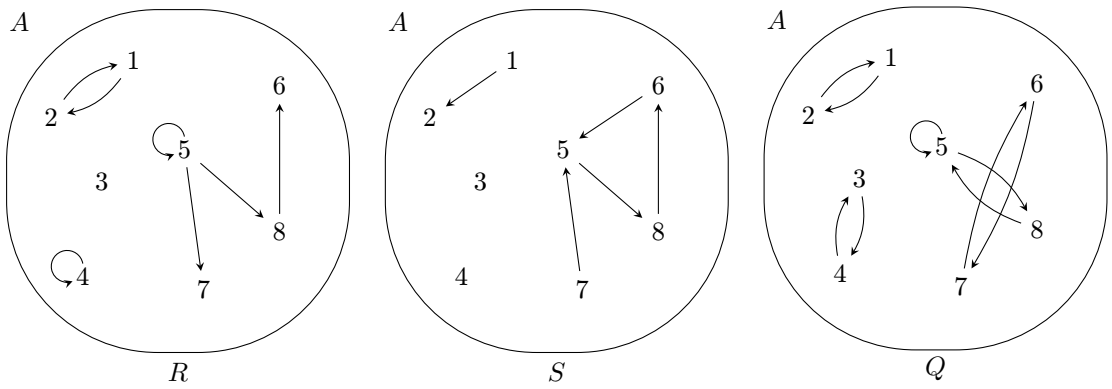




A situação sobre relações binárias definidas num conjunto A é mais divertida.

10.23. Relação como grafo direcionado. Seja A um conjunto e R uma relação binária nele. Podemos representar a R como um *grafo direcionado*, onde, para todos $x, y \in A$, desenhamos uma setinha $x \longrightarrow y$ sse $x \mathrel{R} y$.

• **EXEMPLO 10.24.**
Seja $A = \{1,2,3,4,5,6,7,8\}$. Desenhamos os diagramas de três relações binárias no A:



Os gráficos delas então são os

$$\begin{aligned}
\operatorname{graph} R &= \{(1,2),(2,1),(4,4),(5,5),(5,7),(5,8),(8,6)\} \\
\operatorname{graph} S &= \{(1,2),(5,8),(6,5),(7,5),(8,6)\} \\
\operatorname{graph} Q &= \{(1,2),(2,1),(3,4),(4,3),(5,5),(5,8),(6,7),(7,6),(8,5)\}\,.
\end{aligned}$$

Mais uma vez, aviso que é comum identificar uma relação R com seu gráfico $\operatorname{graph} R$, escrevendo por exemplo $R = \{(1,2),(2,1),\dots\}$. Já fez o Exercício x10.1, né?

▸ **EXERCÍCIO x10.5.**
No mesmo conjunto $A = \{1,2,3,4,5,6,7,8\}$, como parecem os diagramas das relações F, T com gráficos $\operatorname{graph} F = \emptyset$ e $\operatorname{graph} T = A^2$? (x10.5 H 0)

▸ **EXERCÍCIO x10.6.**
Para quais relações podemos ter *duas* setinhas do objeto x para o objeto y? (x10.6 H 0)

§229. Construções e operações em relações

Todas as relações que consideramos nessa secção serão binárias.

D10.25. Definição. Seja R uma relação de A para B. Definimos a sua *relação oposta* (ou *relação dual*) R^{∂} de B para A pela:

$$x \mathrel{R^{\partial}} y \iff^{\text{def}} y \mathrel{R} x.$$

Também é conhecida como a *relação inversa da* R, e a galera que a chama assim usa notação R^{-1}, *mas não vamos usá-la nesse texto*—explicarei o porquê no Cuidado 10.34.

▸ **EXERCÍCIO x10.7.**
A operação $-^{\partial}$ é uma *involução*:

$$\text{para toda relação binária } R,\ \left(R^{\partial}\right)^{\partial} = R.$$

(x10.7 H 0)

• **EXEMPLO 10.26.**
Nos $\mathbb{R}$, a relação oposta ($<^{\partial}$) da ($<$) é a ($>$), e a ($\leq^{\partial}$) é a ($\geq$).

10.27. Composição. Dadas relações compatíveis, podemos formar sua composição $R \diamond S$ numa forma natural. Vamos ver uns exemplos antes de chegar na definição formal.

• **EXEMPLO 10.28.**
Sejam os conjuntos $\mathcal{P}$ de pessoas, $\mathcal{B}$ de livros, e $\mathcal{W}$ de palavras. Considere as relações:

$$\begin{aligned}
\text{Author}(x,y) &\overset{\text{def}}{\iff} x \text{ é um escritor do livro } y\\
\text{Read}(x,y) &\overset{\text{def}}{\iff} x \text{ leu o livro } y\\
\text{Contains}(x,y) &\overset{\text{def}}{\iff} \text{a palavra } y \text{ aparece no livro } x
\end{aligned}$$

Observe que Author e Read são relações de $\mathcal{P}$ para $\mathcal{B}$, e Contains de $\mathcal{B}$ para $\mathcal{W}$. O que seria a relação Author $\diamond$ Read, o que a Author $\diamond$ Contains, e o que a Read $\diamond$ Contains? Antes de defini-las, vamos primeiramente pensar se faz sentido compor essas relações. Realmente Read é componível com Contains (gráças ao $\mathcal{B}$ "no meio") e similarmente sobre a Author com Contains. Por outro lado, não podemos compor as Author e Read em nenhuma ordem! Bem, então Author $\diamond$ Contains e Read $\diamond$ Contains são ambas relações de $\mathcal{P}$ para $\mathcal{W}$. Mas quais? Lembre que para definir uma relação, precisamos determinar completamente quando dois arbitrários x, y são relacionados pela relação. Precisamos então completar as:

$$\begin{aligned}
x \text{ (Author} \diamond \text{Contains) } y &\iff \ldots ? \ldots\\
x \text{ (Read} \diamond \text{Contains) } y &\iff \ldots ? \ldots
\end{aligned}$$

mas como?

!! SPOILER ALERT !!

Bem, botamos:

$$\begin{aligned}
x \text{ (Author} \diamond \text{Contains) } y &\iff \text{a pessoa } x \text{ escreveu algum livro que contem a palavra } y\\
x \text{ (Read} \diamond \text{Contains) } y &\iff \text{a pessoa } x \text{ leu algum livro que contem a palavra } y
\end{aligned}$$

► **EXERCÍCIO x10.8.**
A relação R de $\mathcal{P}$ para $\mathcal{W}$ definida pela

$$R(p,w) \overset{\text{def}}{\iff} \text{a pessoa } p \text{ leu a palavra } w \text{ num livro}$$

é a mesma relação com a $\text{Read} \diamond \text{Contains}$? Em outras palavras:

$$R \overset{?}{=} \text{Read} \diamond \text{Contains}$$

(x10.8 H 1)

Já observamos que não podemos compor as Author e Read em nenhuma ordem, mas podemos aplicar o operador $-^{\partial}$ e compor depois:

► **EXERCÍCIO x10.9.**
Como definarias as relações $\text{Author} \diamond \text{Read}^{\partial}$ e $\text{Read} \diamond \text{Author}^{\partial}$? São iguais? (x10.9 H 0)

Segue mais um exemplo, essa vez usando apenas um conjunto—e logo todas as relações são gratuitamente compatíveis para composição.

► **EXERCÍCIO x10.10.**
Considere as relações

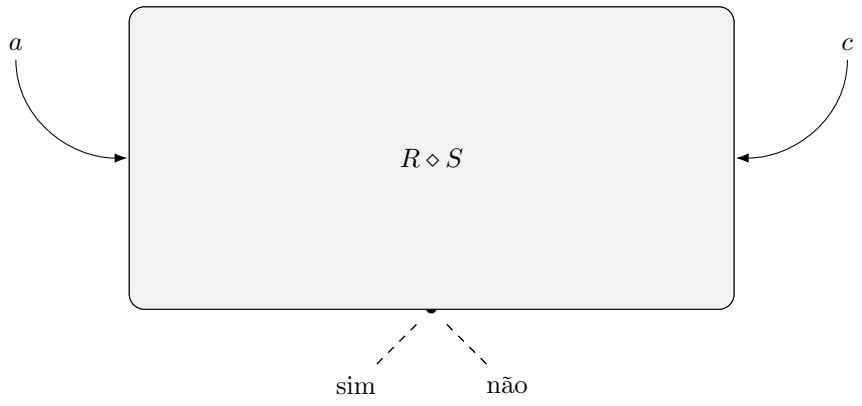
$$\text{Parent}(x,y) \overset{\text{def}}{\iff} x \text{ é a mãe ou o pai de } y$$
$$\text{Child}(x,y) \overset{\text{def}}{\iff} x \text{ é filho ou filha de } y.$$

Como tu definirias diretamente as relações seguintes?:

$\text{Parent} \diamond \text{Parent}$ $\quad$ $\text{Child} \diamond \text{Child}$ $\quad$ $\text{Parent} \diamond \text{Child}$ $\quad$ $\text{Child} \diamond \text{Parent}$

(x10.10 H 0)

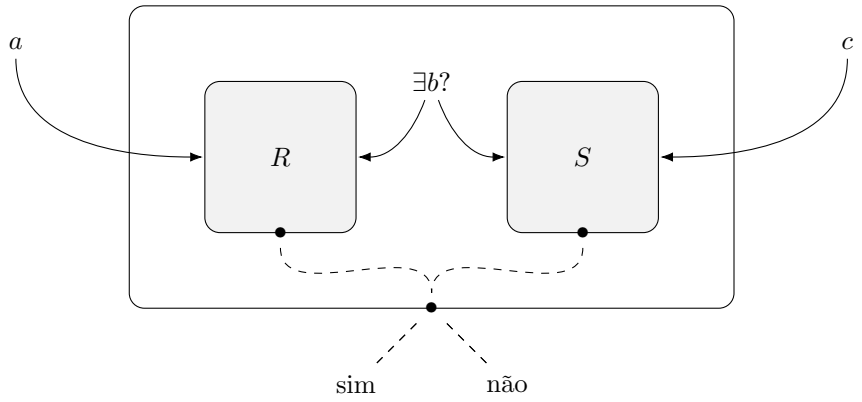
? **Q10.29. Questão.** Como tu imaginas o interior desse black box?



E, como tu definarias a composição de relações?

!! SPOILER ALERT !!

10.30. Composição com black boxes. Talvez as imagens seguintes com black boxes ajudam a pensar numa definição formal.



D10.31. Definição. Sejam conjuntos A, B, C e as relações R de A para B e S de B para C. Definimos a relação $R \diamond S$ de A para C pela

$$a\ (R \diamond S)\ c \iff^{\text{def}} \text{existe } b \in B \text{ tal que } a\ R\ b\ \&\ b\ S\ c.$$

Chamamos a $R \diamond S$ a *composição* da R *com* a S. Quando não existe possibilidade de confusão escrevemos a composição com várias outras notações. Todas as expressões seguintes podem ser usadas:

$$R \diamond S \qquad R \circ S \qquad R\,;S \qquad R \cdot S \qquad RS$$

! **10.32. Cuidado.** Não existe um consensus para a ordem de escrever os R, S usando o símbolo $\circ$. Tome cuidado então enquanto lendo a notação $R \circ S$, pois o que um autor escreve como $R \circ S$, outro pode escrever como $S \circ R$. Quando a composição é denotada por ; a ordem concorda com nossa:

$$a\ (R\,;S)\ c \iff^{\text{def}} \text{existe } y \in B \text{ tal que } a\ R\ y\ \&\ y\ S\ c.$$

Veja também o Cuidado 9.138.

10.33. Propriedade. *Sejam conjuntos A, B, C, D e relações binárias $R : \mathrm{Rel}(A, B)$, $S : \mathrm{Rel}(B, C)$, e $T : \mathrm{Rel}(C, D)$. Então*

$$(R \diamond S) \diamond T = R \diamond (S \diamond T),$$

e logo podemos escrever apenas $R \diamond S \diamond T$.

▸ Esboço. Supomos $a \in A$ e $d \in D$, e mostramos a equivalência

$$a\ ((R \diamond S) \diamond T)\ d \iff a\ (R \diamond (S \diamond T))\ d.$$

□ (10.33P)

▸ **EXERCÍCIO x10.11.**
Escreva uma demonstração em linguagem natural da Propriedade 10.33. (x10.11H0)

▸ **EXERCÍCIO x10.12.**
Demonstre ou refute:

$$\mathrm{Child} \diamond \mathrm{Parent} \stackrel{?}{=} \mathrm{Parent} \diamond \mathrm{Child}\,.$$

(x10.12H1)

▸ **EXERCÍCIO x10.13.**
Considere a $\diamond$ como uma operação binária nas relações binárias num conjunto A. Ela tem *identidade*? Ou seja, existe alguma relação binária I no A, tal que

$$\text{para toda relação } R \text{ no } A, \quad I \diamond R = R = R \diamond I\,?$$

Se sim, defina essa relação I e demonstre que realmente é. Se não, demonstre que não existe. (x10.13H1)

Tendo uma operação binária (composição) e sua identidade (Exercício x10.13) podemos já definir as suas potências.

▸ **EXERCÍCIO x10.14 (Potências).**
Defina formalmente as "potências" R^n duma dada relação binária R num conjunto A, informalmente definida por:

$$x\ (R^n)\ y \stackrel{\text{"def"}}{\iff} x\ \Big(\underbrace{R \diamond \cdots \diamond R}_{n \text{ vezes}}\Big)\ y,$$

válida *para todo* $n \in \mathbb{N}$. (x10.14H12)

▸ **EXERCÍCIO x10.15.**
Demonstre ou refute: *para toda relação binária R num conjunto A, $R \diamond R^\partial = \mathrm{Eq} = R^\partial \diamond R$.* (x10.15H123)

▸ **EXERCÍCIO x10.16.**
Descreva a Coauthors do Exemplo 10.19 em termos da Author. (x10.16H0)

! **10.34. Cuidado (A inversa não é inversa).** Depois dos exercícios x10.15 e x10.16, deve ser claro porque eu preferi chamar a R^∂ a relação *oposta* da R, e usar essa notação em vez de R^{-1} e o nome *inversa*. (Que também usamos pois são os mais comuns!) Se usar a notação R^{-1}, cuidado para não confundir que $R \diamond R^{-1} = \mathrm{Eq} = R^{-1} \diamond R$, pois em geral isso não é verdade. Ou seja: a relação "inversa" R^{-1}, *não é a* $\diamond$*-inversa* da R!

▸ **EXERCÍCIO x10.17 (Some stuff).**
Sejam R, S relações binárias tais que a $R \diamond S$ é definida. Descreva a $(R \diamond S)^\partial$ em termos das R^∂ e S^∂ e demonstre tua afirmação. (x10.17 H 1)

D10.35. Definição (união; intersecção). Sejam $R, S \subseteq A \times B$ relações binárias. Definimos as relações $R \cup S$ e $R \cap S$ no $\mathrm{Rel}\,(A, B)$ pelas

$$x\ (R \cup S)\ y \iff^{\mathsf{def}} x\ R\ y \ \text{ ou } \ x\ S\ y$$
$$x\ (R \cap S)\ y \iff^{\mathsf{def}} x\ R\ y \ \&\ x\ S\ y.$$

Observe que, identificando as relações com seus gráficos, as $R \cup S$ e $R \cap S$ acabam sendo a união e intersecção deles mesmo:

$$\mathrm{graph}\,(R \cup S) = \mathrm{graph}\,R \cup \mathrm{graph}\,S$$
$$\mathrm{graph}\,(R \cap S) = \mathrm{graph}\,R \cap \mathrm{graph}\,S.$$

Claramente generalizamos para famílias de relações $\mathscr{R}$, e assim temos as relações

$$\bigcup \mathscr{R} : \mathrm{Rel}\,(A, B) \qquad x\ (\bigcup \mathscr{R})\ y \iff^{\mathsf{def}} (\exists R \in \mathscr{R})[\,x\ R\ y\,]$$
$$\bigcap \mathscr{R} : \mathrm{Rel}\,(A, B) \qquad x\ (\bigcap \mathscr{R})\ y \iff^{\mathsf{def}} (\forall R \in \mathscr{R})[\,x\ R\ y\,].$$

• **EXEMPLO 10.36.**
Nos reais, a $(<) \cup (=)$ é a relação $(\leq)$, e a $(\leq) \cap (\geq)$ é a relação $(=)$. Substituindo o «é a relação» com o símbolo '$=$' que usamos normalmente a gente acabaria escrevendo essas coisas horrorosas:

$$< \cup = \ = \leq \qquad\qquad \leq \cap \geq \ = \ =.$$

Isso fica *muito* esquisito no olho para parsear; botando parenteses ajuda:

$$((<) \cup (=)) = (\leq) \qquad\qquad ((\leq) \cap (\geq)) = (=).$$

Tente sempre escrever na maneira mais legível e entendível.

§230. Propriedades de relações

Aqui aumentamos nossa terminologia, identificando certas propriedades interessantes que uma relação binária R no X pode ter.

10.37. Reflexão. Olhamos como cada elemento do X relaciona com ele mesmo. Dois casos notáveis aparecem: (i) pode ser que para todo x temos $x\,R\,x$; (ii) pode ser que para nenhum x temos $x\,R\,x$. No primeiro caso, chamamos R *reflexiva*; no segundo, *irreflexiva*. Observe que "irreflexiva" não significa "não reflexiva", etc:

$$\begin{aligned} R \text{ é reflexiva} &\iff \forall x R(x,x) &&\iff \neg\exists x \neg R(x,x) \\ R \text{ não é reflexiva} &\iff \neg\forall x R(x,x) &&\iff \exists x \neg R(x,x) \\ R \text{ é irreflexiva} &\iff \forall x \neg R(x,x) &&\iff \neg\exists x R(x,x) \\ R \text{ não é irreflexiva} &\iff \neg\forall x \neg R(x,x) &&\iff \exists x R(x,x) \end{aligned}$$

onde os quantificadores quantificam sobre o X.

• **EXEMPLO 10.38.**
As relações $(=)$, $(\leq)$, $(\geq)$, nos números e $(=)$, $(\subseteq)$, $(\supseteq)$ nos conjuntos são todas reflexivas. Também reflexivas são as relações «__ nasceu no mesmo pais que __», «__ tem o mesmo primeiro nome com __», etc., definidas entre pessoas. Típicos exemplos de irreflexivas são as $(\neq)$, $(<)$, $(>)$, $(\subsetneq)$, $(\supsetneq)$, «__ é mais baixo que __», «__ e __ nunca estiveram em distância de 2 metros entre si», etc.

10.39. Simetria. Agora examinamos a relação R com respeito à ordem dos seus argumentos. Novamente, certos casos notáveis aparecem: (i) R pode comportar sempre no mesmo jeito independente da ordem dos seus argumentos; nesse caso a chamamos *simétrica*. (ii) O R-relacionamento dum objeto x com outro y pode garantir que o y não esta R-relacionado com o x; a chamamos *assimétrica*. (iii) O único caso onde a R relaciona os mesmos argumentos com as duas possíveis órdens, é quando os dois argumentos são iguais; chamamos a R *antissimétrica*.

• **EXEMPLO 10.40.**
Simétricas: $(=)$, $(\neq)$, «__ e __ são irmãos», «__ e __ são cidades do mesmo país», etc.
Asimétricas: $(<)$, $(\subsetneq)$, $(>)$, $(\supsetneq)$, «__ deve dinheiro para __», «__ está andando na mesma direção e no lado esquerdo de __», «__ é a mãe de __», etc.
Antissimétricas: $(\leq)$, $(\subseteq)$, $(\geq)$, $(\supseteq)$, $(=)$, «a palavra __ aparece, mas não depois da palavra __ no dicionário», etc.

‣ **EXERCÍCIO x10.18.**
Verifique que "não simétrica" não significa nem "assimétrica" nem "antissimétrica", escrevendo todas as fórmulas envolvidas e suas negações, como no 10.37. (x10.18 H 0)

‣ **EXERCÍCIO x10.19.**
Decida a "reflexão" e a "simetria" das relações seguintes:

$$\begin{aligned} R(A,B) &:\iff \text{os conjuntos } A \text{ e } B \text{ são disjuntos} \\ S(A,B) &:\iff |A \setminus B| > 1 \\ T(A,B) &:\iff A \triangle B \neq \emptyset. \end{aligned}$$

Isso quis dizer: para cada uma dessas relações, decida se ela é: reflexiva, irreflexiva, simétrica, assimétrica, antissimétrica. (x10.19 H 0)

▸ **EXERCÍCIO x10.20.**
Mostre que:

$$R \text{ assimétrica} \implies R \text{ irreflexiva.}$$

(x10.20 H 1)

▸ **EXERCÍCIO x10.21.**
Uma das duas direções abaixo é válida:

$$R \text{ assimétrica} \overset{?}{\iff} R \text{ antissimétrica.}$$

Demonstre-a, e mostre que a oposta não é. (x10.21 H 1 2)

▸ **EXERCÍCIO x10.22.**
Seja $R : \mathrm{Rel}\,(X, X)$. Logo

$$R \text{ simétrica} \iff R = R^{\partial}\,.$$

(x10.22 H 0)

10.41. Transições. Às vezes queremos garantir a existência de alguma seta dadas duas ou mais setas. Suponha que $x\ R\ y$ e $y\ R\ z$. Se isso garanta que $x\ R\ z$ chamamos a R *transitiva*; e se isso garanta que $z\ R\ x$, *circular*. Suponha agora que temos dois objetos cada um relacionado com um terceiro. Se isso já é suficiente para garantir que eles também são relacionados, chamamos a relação *left-euclidean*. Similarmente, se a relação de um objeto com dois outros garanta que os outros também relacionam entre si, chamamos a relação *right-euclidean*.

10.42. Por que "euclidean"?. O primeiro axioma de Euclides nos seus *Elementos* (**[Euc02]**) é: *coisas iguais com outra coisa, são iguais entre si também*. Podemos visualizar isso tanto como «$a = c$ e $b = c$ implica $a = b$» (left-euclidean pois a conclusão aconteceu no lado esquerdo); quanto como «$a = b$ e $a = c$ implica $b = c$» (right-euclidean pois a conclusão aconteceu no lado direito).

10.43. Totalidades. Tem duas noções onde uma relação pode "dominar" um conjunto, no sentido de "opiniar" sobre quaisquer x, y nele. A primeira só usa a relação em questão R mesmo: dizemos que R é *total* sse quaisquer x, y são relacionados em pelo menos uma ordem: $x\ R\ y$ ou $y\ R\ x$. A segunda usa a ajuda da igualdade: dizemos que R é *tricotômica* sse para quaisquer x, y exatamente uma das três possibilidades é válida: $x\ R\ y$; $y\ R\ x$; $x = y$.

10.44. Glossário. Resumimos aqui as propriedades que encontramos. Seja X conjunto

e R uma relação binária nele. Definimos as seguintes propriedades:

$x \mathrel{R} x$	reflexiva
$x \mathrel{\not R} x$	irreflexiva
$x \mathrel{R} y \implies y \mathrel{R} x$	simétrica
$x \mathrel{R} y \implies y \mathrel{\not R} x$	assimétrica
$x \mathrel{R} y \;\&\; y \mathrel{R} x \implies x = y$	antissimétrica
$x \mathrel{R} y \;\&\; y \mathrel{R} z \implies x \mathrel{R} z$	transitiva
$x \mathrel{R} y \;\&\; y \mathrel{R} z \implies z \mathrel{R} x$	circular
$x \mathrel{R} y \;\&\; x \mathrel{R} z \implies y \mathrel{R} z$	right-euclidean
$x \mathrel{R} z \;\&\; y \mathrel{R} z \implies x \mathrel{R} y$	left-euclidean
$x \mathrel{R} y$ ou $y \mathrel{R} x$	total
exatamente uma das: $x \mathrel{R} y$; $y \mathrel{R} x$; $x = y$	tricotômica

Para o caso mais geral onde R é uma relação binária de X para Y, temos:

$(\forall x \in X)(\exists y \in Y)[\, x \mathrel{R} y \,]$	left-total
$(\forall y \in Y)(\exists x \in X)[\, x \mathrel{R} y \,]$	right-total ou surjectiva
$y \mathrel{R} x \;\&\; z \mathrel{R} x \implies y = z$	left-unique ou injectiva
$x \mathrel{R} y \;\&\; x \mathrel{R} z \implies y = z$	right-unique ou funcional

▸ **EXERCÍCIO x10.23.**
Para cada uma das relações R, S, Q, F, T do 10.24 e do Exercício x10.5 decida se ela têm ou não, cada uma das propriedades do glossário no 10.44. (x10.23 H 1)

10.45. Proposição. *Seja $X \neq \emptyset$ e $\sim$ uma relação no X. Se $\sim$ é simétrica e transitiva, então ela é reflexiva.*

▸ Demonstração errada. Como ela é simétrica, de $x \sim y$ concluimos que $y \sim x$ também. E agora usando a transitividade, de $x \sim y$ e $y \sim x$, concluimos a $x \sim x$, que mostra que $\sim$ é reflexiva também. ↯

▸ **EXERCÍCIO x10.24.**
Ache o erro na demonstração acima e *demonstre* que a proposição é falsa! (x10.24 H 0)

10.46. Observação (Convenções para diagramas internos). Quando queremos desenhar o diagrama duma relação que sabemos que tem uma certa propriedade, podemos preguiçar e não desenhar todas as suas setas.

Reflexiva: não precisamos botar nenhuma das setinhas-redemoinhos, pois graças à reflexividade são todas implicitas.

Simétrica: não precisamos botar cabeças nas setas, pois para cada seta já é garantida a sua seta-oposta, então botamos apenas uma linha entre dois objetos e já entendemos que existem as setas das duas direções entre si.

Transitiva: não precisamos desenhar setas entre objetos se já existe um caminho entre eles usando outras setas já desenhadas.

Relação de equivalência: não precisamos desenhar nem linhas entre os objetos que relacionam; apenas desenhar regiões por volta de todos os relacionados, algo que vai virar óbvio na Secção §236.

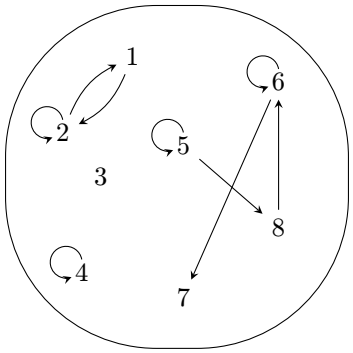
RELAÇÃO DE ORDEM: desenhamos diagramas de Hasse, que vamos encontrar depois (pouco na Nota 11.209 e muito no Capítulo 14).

§231. Fechos

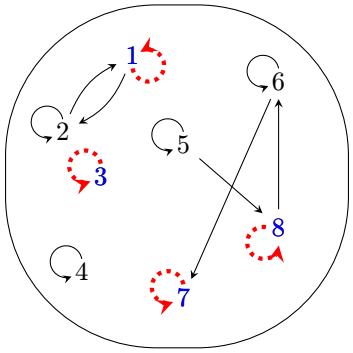
Antes de definir formalmente o conceito importante de fechos, começamos com uns exemplos ilustrativos para os três fechos mais comuns: reflexivo, simétrico, transitivo. A idéia é sempre a mesma, e vamos descrevê-la como um algoritmo.

10.47. A idéia. Começamos com uma relação R, e fixamos uma propriedade desejada (por exemplo, a transitividade). Vamos construir uma nova relação $\bar{R}$, que chamamos o *fecho* da R pela propriedade escolhida. Pense na R como o seu diagrama interno, com suas setinhas. Primeiramente nós nos perguntamos: «a relação já tem essa propriedade?» Caso que sim, não precisamos fazer nada, a relação que temos é o fecho $\bar{R}$ que queríamos construir. Caso que não, quis dizer que tem setinhas que *deveriam estar* no diagrama, mas não estão. (Essas setinhas são as testemunhas que refutam a nossa propriedade.) Vamos adicioná-las na nossa relação. E agora voltamos a perguntar a mesma pergunta, e continuar no mesmo jeito, até finalmente chegar numa relação $\bar{R}$ que realmente satisfaz a propriedade escolhida. Essa relação $\bar{R}$ é o fecho da R a respeito dessa propriedade.

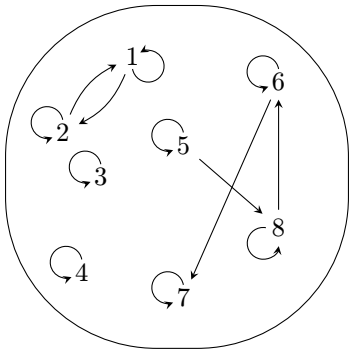
- **EXEMPLO 10.48 (Fecho reflexivo).**
Seja R a relação no A com o diagrama seguinte:



Qual é o fecho reflexivo dela? Bem, primeiramente nós nos perguntamos: será que a relação já é reflexiva? Ela não é. Identificamos então as setinhas-testemunhas desse fato: são as $(1,1)$, $(3,3)$, $(7,7)$, e $(8,8)$.

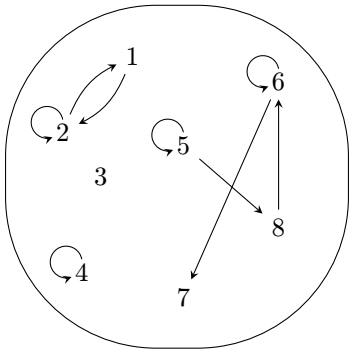


As adicionamos na relação e chegamos em:

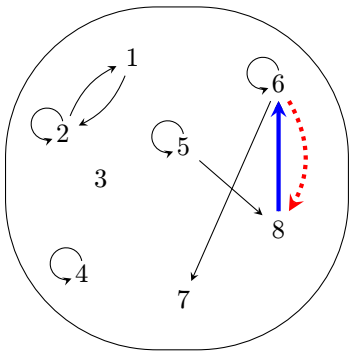


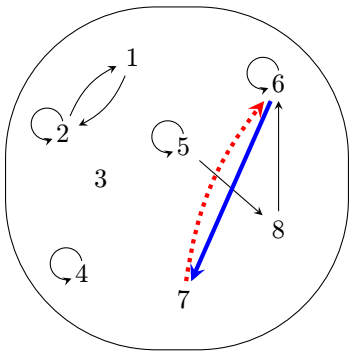
. . . e perguntamos a mesma pergunta: será que ela é reflexiva? Agora é sim! Essa relação então é o *fecho reflexivo* da R.

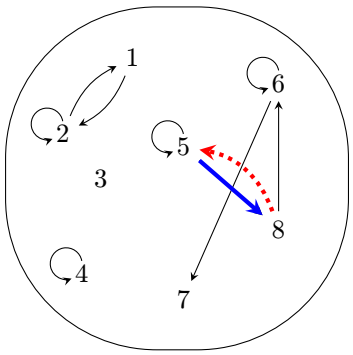
- **EXEMPLO 10.49 (Fecho simétrico).**
Vamos calcular agora o fecho simétrico da mesma relação R do Exemplo 10.48:



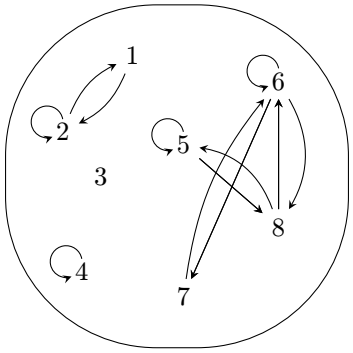
Será que ela já é simétrica? Ela não é por causa das três setinhas seguintes, onde para cada uma mostro em azul a setinha-razão que obriga a setinha-faltante (em vermelho) ser adicionada:





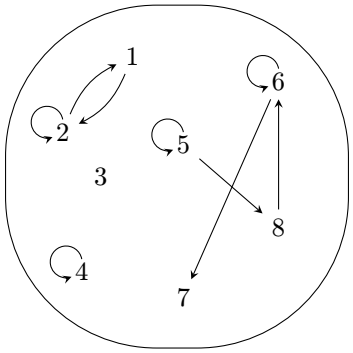


Então adicionamos todas essas setinhas necessárias:

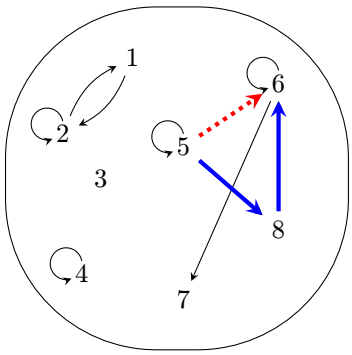


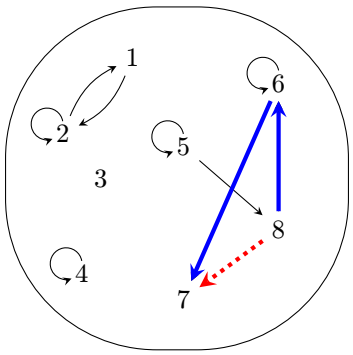
Agora perguntamos novamente: a relação é simétrica? Ela é sim, então paramos aqui. A relação criada é o *fecho simétrico* da R.

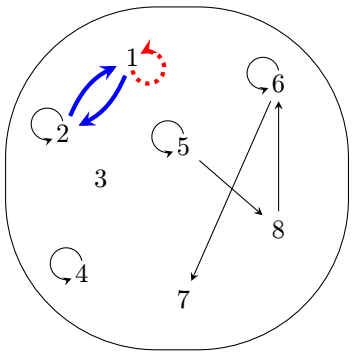
- **EXEMPLO 10.50 (Fecho transitivo).**
Para ser original, seja R a mesma relação dos exemplos 10.48–10.49:



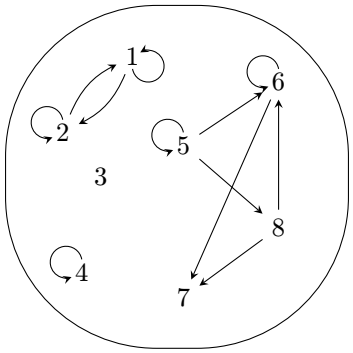
Essa vez vamos calcular o fecho transitivo dela, então começamos com a pergunta: será que a relação já é transitiva? Não é! Então precisamos achar todas as setinhas que deveriam estar nela e não estão e adicioná-las:



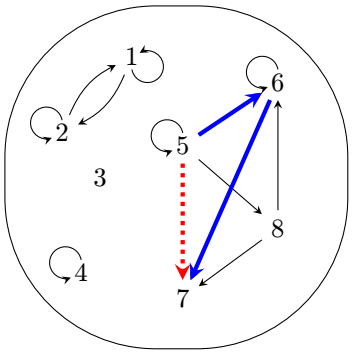


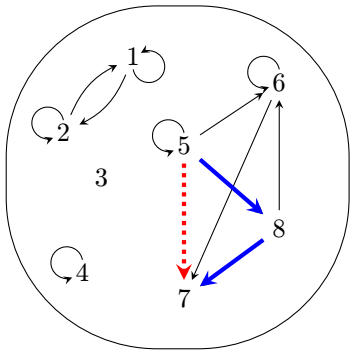


Adicionando todas essas setas necessárias, chegamos na relação:

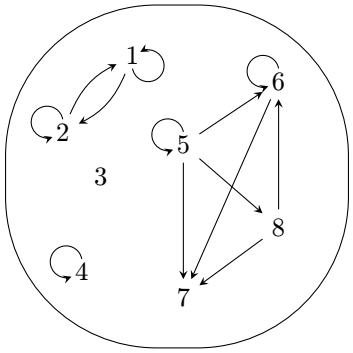


E perguntamos: ela é transitiva? *Ainda não!* Pois, as novas setinhas que adicionamos criaram novos caminhos que obrigam mais uma setinha estar na relação (dois caminhos diferentes explicam a adição dessa mesma setinha nesse caso):





Adicionamos então a setinha $(5, 7)$:



Ela é transitiva agora? Sim, finalmente! Então esse é o *fecho transitivo* da R.

D10.51. "Definição". Seja R uma relação binária num conjunto A, e fixe uma propriedade *razoável* daquelas que aparecem no glossário 10.44. Definimos o fecho da R pela propriedade para ser a relação que criamos se *adicionar* numa maneira *justa* todas as setinhas *necessárias* no diagrama da R até ela virar uma relação com a propriedade desejada.

10.52. Observação (Podemos botar mas não retirar). Note então que o fecho $\bar{R}$ duma relação R tem todas as setinhas que R tem, e possivelmente mais ainda. Ou seja, temos

$$\operatorname{graph} R \subseteq \operatorname{graph} \bar{R}$$

para qualquer fecho escolhido.

Na "Definição" D10.51 enfatizei as palavras «razoável», «justa» e «necessárias». Vamos ver o que cada uma delas quis dizer mesmo.

10.53. Setinhas necessárias. «Adicionar apenas as setinhas *necessárias*» quis dizer que a falta de cada uma dessas setinhas é uma razão que nossa relação não satisfaz a propriedade escolhida. Caso contrário não vamos adiciona-la, *mesmo se sua adição não afeta nada*.

10.54. Maneira justa. «Adicionar setinhas numa maneira *justa*» quis dizer que em nenhum ponto vamos ter que escolher entre duas ou mais setinhas-testemunhas *tais que a adição de apenas uma* seria suficiente para satisfazer a propriedade. Imagine que nesse caso, nossa escolha não seria justa para a setinha não-escolhida (ou para a setinha escolhida, dependendo o ponto de vista). Formar o fecho duma relação deve ser uma operação, e sendo isso deve ser determinística. Imagina então que temos uma propriedade estranha, dizendo que:

$$x\,R\,x \;\&\; y\,R\,y \implies x\,R\,y \text{ ou } y\,R\,x.$$

(Nem adianta tentar achar um nome razoável para essa propriedade.) Agora, a relação R no $\mathbb{N}$ com $\operatorname{graph} R = \{(0,0),(1,1)\}$ claramente não satisfaz essa propriedade. Tentando formar o fecho através dessa propriedade, já na primeira etapa, temos duas "setinhas-testemunhas" que podemos escolher para adicionar: a $(0,1)$ e a $(1,0)$. Graças à restricção de "necessárias", não podemos adicionar ambas, pois assim que adicionar uma, a propriedade já é satisfeita. Por outro lado, não podemos escolher uma das duas numa maneira justa: as duas servem igualmente bem. *Para esse tipo de propriedade então não podemos definir um fecho.* Espero que isso explica também o que eu quis dizer com a palavra «razoável». O Exercício x10.25 esclarecerá isso ainda mais.

▸ **EXERCÍCIO x10.25.**
Por que não falamos de fecho total, irreflexivo, e assimétrico? (x10.25 H 1)

▸ **EXERCÍCIO x10.26.**
Seja R relação num conjunto A. Podemos concluir alguma das afirmações seguintes?:

(i) $t(r(R)) \stackrel{?}{=} r(t(R))$
(ii) $t(s(R)) \stackrel{?}{=} s(t(R))$
(iii) $r(s(R)) \stackrel{?}{=} s(r(R))$

Aqui r, s, t são os fechos reflexivo, simétrico, transitivo respectivamente. (x10.26 H 1 2)

? **Q10.55. Questão.** Como tu definarias formalmente o fecho reflexivo e o fecho simétrico duma relação R?

!! SPOILER ALERT !!

D10.56. Definição (Fecho reflexivo). Seja R relação num conjunto A. Definimos a relação R_{r} pela

$$x\, R_{\mathrm{r}}\, y \iff^{\mathsf{def}} x\, R\, y \text{ ou } x = y$$

Chamamos a R_{r} o *fecho reflexivo* da R. Também usamos a notação $R^{=}$.

▸ **EXERCÍCIO x10.27.**
Alguém definiu o fecho simétrico assim:

> «Seja R relação binária num conjunto A. Seu fecho simétrico é a relação R_{S} definida pela
>
> $$x\, R_{\mathrm{S}}\, y \iff^{\text{“def”}} x\, R\, y \ \&\ y\, R\, x\ .»$$

Ache o erro na definição e mostre que a definição realmente é errada. (x10.27 H 1 2)

D10.57. Definição (Fecho simétrico). Seja R relação num conjunto A. Definimos a relação R_{S} pela

$$x\, R_{\mathrm{S}}\, y \iff^{\mathsf{def}} x\, R\, y \text{ ou } y\, R\, x.$$

Chamamos a R_{S} o *fecho simétrico* da R. Também usamos a notação $R^{\leftrightarrow}$.

▸ **EXERCÍCIO x10.28.**
Alguém definiu o fecho transitivo assim. *Seja R relação binária num conjunto A. Seu fecho transitivo é a relação R_{t} definida pela*

$$x\, R_{\mathrm{t}}\, y \iff^{\text{“def”}} \text{existe } w \in A \text{ tal que } x\, R\, w \ \&\ w\, R\, y.$$

Mas isso não é o fecho transitivo da R. O que é mesmo? (x10.28 H 0)

? **Q10.58. Questão.** Como tu definarias formalmente o fecho transitivo duma relação R?

!! SPOILER ALERT !!

D10.59. Definição (Fecho transitivo). Seja R relação num conjunto A. Definimos as relações R_{t} e R_{rt} pelas

$$x\ R_{\mathrm{t}}\ y \overset{\text{def}}{\iff} x\ R^n\ y \text{ para algum } n \in \mathbb{N}_{>0}. \qquad (\textit{fecho transitivo} \text{ da } R)$$
$$x\ R_{\mathrm{rt}}\ y \overset{\text{def}}{\iff} x\ R^n\ y \text{ para algum } n \in \mathbb{N} \qquad (\textit{fecho reflexivo-transitivo} \text{ da } R)$$

Chamamos a R_{t} o *fecho transitivo* da R, e a R_{rt} o *fecho reflexivo-transitivo* da R. Também usamos as notações R^+ para o R_{t} e R^* para o R_{rt}.

▸ **EXERCÍCIO x10.29.**
Definimos no $\mathbb{N}$ a relação binária $\rightsquigarrow$ pela:

$$a \rightsquigarrow b \overset{\text{def}}{\iff} \text{para algum primo } p,\ ap = b.$$

Qual é o seu fecho reflexivo-transitivo? (x10.29 H 0)

Deixamos as definições de outros fechos para os problemas.

▸ **EXERCÍCIO x10.30.**
Considere a relação $\to$ no $\mathbb{N}$, definida pela:

$$x \to y \overset{\text{def}}{\iff} x + 1 = y.$$

Descreva as relações seguintes:
$\overset{+}{\to}$: seu fecho transitivo;
$\overset{*}{\to}$: seu fecho reflexivo-transitivo;
$\overset{*}{\leftrightarrow}$: seu fecho reflexivo-transitivo-simétrico.

(x10.30 H 0)

▸ **EXERCÍCIO x10.31.**
Considere a relação $\to$ definida pela mesma equação como no Exercício x10.30, mas essa vez no conjunto $\mathbb{R}$. Descreva os mesmos fechos. (x10.31 H 0)

10.60. Observação (E se nunca chegar?). Esse processo descrito no Nota 10.47 pode ser que nunca termina, ou seja esse «até finalmente chegar» que escrevi lá pode ser que nunca chega mesmo numa relação com a propriedade desejada. Por exemplo, considere a $\to$ do Exercício x10.30. Se pensar que começamos com ela no dia 1 e que cada dia que passa adicionamos todas as cetinhas atualmente sendo testemunhas de falta de transitividade, em qual dia vamos chegar numa relação transitiva? *Nunca! E isso seria verdade para um imortal também!* Mas a idéia descrita no 10.47 funciona mesmo assim; é só esquecer essa frase de «finalmente chegar» e entender que pode ser que nunca chegamos numa relação completa, mas mesmo assim, o processo determina uma relação sim: para saber se uma setinha (x, y) está no fecho ou não, é só perguntar se ela vai "entrar" um belo dia ou não.

§232. Bottom-up vs. top-down

Vamos fingir para essa discussão que relações são mesmo os conjuntos das suas setinhas (ou seja, seus gráficos) pois vai facilitar a fala informal e uma notação conjuntista que vou usar. Espero que tu já fez o Exercício x10.1, e logo tu entenderás bem a discussão seguinte tanto no nível informal quanto nos detalhes "verdadeiros" por trás. Vamo lá!

TODO Adicionar desenhos

10.61. Top-down. Imagine que para algum motivo gostamos muito duma propriedade de relações da forma

«se *algo*, então tem que ter essas certas setinhas».

(Pense em transitividade como exemplo "padrão" aqui.) Vamos chamar as relações que tem nossa propriedade de *legais*. Começamos com um conjunto A uma relação nele R bugada, possivelmente ilegal. (Isso quis dizer que não tem a propriedade escolhida.) Procuramos *a* relação $\overline{R}$ para chamar de fecho "legal" da R; esse fecho deve satisfazer:

(L1) $\overline{R} \supseteq R$;
(L2) $\overline{R}$ é legal;

e deve ser "a melhor" entre todas as relações L que satisfazem ambas essas condições. Mas o que significa *melhor*, e o que nos faz acreditar que existe *a* melhor? Aqui melhor quis dizer que a $\overline{R}$ deve ser *fiel* na R, no sentido de não conter setas desnecessárias, setas não fornecidas/necessidadas por causa da relação original R. Como vamos descobrir, tal $\overline{R}$ existe mesmo, e vamos definí-la numa maneira extremamente elegante e legal!

A primeira coisa importante para perceber é que *já sabemos que pelo menos uma relação satisfaz ambas as condições (L1)–(L2) acima:* a relação cheia, trivial True do A. Vamos chamá-la de G—pense "Grande". Com certeza $G \supseteq R$, pois como poderia não ser? G é a relação cheia, ela tem todas as setinhas, então com certeza as setinhas da R também. Pelo mesmo motivo e pela natureza da própria propriedade temos certeza que G também goza da (L2): ela é legal.

Bem, temos uma candidata; mas estamos procurando a melhor, pois essa pode ter *lixo*. Procuramos uma maneira de jogar fora todo o lixo da G.

Uma idéia ruim para conseguir isso seria seguinte: pega uma setinha α do $G \setminus R$ e veja se removendo essa α, tu quebras a "legaldade". Qual o problema com essa abordagem? Bem: vai que tu pegou uma setinha e que observou que ela não pode ser jogada fora, pois duas outras setinhas estão a obrigando ficar mesmo. Mas, por que confiar nessas outras setinhas? Talvez elas mesmas também fazem parte do lixo, e deveriam ser jogadas foras também. Mas então, como escolher onde começar a investigação? Hah! Nem vamos escolher nenhum canto para começar, pois nem vamos começar investigar nada disso! Vamos usar uma maneira bem simples e jogar todo o lixo fora num instante só!

Vamos definir a colecção de todos os candidatos:

$$\mathscr{L}_R \stackrel{\text{def}}{=} \{\, L : \mathrm{Rel}\,(A, A) \;\mid\; L \supseteq R \;\&\; L \text{ é legal} \,\}.$$

Primeiramente observe que sabemos que essa colecção não é vazia, pois se fosse a gente teria um problema grande—tu vai entender logo qual. Realmente, a G é uma das candidatas, então $G \in \mathscr{L}_R$ e logo $\mathscr{L}_R \neq \emptyset$. Agora observe que cada candidato $L \in \mathscr{L}_R$ satisfaz

$$G \supseteq L \supseteq R.$$

Ambas são imediates pela definição do $\mathscr{L}_R$. Tem então dois casos extremos (onde L é uma das G, R) mas no caso geral L fica estritamente entre as relações G e R. Estamos finalmente prontos para a definição linda que prometi, que vai acabar com todo o lixo:

$$\overline{R} \stackrel{\text{def}}{=} \bigcap \mathscr{L}_R.$$

Afirmo que:

(1) $\overline{R} \supseteq R$;
(2) $\overline{R}$ é legal;
(3) $\overline{R}$ é a melhor: não tem lixo nenhum.

Antes de demonstrar esses pontos, primeiramente quero te preocupar com uma outra perguta:

? **Q10.62. Questão.** Alguém poderia reclamar que certas das setinhas que foram jogadas fora nesse processo, por exemplo essa aqui abaixo, foram injustamente tiradas, e talvez eram essenciais, ou seja, necessárias mesmo para a legaldade da relação. O que responderias? Como podemos convencer essa pessoa que a setinha não foi realmente necessária?

!! SPOILER ALERT !!

10.63. Resposta. Observe que essa setinha pertence a uma das candidatas do $\mathscr{L}_R$, mas tem outras candidatas que não têm essa setinha nelas e mesmo assim conseguem ser legais! Ou seja, com certeza essa setinha não pode ser necessária mesmo para a legaldade da relação que estamos procurando!

10.64. O que falta?. Basta demonstrar as (1)–(3) agora. A primeira *deve ser óbvia* para o leitor que já passou pelo Capítulo 8 (até se ele pulou—foi sem querer né?—o Exercício x8.43, que é exatamente isso). As outras duas, tu demonstrarás agora:

▸ **EXERCÍCIO x10.32.**
Demonstre a (2) do Nota 10.61 (x10.32 H 0)

▸ **EXERCÍCIO x10.33.**
Demonstre a (3) do Nota 10.61 (x10.33 H 0)

10.65. Bottom-up.

TODO Descrever como imortal construtor por dia

10.66. Sempre concordam?. Tem situações onde a definição bottom-up e definição top-down discordam! Isso pode acontecer, por exemplo, quando o "imortal" construindo

na maneira bottom-up necessitaria uma infinidade *mais longa que a largura dos naturais*—e se essa frase não fez nenhum sentido agora, tranqüilo, não era pra fazer: volte a relê-la depois de ter estudado *aritmética ordinal* no Secção §332.

§233. Relações de ordem

D10.67. Definição (Ordem). Seja R uma relação binária num conjunto A. Chamamos a R *ordem parcial* sse ela é reflexiva, transitiva, e antissimétrica. Se ela também é total, a chamamos de *ordem total*.

! **10.68. Cuidado.** Quando usamos apenas o termo *ordem*, entendemos como *ordem parcial*. Observe que esta convenção é a oposta que seguimos nas funções, onde um pleno *função* quis dizer *função total*.

• **EXEMPLO 10.69.**
Dado qualquer conjunto X, seus subconjuntos são parcialmente ordenados tanto por $(\subseteq)$ quanto por $(\supseteq)$.

• **EXEMPLO 10.70.**
As $(\leq)$ e $(\geq)$ comuns são ordens totais nos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

▸ **EXERCÍCIO x10.34.**
A relação $(|)$ nos inteiros é uma relação de ordem? (x10.34 H 1)

• **EXEMPLO 10.71.**
A relação $(|)$ no $\mathbb{N}$ é uma ordem parcial. (Demonstraste isso no Exercício x3.101.)

D10.72. Definição (Ordem estrita). Seja R uma relação binária num conjunto A. Chamamos a R *ordem estrita* sse ela é irreflexiva, transitiva, e assimétrica. Se ela também é tricotômica, chamamos-la *ordem estrita total*.

10.73. Observação (Adjectivo implícito). Quando queremos enfatizar que uma relação é uma ordem e não uma ordem estrita, usamos o termo *fraca*. Similarmente com as funções (totais vs. parciais), Dependendo do contexto o *adjectivo implícito* pode mudar. Quando focamos em ordens estritas, "ordem" vira sinônimo de "ordem estrita" e precisamos o adjectivo "fraca" para referir a uma ordem (fraca).

▸ **EXERCÍCIO x10.35 (De fraca para estrita; ida e volta).**
(1) Seja $(\leq)$ ordem num conjunto A. Defina a relação $(<)$ no A pela:

$$x < y \iff^{\text{def}} x \leq y \ \& \ x \neq y.$$

Demonstre que $(<)$ é uma ordem estrita.
(2) Seja $(<)$ ordem estrita num conjunto A, e defina a relação $(\leq)$ no A pela:

$$x \leq y \iff^{\text{def}} x < y \text{ ou } x = y.$$

Demonstre que $(\leq)$ é uma ordem. (x10.35 H 0)

D10.74. Definição (Preordem). Uma relação binária R num conjunto A é chamada *preordem* (ou *quasiordem*) sse ela é reflexiva e transitiva.

- **EXEMPLO 10.75.**
Como demonstramos no Exercício x3.101, a relação $(|)$ nos inteiros é uma preordem.

No Problema II10.20 tu vai justificar o nome "preordem", mostrando que cada preordem R fornece uma ordem R'.

Paramos *por enquanto* o estudo de relações de ordem; voltaremos ao estudo profundo delas no Capítulo 14.

§234. Relações de equivalência

10.76. Equivalência. Considere um conjunto A, onde queremos "identificar" certos elementos deles, talvez porque ligamos apenas sobre uma propriedade, e queremos ignorar os detalhes irrelevantes que nos obrigariam distinguir uns deles. Por exemplo, se A é um conjunto de pessoas, podemos focar apenas na "nacionalidade". Esquecendo todos os outros detalhes então, vamos considerar todos os compatriotas como se fossem "iguais": o termo certo é *equivalentes*. Outra propriedade poderia ter sido o ano que cada pessoa nasceu, ou o primeiro nome, ou até quem é a mãe de cada pessoa. Queremos identificar as propriedades que uma relação desse tipo tem que ter:

(i) Reflexividade: não importa qual foi o critério que escolhemos para "equivaler" os objetos, cada objeto com certeza vai "concordar" com ele mesmo nesse critério.
(ii) Transitividade: se a e b concordam no assunto escolhido, e b e c também, com certeza a e c devem concordar também.
(iii) Simetría: pela natureza da nossa intuição é claro que para decidir se dois elementos serão equivalentes ou não, não precisamos considerá-los numa ordem específica.

Chegamos assim na definição seguinte:

D10.77. Definição. Seja A conjunto e $\sim$ uma relação binária no A. Chamamos $\sim$ uma *relação de equivalência* sse ela é reflexiva, simétrica, e transitiva. Definimos também o

$$\operatorname{EqRel}(A) \stackrel{\text{def}}{=} \{\, R \in \operatorname{Rel}(A,A) \mid R \text{ é uma relação de equivalência} \,\}.$$

- **EXEMPLO 10.78.**
A $(=)$ é uma relação de equivalência.

- **EXEMPLO 10.79.**
A relação $\sim_2$ que relaciona exatamente os inteiros com a mesma paridade

$$x \sim_2 y \iff \text{ambos os } x, y \text{ são pares ou ambos os } x, y \text{ são ímpares.}$$

Essa relação de equivalência é um caso especial da próxima.

▸ **EXERCÍCIO x10.36.**
Seja $m \in \mathbb{N}$. Demonstre que a relação binária nos inteiros definida pela

$$a \equiv_m b \stackrel{\text{def}}{\iff} a \equiv b \pmod{m}$$

é uma relação de equivalência. (x10.36 H 0)

• **EXEMPLO 10.80.**
Em qualquer conjunto P de pessoas, a relação

$$x \sim y \stackrel{\text{def}}{\iff} x \text{ e } y \text{ nasceram no mesmo país}$$

é uma relação de equivalência.

• **EXEMPLO 10.81.**
No conjunto $\mathcal{P}$ de pessoas, a relação

$$x \sim y \stackrel{\text{def}}{\iff} x \text{ e } y \text{ têm a mesma quantidade de filhos}$$

é uma relação de equivalência.

• **EXEMPLO 10.82.**
No conjunto $\mathcal{B}$ de jogadores profissionais de basquete, a relação

$$x \sim y \stackrel{\text{def}}{\iff} x \text{ e } y \text{ jogam no mesmo clube}$$

é uma relação de equivalência.

• **NÃOEXEMPLO 10.83.**
Num conjunto $\mathcal{P}$ de pessoas, a relação

$$x \sim y \stackrel{\text{def}}{\iff} \text{existe comida que } x \text{ e } y \text{ ambos comeram hoje}$$

não é sempre uma relação de equivalência.

▸ **EXERCÍCIO x10.37.**
Por que não? (x10.37 H 1)

• **EXEMPLO 10.84.**
No $\mathbb{R}^2$ considere as relações:

$$\begin{aligned}
\langle x, y\rangle \sim_1 \langle x', y'\rangle &\iff x = x' \\
\langle x, y\rangle \sim_2 \langle x', y'\rangle &\iff y = y' \\
\langle x, y\rangle \sim_{\mathrm{N}} \langle x', y'\rangle &\iff \|\langle x, y\rangle\| = \|\langle x', y'\rangle\|
\end{aligned}$$

Facilmente todas são relações de equivalência.

• **EXEMPLO 10.85.**
No $\mathbb{R}^3$ considere as relações:

$$\begin{aligned}\langle x,y,z\rangle \sim_3 \langle x',y',z'\rangle &\iff z = z'\\ \langle x,y,z\rangle \sim_{1,2} \langle x',y',z'\rangle &\iff x = x' \;\&\; y = y'\\ \langle x,y,z\rangle \sim_{\mathrm{N}} \langle x',y',z'\rangle &\iff \|\langle x,y,z\rangle\| = \|\langle x',y',z'\rangle\|\end{aligned}$$

Facilmente todas são relações de equivalência.

▸ **EXERCÍCIO x10.38.**
Mudamos o "e" para "ou" na segunda relação do Exemplo 10.85:

$$\langle x,y,z\rangle \sim \langle x',y',z'\rangle \iff x = x' \text{ ou } y = y'$$

A $\sim$ é uma relação de equivalência? (x10.38 H 1)

▸ **EXERCÍCIO x10.39.**
Seja A um conjunto qualquer. Quais relações de equivalência podes já definir nele, sem saber absolutamente nada sobre seus elementos? (x10.39 H 0)

▸ **EXERCÍCIO x10.40.**
Seja A conjunto com $|A| = 3$. Quantas relações de equivalência podemos definir no A? (x10.40 H 1)

▸ **EXERCÍCIO x10.41.**
Seja R uma relação binária num conjunto A. O.s.s.e.:
(i) R é uma relação de equivalência;
(ii) R é reflexiva e circular;
(iii) R é reflexiva e left-euclideana;
(iv) R é reflexiva e right-euclideana. (x10.41 H 0)

▸ **EXERCÍCIO x10.42.**
Seja real $\varepsilon \in (0,1)$, e defina a relação $\approx_\varepsilon$:

$$x \approx_\varepsilon y \overset{\text{def}}{\iff} (x-y)^2 < \varepsilon.$$

A $\approx_\varepsilon$ é uma relação de equivalência? (x10.42 H 1 2 3 4 5)

D10.86. Definição. Seja A um conjunto e $\sim$ uma relação de equivalência no A. Para cada $a \in A$, definimos a *classe de equivalência do* a como o conjunto de todos os membros de A que $\sim$-relacionam com o a. Formalmente definimos

$$[a]_\sim \stackrel{\text{def}}{=} \{\, x \in A \mid x \sim a \,\}.$$

Às vezes aparece também a notação $[a/\sim]$. Quando a relação de equivalência é implicita pelo contexto denotamos a $[a]_\sim$ apenas por $[a]$.

▸ **EXERCÍCIO x10.43.**
Sejam A conjunto, $a \in A$, e $\sim$ relação de equivalência no A. Considere as funções seguintes definidas com buracos:

$$[-]_\sim : \ldots?\ldots \qquad [a]_ : \ldots?\ldots \qquad [-]_ : \ldots?\ldots$$

Escreva tipos válidos para essas funções. (x10.43 H 0)

▸ **EXERCÍCIO x10.44.**
Sejam $\sim$ uma relação de equivalência num conjunto X, e $a, b \in X$. Mostre que as afirmações seguintes são equivalentes:
(i) $a \sim b$;
(ii) $[a] = [b]$;
(iii) $[a] \cap [b] \neq \emptyset$.
(x10.44 H 0)

10.87. Partição. Voltamos de novo para nosso conjunto A do 10.76, mas esta vez sem uma predeterminada propriedade para focar. Esta vez vamos dividir os elementos do A em *classes*, tais que cada membro do A pertencerá a *exatamente uma delas*, e cada uma delas terá pelo menos um membro do A. E nem vamos justificar essa separação, explicando o como ou o porquê. Esse tipo de colecção de classes já encontramos na Secção §195: é o que chamamos de *partição*; aqui uma reformulação da Definição D8.154:

D10.88. Definição. Seja A conjunto e $\mathscr{A} \subseteq \wp A$ uma família de subconjuntos de A. $\mathscr{A}$ é uma *partição* de A, sse:
(P1) $\bigcup \mathscr{A} = A$;
(P2) os membros de $\mathscr{A}$ são disjuntos dois-a-dois;
(P3) $\emptyset \notin \mathscr{A}$.
Chamamos de *classes* os membros da $\mathscr{A}$.

▸ **EXERCÍCIO x10.45.**
Verifique que as definições D8.154 e D10.88 são, de fato, equivalentes.
(x10.45 H 0)

▸ **EXERCÍCIO x10.46.**
Podemos trocar o (P1) da Definição D10.88 por

$$\text{(P1')} \quad \bigcup \mathscr{A} \supseteq A \ ?$$

(x10.46 H 1)

▸ **EXERCÍCIO x10.47.**
Podemos trocar o (P2) da Definição D10.88 por

$$\text{(P2')} \quad \bigcap \mathscr{A} = \emptyset \ ?$$

(x10.47 H 1 2)

TODO Check blending

Intervalo de problemas

▸ **PROBLEMA Π10.1.**
Seja R uma preordem num conjunto A. Demonstre que R é *idempotente*, ou seja, $R = R \diamond R$.
(Π10.1 H 0)

▸ **PROBLEMA Π10.2.**
Seja S uma relação binária num conjunto A tal que

$$\left(S \diamond S^{\partial}\right) \text{ é irreflexiva.}$$

Qual é o gráfico da S? Demonstre tua resposta. (Π10.2 H 1)

▸ **PROBLEMA Π10.3.**
Sejam R, S relações binárias e transitivas no A. Podemos concluir que $R \diamond S$ também é transitiva? Se sim, demonstre; se não, mostre um contraexemplo. (Π10.3 H 1)

▸ **PROBLEMA Π10.4.**
Seja $R : \mathrm{Rel}\,(X, X)$. Demonstre que para todo $n \in \mathbb{N}$,

$$(R^n)^{\partial} = \left(R^{\partial}\right)^n.$$

(Π10.4 H 1)

▸ **PROBLEMA Π10.5 (O paradoxo de Condorcet).**
Seja $P \neq \emptyset$ um conjunto de pessoas e $C \neq \emptyset$ um conjunto de candidatos. Seja $\succcurlyeq$ a relação binária no C definida pela

$$x \succcurlyeq y \iff^{\text{def}} \text{ a maioria da população do } P \text{ prefere } x \text{ do que } y.$$

Podemos concluir que $\succcurlyeq$ é transitiva? Responde "sim" e demonstre; ou "não" e mostre um contraexemplo. (Π10.5 H 1)

▸ **PROBLEMA Π10.6.**
Sejam $A \xrightarrow{f} B$ e $\rightsquigarrow$ uma relação transitiva no A. Definimos a relação R no B pela

$$b \mathrel{R} b' \iff^{\text{def}} \text{ existem } a, a' \in A \text{ tais que } f(a) = b,\ f(a') = b', \text{ e } a \rightsquigarrow a'.$$

Podemos concluir que R também é transitiva? Se sim, demonstre; se não, mostre um contraexemplo. (Π10.6 H 1 2)

▸ **PROBLEMA Π10.7.**
O que muda no Problema Π10.6 se adicionar a hipótese que f é injetora? Demonstre tua afirmação. (Π10.7 H 0)

▸ **PROBLEMA Π10.8.**
Seja a relação $\to$ no $\mathbb{N}$ definida pela

$$a \to b \iff^{\text{def}} a + 1 = b.$$

Dê uma definição simples da relação $\to^n$ para quem não sabe nem de iterações nem de composições de relações (e sequer quer aprender essas noções). Demonstre tua afirmação, que a relação $\to^n$ é igual à relação que tu definiu. (Π10.8 H 1)

▸ **PROBLEMA Π10.9.**
Sejam conjunto A com $|A| > 2$, e n inteiro par positivo. No A^n defina:

$$a \sim b \iff |\{\, i \in \overline{n} \mid a_i = b_i \,\}| \geq n/2,$$

onde $a =: \langle a_0, \ldots, a_{n-1} \rangle$ e $b =: \langle b_0, \ldots, b_{n-1} \rangle$. A $\sim$ é uma relação de equivalência? (Π10.9 H 0)

▸ **PROBLEMA Π10.10.**
Considere as relações seguintes no $(\mathbb{Z} \to \mathbb{Z})$:

$$\begin{aligned}
f \sim g &\iff (\exists u \in \mathbb{Z}\quad)(\forall x \in \mathbb{Z})[\, f(x) = g(x+u) \,] \\
f \approx g &\iff (\exists u \in \mathbb{Z}_{\geq 0})(\forall x \in \mathbb{Z})[\, f(x) = g(x+u) \,] \\
f \wr g &\iff (\exists u \in \mathbb{Z}\quad)(\forall x \in \mathbb{Z})[\, f(x) = g(x) + u \,] \\
f \wr\!\!\wr g &\iff (\exists u \in \mathbb{Z}_{\geq 0})(\forall x \in \mathbb{Z})[\, f(x) = g(x) + u \,].
\end{aligned}$$

Para cada uma dessas relações, decida se é: (ir)reflexiva; transitiva; (a(nti)s)simétrica. (Π10.10 H 1)

▸ **PROBLEMA Π10.11.**
Defina as relações seguintes no $(\mathbb{N} \to \mathbb{N})$ assim:

$$\begin{aligned}
f \overset{\text{z}}{=} g &\iff f(0) = g(0) \\
f \overset{\text{e}}{=} g &\iff f(2n) = g(2n) \text{ para todo } n \in \mathbb{N} \\
f \overset{\text{o}}{=} g &\iff f(2k+1) = g(2k+1) \text{ para todo } k \in \mathbb{N} \\
f \overset{\infty}{=} g &\iff f(n) = g(n) \text{ para uma infinidade de } n \in \mathbb{N}.
\end{aligned}$$

(i) Para cada uma da $\overset{\text{z}}{=}, \overset{\text{e}}{=}, \overset{\text{o}}{=}, \overset{\infty}{=}$, decida se é uma relação de equivalência ou não.
(ii) Demonstre ou refute a afirmação seguinte: *a relação* $(\overset{\text{e}}{=} \diamond \overset{\text{o}}{=})$ *é a relação trivial* True.

(Π10.11 H 1)

▸ **PROBLEMA Π10.12.**
No conjunto $(\mathbb{R} \to \mathbb{R})$ definimos:

$$\begin{aligned}
f \approx g &\iff \text{o conjunto } \{\, x \in \mathbb{R} \mid f(x) = g(x) \,\} \text{ é infinito;} \\
f \sim g &\iff \text{o conjunto } \{\, x \in \mathbb{R} \mid f(x) \neq g(x) \,\} \text{ é finito.}
\end{aligned}$$

Demonstre que:
(i) uma delas é relação de equivalência;
(ii) a outra não é. (Π10.12 H 1 2 3)

▸ **PROBLEMA Π10.13.**
Defina no $(\mathbb{R} \to \mathbb{R})$ as relações seguintes:

$$\begin{aligned}
f \overset{\exists\forall}{\leq} g &\iff (\exists n \in \mathbb{N})(\forall x \geq n)[\, f(x) \leq g(x) \,] \\
f \overset{\forall\exists}{\leq} g &\iff (\forall n \in \mathbb{N})(\exists x \geq n)[\, f(x) \leq g(x) \,] \\
f \overset{\exists\forall}{<} g &\iff (\exists n \in \mathbb{N})(\forall x \geq n)[\, f(x) < g(x) \,] \\
f \overset{\forall\exists}{<} g &\iff (\forall n \in \mathbb{N})(\exists x \geq n)[\, f(x) < g(x) \,]
\end{aligned}$$

Para cada uma das relações acima, decida se ela tem ou não cada uma das propriedades de uma ordem total, e de uma ordem estrita. (Π10.13 H 0)

▸ **PROBLEMA Π10.14 (implementando funções como relações e vice versa).**
Já encontramos a idéia de *implementação* de algum conceito matemático no Capítulo 9 (§209, Π9.18, Π9.19). Como tu definiria funções como relações, e como relações como funções? Dê apenas um esboço da tua idéia, sem entrar em muitos detalhes. (Π10.14H0)

§235. Partições

§236. Conjunto quociente

Os dois conceitos de "relação de equivalência" e "partição", parecem diferentes mas realmente são apenas duas formas diferentes de expressar a mesma idéia. Cada relação de equivalência determina uma partição; e vice-versa: cada partição determina uma relação de equivalência. Bora demonstrar isso!

▸ **EXERCÍCIO x10.48 (Cuidado!).**
Tentando investigar isso, começando com uma relação de equivalência R, um aluno tentou definir a partição correspondente $\mathscr{A}_R$ assim:

$$\begin{aligned} C \in \mathscr{A}_R \iff^{\text{def}} & C \subseteq A \\ & \;\&\; C \neq \emptyset \\ & \;\&\; (\forall c, d \in C)[\, c \mathrel{R} d \,]. \end{aligned}$$

Qual o erro na definição do aluno? O que faltou escreverer para virar uma definição correta? (x10.48H123)

▸ **EXERCÍCIO x10.49 (De equivalência para partição).**
Seja $\sim$ relação de equivalência num conjunto A. Escreva formalmente como definir uma partição $\mathscr{A}_\sim$ do A em que suas classes são feitas por todos os $\sim$-relacionados. Demonstre que realmente é uma partição. (x10.49H1)

▸ **EXERCÍCIO x10.50.**
Explique onde precisou cada uma das propriedades da Definição D10.77 (reflexividade, transitividade, simetria) na tua resolução do Exercício x10.49. (x10.50H0)

A partição definida no Exercício x10.49 é muito importante e merece seu próprio nome e sua própria notação. Definimos agora.

D10.89. Definição. Seja A um conjunto e $\sim$ uma relação de equivalência no A. Definimos o *conjunto quociente* de A por $\sim$ para ser a colecção de todas as classes de equivalência através da $\sim$. Formalmente:

$$A/\!\sim \stackrel{\text{def}}{=} \{\, [a]_\sim \mid a \in A \,\}.$$

▸ **EXERCÍCIO x10.51.**
Sejam A conjunto e $\sim$ relação de equivalência no A. Considere a função seguinte definida com buraco:

$$A/- : \ \ldots ? \ldots$$

Escreva um tipo válido para essa função. (x10.51 H 0)

10.90. Enxergando o conjunto quociente. Tendo um conjunto A e uma relação de equivalência $(\sim)$, no conjunto quociente $A/\sim$ a relação de equivalência $(\sim)$ se vira igualdade $(=)$ mesmo. Numa maneira, $A/\sim$ é o mundo que chegamos se nossa $(\sim)$ virar para ser a nossa $(=)$. O mundo onde não conseguimos enxergar diferenças entre objetos $(\sim)$-relacionados. Para dar um exemplo, considere o conjunto dos inteiros $\mathbb{Z}$, e a relação de equivalência $(\sim)$ definida pela

$$x \sim y \iff^{\text{def}} x \equiv y \pmod 2,$$

ou seja, $(\sim)$ relaciona os inteiros com a mesma *paridade* (Exemplo 10.79). Vamos olhar para nosso conjunto:

$$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Quantos elementos ele tem? Uma infinidade, correto? Sim, pois todos os

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

são distintos dois-a-dois. Vamos lembrar uma propriedade fundamental de conjuntos: quantos elementos tem o

$$\{7, 7, 7, 5, 0, 8, 8\}?$$

Temos escrito 7 termos para ser exatamente os membros desse conjunto, mas quantos elementos ele tem mesmo? 4, pois num conjunto não existe a noção de *quantas vezes* um membro pertence a ele; só a noção de pertencer. E isso é uma conseqüência imediata da definição de igualdade de conjuntos. Lembre se:

$$A = B \iff^{\text{def}} (\forall x)[\, x \in A \iff x \in B\,]$$

e logo

$$\{7, 7, 7, 5, 0, 8, 8\} = \{0, 8, 7, 5\}$$

pois realmente para todo x,

$$x \in \{7, 7, 7, 5, 0, 8, 8\} \iff x \in \{0, 8, 7, 5\}$$

e, sendo iguais não pode ser que eles têm cardinalidades diferentes! Voltando para o conjunto de inteiros

$$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

agora imagina que perguntamos sobre sua cardinalidade uma pessoa $\sim$-cega. O que quis dizer $\sim$-cega? Ela não consegue enxergar como distintos objetos relacionados pela $\sim$. O que ela vai responder em nossa pergunta? «2». Pois, para essa pessoa os

$$\ldots, -4, -2, 0, 2, 4, \ldots$$

são todos indistingüíveis, e a mesma coisa sobre os

$$\ldots, -5, -3, -1, 1, 3, 5, \ldots$$

O conjunto quociente $\mathbb{Z}/\sim$ então, é o conjunto que ela enxerga. Só tem um probleminha agora: *quais* são esses dois membros do conjunto que ela enxerga? A resposta correta aqui pode aparecer chocante mas é a seguinte:

Não importa!

Uma escolha natural seria escolher como membros do $\mathbb{Z}/\sim$ os dois conjuntos:

$$\{\ldots,-4,-2,0,2,4,\ldots\} \qquad \text{e} \qquad \{\ldots,-5,-3,-1,1,3,5,\ldots\}$$

chegando assim no

$$\mathbb{Z}/\sim = \{\{\ldots,-4,-2,0,2,4,\ldots\},\{\ldots,-5,-3,-1,1,3,5,\ldots\}\}.$$

De fato, pela Definição D10.89 do conjunto quociente, $\mathbb{Z}/\sim$ realmente *é* esse conjunto. E isso faz sentido, pois uma definição de A/R precisa determinar completamente um objeto. Mas uma outra escolha poderia ser, por exemplo, o conjunto

$$\{0,1\}$$

ou qualquer conjunto feito escolhendo outros "rótulos" para cada classe de equivalência:

$$\{\mathbf{0},\mathbf{1}\}, \quad \{\text{even},\text{odd}\}, \quad \{\text{E},\text{O}\}, \quad \{\emptyset,\{\emptyset\}\}, \quad \ldots$$

Basta só ter exatamente dois membros. Toda esta conversa chega no teorema e na definição seguintes:

Θ10.91. Teorema. *Seja A conjunto e $\sim$ uma relação binária nele. $A\sim$ é uma relação de equivalência se e somente se existe conjunto Q e surjecção*

(QS1) $$\pi : A \twoheadrightarrow Q$$

tal que $(\sim) = (\approx_\pi)$ (Definição D10.99), ou seja, tal que

(QS2) $$x \sim y \iff \pi(x) = \pi(y).$$

▸ Esboço. ($\Rightarrow$). O conjunto Q é o $A/\sim$ e a surjecção π é a "projecção canônica" $[-]_\sim$. ($\Leftarrow$). Demonstrado no Exercício x10.61. □

D10.92. Definição. No contexto do Teorema Θ10.91, quando temos π e Q que satisfazem as (QS1) e (QS2), dizemos que Q é um *quociente* de A por $\sim$, e que π é uma *surjecção determinante* da $\sim$.

10.93. Observação. A demonstração do Teorema Θ10.91 fornece o quociente $A/\sim$ e a surjecção determinante $\lambda x\,.\,[x]_\sim$ (ou, com buracos, $[-]_\sim$) que mapeia cada membro de A a sua classe de equivalência. Vamos dizer que esse será o "conjunto quociente oficial", e a "surjecção determinante oficial". Mas dependendo do uso, pode ser que para uns casos é melhor utilizar outro quociente e outra surjecção determinante. E até pior—ou, na verdade, melhor—pessoas diferentes podem escolher quocientes diferentes como *mais iluminantes*. Vamos ver uns exemplos. Em cada um, vamos ver o oficial, e comparar com uma alternativa melhor. Vamos usar a notação

$$A/\sim \text{ "=" } Q$$

para afirmar que Q é *um* quociente que possivelmente parece mais iluminante do que o oficial.

• **EXEMPLO 10.94.**
Considere um conjunto de pessoas P. Na relação do Exemplo 10.80

$$x \sim y \overset{\text{def}}{\iff} x \text{ e } y \text{ nasceram no mesmo país}$$

o conjunto quociente oficial é feito por conjuntos de pessoas compatriotas. Uma escolha melhor seria usar os próprios países como quociente, e a

$$\pi(x) = \text{o país em que } x \text{ nasceu.}$$

Para ser sobrejetora mesmo, no quociente não vamos incluir paises em quais nenhuma pessoa (de P) nasceu. Seja C esse conjunto de paises c onde pelo menos uma pessoa $p \in P$ nasceu. Então temos

$$P/\sim \text{“=”} C.$$

Num certo sentido, *dividindo esse conjunto de pessoas P pela relação $\sim$*, chegamos no conjunto de paises C.

▸ **EXERCÍCIO x10.52.**
Na relação do Exemplo 10.81

$$x \sim y \overset{\text{def}}{\iff} x \text{ e } y \text{ têm a mesma quantidade de filhos}$$

qual é o conjunto quociente (oficial)? Qual tu escolharia como melhor? (x10.52 H 0)

▸ **EXERCÍCIO x10.53.**
Na relação do Exemplo 10.82

$$x \sim y \overset{\text{def}}{\iff} x \text{ e } y \text{ jogam no mesmo clube}$$

qual é o conjunto quociente (oficial)? Qual tu escolharia como melhor? (x10.53 H 0)

• **EXEMPLO 10.95.**
Vamos descrever geometricamente as classes de equivalência das relações do Exemplo 10.84 no $\mathbb{R}^2$, ou seja, determinar os conjuntos quocientes correspondentes. Lembramos as relações:

$$\begin{aligned}
\langle x, y\rangle \sim_1 \langle x', y'\rangle &\iff x = x' \\
\langle x, y\rangle \sim_2 \langle x', y'\rangle &\iff y = y' \\
\langle x, y\rangle \sim_{\mathrm{N}} \langle x', y'\rangle &\iff \|\langle x, y\rangle\| = \|\langle x', y'\rangle\|
\end{aligned}$$

Em cada classe de equivalência da $\sim_1$ então, estão todos os pares que concordam na sua primeira coordenada. Ou seja, cada classe é uma retas vertical, e o conjunto quociente é colecção de todas essas linhas. Olhando ainda mais de longe, podemos “identificar” cada reta com seu representante canônico que fica no eixo-x, ou seja, podemos dizer que

$$\mathbb{R}^2/\sim_1 \text{“=”} \mathbb{R}.$$

A situação é similar para a $\sim_2$, so que essa vez são todas as retas horizontais, mas olhando novamente de longe, identificamos cada reta com seu representante canônico que agora fica no eixo-y, ou seja, novamente temos

$$\mathbb{R}^2/\sim_2 \text{“=”} \mathbb{R}.$$

Sobe a $\sim_{\mathrm{N}}$, a classes do seu conjunto quociente são todos os cíclos com centro a origem $(0,0)$, incluindo o "ciclo-trivial" com raio 0, que acaba sendo apenas o ponto $(0,0)$ mesmo. Essa vez, identificando cada cíclo com seu raio, chegamos na

$$\mathbb{R}^2/{\sim_{\mathrm{N}}} \text{ “=” } \mathbb{R}_{\geq 0}.$$

Por enquanto, entendemos todas essas "=" apenas como um "modo de falar". Cuidado pois nenhuma delas é uma verdadeira (=)! Os dois lados dessas "igualdades" são conjuntos cujos membros nem são objetos do mesmo tipo! No lado esquerdo pertencem *conjuntos de pares de números reais*, no lado direito pertencem *números reais*.

▸ **EXERCÍCIO x10.54.**
Descreva geometricamente e algebricamente os conjuntos quocientes das relações de equivalência do Exemplo 10.85. (x10.54 H 1)

▸ **EXERCÍCIO x10.55.**
Seja $m \in \mathbb{N}_{>1}$. Já demonstrou no Exercício x10.36 que a relação de congruência módulo m é uma relação de equivalência. Vamos denotá-la '$\equiv_m$'. Então: qual é o seu conjunto quociente? Também: seguindo a idéia do Exemplo 10.95, com que tu "identificaria" o $\mathbb{Z}/{\equiv_m}$? (x10.55 H 0)

▸ **EXERCÍCIO x10.56.**
Continuando: quais são as relações $\equiv_0$ e $\equiv_1$? (x10.56 H 1)

▸ **EXERCÍCIO x10.57.**
Descreva o conjunto quociente $\mathbb{N}/{\overset{*}{\leftrightarrow}}$ do Exercício x10.30. (x10.57 H 0)

Já vimos que cada relação de equivalência determina uma partição: seu conjunto quociente. Mas parece que a partição é um conceito mais geral, pois nos permite "separar em classes" um conjunto numa forma que não é obrigada seguir nenhuma lógica ou regra: sem nenhuma relação de equivalência "por trás". Ou seja: *talvez tem partições que não são conjuntos quocientes de nenhuma relação de equivalência.* Mas essa intuição razoável é enganosa! Vamos investigar agora o caminho de volta: mostrar que cada partição $\mathscr{A}$ também determina uma relação de equivalência $\sim_{\mathscr{A}}$, e sim, a partição $\mathscr{A}$ é um conjunto quociente: o $A/{\sim_{\mathscr{A}}}$!

▸ **EXERCÍCIO x10.58 (de partição para equivalência).**
Seja A conjunto e $\mathscr{A}$ partição dele. Escreva claramente como definir uma relação de equivalência $\sim_{\mathscr{A}}$ no A tal que $A/{\sim_{\mathscr{A}}} = \mathscr{A}$. (x10.58 H 1 2)

▸ **EXERCÍCIO x10.59.**
Explique onde precisou cada uma das condições (P1)–(P3) da Definição D10.88 na tua resolução do Exercício x10.58. (x10.59 H 0)

D10.96. Definição. Chamamos a $\sim_{\mathscr{A}}$ a *relação de equivalência induzida pela* $\mathscr{A}$. Similarmente chamamos o conjunto quociente $A/{\sim}$ a *partição induzida pela* $\sim$.

▸ **EXERCÍCIO x10.60.**
Seja A conjunto finito com $|A| = 3$. Quantas partições de A existem? Por que isso resolve o Exercício x10.40? (x10.60 H 0)

10.97. Resumo. O coração dessa secção fica nos exercícios x10.49 e x10.58. Vamos resumir o que tá acontecendo. Para qualquer conjunto A definimos os conjuntos $\mathrm{EqRel}(A)$ de todas as suas relações de equivalência e $\mathrm{Part}(A)$ de todas as suas partições:

$$\mathrm{EqRel}(A) \stackrel{\text{def}}{=} \{\, \sim \mid \sim \text{ é uma relação de equivalência no } A \,\}$$
$$\mathrm{Part}(A) \stackrel{\text{def}}{=} \{\, \mathscr{A} \mid \mathscr{A} \text{ é uma partição do } A \,\}.$$

Dado conjunto A encontramos como definir *funções*

$$\mathrm{EqRel}(A) \underset{\textit{eqrelize}}{\overset{\textit{quotient}}{\rightleftarrows}} \mathrm{Part}(A)$$

que "traduzem" qualquer relação de equivalência para sua partição induzida e qualquer partição para sua relação de equivalência induzida. São definidas pelas:

$$\textit{quotient}(\sim) \stackrel{\text{def}}{=} A/\!\sim \qquad\qquad x\ (\textit{eqrelize}(\mathscr{A}))\ y \iff (\exists C \in \mathscr{A})[\, x, y \in C \,].$$

Essas traduções são fieis, no sentido de:

$$\textit{quotient} \circ \textit{eqrelize} = \mathrm{id}_{\mathrm{Part}(A)} \qquad\qquad \textit{eqrelize} \circ \textit{quotient} = \mathrm{id}_{\mathrm{EqRel}(A)}.$$

De fato, ambas são bijecções, e cada uma é a inversa da outra. Com as primeiras notações que usamos e também com palavras, temos:

$\sim_{\mathscr{A}_\sim} = \sim$ «a relação induzida pela partição induzida pela $\sim$ é a própria $\sim$»;
$\mathscr{A}_{\sim_{\mathscr{A}}} = \mathscr{A}$ «a partição induzida pela relação induzida pela $\mathscr{A}$ é a própria $\mathscr{A}$».

Não se preocupe se o conceito do *conjunto quociente* ainda parece meio distante ou abstrato demais. Ataque os problemas e os exercícios, e confie que estudando teoria dos grupos (Capítulo 11) isso vai mudar!

10.98. Dois lados da mesma moeda. Vimos aqui que "partição" e "classe de equivalência" são *dois lados da mesma moeda*. Considere um conjunto A.

(1) Quando precisamos *definir uma relação de equivalência* no A, podemos *definir uma partição* $\mathscr{A}$ de A e usar a $\sim_{\mathscr{A}}$.
(2) Conversamente, quando precisamos *definir uma partição* no A, podemos *definir uma relação de equivalência* $\sim$ no A e usar a $A/\!\sim$.
(3) Além disso, quando temos uma relação $\sim$ no A e precisamos *demonstrar que ela é uma relação de equivalência*, podemos definir uma família $\mathscr{A}$ de subconjuntos de A, *demonstrar que ela é uma partição*, e mostrar que:
$$x \sim y \iff (\exists C \in \mathscr{A})[\, x, y \in C \,].$$
(4) Finalmente, quando temos uma família $\mathscr{A}$ de subconjuntos de A e precisamos *demonstrar que ela é uma partição*, podemos definir a relação $\sim_{\mathscr{A}}$ pela
$$x \sim_{\mathscr{A}} y \iff (\exists C \in \mathscr{A})[\, x, y \in C \,]$$
e *demonstrar que ela é uma relação de equivalência.*

Não esqueça essas dicas!

D10.99. Definição. Seja $f : X \to Y$ e defina a relação binária $\approx_f$ no X pela

$$x_1 \approx_f x_2 \stackrel{\text{def}}{\iff} f(x_1) = f(x_2).$$

Chamamos a $\approx_f$ o *kernel* da f, e seu conjunto quociente a *coimagem* da f. Usamos também os símbolos $\ker f$ e $\operatorname{coim} f$ respectivamente.

▸ **EXERCÍCIO x10.61.**
Com os dados da Definição D10.99 mostre que $\approx_f$ é uma relação de equivalência e descreva os elementos da coimagem. O que podemos dizer se f é injetora? Se ela é sobrejetora? (x10.61 H 0)

▸ **EXERCÍCIO x10.62.**
Seja $f : A \to B$ e seja $\sim_B$ uma relação de equivalência no B. Defina a $\approx_{f,\sim_B}$ no A pela

$$x_1 \approx_{f,\sim_B} x_2 \stackrel{\text{def}}{\iff} f(x_1) \sim_B f(x_2).$$

A $\approx_{f,\sim_B}$ é uma relação de equivalência? (x10.62 H 0)

▸ **EXERCÍCIO x10.63.**
Mostre que todas as relações dos exemplos 10.84 e 10.85 são casos especiais do Exercício x10.61 (e logo são relações de equivalência "gratuitamente"). (x10.63 H 1)

§237. Relações recursivas

Aqui são exemplos familiares para definir recursivamente relações.

• **EXEMPLO 10.100.**
No $\mathbb{N}$ definimos:

$$\begin{aligned} \operatorname{Even}(0). & \qquad \neg\operatorname{Odd}(0). \\ \operatorname{Even}(n+1) &\stackrel{\text{def}}{\iff} \neg\operatorname{Even}(n) \qquad \operatorname{Odd}(n+1) \stackrel{\text{def}}{\iff} \neg\operatorname{Odd}(n) \end{aligned}$$

Ou, alternativamente, usando duas bases:

$$\begin{aligned} \operatorname{Even}(0). & \qquad \neg\operatorname{Odd}(0). \\ \neg\operatorname{Even}(1). & \qquad \operatorname{Odd}(1). \\ \operatorname{Even}(n+2) &\stackrel{\text{def}}{\iff} \operatorname{Even}(n) \qquad \operatorname{Odd}(n+2) \stackrel{\text{def}}{\iff} \operatorname{Odd}(n) \end{aligned}$$

• **EXEMPLO 10.101 (Recursão mutual).**

$$\begin{aligned} \operatorname{Even}(0). & \qquad \neg\operatorname{Odd}(0). \\ \operatorname{Even}(n+1) &\stackrel{\text{def}}{\iff} \operatorname{Odd}(n) \qquad \operatorname{Odd}(n+1) \stackrel{\text{def}}{\iff} \operatorname{Even}(n) \end{aligned}$$

Num paradigma de programação declarativa, na *programação lógica*, programamos definindo relações nesse jeito.

§238. Programação lógica

TODO Escrever e combinar com a seção anterior

§239. Relações de ordem superior

Talvez você já se perguntou o que acontece se numa frase como a

«João ama Maria»

em vez de substrituir os objetos "João" e "Maria" com buracos, substituir o próprio verbo "amar":

«João __ Maria».

Chegamos assim no conceito de relações de ordem superior. Não vale a pena investigar (ainda) esse conceito pois necessita mais umas ferramentas (e pouco mais maturidade). Voltamos depois de estudar programação lógica (Secção §238) e lógicas de ordem superior (Secção §367).

§240. Pouco de cats—categorias e relações

TODO Escrever

Problemas

▸ **PROBLEMA Π10.15.**
Defina no $\mathbb{Z} \times \mathbb{Z}_{\neq 0}$ a relação

$$\langle a, b\rangle \approx \langle c, d\rangle \overset{\text{def}}{\iff} ad = bc$$

Mostre que $\approx$ é uma relação de equivalência e descreva suas classes de equivalência: $\mathbb{Z} \times \mathbb{Z}_{\neq 0}/\approx$ "$=$"? (Π10.15 H 0)

▸ **PROBLEMA Π10.16.**
Defina no $\mathbb{Q}$ a relação

$$r \sim s \overset{\text{def}}{\iff} r - s \in \mathbb{Z}.$$

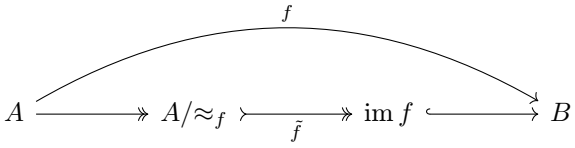
Demonstre que $\sim$ é uma relação de equivalência e descreva as classes do $\mathbb{Q}/\sim$. (Π10.16 H 0)

▸ **PROBLEMA Π10.17.**
Defina no $\mathbb{R}$ a relação

$$x \sim y \overset{\text{def}}{\iff} x - y \in \mathbb{Q}.$$

Demonstre que $\sim$ é uma relação de equivalência e descreva as classes do $\mathbb{R}/\!\sim$. (Π10.17H0)

▸ **PROBLEMA Π10.18 (Agora é fácil).**
Resolvemos o Problema Π9.5. Seja $f : A \to B$ uma função qualquer, e considere a $(\approx_f)$ da Definição D10.99. Então f pode ser "decomposta" assim:



onde a primeira função é a "projecção" $[-]$, a terceira é a inclusão $\operatorname{im} f \subseteq B$, e a bijecção no meio é a função definida pela

$$\tilde{f}([a]) = f(a),$$

que garanta a comutatividade do diagrama acima. Mesmo assim, falta demonstrar umas coisas. Ache o que, e prove. (Π10.18H12)

10.102. Com palavras da rua. Já encontramos várias vezes situações onde a troca dos $\forall\exists$ para $\exists\forall$ mudou completamente o significado (o Nota 2.37 é o mais ilustrativo). Vamos focar agora no caso onde o universo é o $\mathbb{N}$, o primeiro quantificador quantifica o n sobre todo o $\mathbb{N}$, mas o segundo quantifica todos os naturais *começando com esse* n. Tu já fez o Problema Π8.13, certo? Seria bom achar aqui mais uma maneira de entender essa situação, explicando os dois significados *com palavras de rua.* A situação aqui é parecida:

$$(\exists n \in \mathbb{N})(\forall x \geq n)[\ \text{algo}\ ]$$
$$(\forall n \in \mathbb{N})(\exists x \geq n)[\ \text{algo}\ ].$$

Supondo que esse "algo" tá dizendo que «x é legal», as afirmações acima com palavras de rua ficam assim:

$$(\exists n \in \mathbb{N})(\forall x \geq n)[\ x \text{ é legal}\ ] \quad \text{«A partir dum ponto, todos são legais.»}$$
$$(\forall n \in \mathbb{N})(\exists x \geq n)[\ x \text{ é legal}\ ] \quad \text{«Sempre vai ter legais.»}$$

Assim, ambas nos permitem concluir que tem uma infinidade de legais. Mas quantos *ilegais* tem? A primeira nos permite concluir que tem apenas uma quantidade finita de ilegais, pois, escolhendo tal $n_0 \in \mathbb{N}$ cuja existência é afirmada sabemos que todas as possíveis excessões (os "possivelmente ilegais") estão entre eles: $0, 1, \ldots, n_0 - 1$. Note que isso não quis dizer que todos eles são ilegais. Por outro lado, a segunda, não nos permite concluir isso. O fato que "sempre vai ter legais", não exclue a possibilidade de "sempre vai ter ilegais" também! Por exemplo, sempre vai ter números pares, mas sempre vai ter números ímpares também, né? Os problemas seguintes brincam com essas idéias.

▸ **PROBLEMA Π10.19.**
Defina no $(\mathbb{N} \to \mathbb{N})$ as relações seguintes:

$$f \overset{\exists\forall}{=} g \iff^{\text{def}} (\exists n \in \mathbb{N})(\forall x \geq n)[\, f(x) = g(x)\,]$$
$$f \overset{\forall\exists}{=} g \iff^{\text{def}} (\forall n \in \mathbb{N})(\exists x \geq n)[\, f(x) = g(x)\,]$$

Para cada uma das relações acima, decida se ela é relação de equivalência (demonstre ou refute). Se é, descreva seu conjunto quociente. (Π10.19 H 0)

▸ **PROBLEMA Π10.20 (Por que preordem?).**
Justifique o nome "preordem": mostre como começando com uma preordem R num conjunto A, podemos construir uma relação R' consultando a R. Pode demonstrar essa afirmação em vários jeitos, mas o objectivo é achar a ordem R' mais natural e a mais *justa*, seguindo a preordem R. (Π10.20 H 1)

▸ **PROBLEMA Π10.21 (Números Bell).**
Seja A conjunto finito. Quantas partições de A existem? (Π10.21 H 1 2 3 4 5 6 7 8 9 10)

▸ **PROBLEMA Π10.22.**
No $(\mathbb{N} \to \mathbb{R})$ defina a relação

$$a \sim b \iff^{\text{def}} \lim_n a_n = \lim_n b_n \text{ ou nenhum dos dois limites é definido.}$$

descreva o $(\mathbb{N} \to \mathbb{R})/\!\sim$. (Π10.22 H 0)

▸ **PROBLEMA Π10.23.**
No conjunto $\mathbb{R}$ defina as relações:

$$x \smile y \iff^{\text{def}} x \leq y \;\&\; \neg(\exists n \in \mathbb{Z})[\, x \leq n \leq y\,]$$
$$x \frown y \iff^{\text{def}} x \leq y \;\&\; \neg(\exists n \in \mathbb{Z})[\, x < n < y\,]$$

Sejam $\breve{\smile}$ o fecho reflexivo-simétrico da $\smile$, e $\breve{\frown}$ o fecho simétrico da $\frown$.

(i) Demonstre que $\breve{\smile}$ é uma relação de equivalência; (ii) Demonstre ou refute a afirmação: $\breve{\frown}$ *é uma relação de equivalência.* (Π10.23 H 1 2)

▸ **PROBLEMA Π10.24 (Fecho cíclico, fechos euclideanos).**
Seja R uma relação num conjunto A. Defina seus fechos: cíclico (R°), left-euclideano ($R^{\triangleright}$), right-euclideano ($R^{\triangleleft}$). (Π10.24 H 0)

▸ **PROBLEMA Π10.25.**
Seja R relação binária num conjunto A. Dê uma definição recursiva do fecho transitivo R_{t}. (Π10.25 H 0)

Leitura complementar

O [Vel06: Cap. 4] defina e trata relações diretamente como conjuntos, algo que não fazemos nesse texto. De novo: muitos livros seguem essa abordagem, então o leitor é conselhado tomar o cuidado necessário enquanto estudando esses assuntos. Nos vamos *implementar* e tratar relações como conjuntos apenas no Capítulo 16.

Sobre programação lógica: [Llo87], [SS94], [MN12].

CAPÍTULO 11

TEORIA DOS GRUPOS

Neste capítulo vamos ver os "baby steps" da teoria dos grupos. Os grupos têm uma quantidade de leis perfeita que fornecem uma estrutura ideal para começar nosso estudo de *algebra abstrata*. Depois estudamos mais teorias de outras estruturas algébricas, e até descubrimos como podemos abstrair tais teorias algébricas e elaborar um estudo universal delas.

Notas históricas

A teoria dos grupos é principalmente atribuída no trabalho do gigante Galois. Ele morreu muito jovem (20 anos) baleado num duel. Sua biografia sendo bastante romântica e aventurosa, naturalmente atrai muita atenção, muitas lendas, umas exageradas, outras não. Mas seu trabalho matemático não precisa nenhum toque de exagero. Ele introduziu o conceito de grupo e começou estudar sua teoria. Ele conseguiu perceber, construir, e abstrair numa maneira tão profunda e original que o resto da humanidade demorou para entender e apreciar. O que chamamos hoje de *teoria dos grupos* e de *teoria de Galois* nasceram na cabeça desse menino francês, e os *corpos finitos* também! A teoria de Galois conecta as duas teorias, de grupos e de corpos.

Abel, um matemático norueguês que morou na mesma época (e também morreu jovem: 26 anos) estudou uns assuntos parecidos, e hoje em dia chamamos uma classe de grupos de *abelianos* como homenagem a ele. Uma das coisas que Abel conseguiu demonstrar foi que não existe uma única fórmula para "matar" todas as equações de quinto grau. Esse teorema é conhecido como Abel–Ruffini: Ruffini atacou o problema com uma demonstração complicada que, mesmo que Cauchy a aceitou como convincente, ela realmente tava incompleta; foi Abel que matou o problema no 1826 numa maneira completa e concisa. Mas o teorema de Abel deixa a possibilidade de existir, por exemplo, uma família de fórmulas, ou até uma fórmula diferente para resolver cada polinómio de quinto grau separadamente.

É a teoria de Galois que ilumina mesmo a situação: graças à ela sabemos que tem polinómios que não são resolutíveis por nenhuma fórmula. E bem mais que isso.

Três problemas abertos na epoca desde os gregos antigos eram as construções de régua e compaço seguintes: (1) trissecção do ângulo; (2) quadratura do cíclo; (3) duplicação do cubo. No (1) são dadas duas linhas que interesetam num ponto único, formando assim um ângulo. O problema pede construir duas linhas que dividem esse ângulo em 3 ângulos iguais. No (2) é dado um cíclo e seu ráio e o objectivo é construir um quadrado com a mesma área. No (3) é dado um cubo e queremos construir um cubo com volume duplo.[73]

Wantzel no 1837 demonstrou a *impossibilidade* desses três problemas. Para os (1) e (2), sua demonstração dependeu do fato que π é *transcendental*. Na época a transcendentalidade do π era apenas uma conjectura, proposta por Lambert no 1768 (no mesmo artigo onde *demonstrou* a sua irracionalidade). A conjectura vira teorema bem depois, no ano 1882, por von Lindemann. Mesmo que esse trabalho de Wantzel é depois da

[73] Na verdade, é dada a *aresta* dum cubo com volume V, é o problema é construir a aresta dum cubo com volume $2V$. Ou seja, chamando o tamanho da aresta dada 1, construir segmento com tamanho $\sqrt[3]{2}$.

morte de Galois, ele não aproveitou a teoria de Galois pois ela demorou bastante para ser publicada (1846), e ainda mais para ser entendida e aproveitada!

Novamente, é a teoria de Galois que ilumina a situação: ela oferece as ferramentas para demonstrar com elegância e clareza todos esses teoremas difíceis!

§241. Permutações

11.1. Vamos começar considerando o conjunto S_n de todas as permutações dum conjunto com n elementos, i.e., todas as endofunções bijetivas. Escolhemos o $\{1, 2, \ldots, n\}$ como nosso conjunto mas esta escolha é inessencial. Logo temos

$$S_n \stackrel{\text{def}}{=} (\{1, \ldots, n\} \rightarrowtail\!\!\!\!\!\twoheadrightarrow \{1, \ldots, n\})$$

e, em particular,

$$S_3 = (\{1, 2, 3\} \rightarrowtail\!\!\!\!\!\twoheadrightarrow \{1, 2, 3\}).$$

Quantos elementos tem o S_3? Lembramos[74] que são

$$|S_3| = P_{\mathsf{tot}}(3) = 3! = 3 \cdot 2 \cdot 1 = 6.$$

Nosso primeiro objectivo é achar todos esses 6 membros de S_3.

Primeiramente, a identidade $\mathrm{id}_{\{1,2,3\}} \in S_3$ pois é bijetiva. Para continuar, introduzimos aqui uma notação bem práctica para trabalhar com permutações:

D11.2. Notação. Denotamos a bijecção $f \in S_n$ assim:

$$f \equiv \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$$

Por exemplo, a identidade de S_3, e a permutação φ que troca apenas o primeiro com o segundo elemento são denotadas assim:

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad\qquad \varphi := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Considere agora uma permutação do S_8 e uma do S_{12}:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 4 & 6 & 5 & 7 & 8 \end{pmatrix}; \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 1 & 4 & 5 & 10 & 6 & 11 & 9 & 12 & 8 & 7 \end{pmatrix}.$$

Podemos quebrá-las em *ciclos* escrevendo

$$(1\ 2\ 3)(5\ 6) \qquad\qquad (1\ 2\ 3)(6\ 10\ 12\ 7)(8\ 11)$$

respectivamente. Entendemos o ciclo $(1\ 2\ 3)$ como $1 \mapsto 2 \mapsto 3 \mapsto 1$:

$$(\ 1 \overset{\curvearrowright}{\mapsto} 2 \mapsto 3\ )$$

[74] Se não lembramos, veja a Proposição 5.7 e a §120 em geral. Depois disso, lembramos!

Observe que não há uma única maneira de denotar um cíclo com essa notação; por exemplo:

$$(1\ 3\ 2) = (3\ 2\ 1) = (2\ 1\ 3) = \quad 1 \to 3 \to 2 \to 1$$

mas mesmo assim preferimos botar o menor número na primeira posição na escrita; optamos para o $(1\ 3\ 2)$ neste caso.

▸ **EXERCÍCIO x11.1.**
Verifique que as duas permutações que escrevemos usando ciclos realmente correspondem nas permutações anteriores. (x11.1H0)

! **11.3. Cuidado.** Para usar a notação com ciclos para denotar os membros de algum S_n, precisamos esclarecer o n—algo que não é necessário com a notação completa, onde esta informação é dedutível pela sua forma. Por exemplo as duas permutações

$$\underbrace{\begin{pmatrix}1&2&3&4&5\\2&1&3&5&4\end{pmatrix}}_{(1\ 2)(4\ 5)} \quad \text{e} \quad \underbrace{\begin{pmatrix}1&2&3&4&5&6&7\\2&1&3&5&4&6&7\end{pmatrix}}_{(1\ 2)(4\ 5)}$$

compartilham a mesma forma usando a notação com ciclos! Olhando para as formas acima, sabemos que a primeira é um membro do S_5, e a segunda do S_7.

Mais um defeito dessa notação é que não temos como denotar a identidade numa forma consistente: podemos concordar denotá-la pelo (1) ou $(\ )$, mas na práctica optamos para o id mesmo.

11.4. Os membros de S_3. Já achamos 2 dos 6 elementos de S_3:

$$\mathrm{id} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \qquad \varphi := \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (1\ 2)$$

Sabendo que a composição de bijecções é bijecção (Exercício x9.41), tentamos a

$$\varphi^2 = \varphi\circ\varphi = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = \mathrm{id}$$

e voltamos para a própria id! Uma outra permutação no S_3 é a

$$\psi := \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (1\ 2\ 3).$$

Vamos agora ver quais diferentes permutações ganhamos combinando essas:

$$\psi^2 = \psi\circ\psi = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (1\ 3\ 2)$$
$$\varphi\circ\psi = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (2\ 3)$$
$$\psi\circ\varphi = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (1\ 3)$$

E achamos 6 membros distintos do S_3.[75] Mas $|S_3| = 6$, e logo achamos *todos* os membros de $S_3 = \{\mathrm{id}, \varphi, \psi, \psi^2, \varphi\psi, \psi\varphi\}$:

$$\begin{array}{lll} \mathrm{id} = (\,) & \psi = (1\ 2\ 3) & \varphi \circ \psi = (2\ 3) \\ \varphi = (1\ 2) & \psi^2 = (1\ 3\ 2) & \psi \circ \varphi = (1\ 3). \end{array}$$

11.5. Observação. Preciso mesmo calcular os últimos números das permutações? Vamos voltar no momento que estamos calculando o $\varphi\circ\psi$; acabamos de calcular as imagens de 1 e 2:

$$\begin{array}{ccc} 1 & 2 & 3 \\ {\scriptstyle\psi}\downarrow & \downarrow & \\ 2 & 3 & \\ {\scriptstyle\varphi}\downarrow & \downarrow & \\ 1 & 3 & ? \end{array}$$

Estamos então aqui:

$$\varphi \circ \psi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & ? \end{pmatrix}$$

Agora podemos continuar do mesmo jeito, para calcular a imagem de 3:

$$\begin{array}{ccc} 1 & 2 & 3 \\ {\scriptstyle\psi}\downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \\ {\scriptstyle\varphi}\downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{array}$$

e assim chegar no

$$\varphi \circ \psi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Mas, $\varphi\circ\psi$ é uma bijecção (pois φ, ψ são, e Exercício x9.41), e logo podemos concluir desde o penúltimo passo que $(\varphi \circ \psi)\ 3 = 2$. Mesmo assim, sendo humanos, faz sentido achar esse último valor *com as duas maneiras*. Assim, caso que elas chegam em resultados diferentes, teriamos um aviso sobre (pelo menos) um erro nos nossos cálculos anteriores!

▸ **EXERCÍCIO x11.2.**
Qual das duas propriedades de bijecção estamos usando na Observação 11.5 para concluir que $(\varphi \circ \psi)\ 3 = 2$ sem calculá-lo explicitamente? (x11.2H0)

▸ **EXERCÍCIO x11.3.**
Calcule a $\psi \circ \psi^2$ e justifique que ela é igual à $\psi^2 \circ \psi$. (x11.3H0)

▸ **EXERCÍCIO x11.4.**
Calcule as $\varphi \circ \psi^2$ e $\psi^2 \circ \varphi$. (x11.4H0)

[75] Por que são distintos? Veja Exercício x11.6 por exemplo.

11.6. Abstraindo (maneira ruim). Temos um conjunto (ou um tipo) cujos membros podemos "combinar". Destacamos as seguintes propriedades que são satisfeitas:

(G0) O conjunto é fechado sobre a operação.[76]
(G1) A operação é associatíva.
(G2) A operação tem identidade no conjunto.
(G3) Cada elemento do conjunto possui inverso no conjunto.

Conjuntos onde é definida uma operação que satisfaz essas propriedades aparecem com freqüência, e vamos ver que são suficientes para construir uma teoria rica baseada neles.

11.7. Abstraindo (maneira boa). Temos um mundo G (pense num tipo ou num conjunto) em qual podemos fazer três operações-perguntas:

(op) dando um habitante x e um habitante y podemos solicitar a combinação deles xy;
(id) podemos solicitar um destacado membro do mundo a qual vamos referir como *a identidade do mundo*;
(inv) dando um habitante x podemos solicitar um correspondente membro do mundoujo nome é *o inverso do* x.

Resumindo, temos:

$$op : G \times G \to G \qquad id : G \qquad inv : G \to G.$$

Essas operações satisfazem:

(Ass) $(xy)z = x(yz)$.
(Id) $ex = x = xe$
(Inv) $x'x = e = xx'$

Esse padrão (conjunto com tais operações respeitando tais leis) aparecem com freqüência, e vamos ver que são suficientes para construir uma teoria rica baseada neles.

§242. O que é um grupo?

Seguindo a abstracção do 11.7, chegamos numa primeira definição:

D11.8. Definição (Grupo). Um conjunto G com uma operação binária $*$ é um *grupo* sse: o G é $*$-*fechado*; a $*$ é *associativa*; a $*$ tem *identidade* no G; cada elemento de G possui $*$-*inverso*.

Anticipando o dicionário relevante (Definição D8.165) vamos esclarecer pouco essa definição:

D11.9. "Definição" (Grupo). Um conjunto G com uma operação binária $*$ no G é um *grupo* sse as leis seguintes

(G0) $$a, b \in G \implies a * b \in G$$
(G1) $$a * (b * c) = (a * b) * c$$
(G2) existe $e \in G$ tal que para todo $a \in G$, $e * a = a = a * e$
(G3) para todo $a \in G$, existe $y \in G$, tal que $y * a = e = a * y$

[76] Aplicando a operação em quaisquer membros do nosso conjunto, o resultado pertence ao conjunto.

são satisfeitas. ↯

11.10. Leis vs. axiomas. As (G0)–(G3) são conhecidas como *as leis de grupos*, ou *os axiomas de grupos*. Tentarei evitar—mas não sempre!—usar a palavra *axioma* com esse sentido, optando para a palavra *lei* mesmo, pois chamamos de "axioma" algo que aceitamos como verdade em nosso univérso (mais sobre isso no Capítulo 16), mas nesse caso não estamos afirmando a veracidade das (G0)–(G3). Faz apenas parte do que significa "ser grupo". Se um conjunto estruturado satisfaz todas as leis, bem, ele ganha o direito de ser chamado um "grupo". Se não, beleza, ele não é um grupo.

! **11.11. Aviso (abuso notacional).** Lembra-se o abuso notacional que introduzímos no 8.161: usamos $a, b \in \mathcal{G}$, $G = (G\,;\bullet)$, etc.

11.12. Grupos multiplicativos e aditivos. Dependendo da situação, podemos adoptar um "jeito multiplicativo" para a notação dum grupo, ou um "jeito additivo"—ou ficar realmente com um jeito neutro. Num *grupo multiplicativo* usamos $\cdot$ para denotar a operação do grupo, aproveitamos a convenção de omitir o símbolo totalmente, usando apenas justaposição: $a(bc)$ significa $a \cdot (b \cdot c)$ por exemplo. A identidade parecerá com e ou 1, e a^{-1} será o inverso de a. Num *grupo aditivo* usamos $(+)$ para denotar a operação do grupo, a identidade parecerá com e ou 0; e $-a$ será o inverso de a. Naturalmente usamos $*$, $\bullet$, etc. para denotar operação de grupo, e para sua identidade, e a^{-1} para denotar o inverso de a. É importante entender que os termos "grupo multiplicativo" e "grupo aditivo" usados assim não carregam nenhum significado matemático mesmo: apenas mostram uma preferência notacional. Mas quando um conjunto já tem adição e/ou multiplicação definida (como por exemplo os reais), então usamos frases como "o grupo aditivo dos reais" para referir ao $(\mathbb{R}\,;+)$, e até "o grupo multiplicativo dos reais" para referir ao $(\mathbb{R}_{\neq 0}\,;\cdot)$, considerando óbvio o "sem o zero", pois *com* o zero nem é grupo (Exercício x11.10).

Para entender melhor as quatro leis de grupo, as escrevemos novamente, essa vez sem deixar nenhum quantificador como implícito, e começando com um *conjunto estruturado* com uma operação binária:

D11.13. "Definição" (Grupo (2)). Um conjunto estruturado $\mathcal{G} = (G\,;*)$ é um *grupo* sse

$$\begin{aligned}
&\text{(G0)} && (\forall a, b \in G)[\,a * b \in G\,]\\
&\text{(G1)} && (\forall a, b, c \in G)[\,a * (b * c) = (a * b) * c\,]\\
&\text{(G2)} && (\exists e \in G)(\forall a \in G)[\,e * a = a = a * e\,]\\
&\text{(G3)} && (\forall a \in G)(\exists y \in G)[\,y * a = e = a * y\,].
\end{aligned}$$

Chamamos o elemento garantido pela (G2) a *identidade* do grupo, chamamos o y da (G3) o *inverso* de a. ↯

▸ **EXERCÍCIO x11.5.**
Tá tudo certo com as definições D11.9 e D11.13? (x11.5H12)

11.14. Galois, Abel, Cayley. Como vimos, na mesma época o Galois e o Abel chegaram na idéia abstrata de grupo. Galois mesmo escolheu a palavra «group» para esse conceito. A definição "moderna" de grupo como conjunto munido com operação que satisfaz as leis (G0)–(G3) é de Cayley. Como Abel focou em grupos cuja operação é comutativa, chamamos esses grupos de abelianos:

D11.15. Definição (Grupo abeliano). Um grupo é *comutativo* (também: *abeliano*) sse sua operação é comutativa:

(GA) $$(\forall a, b \in G)[\, a * b = b * a \,].$$

11.16. Esquematicamente:

$$\left.\begin{array}{c}\text{(fechado)}\\ \text{(associatividade)}\\ \text{(identidade)}\\ \text{(inversos)}\\ \text{(comutatividade)}\end{array}\right\}\text{grupo}\Bigg\}\text{grupo abeliano}$$

• **EXEMPLO 11.17.**
Verifique que S_3 é um grupo. Ele é abeliano?
RESOLUÇÃO. Precisamos verificar as leis de grupo.
(G0). Para demonstrar que S_3 é $(\circ)$-fechado, precisamos verificar que para todo $a, b \in S_3$, $a \circ b \in S_3$. Pela definição do S_3, isso segue pelo Exercício x9.41 (3).
(G1). Já demonstramos a associatividade da $\circ$ na Teorema Θ9.186.
(G2). Facilmente verificamos que a $\mathrm{id}_{\{1,2,3\}}$ é a identidade do $(S_3\,;\circ)$, pela sua definição.
(G3). Cada bijecção tem uma função-inversa, que satisfaz as equações dessa lei pela definição de função-inversa. (Veja Definição D9.162 e Exercício x9.60.)
(GA). Basta mostrar pelo menos um contraexemplo, ou seja, duas permutações a, b do S_3 tais que $a \circ b \neq b \circ a$. Agora preciso saber o que significa igualdade entre *funções* (Definição D9.28). Escolho os φ, ψ. Já calculamos as $\varphi \circ \psi$ e $\psi \circ \varphi$ e são diferentes.
Logo, S_3 é um grupo não abeliano.

▸ **EXERCÍCIO x11.6.**
E por que $\varphi \circ \psi \neq \psi \circ \varphi$? (x11.6H0)

11.18. E por que $1 \neq 3$?. Na resolução do Exercício x11.6 nosso argumento reduziu o que queríamos demonstrar à afirmação $1 \neq 3$. *E por que* $1 \neq 3$*?* Bem, precisamos saber o que significa igualdade no $\mathbb{N}$! Mas podemos já considerar o $1 \neq 3$ como um fato conhecido sobre os números naturais. Depois, no Capítulo 16, vamos *fundamentar* o $\mathbb{N}$ na teoria de conjuntos, e logo vamos ter como realmente demonstrar essa afirmação para nosso $\mathbb{N}$, por exemplo.

▸ **EXERCÍCIO x11.7.**
Ache o inverso de cada elemento de S_3.[77] (x11.7H0)

[77] Se tu já fez isso para resolver o Exemplo 11.17, não foi necessário. Por quê? Veja a resolução do 11.17 mesmo.

Agora vamos dar mais uma definição de grupo, essa vez usando um conjunto estruturado de tipo diferente: além de ter uma operação binária, tem uma constante também:

D11.19. Definição (Grupo (2,0)). Um conjunto estruturado $\mathcal{G} = (G\,;*,e)$ é um grupo sse

$$\begin{aligned}
&\text{(G0)} && (\forall a,b\in G)[\,a*b\in G\,]\\
&\text{(G1)} && (\forall a,b,c\in G)[\,a*(b*c)=(a*b)*c\,]\\
&\text{(G2)} && (\forall a\in G)[\,e*a=a=a*e\,]\\
&\text{(G3)} && (\forall a\in G)(\exists y\in G)[\,y*a=e=a*y\,].
\end{aligned}$$

▸ **EXERCÍCIO x11.8.**
Tá tudo certo com a Definição D11.19? (x11.8H0)

11.20. Observação. O e que aparece na (G3) não é "a identidade do $\mathcal{G}$". É sim a constante que aparece na estrutura do $(G\,;*,e)$, que—graças à (G2)—é *uma* identidade do $\mathcal{G}$. No Lema Λ11.35 vamos demonstrar que cada grupo tem identidade única, e a partir dessa demonstração, vamos ganhar o direito de usar o artigo definido "a".

? **Q11.21. Questão.** Já encontramos definições de grupo como conjunto estruturado com assinaturas de aridades (2) e $(2,0)$. Como definarias com assinatura de aridades $(2,1,0)$?

!! SPOILER ALERT !!

D11.22. Definição (Grupo (2,1,0)). Um conjunto estruturado $\mathcal{G} = (G\,;*,{}^{-1},e)$ onde $*$ é uma operação binária, ${}^{-1}$ unária, e e uma constante é um *grupo* sse:

(G0) G é $*$-fechado;
(G1) $*$ é associativa;
(G2) e é uma $*$-identidade;
(G3) para todo $a\in G$, a^{-1} é um $*$-inverso do a.

Formulamente:

$$\begin{aligned}
&\text{(G0)} && (\forall a,b\in G)[\,a*b\in G\,]\\
&\text{(G1)} && (\forall a,b,c\in G)[\,a*(b*c)=(a*b)*c\,]\\
&\text{(G2)} && (\forall a\in G)[\,e*a=a=a*e\,]\\
&\text{(G3)} && (\forall a\in G)\big[\,a^{-1}*a=e=a*a^{-1}\,\big].
\end{aligned}$$

D11.23. Definição (Ordem de grupo). O número de elementos de um grupo G é sua *ordem*. Denotamos a ordem de G com: $o(G)$, $\operatorname{ord}(G)$, ou até $|G|$ quando não existe ambigüidade. Se o carrier set do grupo é infinito, escrevemos $o(G) = \infty$.

▸ **EXERCÍCIO x11.9.**
Já conhecemos um grupo finito bem, o S_3, com $o(S_3) = 6$. No Exercício x11.15 demonstrarás que para todo $n \in \mathbb{N}$, o S_n é um grupo. Seja $m \in \mathbb{N}$. Tem como achar um grupo com ordem m? Observe que como sabemos que $o(S_n) = n!$, podemos já achar um grupo com ordem m para qualquer m que fosse um fatorial. Por exemplo, se $m = 120$ já temos o grupo S_5, pois $o(S_5) = 5! = 120$. Mas para um m arbitrário, existe grupo de ordem m? (x11.9H1)

11.24. Observação (Uma lei que não é lei). Talvez resolvendo os exercícios x11.5 e x11.8, tu já percebeste algo redundante na "Definição" D11.13: *pra que essa (G0)?* O $(G\,;*)$ é um conjunto estruturado cuja estrutura tem uma *operação binária*, ou seja uma *função*

$$* : G \times G \to G.$$

Logo, a (G0) não tem absolutamente nada pra oferecer: *necessariamente*

$$(\forall a, b \in G)[\, a * b \in G\,]$$

pois $* : G \times G \to G$. Observe que se relaxar a definição de conjunto estruturado para permitir operações *parciais* (Definição D9.213) o (G0) vira lei necessária mesmo e afirma simplesmente que $*$ é total. Mas nosso padrão de operação foi operação total mesmo, e, nesse sentido, *as leis de grupo* são as (G1)–(G3).[78] *Mesmo assim*, é comum encontrar a (G0) como axioma de grupo, e se tirá-la não ganhamos nada mesmo. Suponha que tu trabalhas com a (G0) como lei que faz parte da tua definição de grupo; e teu amigo trabalha apenas com as (G1)–(G3). Inicialmente parece que teu amigo vai ter menos trabalho pra fazer quando precisar demonstrar que um $(G\,;*)$ é um grupo. Mas não é assim: a definição começa com um *conjunto estruturado* cuja estrutura inclui a operação binária $*$. Ou seja, para demonstrar que $(G\,;*)$ é um grupo ele vai precisar demonstrar que $*$ realmente é uma operação

$$* : G \times G \to G$$

ou seja, (G0), ou seja, ele não vai ter menos trabalho; se preocupe não!

§243. Exemplos e nãœxemplos

• **EXEMPLO 11.25 (Com números).**
Todos os seguintes conjuntos estruturados são grupos:

- $(A\,;+,0)$, onde $A := \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
- $(B\,;\cdot,1)$, onde $B := \mathbb{Q}_{\neq 0}, \mathbb{R}_{\neq 0}$;
- $(C\,;\cdot,1)$, onde $C := \{1,-1\}, \{1,i,-1,-i\} \subseteq \mathbb{C}$.

• **NÃOEXEMPLO 11.26 (Com números).**
E *nenhum* dos seguintes é um grupo: $(\mathbb{N}\,;+)$; $(\mathbb{R}\,;\cdot,1)$; $(\mathbb{Z}_{\neq 0}\,;\cdot,1)$; $(\mathbb{R}\,;+,1)$.

[78] E por isso denotei a primeira com '0', não foi questão de começar a conta com o primeiro Nat.

▸ **EXERCÍCIO x11.10.**
Por quê? (x11.10H0)

• **NÃOEXEMPLO 11.27 (Strings).**
Sejam $\Sigma \neq \emptyset$ um alfabeto finíto, e S o conjunto de todos os strings finitos formados por símbolos do Σ. O $(S\,;+)$ onde $(+)$ é a *concatenação* de strings *não* é um grupo.

▸ **EXERCÍCIO x11.11.**
Para cada uma das leis (G0)–(GA), decida se é satisfeita pelo $(S\,;+)$ do Nãoexemplo 11.27. Se é, demonstre; se não é, refute! (x11.11H0)

▸ **EXERCÍCIO x11.12.**
Sejam $B = \{\, 2^m \mid m \in \mathbb{Z} \,\}$ e $B_0 = B \cup \{0\}$. Considere os conjuntos estruturados

$$(B\,;+) \qquad (B\,;\cdot) \qquad (B_0\,;+) \qquad (B_0\,;\cdot).$$

Para cada um deles decida se satisfaz cada uma das leis (G0)–(GA). (x11.12H0)

▸ **EXERCÍCIO x11.13.**
Mostre mais grupos formados de números dos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, e uma operação não-padrão da sua escolha. (x11.13H0)

• **EXEMPLO 11.28 (Matrizes).**
Considere os conjuntos seguintes:

$$A = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2\times 2} \mid a,b,c,d \in \mathbb{R} \right\} \qquad M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2\times 2} \mid ad - bc \neq 0 \right\}.$$

O A com a adição de matrízes vira um grupo $(A\,;+)$, mas com a multiplicação não: não todos os seus membros tem inverso. Por outro lado, graças à condição no filtro na definição do conjunto M, todos os seus membros são matrízes invertíveis, e $(M\,;\cdot)$ realmente é um grupo.

▸ **EXERCÍCIO x11.14 (matrizes).**
O $(M\,;+)$ é? (x11.14H1)

• **EXEMPLO 11.29 (Adição modular).**
O $\overline{n} \stackrel{\text{def}}{=} \{0,\ldots,n-1\}$ com a operação $+_n$ da adição módulo n. Qual é o inverso de um elemento a nesse caso? É o $n-a$, pois $a +_n (n-a) = 0 = (n-a) +_n a$.

D11.30. Definição. Denotamos o grupo do Exemplo 11.29 por $\mathbb{Z}_n$.

• **NÃOEXEMPLO 11.31 (Multiplicação modular).**
O $\overline{n} \stackrel{\text{def}}{=} \{0,\ldots,n-1\}$ com a operação $\cdot_n$ da multiplicação módulo n, não é um grupo, pois o 0 não tem inverso. E se jogar fora o problemático 0? Talvez vira um grupo. Mas não: o $(\{1,\ldots,5\}\,;\cdot_6)$ também não é um grupo, pois não é fechado: $2 \cdot_6 3 = 0$.

D11.32. Definição. Usamos S_n para denotar o conjunto de todas as permutações dum conjunto de tamanho $n \in \mathbb{N}$. Para definir mesmo o S_n escolhemos o conjunto canônico:

$$S_n \stackrel{\text{"def"}}{=} (\{1, \ldots, n\} \rightarrowtail\!\!\!\!\twoheadrightarrow \{1, \ldots, n\}).$$

Para qualquer $n \in \mathbb{N}$, chamamos o $(S_n \,;\, \circ)$ o *grupo simétrico* de tamanho n.

▸ **EXERCÍCIO x11.15.**
Justifique a Definição D11.32: demonstre que o grupo simétrico S_n realmente é um grupo. Ele é abeliano? (x11.15H0)

▸ **EXERCÍCIO x11.16 (Conjuntos).**
Seja A conjunto. Com quais das operações $\cup$, $\cap$, $\triangle$, e $\setminus$, o $\wp A$ é um grupo? (x11.16H0)

▸ **EXERCÍCIO x11.17 (Funções reais: adição pointwise).**
O $(\mathbb{R} \to \mathbb{R})$ com operação a pointwise $(+)$, é um grupo?[79] Ele é abeliano? (x11.17H0)

▸ **EXERCÍCIO x11.18 (Funções reais: multiplicação pointwise).**
O $(\mathbb{R} \to \mathbb{R}) \setminus \{\lambda x \,.\, 0\}$ com operação a pointwise $(\cdot)$, é um grupo? Ele é abeliano? (x11.18H0)

Lembre que já usamos $\times$ entre *conjuntos* A, B para formar seu produto cartesiano $A \times B$; e também entre *funções* $f : A \to B$, $g : C \to D$ para formar seu produto $f \times g : (A \times C) \to (B \times D)$. Vamos agora sobrecarregar ainda mais esse $\times$:

D11.33. Definição (Produtos diretos). Sejam $\mathcal{G}_1 = (G_1 \,;\, *_1)$ e $\mathcal{G}_2 = (G_2 \,;\, *_2)$ grupos. Definimos o grupo

$$\mathcal{G}_1 \times \mathcal{G}_2 = (G_1 \times G_2 \,;\, *),$$

onde $*$ é a operação definida pela

$$\langle x_1, x_2 \rangle * \langle y_1, y_2 \rangle = \langle x_1 *_1 y_1, x_2 *_2 y_2 \rangle \,.$$

▸ **EXERCÍCIO x11.19.**
Demonstre que realmente é um grupo. (x11.19H0)

D11.34. Definição (grupo oposto). Seja $\mathcal{G} = (G \,;\, *, {}^{-1}, e)$ grupo. Definimos no $|\mathcal{G}|$ a operação binária $*'$ pela:

$$x *' y = y * x.$$

Chamamos o $(G \,;\, *')$ de *grupo oposto do* $\mathcal{G}$, e o denotamos por $\mathcal{G}^{\text{op}}$.

▸ **EXERCÍCIO x11.20.**
Justifique o nome escolhido na Definição D11.34: demonstre que o $\mathcal{G}^{\text{op}}$ é um grupo. (x11.20H0)

[79] Qual operação é a pointwise $(+)$? Veja a Definição D9.203.

Chegam os exemplos por enquanto. Vamos começar ver a *teoria* de grupos, investigando propriedades que todos os grupos necessariamente têm. Ou seja, procuramos as *conseqüências das leis* (G0)–(G3).

§244. Primeiras conseqüências

Λ11.35. Lema (unicidade da identidade). *Em todo grupo G existe único elemento e que satisfaz a (G2).*

▸ Esboço. Seja G grupo. Sabemos que existe pelo menos uma identidade no G pela (G2), então precisamos mostrar que existe no máximo uma (unicidade). Vamos supor que e_1, e_2 são identidades do G, e usando as leis (G0)–(G2) mostrar que $e_1 = e_2$. □ (Λ11.35P)

Uma demonstração errada desse lemma aparece no Problema Π11.3, onde peço identificar seus erros.

? **Q11.36. Questão.** O que acabamos de ganhar?

11.37. Resposta. Ganhamos o direito de usar o artigo definido: para cada grupo $\mathcal{G}$ falar *da* identidade do $\mathcal{G}$, em vez *duma* identidade do $\mathcal{G}$. Observe que dado algum $a \in \mathcal{G}$ ainda não podemos falar sobre *o* inverso de a, mas apenas sobre *um* inverso de a, pois por enquanto a (G3) garanta que pelo menos um inverso existe. Vamos resolver isso agora.

! **11.38. Cuidado.** Os a e b que aparecem nas (1)–(2) na demonstração do Lema Λ11.35 são *variáveis ligadas* aos correspondentes «para todo $__ \in G$» e logo, "nascem" com essa frase e "morrem" no fim da mesma linha![80] Daí, não faz sentido afirmar logo após das (1)–(2) algo do tipo $e = a * e$, pois o a não foi declarado! Podemos escrever as duas afirmações sem usar o nome a: *para cada elemento do G, operando com o e_1 ao qualquer lado (direito ou esquerdo), o resultado é o próprio elemento.* E para enfatizar ainda mais a independência do a que aparece na (1) com o b que aparece na (2) escolhemos variáveis diferentes. Mas isso é *desnecessário*, em geral vamos reusar variáveis ligadas quando não gera confusão—e aqui não geraria nenhuma.

▸ **EXERCÍCIO x11.21.**
O que muda na demonstração do Lema Λ11.35 se usar a mesma variável ligada nas afirmações (1) e (2)? (x11.21H0)

Λ11.39. Lema (unicidade dos inversos). *Em todo grupo G, cada $a \in G$ tem exatamente um inverso a^{-1} que satisfaz a (G3).*

▸ Esboço. Supondo que existe um certo $a \in G$ que possui inversos $a_1, a_2 \in G$, mostramos que necessariamente $a_1 = a_2$. Ganhamos isso como corolário do Lema Λ11.41. (Como?) □ (Λ11.39P)

[80] Veja a Secção §6 também.

! **11.40. Cuidado (Dependências de demonstrações).** Até realmente demonstrar as leis de cancelamento (Λ11.41) não temos a unicidade dos inversos (Λ11.39). Dado um elemento a dum grupo G não podemos ainda falar *do* inverso do a, nem usar a notação a^{-1} (seria mal-definida), etc.[81] Crucialmente, não podemos usar nada disso em nossa demonstração do Λ11.41; caso contrário criamos uma loope de dependências. "Forward dependencies" são perigosos exatamente por causa disso, e nós as evitamos mesmo.[82]

Λ11.41. Lema (Leis de cancelamento). *Seja $\mathcal{G} = (G\,;*,e)$ grupo. Então as leis de cancelamento pela esquerda e pela direita*

$$\text{(GCL)} \qquad (\forall a,x,y\in G)[\,a*x=a*y \implies x=y\,]$$
$$\text{(GCR)} \qquad (\forall a,x,y\in G)[\,x*a=y*a \implies x=y\,]$$

são válidas em G.

▸ Esboço. Sejam $a,x,y\in G$ tais que

$$a*x=a*y. \tag{1}$$

Queremos demonstrar $x=y$. Tome a (1) então, e usando umas das leis de grupo—comece com a (G3)—chegue no desejado $x=y$, demonstrando assim a (GCL). A (GCR) é similar. □ (Λ11.41P)

▸ **EXERCÍCIO x11.22.**
Os conversos das leis de cancelamento (GCL) & (GCR) são válidos? (x11.22H12)

▸ **EXERCÍCIO x11.23.**
Refuta: para todo grupo $(G\,;*,e)$ e $a,x,y\in G$

$$a*x=y*a \implies x=y$$

(x11.23H123)

▸ **EXERCÍCIO x11.24.**
Um aluno achou o seguinte contraexemplo para refutar a lei no x11.23:

nos reais com multiplicação, temos $0\cdot 1=2\cdot 0$ mas $1\neq 2$.

Por que sua resposta é errada? (x11.24H1)

▸ **EXERCÍCIO x11.25.**
Ache uma demonstração do Lema Λ11.39 que não precisa das leis de cancelamento. (x11.25H0)

---

[81] Na verdade, se a gente usa como definição de grupo a D11.22, temos como usar a notação a^{-1} sim, mas ainda não podemos afirmar que a^{-1} é a inversa do a. *Uma*, sim.

[82] Aqui escolhi essa abordagem para enfatizar a importância de ficar alertos para identificar chances de afirmar e demonstrar lemmas separadamente, os usando em nossa demonstração e para demonstrar outros teoremas depois à vontade. Fazemos isso exatamente no mesmo jeito que um bom programador percebe padrões nos seus programas e suas funções e separa certas partes para outras funções, as chamando depois à vontade.

11.42. Observação (Qual a estrutura dos teus grupos?). Suponha que na nossa estrutura não temos a operação unária de $^{-1}$. Provando finalmente a unicidade dos inversos (Λ11.39) ganhamos então em cada grupo G uma *função* (unária) de inverso

$$inv : G \to G.$$

Sua *totalidade* já era garantida pela (G3), que nesse caso é a:

$$(\forall a \in G)(\exists y \in G)[\, y * a = e = a * y \,] \tag{G3}$$

e agora acabamos de ganhar sua *determinabilidade* com o Lema Λ11.39. Ou seja: *função!* Podemos finalmente definir uma notação para denotar o inverso de qualquer $a \in G$. Similarmente, se na nossa estrutura não temos a constante e, então demonstrando a unicidade da identidade ganhamos o direito de definir uma notação para a identidade dum grupo G. Cuidado, pois agora a (G2) tá apenas afirmando a existência *duma* identidade:

$$(\exists e \in G)(\forall a \in G)[\, e * a = a = a * e \,] \tag{G2}$$

mas graças ao Lema Λ11.35 sabemos que é única então podemos definir uma notação pra ela. Vamos fazer essas duas coisas agora:

D11.43. Definição (identidade para estruturas incompletas). Seja $(G\,;*)$ grupo. Denotamos a única identidade de G por e_G, ou simplesmente e se o grupo G já é implícito pelo contexto.

D11.44. Definição (inversos para estruturas incompletas). Seja $(G\,;*)$ ou $(G\,;*,e)$ grupo. Para qualquer $a \in G$, definimos o

$$a^{-1} \stackrel{\text{def}}{=} \text{o único inverso de } a \text{ no } G.$$

! 11.45. Cuidado (a escolha de estrutura: escrevendo justificativas). Um matemático tá trabalhando com grupos $(G\,;*)$, e ta querendo justificar que

$$a * e_G = a.$$

Qual seria a justificativa que ele vai escrever? Ele não pode dizer «pela (G2)», pois a (G2) ta afirmando apenas a existência duma identidade; ela não ta afirmando nada sobre esse e_G ali. A justificativa dele seria:

$$\text{«pela definição do } e_G\text{»}.$$

Por outro lado, um matemático que trabalha com grupos cuja estrutura já tem a constante e nela, ou seja, com grupos $(G\,;*,e)$ ou $(G\,;*,^{-1},e)$, justificaria o mesmo passo assim:

$$\text{«pela (G2R)»}.$$

Similarmente sobre a justificativa de uma igualdade como a

$$a^{-1} * a = e_G.$$

Um matemático que trabalha com $(G\,;*,^{-1},e)$ justificaria com um simples

«pela (G3L)».

Mas para os matemáticos que não tem a operação de inverso na sua estrutura, a justificativa seria

«pela definição do a^{-1}».

Nesse texto vou usar ambas as abordagens.

Tendo ganhado unicidade da identidade e dos inversos, vamos responder agora em duas perguntas.

? **Q11.46. Questão (1).** Num grupo G, dado $a \in G$, o que precisamos mostrar para demonstrar que um certo $y \in G$ é o inverso de a?

11.47. Resposta errada. Basta mostrar que $a*y = e$ (ou, alternativamente, que $y*a = e$) pois, *graças à unicidade dos inversos*, apenas um membro do grupo pode satisfazer essa equação, e logo necessariamente $y = a^{-1}$.

? **Q11.48. Questão (2).** Num grupo G, o que precisamos mostrar para demonstrar que um certo $u \in G$ é a identidade do grupo?

11.49. Resposta errada. Basta achar um $a \in G$ tal que $a*u = a$ (ou, alternativamente, tal que $u*a = a$), pois, *graças à unicidade da identidade*, apenas um membro do grupo pode satisfazer essa equação, e logo necessariamente $u = e$.

11.50. Cadê o erro?. O *raciocínio* nas duas respostas é errado numa maneira parecida:

Na (1), pode ser que y satisfaz a $a*y = e$ sem y ser o inverso do a. *E isso não violaria a unicidade do inverso* a^{-1}, pois pela definição de *inverso do* a, ambas equações $a*y = e = y*a$ precisam ser satisfeitas, e talvez $y*a \neq e$.

Na (2), pode ser que u satisfaz $a*u = a$ para algum membro $a \in G$ sem u ser a identidade do grupo. *E isso não violaria a unicidade da identidade* e, pois pela definição de *identidade do* G, o u precisa satisfazer ambas as $a*u = e = u*e$ e mesmo se satisfaria ambas isso não seria sufiziente: ele tem que as satisfazer não apenas *para algum* $a \in G$ que deu certo, mas *para todo* $a \in G$! Ou seja: o fato que achamos *algum* $a \in G$ tal que $a*u = a(= u*a)$ não quis dizer que esse u merece ser chamado *a identidade do* G ainda, pois talvez tem membros $c \in G$ tais que $c*u \neq c$ ou $u*c \neq c$.

! **11.51. Aviso.** Os raciocínios acima sendo errados não quis dizer que as afirmações também são! Na verdade, nos dois casos podemos realmente ganhar o que queremos: identidades e inversos *mais baratos*, sem pagar todo o preço das definições. Ambos resultados seguem como corolários diretos do Lema Λ11.59 que vamos demonstrar daqui a pouco.

Por enquanto, vamos continuar pesquisando o que mais podemos concluir assim que tivermos um grupo G, e voltaremos logo nessas duas questões.

? **Q11.52. Questão.** Se a, b são membros de algum grupo $(G\,;*,e)$, podemos concluir algo sobre os...

$$e^{-1} \stackrel{?}{=} \ldots? \qquad \left(a^{-1}\right)^{-1} \stackrel{?}{=} \ldots? \qquad (a*b)^{-1} \stackrel{?}{=} \ldots?$$

!! SPOILER ALERT !!

Resposta. Sim:

$$e^{-1} \stackrel{?}{=} e \qquad \left(a^{-1}\right)^{-1} \stackrel{?}{=} a \qquad (a*b)^{-1} \stackrel{?}{=} b^{-1}*a^{-1}.$$

Mas precisamos demonstrar cada uma delas.

11.53. Interpretações diferentes. Considere a primeira afirmação acima:

$$e^{-1} = e.$$

De quantas maneiras podemos ler (entender) essa equação, e o que seria uma demonstração de cada uma dessas maneiras?

MANEIRA 1: $\underbrace{e^{-1}}_{\text{isso}}\ \underbrace{=}_{\text{é}}\ \underbrace{e}_{\text{a identidade do grupo.}}$

MANEIRA 2: $\underbrace{e}_{\text{isso}}\ \underbrace{=}_{\text{é}}\ \underbrace{e^{-1}}_{\text{o inverso de } e.}$

MANEIRA 3: $\underbrace{e^{-1}}_{\text{isso}}\ \underbrace{=}_{\text{é}}\ \underbrace{e}_{\text{isso.}}$

Com a primeira, o que precisamos mostrar é que o objeto e^{-1} satisfaz a definição de ser a identidade do grupo, ou seja:

$$\text{para todo } a \in G,\ e^{-1}*a = a = a*e^{-1}.$$

Com a segunda, precisamos mostrar que a coisa vermelha é o inverso da coisa azul. Mas o que significa ser inverso de algo? Precisamos mostrar que:

$$e*e = e$$
$$e*e = e.$$

Com a terceira, a única coisa que podemos fazer é começar calcular até finalmente chegar nessa igualdade.

11.54. Conselho. Cada vez que tu queres demonstrar uma igualdade que envolve certas noções, tente "ler" o que a igualdade realmente afirma em várias maneiras diferentes. Cada uma é uma chance para te dar uma idéia de como demonstrá-la!

Λ11.55. Lema (inverso da identidade). *Em todo grupo G, $e^{-1} = e$.*

Demonstração. Basta mostrar que e é o inverso de e, ou seja, que ele satisfaz $ee = e$, algo imediato pela definição da identidade e. ∎

Das três maneiras analisadas acima, escolhi a segunda. Investigue as outras duas:

▸ **EXERCÍCIO x11.26.**
Ache uma demonstração alternativa do Lema Λ11.55, baseada na primeira maneira do 11.53. (x11.26H0)

▸ **EXERCÍCIO x11.27.**
E uma baseada na terceira. (x11.27H0)

Λ11.56. Lema (inverso de inverso). *Em todo grupo G, $\left(a^{-1}\right)^{-1} = a$ para todo $a \in G$.*

▸ Esboço. Uma maneira de ler a afirmação: *«a é o inverso de a^{-1}»*. Usando o que significa ser inverso de alguém chegamos no resultado. Alternativamente, usamos as definições dos inversos envolvidos para ganhar duas equações. Com elas, chegamos na equação desejada. □ (Λ11.56P)

▸ **EXERCÍCIO x11.28.**
Desenhe um diagrama cuja comutatividade é a lei que tu acabou de demonstrar. (x11.28H0)

11.57. Observação. É comum adivinhar erroneamente que em geral $(a * b)^{-1} = a^{-1} * b^{-1}$. O erro é feito pois, acostumados com certos grupos *bem especiais* como o $(\mathbb{R}_{\neq 0}\ ;\ \cdot)$ (onde essa lei realmente é válida), generalizamos para o caso geral de grupos, sem perceber algo estranho e esquisito que acontece nessa equação. Repensando em nosso exemplo-guia de grupos, o S_3, o que significa $a * b$? «Faça a b, depois a a.» E o que signfica $(a * b)^{-1}$ então? «Desfaça a $(a * b)$.» E se aplicar uma transformação b, e depois mais uma a, qual seria o jeito para desfazer tudo isso e voltar na configuração inicial? «Desfaça a a, e depois desfaça a b.» Ou seja, $b^{-1} * a^{-1}$. Isso é bem natural sim: para desfazer uma seqüência de ações, começamos desfazenso a última, depois a penúltima, etc., até finalmente desfazer a primeira. Sendo o inverso então, faz sentido que *a ordem é a inversa também!* E nos reais, por que não foi a inversa? Foi sim! É apenas que o $(\mathbb{R}_{\neq 0}\ ;\ \cdot)$ é um grupo abeliano; em outras palavras a "ordem que acontecem os membros" não importa. Mas tudo isso é apenas uma *intuição correta* para adivinhar essa lei. Precisamos demonstrá-la. Bora!

Λ11.58. Lema (inverso de produto). *Em todo grupo G, $(a * b)^{-1} = b^{-1} * a^{-1}$ para todo $a, b \in G$.*

▸ Esboço. Queremos mostrar que $b^{-1} * a^{-1}$ é o inverso do $a * b$. Mas o que «ser o inverso do $a * b$» significa? Precisamos verificar que o $b^{-1} * a^{-1}$ satisfaz a definição:

$$\left(b^{-1} * a^{-1}\right) * (a * b) = e = (a * b) * \left(b^{-1} * a^{-1}\right).$$

Agora só basta fazer esse cálculo mesmo. □ (Λ11.58P)

▸ **EXERCÍCIO x11.29.**
Desenhe um diagrama cuja comutatividade é a lei que tu acabou de demonstrar. (x11.29 H 1 2 3)

Λ11.59. Lema (resolução de equações: Latin square). *Seja G grupo. Para quaisquer $a, b, x, y \in G$, cada uma das equações abaixo tem resolução única para x e y:*

$$a * x = b \qquad\qquad y * a = b$$

▸ Esboço. Aplicando o inverso de a em cada equação pelo lado certo, achamos que as soluções necessariamente são $x = a^{-1} * b$ e $y = b * a^{-1}$. □ (Λ11.59P)

11.60. Observação. Isso quis dizer que dada uma equação $a * b = c$, cada um dos a, b, c é determinado pelos outros dois! Assim, podemos *definir* por exemplo o objeto x como *a única solução da* $a * x = b$, etc.

11.61. Corolário (inversos mais baratos). *Seja G grupo e $a, y \in G$ tais que $a * y = e$ ou $y * a = e$. Logo $y = a^{-1}$.*

11.62. Corolário (identidade mais barata). *Seja G grupo $u \in G$. Se para algum $a \in G$, $au = a$ ou $ua = a$, então u é a identidade do grupo: $u = e$.*

▸ **EXERCÍCIO x11.30.**
Ganhamos esses resultados (Corolário 11.61 e 11.62) como corolários do Lema Λ11.59. Mostre como ganhá-los como corolários das leis de cancelamento. (x11.30 H 0)

▸ **EXERCÍCIO x11.31.**
Seja G grupo. Demonstre a equivalência:

$$G \text{ abeliano} \iff \text{para todo } a, b \in G,\ (ab)^{-1} = a^{-1}b^{-1}.$$

(x11.31 H 0)

11.63. Critérion (Definição de grupo com cancelamento). *Seja $\mathcal{G} = (G\ ;\ *)$ um conjunto finito estruturado que satisfaz:*

(G0)	$(\forall a, b \in G)[\, a * b \in G\,]$
(G1)	$(\forall a, b, c \in G)[\, a * (b * c) = (a * b) * c\,]$
(GCL)	$(\forall a, x, y \in G)[\, a * x = a * y \implies x = y\,]$
(GCR)	$(\forall a, x, y \in G)[\, x * a = y * a \implies x = y\,].$

Então $\mathcal{G}$ é um grupo.

Demonstração. Problema Π11.5 ▮

▸ **EXERCÍCIO x11.32.**
Mostre que não podemos apagar o "finito" das nossas hipoteses. (x11.32 H 1)

11.64. Critérion (Definição unilateral "one-sided" de grupo). *Seja* $\mathcal{G} = (G\,;*,e)$ *um conjunto estruturado que satisfaz:*

(G0) $(\forall a,b\in G)[\,a*b\in G\,]$
(G1) $(\forall a,b,c\in G)[\,a*(b*c)=(a*b)*c\,]$
(G2R) $(\forall a\in G)[\,a*e=a\,]$
(G3R) $(\forall a\in G)(\exists y\in G)[\,a*y=e\,]$

Então $\mathcal{G}$ *é um grupo. Similarmente se adicionar as*

(G2L) $(\forall a\in G)[\,e*a=a\,]$
(G3L) $(\forall a\in G)(\exists y\in G)[\,y*a=e\,]$.

Demonstração. Problema Π11.4. ∎

▸ **EXERCÍCIO x11.33.**
Verifique que mesmo se conseguir demonstrar as

(G2L) $(\forall a\in G)[\,e*a=a\,]$
(G3L) $(\forall a\in G)(\exists y\in G)[\,y*a=e\,]$

isso não nos permite deduzir trivialmente as (G2) e (G3)! Explique o porquê. (x11.33H0)

▸ **EXERCÍCIO x11.34.**
Podemos substituir a (G3R) do Critérion 11.64 por

(G3L) $(\forall a\in G)(\exists y\in G)[\,y*a=e\,]$

e ainda concluir que $\mathcal{G}$ é grupo? Ou seja, se a operação possui R-identidade, e se cada membro tem L-inverso, o $\mathcal{G}$ é necessariamente um grupo? (Obviamente a resposta na pergunta simétrica deve ser a mesma.) (x11.34H1234)

§245. Tabelas Cayley

? **Q11.65. Questão.** De quantas maneiras podemos definir uma operação binária $*$ num conjunto finito G, tal que $(G\,;*)$ é um grupo?

!! SPOILER ALERT !!

11.66. O que determina uma operação. O que significa *definir uma operação* (binária)? Seguindo nossa definição de igualdade (extensional) entre funções, precisamos deixar claro para qualquer $\langle x, y\rangle \in G \times G$, seu único valor $x * y \in G$. Vamos brincar com os casos mais simples. Se $|G| = 0$, não tem como virar um grupo, pois todo grupo tem pelo menos um membro: sua identidade. Se $|G| = 1$, só tem uma operação possível, pois não existe nenhuma opção para o valor $e * e$: necessariamente $e * e = e$. E essa opção realmente vira-se o $(G\,; *)$ um grupo (trivial).

11.67. Os casos 2,3,4. Vamos dizer que temos um conjunto G com $|G| = 4$. Não sabemos nada sobre seus membros, podem ser números, letras, pessoas, funções, conjuntos, sapos, sei-lá:

$$G = \{\bullet, \bullet, \bullet, \bullet\}\,.$$

Então faz sentido começar nossa investigação dando uns nomes para esses membros, por exemplo a, b, c, d, onde não vamos supor nada mais sobre eles exceto que são distintos dois-a-dois.

$$\text{«Sejam } G =: \{a, b, c, d\}.\text{»}$$

Sera que podemos fazer algo melhor? Querendo tornar o G em grupo, sabemos que ele vai ter exatamente uma identidade, então melhor denotá-la com e, e escolher nomes para os outros três membros do G:

$$G = \{e, a, b, c\}\,.$$

Similarmente, caso que $|G| = 2$ ou 3, teremos $G = \{e, a\}$ ou $G = \{e, a, b\}$ respectivamente.

11.68. Tabelas Cayley. Temos então que ver o que podemos botar nos ? para completar as *tabelas Cayley* abaixo:

$*$	e	a
e	?	?
a	?	?

$*$	e	a	b
e	?	?	?
a	?	?	?
b	?	?	?

$*$	e	a	b	c
e	?	?	?	?
a	?	?	?	?
b	?	?	?	?
c	?	?	?	?

Mas, não todos os ? realmente representam uma escolha, pois certos deles são determinados; e cada vez que fazemos uma escolha para um deles, possivelmente nossas opções próximas deminuiam. Para começar, como $e * x = x = x * e$ para qualquer x do grupo, a primeira linha e a primeira coluna da tabela já são determinadas:[83]

$*$	e	a
e	e	a
a	a	?

$*$	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

$*$	e	a	b	c
e	e	a	b	c
a	a	?	?	?
b	b	?	?	?
c	c	?	?	?

[83] De fato, foi por isso que Cayley realmente nem escreveu a coluna e a linha "exterior", tomando a convenção que o elemento que aparece primeiro é a sua identidade. Para um grupo de três elementos então, ele começaria assim:

a	b	c
b	?	?
c	?	?

que, seguindo nossa convenção com 'e', escreveríamos

e	a	b
a	?	?
b	?	?

Exatamente por causa dessa observação, em geral omitimos a primeira coluna e a primeira linha dessas tabelas, escrevendo as três tabelas acima nesse jeito:

e	a
a	?

e	a	b
a	?	?
b	?	?

e	a	b	c
a	?	?	?
b	?	?	?
c	?	?	?

? **Q11.69. Questão.** O que tu podes botar nos ? para chegar num grupo? O que muda se tu queres construir um grupo abeliano?

!! SPOILER ALERT !!

11.70. 2 membros. Vamos começar no caso mais simples, onde temos apenas um ? para preencher. Em teoria temos duas opções: e, a. Mas precisamos verificar se o conjunto realmente torna-se um grupo ou não. Escolha a:

e	a
a	a

Qual seria o inverso do a? Nenhum! Assim o (G3) será violado, ou seja, não podemos escolher o a. Se escolher nossa única outra opção (e) temos:

e	a
a	e

Que realmente é um grupo.

▸ **EXERCÍCIO x11.35.**
Verifique! (x11.35 H 0)

▸ **EXERCÍCIO x11.36.**
Ache todas as operações possíveis que tornam um conjunto com 3 membros um grupo. (x11.36 H 1)

11.71. Jogando "Grupoku". Investigar todas as possíveis escolhas para os ? parece como um jogo de Sudoku, só que nossa restricção não é com a soma dos números de cada linha e cada coluna como no Sudoku—nem poderia ser isso: nossos membros possivelmente nem são números—mas as leis (G0)–(G3) que tem que ser satisfeitas. E caso que queremos criar um grupo abeliano, a (GA) também.

▸ **EXERCÍCIO x11.37.**
Que restricções pode afirmar que temos nesse jogo de "Grupoku", graças todos os resultados que temos demonstrado até agora sobre grupos? E se queremos um grupo abeliano, muda o quê? (x11.37 H 0)

▸ **EXERCÍCIO x11.38.**
Ache todas as operações possíveis que tornam um conjunto com 4 membros um grupo. (x11.38H1)

▸ **EXERCÍCIO x11.39.**
Tem grupos de ordem 1? De 0? (x11.39H0)

§246. Potências e ordens

D11.72. Definição. Seja a elemento dum grupo $(G\,;*,e)$. Definimos suas potências a^{*n} onde $n\in\mathbb{N}$ recursivamente:

$$a^{*0} \stackrel{\text{def}}{=} e$$
$$a^{*n+1} \stackrel{\text{def}}{=} a * a^{*n}$$

Quando a operação $*$ é entendida pelo contexto escrevemos apenas a^n em vez de a^{*n}.

▸ **EXERCÍCIO x11.40.**
Demonstre que a definição alternativa de exponenciação ao natural

$$a^{*0} = e$$
$$a^{*n+1} = a^{*n} * a$$

é equivalente. (x11.40H1234567)

TODO connect this with Problema Π4.19

Acabaste de demonstrar um teorema bem mais geral do que parece no enunciado do Exercício x11.40! É o seguinte:

Θ11.73. Teorema. *Seja A um conjunto estruturado e $*$ uma operação binária e associativa no A, com identidade u. As duas definições de potências*

$$a^{*0} = u \qquad\qquad a^{*0} = u$$
$$a^{*n+1} = a * a^n \qquad\qquad a^{*n+1} = a^n * a$$

são equivalentes, ou seja, as duas operações definidas são iguais.

Demonstrado. No Exercício x11.40, pois as únicas coisas que precisamos na sua demonstração foram exatamente as hipoteses desse teorema. ∎

Θ11.74. Teorema. *A operação de exponenciação definida no Teorema Θ11.73 satisfaz as leis:*

(1) $(\forall n,m\in\mathbb{N})(\forall a\in A)[\,a^{m+n} = a^m * a^n\,]$;
(2) $(\forall n,m\in\mathbb{N})(\forall a\in A)[\,a^{m\cdot n} = (a^m)^n\,]$;
(3) $(\forall n\in\mathbb{N})[\,e^n = e\,]$.

Já demonstrado. Como observamos no Teorema Θ9.154 também, quando demonstramos por indução as leis nos exercícios x4.19, x4.20, e x4.21, usamos apenas a *associatividade* e a *identidade* da multiplicação e *não usamos sua definição*. Logo a mesma demonstração serve aqui, trocando a multiplicação por nossa $*$. ∎

TODO Teaser/remark about Capítulo 12

▸ **EXERCÍCIO x11.41.**
Mostre que, *em geral*, $(a*b)^2 \neq a^2 * b^2$. (x11.41H0)

TODO check the following exercise for dups and position

▸ **EXERCÍCIO x11.42.**
Seja G grupo finito. Para todo $a \in G$, existe $n \in \mathbb{N}_{>0}$ tal que $a^n = e$. Demonstre: (i) diretamente; (ii) usando a contrapositiva; (iii) usando reductio ad absurdum. (x11.42H0)

! **11.75. Cuidado.** Neste momento então, para qualquer grupo G e qualquer $a \in G$, o símbolo a^w é definido *apenas* para $w := -1, 0, 1, 2, \ldots$ e nada mais! Vamos agora estender para os valores $w := -2, -3, -4, \ldots$ num jeito razoável.

? **Q11.76. Questão.** O que você acha que deveria ser denotado por a^{-2}?

!! SPOILER ALERT !!

Resposta. Bem, tem duas interpretações, ambas razoáveis:

$$a^{-2} \stackrel{?}{=} \begin{cases} \left(a^{-1}\right)^2 & \text{(o quadrado do inverso do } a\text{)} \\ \ldots \text{ou} \ldots & \\ \left(a^2\right)^{-1} & \text{(o inverso do quadrado do } a\text{)} \end{cases}$$

As duas interpretações são equivalentes:

▸ **EXERCÍCIO x11.43.**
Seja G grupo. Para todo $a \in G$, $\left(a^{-1}\right)^2 = \left(a^2\right)^{-1}$. Ou seja, o diagrama

$$\begin{array}{ccc} G & \xrightarrow{\cdot^{-1}} & G \\ \downarrow{\scriptstyle \cdot^2} & & \downarrow{\scriptstyle \cdot^2} \\ G & \xrightarrow{\cdot^{-1}} & G \end{array}$$

comuta. (x11.43H123)

▸ **EXERCÍCIO x11.44.**
Generalize o Exercício x11.43 para $n \in \mathbb{N}$: *para todo grupo G e todo $n \in \mathbb{N}$, se $a \in G$ então* $\left(a^{-1}\right)^n = \left(a^n\right)^{-1}$. (x11.44H12)

D11.77. Definição. Seja a elemento dum grupo $(G\,;*,e)$. Definimos para todo $n\in\mathbb{N}_{>0}$.

$$a^{-n}\stackrel{\text{def}}{=}\left(a^{-1}\right)^n$$

Note que graças ao Exercício x11.44 a definição alternativa de exponenciação ao inteiro negativo $a^{-n}\stackrel{\text{def}}{=}(a^n)^{-1}$ é equivalente.

11.78. Propriedade (Potências). *Sejam G grupo, $a\in G$, e $m,n\in\mathbb{Z}$. Temos:*
(1) $a^m*a^n=a^{m+n}$;
(2) $(a^m)^n=a^{m\cdot n}$;
(3) $e^n=e$;
(4) $(a^n)^{-1}=\left(a^{-1}\right)^n$.

▸ Esboço. Demonstramos a (4) primeiro para $m,n\in\mathbb{N}$ por indução—as (1)–(3) já demonstramos (Teorema Θ11.74). Depois consideramos os casos de inteiros negativos para as quatro leis. □

▸ **EXERCÍCIO x11.45.**
Seja G grupo tal que para todo $a,b\in G$, $(ab)^2=a^2b^2$. Logo, G é abeliano. (x11.45 H 1)

D11.79. Definição (Ordem de membro em grupo). Seja $(G\,;*,e)$ grupo e $a\in G$. Chamamos *ordem* de a o menor positivo $n\in\mathbb{N}$ tal que $a^n=e$, se tal n existe; caso contrário, dizemos que o a tem ordem infinita. Usamos a mesma notação como no caso de ordem de grupos: $o(a)$, $\operatorname{ord}(a)$, ou $|a|$, com os mesmos cuidados. Logo:

$$o(a)=\begin{cases}\min\{\,n\in\mathbb{N}_{>0}\mid a^n=e\,\}, & \text{se } \{\,n\in\mathbb{N}_{>0}\mid a^n=e\,\}\neq\emptyset\\ \infty, & \text{caso contrário.}\end{cases}$$

• **EXEMPLO 11.80.**
No S_3, temos

$$o(\mathrm{id})=1\qquad o(\varphi)=2\qquad o(\psi)=3$$
$$o(\varphi\circ\psi)=2\qquad o\left(\psi^2\right)=3.$$
$$o(\psi\circ\varphi)=2$$

▸ **EXERCÍCIO x11.46.**
Verifique os números do Exemplo 11.80. (x11.46 H 0)

▸ **EXERCÍCIO x11.47.**
Seja G grupo e $a\in G$. Se existe $m\in\mathbb{Z}_{\neq0}$ tal que $a^m=e$, então $o(a)<\infty$. (x11.47 H 12)

Λ11.81. Lema. *Sejam G grupo e $a\in G$, e suponha $o(a)=n\in\mathbb{N}$. Existem exatamente n distintas potências de a.*

▸ Esboço. As potências de a são as:

$$\ldots,a^{-2},a^{-1},a^0,a^1,a^2,\ldots,a^{n-1},a^n,a^{n+1},a^{n+2},\ldots$$

Queremos demonstrar que, no final das contas, nesta lista aparecem exatemente n distintos membros de G. Ou seja,

$$\left|\{\, a^k \mid k \in \mathbb{Z} \,\}\right| = n.$$

Consideramos os

$$a^0, a^1, \ldots, a^{n-1}$$

e usando a definição de $o(a)$ demonstramos:

EXISTÊNCIA: os $a^0, \ldots, a^{n-1}$ são distintos dois-a-dois.
Ou seja: para todo $i, j \in \{0, \ldots, n-1\}$ com $i \neq j$, temos $a^i \neq a^j$.

UNICIDADE: para todo $M \in \mathbb{Z}$ o a^M é um dos $a^0, \ldots, a^{n-1}$.
Sabemos diretamente pela sua definição que $a^0 = e$, e que $a^n = e$, pois $o(a) = n$. Com pouca imaginação chegamos na idéia que a cadeia de membros

$$\ldots,\ a^{-2},\ \ a^{-1},\ \ a^0,\ a^1,\ a^2,\ \ldots,\ a^{n-1},\ a^n,\ a^{n+1},\ a^{n+2},\ \ldots$$

é feita por uma copia de $a^0, \ldots, a^{n-1}$ se repetindo infinitamente para as duas direções:

$$\ldots,\ a^{n-2},\ a^{n-1},\ a^0,\ a^1,\ a^2,\ \ldots,\ a^{n-1},\ a^0,\ a^1,\quad a^2,\quad \ldots$$

Aplicando a divisão de Euclides (Lemma da Divisão de Euclides Λ3.82) no M por n, ganhamos $q, r \in \mathbb{Z}$ tais que:

$$M = q \cdot n + r, \qquad 0 \leq r < n.$$

Só basta calcular o a^M para verificar que realmente é um dos $a^0, \ldots, a^{n-1}$. □ (Λ11.81P)

▸ **EXERCÍCIO x11.48.**
Leia a demonstração do Lema Λ11.81 e escreva uma que não usa *reductio ad absurdum*. (x11.48H0)

? **Q11.82. Questão.** Se $a^m = e$ para algum $m \in \mathbb{Z}$, o que podemos concluir sobre o m e a $o(a)$? Se $o(a) = \infty$, o que podemos concluir sobre todas as potências de a?

!! SPOILER ALERT !!

Λ11.83. Lema. *Sejam $(G\,;*)$ grupo, $a \in G$, e $m \in \mathbb{Z}$. Logo*

$$a^m = e \iff o(a) \mid m.$$

DEMONSTRAÇÃO. ($\Leftarrow$): Como $o(a) \mid m$, temos $m = ko(a)$ para algum $k \in \mathbb{Z}$. Calculamos:

$$a^m = a^{ko(a)} = a^{o(a)k} = \left(a^{o(a)}\right)^k = e^k = e.$$

($\Rightarrow$): Para demonstrar que $o(a) \mid m$, aplicamos o Lemma da Divisão de Euclides Λ3.82 da divisão de Euclides, dividindo o m por $o(a)$, e ganhando assim inteiros q e r tais que

$$m = o(a)q + r \qquad 0 \leq r < o(a).$$

Vamos demonstrar que o resto $r = 0$. Calculamos:

$$e = a^m = a^{o(a)q+r} = a^{o(a)q} * a^r = \left(a^{o(a)}\right)^q * a^r = e^q * a^r = e * a^r = a^r.$$

Ou seja, $a^r = e$ com $0 \leq r < o(a)$, então pela definição de $o(a)$ como o mínimo inteiro positivo n que satisfaz a $a^n = e$, o r não pode ser positivo. Logo $r = 0$ e $o(a) \mid m$. ∎

Λ11.84. Lema. *Sejam G grupo e $a \in G$. Se $o(a) = \infty$, então as potências de a são distintas dois-a-dois.*

▸ Esboço. Precisamos demonstrar que para todo $r, s \in \mathbb{Z}$,

$$a^r = a^s \implies r = s.$$

Sem perda de generalidade suponhamos $s \leq r$ e usando a hipótese chegamos em $a^{r-s} = e$; e como a ordem de a é infinita, temos $r - s = 0$ e logo $r = s$. □ (Λ11.84P)

§247. Escolhendo as leis

Como escolhemos as leis (G0)–(G3)? Por que essas? Por que não botamos a (GA)? Por que botamos a (G3)? Vamos discutir pouco sobre essas perguntas.

11.85. Mais teoremas ou mais modelos?. Óbvio que adicionando mais leis na definição de grupo, a gente poderia demonstrar mais teoremas. Mas o que ganhamos em teoremas, perdemos em generalidade da nossa teoria: menos coisas vão acabar sendo *modelos* dos nossos axiomas, e logo esse bocado de teoremas que vamos conseguir demonstrar não poderá ser aproveitado em muitos contextos diferentes. Adicionando a (GA) nos axiomas de grupo por exemplo, os S_n iam parar de ser grupos, e não teriamos nenhum teorema "de graça" pra eles. Como eu afirmei na introdução desse capítulo, a escolha (G0)–(G3) tem um equilibrio muito bom entre riquesa da teoria e diversidade de modelos. Faz sentido tirar o (G3)? Claro que sim; chegamos numa estrutura com mais modelos (e menos teoremas), que com certeza vale a pena estudar. O nome dessa estrutura é *monóide*, que estudamos no 12.

11.86. Evite redundâncias. Vamos dizer que estamos escolhendo as leis para a definição de grupo. Já escolhemos as (G0)–(G3), mas queremos que em cada grupo seja possível cancelar pela esquerda (GCL) e pela direita (GCR). Mesmo assim, não faz sentido adiconar as (GCL)–(GCR) como leis, pois como a gente descobriu no Lema Λ11.41, ambas são *teoremas* da teoria dos (G0)–(G3). Similarmente, escolhemos os axiomas (G2) e (G3) que garantam a existência *duma* identidade e para cada membro *dum* inverso, em vez de botar como leis as proposições mais fortes que afirmam as *unicidades* deles também. Por quê? A resposta é parecida: se for possível, preferimos limitar nossos axiomas nas versões mais fracas possíveis para elaborar nossa teoria. Nesse caso, a gente também descobriu que mesmo com os (G2)–(G3) as unicidades são garantidas na nossa teoria, agora como *teoremas* (Λ11.35 e Λ11.39).

11.87. Clareza e intuitividade vs. mão-de-vaca. Por outro lado, optamos para botar as leis (G2)–(G3), em vez do par mais fraco (G2L)–(G3L), ou do (G2R)–(G3R), que como tu sabes—ou como tu vai descobrir quando finalmente resolver o Problema Π11.4—qualquer um par poderia substituir o par (G2)–(G3), sem afetar a teoria pois os (G2)–(G3) viram teoremas nesse caso (Critérion 11.64). Por que não escolher como axiomas dos grupos os (G0),(G1),(G2L),(G3L) então? Aqui é mais difícil justificar essa escolha. Queremos achar um *equilíbrio* entre a economia, fraqueza, e quantidade dos axiomas num lado; e a clareza e intuitividade no outro. Não queremos exagerar nem no lado de clareza (sendo redundantes), nem no lado de economia (sendo mão-de-vaca). Escolhendo as (G2L)–(G3L) como axiomas, daria um toque assimétrico na definição do que é um grupo. Pelas leis apareceria (erroneamente) que a operação dum grupo trata seus dois lados em maneiras diferentes, prejudicando ou favorecendo um em comparação com o outro. Botamos então como leis as (G2)–(G3) e demonstramos como *critérion* (11.64) que assim que os (G0),(G1),(G2L),(G3L) são satisfeitos, temos um grupo (e similarmente para os (G2R)–(G3R)). Nossas leis escolhidas ((G0)–(G3)) estão falando claramente para nosso coração. Cada um é simples; descreve uma propriedade simples e significante. Imagine se alguém definir que o $(G\,;*,^{-1},e)$ é um *grupo* sse satisfaz uma lei única e bizarra, como a

$$\text{(GKUN)}\qquad (\forall a,b,c\in G)\left[\left(\left(c*(a*b)^{-1}\right)^{-1}*\left(c*b^{-1}\right)\right)*\left(b^{-1}*b\right)^{-1}=a\right].$$

Dá pra entender no teu coração qualquer coisa sobre o G e sua alma? Dá pra entender, olhando para essa lei única, se tem alguma operação associativa com identidade e inversos por aí? Por incrível que pareça, eu nem tô brincando sobre a lei (GKUN). Realmente, Kunen construiu o (GKUN) e demonstrou que a teoria do (GKUN) sozinho e a mesma da teoria dos (G1)+(G2)+(G3) (veja **[Kun92]**)! Ou seja:

$$\mathcal{G}\text{ satisfaz a (GKUN)}\overset{!!}{\iff}\mathcal{G}\text{ é grupo.}$$

Considerei aqui a (G0) como automaticamente garantida (e logo redundante) pelo fato de ter uma operação (total) na minha estrutura. A volta é muito fácil, e tu demonstrarás agora no Exercício x11.49; deixo o converso para o Problema Π11.10.

TODO Clarificar single axioms; elaborar e mostrar mais

▸ **EXERCÍCIO x11.49.**
Demonstre a (⇐). (x11.49 H 1)

11.88. Modularidade. Também é bom ter *modularidade* entre nossos axiomas, em tal forma que facilita tirar um, botar outro, e chegar numa teoria diferente mas interessante também. Continuando no mesmo exemplo da definição unilateral de grupos, suponha que tiramos o (G3L), que é nosso axioma de L-inversos. Onde chegamos? Numa estrutura verdadeiramente L-lateral—esquisito!

11.89. Demonstrando a indemonstabilidade. Alguém poderia pensar (razoavelmente) que a inclusão do (G3) nos axiomas de grupos foi desnecessária. A gente deveria derivá-lo como conseqüência do resto dos axiomas, na mesma maneira que demonstramos tantas outras proposições. Aceitando o desafio começamos pensar para achar uma demonstração do (G3) a partir dos (G0)–(G2). E o tempo passa, passa, e passa...

E não conseguimos demonstrar. *Isso não quis dizer que o (G3) é indemonstrável!* Talvez amanha a gente terá uma idéia nova e conseguir demonstrá-lo; ou talvez amanhã

um rapaz mais esperto vai achar uma demonstração. Mas, nesse caso, não vai não. Pois podemos *demonstrar* que o (G3) é realmente *indemonstrável* pelos (G0)–(G2).

▸ **EXERCÍCIO x11.50.**
Como? O que seria um argumento convencente sobre isso? E em geral, como podemos demonstrar a indemonstrabilidade duma proposição ψ a partir dumas proposições $\varphi_1, \dots, \varphi_n$? Depois de deixar claro tua estratégia demonstre que realmente:

- a (GA) não é uma conseqüência das (G0)–(G3);
- a (G3) não é uma conseqüência das (G0)–(G2);
- a (G2) não é uma conseqüência das (G0)–(G1);
- a (G1) não é uma conseqüência da (G0).

(x11.50 H 1 2)

Não se preocupe demais com essas questões; com mais experiência e maturidade tu vai reconhecer e apreciar os motivos dessas escolhas, e tu elaborarás teu próprio gosto, instinto, e talento, para escolher axiomas. Mas chega! Voltamos a estudar a teoria dos grupos agora.

§248. Conjugação de grupo

D11.90. Definição (Conjugados). Seja G grupo e $a \in G$. Para qualquer $g \in G$, o gag^{-1} é chamado um *conjugado* de a.

D11.91. Definição (conjugação). Seja G um grupo. A *conjugação do* G é a relação $\approx : \mathrm{Rel}\,(G, G)$ definida pela

$$\begin{aligned} a \approx b &\overset{\mathsf{def}}{\iff} a \text{ é um conjugado de } b \\ &\iff (\exists g \in G)\big[\, a = gbg^{-1} \,\big]. \end{aligned}$$

▸ **EXERCÍCIO x11.51.**
Seja G grupo. A conjugação $\approx$ do G é uma relação de equivalência. (x11.51 H 0)

D11.92. Definição (Classe de conjugação). Seja G grupo e $a \in G$. A *classe de conjugação* de a é o conjunto

$$\mathrm{Cls}\,(a) \overset{\mathsf{def}}{=} \left\{\, gag^{-1} \;\middle|\; g \in G \,\right\},$$

ou seja, $\mathrm{Cls}\,(a)$ é a classe de equivalência do a através da relação «é um conjugado de».

▸ **EXERCÍCIO x11.52.**
Seja G grupo. Calcule a $\mathrm{Cls}\,(e)$. (x11.52 H 1)

▸ **EXERCÍCIO x11.53.**
Ache todas as classes de conjugação de S_3. (x11.53 H 1)

D11.93. Definição (conjugadores). Seja G grupo e $g \in G$. Definimos a função $\sigma_g : G \to G$ pela

$$\sigma_g x = gxg^{-1}.$$

Chamamos a σ_g de *g-conjugador*. Observe que o conjugador σ_g é um ator: $\left(g_g^{-1}\right)$.

▸ **EXERCÍCIO x11.54.**
Sejam G grupo e $g, a \in G$. Para todo $n \in \mathbb{Z}$, $\left(gag^{-1}\right)^n = ga^n g^{-1}$. Em outras palavras, a conjugação por membro respeita as potências:

$$\sigma_g(a^n) = (\sigma_g a)^n$$

para todo $n \in \mathbb{Z}$. (x11.54 H 1)

▸ **EXERCÍCIO x11.55.**
Se x, y são conjugados, então para todo n inteiro, x^n e y^n também são. (x11.55 H 1)

A idéia de conjugação deve aparecer meio aleatória pra ti neste momento, mas não tanto como logo depois da definição (agora pelo menos tu já demonstrou muitas propriedades interessantes). Logo vamos descobrir que os subgrupos que são *fechados pela conjugação* (ou *fechados pelos conjugados*) são muito interessantes. Paciência.

Intervalo de problemas

▸ **PROBLEMA Π11.1.**
Sejam G grupo e $a, b \in G$. Definimos as funções $f, g, h : G \to G$ pelas

$$f(x) = ax \qquad g(x) = xa \qquad h(x) = axb.$$

Demonstre que as f, g, h são bijecções e ache suas inversas. (Π11.1 H 0)

▸ **PROBLEMA Π11.2.**
Na Secção §309 demonstramos que as leis de cancelamento implicam a existência de únicos inversos. Lembre-se que o $(\mathbb{N}\,;+)$ não é um grupo pois não satisfaz a (G3). Mesmo assim, no $(\mathbb{N}\,;+)$ ambas as leis de cancelamento são válidas. Então, isso implica a existência de inversos únicos! Qual o erro aqui? (Π11.2 H 1)

▸ **PROBLEMA Π11.3.**
Considere essa suposta demonstração da unicidade da identidade (Lema Λ11.35):

> «Seja G grupo e suponha que temos identidades $e_1, e_2 \in G$. Seja $a \in G$. Como e_1 é identidade, temos $a * a^{-1} = e_1$ (1). Como e_2 é identidade, também temos $a * a^{-1} = e_2$ (2). Pelas (1) e (2), como os lados esquerdos são iguais, o lados direitos também são. Ou seja, $e_1 = e_2$ que foi o que queremos demonstrar.»

Identifique todos os erros nessa tentativa de demonstração. (Π11.3H0)

▸ **PROBLEMA Π11.4 (leis unilaterais de grupo).**
Demonstre o Critérion 11.64. Cuidado: lembre-se o Exercício x11.33. (Π11.4H1234)

▸ **PROBLEMA Π11.5.**
Demonstre o Critérion 11.63. (Π11.5H123)

▸ **PROBLEMA Π11.6.**
Podemos apagar um dos (GCL), (GCR) das hipoteses do Critérion 11.63? (Π11.6H12)

▸ **PROBLEMA Π11.7.**
Membros da mesma classe de conjugação tem a mesma ordem. (Π11.7H12)

▸ **PROBLEMA Π11.8.**
Ache uma propriedade interessante que tem a ver com conjugados, tal que para todo grupo G,

$$G \text{ abeliano} \iff \text{essa propriedade.}$$

Demonstre tua afirmação! (Π11.8H12)

▸ **PROBLEMA Π11.9 (Futurama).**
No episódio «The prisoner of Benda» do seriado *Futurama*, a galera resolve seu problema usando teoria dos grupos! um teorema ficou enunciado e demonstrado por Keeler, o escritor desse episódio, e foi a primeira (e provavelmente única) vez que um teorema matemático foi publicado num seriado! o teorema ficou conhecido como o *Futurama theorem*. Assista o episódio, entenda o enunciado do teorema, e demonstre! (Π11.9H0)

▸ **PROBLEMA Π11.10.**

TODO Escrever

(Π11.10H0)

§249. Subgrupos

D11.94. Definição (Subgrupo). Seja $(G\ ;\ *, e)$ grupo. Um subconjunto $H \subseteq G$ é um *subgrupo* de G sse H é um grupo com a mesma operação $*$. Escrevemos $H \leq G$. Chamamos os $\{e\}$ e G *subgrupos triviais* de G.

11.95. Observação (A mesma mesmo?). Na Definição D11.94 falamos que H é um grupo com *a mesma operação* $*$. Literalmente as duas operações são diferentes, pois seus domínios são diferentes. O que entendemos com essa frase aqui é que o conjunto H é um grupo com operação *a restricção da* $*$ *no* $H \times H$. Com símbolos, $(H\ ;\ *|_{H\times H})$ é um grupo. (Lembre-se a Definição D9.161.)

▸ **EXERCÍCIO x11.56.**
Verifique que para todo grupo $(G\,;*,e)$, temos $\{e\} \leq G$. (x11.56H0)

• **EXEMPLO 11.96 (Números reais).**
(1) Considere o grupo $(\mathbb{R}\,;+)$. Observe que $\mathbb{Q}$ e $\mathbb{Z}$ são subgrupos dele, mas $\mathbb{N}$ não é.
(2) Considere o grupo $(\mathbb{R}_{\neq 0}\,;\cdot)$. Observe que $\{1,-1\}$, $\mathbb{Q}_{\neq 0}$, e para qualquer $\alpha \in \mathbb{R}_{\neq 0}$ o conjunto $\{\,\alpha^k \mid k \in \mathbb{Z}\,\}$ são todos subgrupos dele, mas $\mathbb{Z}$ e $\{\,\alpha^n \mid n \in \mathbb{N}\,\}$ não são.

▸ **EXERCÍCIO x11.57.**
Considere o grupo $\mathcal{Q} := (\mathbb{Q} \setminus \{0\}\,;\cdot)$ e seus subconjuntos:

$$Q_1 := \{\,p/q \mid p,q \in \mathbb{Z},\ p \text{ e } q \text{ ímpares}\,\}$$
$$Q_2 := \{\,p/q \mid p,q \in \mathbb{Z},\ p \text{ ímpar},\ q \text{ par}\,\}$$
$$Q_3 := \{\,p/q \mid p,q \in \mathbb{Z},\ p \text{ par},\ q \text{ ímpar}\,\}.$$

Para quais dos $i = 1,2,3$ temos $Q_i \leq \mathcal{Q}$? (x11.57H0)

11.97. Propriedade. $H \leq G \implies H \neq \emptyset$.

DEMONSTRAÇÃO. Como H é um grupo, necessariamente $e \in H$. ∎

▸ **EXERCÍCIO x11.58.**
Demonstre que para todo $m \in \mathbb{Z}$, $m\mathbb{Z} \leq (\mathbb{Z}\,;+)$, onde $m\mathbb{Z} \stackrel{\text{def}}{=} \{\,mk \mid k \in \mathbb{Z}\,\}$. (x11.58H0)

▸ **EXERCÍCIO x11.59.**
Ache uns subgrupos não-triviais do $(\mathbb{R} \setminus \{0\}\,;\cdot)$. (x11.59H0)

11.98. Observação (Associatividade de graça). Seja $(G\,;*)$ grupo, e tome um $H \subseteq G$. Para ver se $H \leq G$, seguindo a definição, precisamos verificar as (G0)–(G3) no $(H\,;*)$. Mas a lei (G1) da associatividade não tem como ser violada no $(H\,;*)$. O que significaria violar essa lei?

Teriamos $a,b,c \in H$, tais que $a*(b*c) \neq (a*b)*c$.

Mas como $H \subseteq G$, nos teriamos o mesmo contraexemplo para a (G1) de G, impossível pois G é um grupo mesmo (e a operação é a mesma). Logo, jamais precisaramos verificar a (G1) para um possível subgrupo.

E isso não é o único "desconto" que temos quando queremos demonstrar que $H \leq G$. Vamos ver mais dois critéria agora:

11.99. Critérion (Subgrupo). *Se H é um subconjunto não vazio do grupo $(G\,;*,e)$, então:*

$$\left.\begin{array}{lcl} (0) & \emptyset \neq H \subseteq G & (H \text{ é não vazio}) \\ (1) & (\forall a,b \in G)[\,a,b \in H \implies a*b \in H\,] & (H \text{ é } *\text{-fechado}) \\ (2) & (\forall a \in G)\big[\,a \in H \implies a^{-1} \in H\,\big] & (H \text{ é } {}^{-1}\text{-fechado}) \end{array}\right\} \implies H \leq G$$

▸ ESBOÇO. Observamos que a associatividade é garantida pelo fato que G é grupo, então basta demonstrar que $e \in H$. Por isso, usamos a hipótese $H \neq \emptyset$ para tomar um $a \in H$ e usando nossas (poucas) hipoteses concluimos que $e \in H$ também. □ (11.99P)

11.100. O esqueleto dessa demonstração. Vamos lembrar o tema de árvores, escrevendo a demonstração do Critério 11.99 assim:

$$\dfrac{\dfrac{\dfrac{h\in H}{h^{-1}\in H}\qquad h\in H}{h^{-1}h\in H}}{e\in H}$$

Quais são as justificações de cada linha de inferência?

$$\dfrac{\dfrac{\dfrac{h\in H}{h^{-1}\in H}\ H\ {}^{-1}\text{-fechado}\qquad h\in H}{h^{-1}h\in H}\ H\ *\text{-fechado}}{e\in H}\ \text{def. } h^{-1}$$

11.101. Observação. Observe que como $H\subseteq G$, a afirmação

$$(\forall a,b\in G)[\,a,b\in H\implies ab\in H\,]$$

é equivalente à

$$(\forall a,b\in H)[\,ab\in H\,].$$

No próximo critério vamos escrever nessa forma mais curta.

11.102. Critério (Subgrupo finito). *Se $(G\,;*,e)$ é um grupo e H é um subconjunto finito e não vazio do G, fechado sobre a operação $*$, então H é um subgrupo de G. Em símbolos:*

$$\left.\begin{array}{lll}(0)&\emptyset\neq H\subseteq_{\text{fin}} G&(H\text{ é }\textit{finito}\text{ e não vazio})\\(1)&(\forall a,b\in H)[\,a*b\in H\,]&(H\text{ é }*\text{-fechado})\end{array}\right\}\implies H\leq G$$

▸ Esboço. Basta demonstar o (2) para aplicar o Critério 11.99. Tome um $a\in H$ e considere a seqüência das suas potências $a,a^2,a^3,\ldots\in H$. Como o H é finito vamos ter um elemento repetido, $a^r=a^s$ com inteiros $r>s>0$, e usamos isso para achar qual dos $a,a^2,a^3,\ldots$ deve ser o a^{-1}, demonstrando assim que $a^{-1}\in H$. □ (11.102P)

11.103. Critério (subgrupo: "one-test"). *Se G é um grupo e $\emptyset\neq H\subseteq G$ tal que*

$$\text{para todo } a,b\in H,\ ab^{-1}\in H,$$

então $H\leq G$. Em símbolos:

$$\left.\begin{array}{ll}(0)&\emptyset\neq H\subseteq G\\(1)&(\forall a,b\in H)\big[\,a*b^{-1}\in H\,\big]\end{array}\right\}\implies H\leq G$$

Demonstração. Exercício x11.60. ∎

11.104. Observação. Em todos esses critérios, as direções ($\Leftarrow$) também são válidas (e suas demonstrações devem ser óbvias).

▸ **EXERCÍCIO x11.60.**
Demonstre o Critérion 11.103. (x11.60 H 1)

▸ **EXERCÍCIO x11.61.**
Mostre que $\leq$ é uma relação de ordem:

$$G \leq G$$
$$K \leq H \;\&\; H \leq G \implies K \leq G$$
$$H \leq G \;\&\; G \leq H \implies H = G.$$

(x11.61 H 0)

▸ **EXERCÍCIO x11.62 (Matrizes).**
Verificamos que

$$G := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{R}^{2\times 2} \;\middle|\; ad - bc \neq 0 \right\}$$

com multiplicação é um grupo no Exemplo 11.28. Considere seus subconjuntos:

$$G_{\mathbb{Q}} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Q}^{2\times 2} \;\middle|\; ad - bc \neq 0 \right\} \qquad H := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; a, b, d \in \mathbb{R},\; ad \neq 0 \right\}$$
$$G_{\mathbb{Z}} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2} \;\middle|\; ad - bc \neq 0 \right\} \qquad K := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{R} \right\}$$
$$G_{\mathbb{N}} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{N}^{2\times 2} \;\middle|\; ad - bc \neq 0 \right\} \qquad L := \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \;\middle|\; a \in \mathbb{R},\; a \neq 0 \right\}$$

Para cada relação de $(\subseteq)$ válida entre 2 dos 7 conjuntos acima, decida se a correspondente relação $\leq$ também é válida. (x11.62 H 0)

• **EXEMPLO 11.105 (Aritmética modular).**
Considere o grupo $(\overline{6}\;;\; +_6)$ onde $+_6$ é a adição modulo 6. Os $\{0, 2, 4\}$ e $\{0, 3\}$ são seus únicos subgrupos não-triviais.

• **EXEMPLO 11.106 (Permutações).**
O $\{\mathrm{id}, \varphi\}$ é um subgrupo de S_3, onde $\varphi = (1\ \ 2)$.

▸ **EXERCÍCIO x11.63.**
Ache todos os subgrupos do S_3. (x11.63 H 1)

• **EXEMPLO 11.107 (Funções reais).**
Seja $F = (\mathbb{R} \to \mathbb{R}_{\neq 0})$ com operação a multiplicação pointwise (Definição D9.203). Os subconjuntos seguintes de F são todos subgrupos dele:

$$\{\, f \in F \mid f \text{ contínua} \,\} \qquad \{\, f \in F \mid f(0) = 1 \,\}$$
$$\{\, f \in F \mid f \text{ constante} \,\} \qquad \{\, f \in F \mid f(r) = 1 \text{ para todo } r \in \mathbb{Q} \,\}$$

• **EXEMPLO 11.108 (Conjuntos).**
Sejam A conjunto, e $X \subseteq A$. Lembra que $(\wp A\ ;\ \triangle)$ é um grupo (Exercício x11.16). Os $\{\emptyset, X\}$ e $\{\emptyset, X, A \setminus X, A\}$ são subgrupos dele, mas os $\{\emptyset, X, A\}$ e $\{\emptyset, X, A \setminus X\}$ não são.

▸ **EXERCÍCIO x11.64.**
Por que não? (x11.64 H 1)

▸ **EXERCÍCIO x11.65.**
Seja G grupo, e $H_1, H_2 \leq G$. Então $H_1 \cap H_2 \leq G$. (x11.65 H 12)

▸ **EXERCÍCIO x11.66.**
Trocamos o $\cap$ para $\cup$ no Exercício x11.65.
(i) Ache o erro na demonstração seguinte:

> «Como $H := H_1 \cap H_2 \subseteq G$, precisamos mostrar que H é fechado sobre a operação:
>
> | | |
> |---|---|
> | Sejam $a, b \in H_1 \cup H_2$. | |
> | Logo $a, b \in H_1$ ou $a, b \in H_2$. | (def. $\cup$) |
> | Logo $ab \in H_1$ ou $ab \in H_2$. | (H_1 e H_2 grupos) |
> | Logo $ab \in H_1 \cup H_2$. | (def. $\cup$) |
>
> e sobre os inversos:
>
> | | |
> |---|---|
> | Seja $a \in H_1 \cup H_2$. | |
> | Logo $a \in H_1$ ou $a \in H_2$. | (def. $\cup$) |
> | Logo $a^{-1} \in H_1$ ou $a^{-1} \in H_2$. | (H_1 e H_2 grupos) |
> | Logo $a^{-1} \in H_1 \cup H_2$. | (def. $\cup$) |
>
> Portanto, $H_1 \cup H_2 \leq G$.»

(ii) Demonstre que a proposição não é válida. (x11.66 H 0)

▸ **EXERCÍCIO x11.67.**
Generalize a Exercício x11.65 para intersecções arbitrárias: se G é um grupo, e $\mathscr{H}$ uma família não vazia de subgrupos de G, então $\bigcap \mathscr{H} \leq G$. (x11.67 H 0)

▸ **EXERCÍCIO x11.68.**
Seja G conjunto e $H \leq G$. Defina no G a relação R_H pela

$$a\ R_H\ b \iff^{\text{def}} ab^{-1} \in H.$$

Decida se a relação R_H é uma relação de ordem parcial, de ordem total, de equivalência, ou nada disso. (x11.68 H 1)

§250. Geradores

D11.109. Definição. Sejam G grupo e $a \in G$. Chamamos o

$$\begin{aligned}\langle a\rangle &\stackrel{\text{def}}{=} \{\, a^m \mid m \in \mathbb{Z} \,\} \\ &= \{\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots\}\end{aligned}$$

o *subgrupo de G gerado por a*.

▸ **EXERCÍCIO x11.69.**
Justifica a palavra "subgrupo" na Definição D11.109. Ou seja, demonstre que para qualquer grupo G e qualquer $a \in G$, $\langle a\rangle \leq G$. (x11.69 H 1)

▸ **EXERCÍCIO x11.70.**
Seja $(G\,;*,e)$ grupo. Calcule o $\langle e\rangle$. (x11.70 H 0)

▸ **EXERCÍCIO x11.71.**
Nos inteiros com adição, calcule os $\langle 4\rangle$, $\langle 4\rangle \cap \langle 6\rangle$, $\langle 4\rangle \cap \langle 15\rangle$, e $\langle 4\rangle \cup \langle 6\rangle$.
Quais deles são subgrupos do $\mathbb{Z}$? (x11.71 H 0)

? **Q11.110. Questão.** Como tu generalizarias o «subgrupo gerado por $a \in G$» para «subgrupo gerado por $A \subseteq G$»? Ou seja, como definirias o $\langle A\rangle$ para qualquer $A \subseteq G$?

Falando de *generalização*, a idéia é que queremos definir o $\langle A\rangle$ num jeito *razoável* e tal que $\langle\{a\}\rangle = \langle a\rangle$.

!! SPOILER ALERT !!

11.111. Queremos generalizar o conceito de geradores para definir $\langle A\rangle$, onde $A \subseteq G$. Seguindo ingenuamente a definição de $\langle a\rangle$, uma primeira abordagem seria botar

$$\langle A\rangle = \{\, a^m \mid a \in A,\ m \in \mathbb{Z} \,\}$$

e chamar $\langle A\rangle$ o subgrupo de G gerado por A. ↯

▸ **EXERCÍCIO x11.72.**
Qual o problema com a definição de $\langle A\rangle$ acima? (x11.72 H 1 2)

▸ **EXERCÍCIO x11.73.**
Tentando generalizar primeiramente para o caso mais simples de «subgrupo gerado por dois membros $a, b \in G$», alguém definiu o $\langle a, b\rangle$ para quaisquer $a, b \in G$ assim:

$$\langle a, b\rangle \stackrel{\text{def}}{=} \{\, a^m b^n \mid m, n \in \mathbb{Z} \,\}.$$

Existe um problema. Qual? (x11.73 H 1)

Vamos finalmente definir o $\langle A\rangle$.

D11.112. Definição (direta). Sejam $(G\,;*)$ grupo e $A \subseteq G$. Chamamos o

$$\langle A\rangle \stackrel{\text{def}}{=} \left\{\, a_0 * \cdots * a_{k-1} \;\middle|\; k \in \mathbb{N};\ i \in \overline{k};\ a_i \in A \text{ ou } {a_i}^{-1} \in A \,\right\}.$$

o *subgrupo de G gerado por A*. Ou seja, os membros de $\langle A\rangle$ são os produtos finitos feitos por membros de A e seus inversos. Abusando a notação, escrevemos também $\langle a_1, a_2, \ldots, a_n\rangle$ para o $\langle\{a_1, a_2, \ldots, a_n\}\rangle$.

11.113. Observação. Lembre-se (Nota 8.166) que para $k = 0$ a expressão acima é a identidade e, e logo $e \in \langle A\rangle$ para qualquer A.

11.114. Propriedade. *As alternativas definições são equivalentes:*

$$\langle A\rangle = \begin{cases} \left\{\, a_0^{m_0} * \cdots * a_{k-1}^{m_{k-1}} \;\middle|\; k \in \mathbb{N};\ i \in \overline{k};\ m_i \in \mathbb{Z};\ a_i \in A \,\right\} \\ \left\{\, a_0^{m_0} * \cdots * a_{k-1}^{m_{k-1}} \;\middle|\; k \in \mathbb{N};\ i \in \overline{k};\ m_i \in \{-1, 1\};\ a_i \in A \,\right\} \\ \left\{\, a_0 * \cdots * a_{k-1} \;\middle|\; k \in \mathbb{N};\ i \in \overline{k};\ a_i \in A \text{ ou } {a_i}^{-1} \in A \,\right\}. \end{cases}$$

▸ **EXERCÍCIO x11.74.**
Sejam G grupo e um subconjunto dele $A = \{a, b, c, d\}$. Mostre que $a^3b^{-2}cb^3d^{-1} \in \langle A\rangle$ para todas as três definições equivalentes da Propriedade 11.114. Ou seja, para cada um desses conjuntos, decida quais são todas as atribuições necessárias que satisfazem o "filtro" de cada conjunto. (x11.74 H 0)

D11.115. Definição (Palavra). Chamamos dum termo feito por membros dum grupo G operados entre si de *palavra* de G. Especificando um subconjunto $A \subseteq G$, uma A-palavra seria uma palavra de G feita usando apenas membros de A e seus inversos.

• **EXEMPLO 11.116.**
Seja G grupo e $A = \{w, x, y, z\}$ um subconjunto de G. Umas A-palavras são as:

$$wxyz \qquad x^{-1} \qquad wwwwwww \qquad wxxy^{-1}yyywz^{-1}w \qquad z^{-1}z^{-1}z^{-1}yy^{-1}zzxx^{-1}z$$

Podemos usar exponentes para abreviar essas palavras:

$$wxyz \qquad x^{-1} \qquad w^7 \qquad wx^2y^{-1}y^3wz^{-1}w \qquad z^{-3}yy^{-1}z^2xx^{-1}z.$$

e às vezes até usamos um "overline" para indicar os inversos:

$$wxyz \qquad \overline{x} \qquad w^7 \qquad w\,x^2\,\overline{y}\,y^3\,w\,\overline{z}\,w \qquad \overline{z}^3\,y\,\overline{y}\,z^2\,x\,\overline{x}\,z.$$

Observe que começando com uma palavra podemos *computar* seu valor, sendo uma palavra onde não aparecem consecutivos objetos canceláveis, aplicando um passo cada vez: selecionando um tal par e o apagando.

11.117. Observação. Com essa definição o $\langle A\rangle$ é feito por os valores de todas as A-palavras.

▸ **EXERCÍCIO x11.75.**
Dado grupo G, calcule os $\langle\emptyset\rangle$ e $\langle G\rangle$. (x11.75 H 1)

▸ **EXERCÍCIO x11.76.**
Demonstre que $\langle A\rangle \leq G$ para qualquer grupo G e qualquer $A \subseteq G$. (x11.76 H 0)

? **Q11.118. Questão.** Temos duas mais caracterizações do $\langle A\rangle$ especialmente importantes: bottom-up e top-down. A gente já encontrou algo similar, definindo os fechos de relações (especialmente o fecho transitivo) no Capítulo 10, §231. Como descreverias os dois processos para definir o $\langle A\rangle$?

!! SPOILER ALERT !!

11.119. Bottom-up, informalmente. Começamos com um conjunto T onde botamos todos os elementos que desejamos no subgrupo (os elementos de A nesse caso), e enquanto isso não forma um grupo, ficamos nos perguntando *por que não*. A resposta sempre é que (pelo menos) uma lei de grupo ((G0)–(G3)) está sendo violada. Vendo as leis, isso sempre quis dizer que um certo elemento tá faltando:

- (G0) violada: para alguns $s,t \in T$, o $s*t \notin T$.
- (G1) violada é impossível (veja Observação 11.98).
- (G2) violada: a identidade $e \notin T$.
- (G3) violada: para algum $t \in T$, seu inverso $t^{-1} \notin T$.

E agora?

- (G0) violada? Resolução: adicione o st: $T \cup \{st\}$.
- (G2) violada? Resolução: adicione o e: $T \cup \{e\}$.
- (G3) violada? Resolução: adicione o t^{-1}: $T \cup \{t^{-1}\}$.

Como resolver cada um desses três possíveis problemas então? Adicionando os membros culpados! E depois? Se o conjunto já virou um grupo, paramos. Se não, continuamos. Ficamos *adicionando* os membros culpados (os faltantes) e repetindo a mesma pergunta, até chegar num conjunto que não viola nenhuma das leis, ou seja, um grupo mesmo. É o conjunto T que tem todos os elementos de A e todos os necessários de G para formar um grupo.

Cuidado: é tentoso pensar como resolução *retirar* os s,t, no caso da (G0), ou o t no caso da (G3). Por exemplo, alguém poderia pensar que o problema no caso da violada (G0), foi a presença dos s,t no T; mas não é! O problema é a ausência do st. Lembre nossa intuição: queremos começar com o A e sem perder nenhum dos seus membros, chegar num subgrupo de G, adicionando apenas os necessários.

Θ11.120. Teorema (Bottom-up, formalmente). *Sejam G grupo e $A \subseteq G$. Definimos a seqüência de conjuntos:*

$$\begin{aligned} A_0 &= A \\ A_{n+1} &= A_n \cup \underbrace{\{\, ab \mid a,b \in A_n \,\}}_{\text{(G0)}} \cup \underbrace{\{e\}}_{\text{(G2)}} \cup \underbrace{\{\, a^{-1} \mid a \in A_n \,\}}_{\text{(G3)}}. \end{aligned}$$

Logo temos:

$$A = A_0 \subseteq A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$$
$$\langle A \rangle = \bigcup_{n=0}^{\infty} A_n.$$

▸ Esboço. Demostrar $A_n \subseteq A_{n+1}$ para todo $n \in \mathbb{N}$ é imediato por indução. Para a afirmação principal, que $\langle A \rangle = \bigcup_{n=0}^{\infty} A_n$, demonstramos cada direção separadamente: para a $(\subseteq)$, tome um arbitrário membro $\alpha \in \langle A \rangle$ e ache $w \in \mathbb{N}$ tal que $\alpha \in A_w$; para a $(\supseteq)$, basta demonstrar que cada um dos $A_0, A_1, A_2, \ldots$ é subconjunto de $\langle A \rangle$. Podes—aliás, deves—usar indução. □

• **EXEMPLO 11.121.**
Pensando em como demonstrar formalmente o Teorema Θ11.120, talvez ajuda considerar um exemplo específico para entender melhor como funciona. Considere então um $A = \{a, b\} \subseteq G$ e um $a^3b^{-8} \in \langle A \rangle$. Como podemos demonstrar que $a^3b^{-8} \in \bigcup_n A_n$? Basta achar um $n \in \mathbb{N}$ tal que $a^3b^{-8} \in A_n$; mas qual n serve aqui? Vamos plantar uma árvore abreviada e rascunhosa:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{b \in A}{b \in A_0} \quad \dfrac{b \in A}{b \in A_0}}{b^2 \in A_1} \quad \dfrac{\dfrac{b \in A}{b \in A_0}}{b \in A_1}}{b^3 \in A_2} \quad \dfrac{\vdots}{b \in A_2}}{b^4 \in A_3}}{\dfrac{\vdots}{b^7 \in A_6}} \quad \dfrac{\vdots}{b \in A_6}}{b^8 \in A_7} \quad \dfrac{\dfrac{\dfrac{a \in A}{a \in A_0}}{a^2 \in A_1} \quad \dfrac{\dfrac{a \in A}{a \in A_0}}{a \in A_1}}{a^3 \in A_2}}{\dfrac{b^{-8} \in A_8}{a^3b^{-8} \in A_9} \quad \dfrac{}{a^3 \in A_8}}$$

Então já sabemos que o $n := 9$ é suficiente e logo concluimos que $a^3b^{-8} \in \bigcup_n A_n$.

▸ **EXERCÍCIO x11.77.**
Justifique as linhas de inferência da árvore do Exemplo 11.121. (x11.77 H 0)

▸ **EXERCÍCIO x11.78.**
Com uma árvore mais baixa demonstre que $a^3b^{-8} \in A_5$. (x11.78 H 1 2)

11.122. Top-down, informalmente. Começamos considerando o próprio G como um possível candidato para ser o subgrupo de G gerado por o conjunto A. No final das contas, $G \leq G$, e também $G \supseteq A$. Mas no G existe possível "lixo": membros fora do A cuja presença não foi justificada como necessária pelas leis de grupo. Precisamos filtrar esse lixo, para ficar apenas com os membros "necessários". Quais são esses membros? Bem, se conseguir formar um subgrupo $H \leq G$ tal que $H \supseteq A$ e que *não* tem alguns dos membros, isso quis dizer que eles não são realmente necessários; ou seja, é lixo. Então quem fica mesmo? Ficam apenas aqueles que pertencem a *todos* os subgrupos de G que contêm o A. Estes membros são exatamente os membros do $\langle A \rangle$.

11.123. Top-down: nível coração. Vamos pensar em nosso alvo (o $\langle A \rangle$) como o *menor* de todos os subgrupos de G que contêm o A. O que significa esse «menor»? Menor em qual ordem? Não ligamos sobre quantidade de elementos aqui. Menor quis dizer subgrupo—lembra que $\leq$ é uma ordem (Exercício x11.61), né?—ou ($\subseteq$)-menor, que *nesse caso* acaba sendo equivalente. O que tudo isso quis dizer? Queremos definir o $\langle A \rangle$ como *aquele* conjunto $\overline{A}$ que satisfaz: (i) $A \subseteq \overline{A} \leq G$; e (ii) para todo K tal que $A \subseteq K \leq G$, temos $\overline{A} \leq K$. Observe que nada muda se trocar o '$\leq$' por '$\subseteq$' na última condição; pois como $\langle A \rangle$ e K são subgrupos de G, as afirmações $\overline{A} \subseteq K$ e $\overline{A} \leq K$ são equivalentes.

Podemos parar nossa definição aqui? Não, pois esse «aquele» acima não foi merecido ainda: como sabemos que existe tal conjunto? Felizmente, graças à (ii), se tal conjunto existe, ele é único (Exercício x11.83).

Começamos com a família $\mathscr{H}$ de *todos* os subgrupos de G que contêm o A:

$$\mathscr{H} = \{\, H \mid A \subseteq H \leq G \,\}.$$

Afirmamos que o conjunto que procuramos é o $\bigcap \mathscr{H}$. Basta verificar que ele satisfaz todas as condições, algo que tu vai fazer agora nos exercícios abaixo, mas antes disso...

▸ **EXERCÍCIO x11.79.**
Mesmo verificando essas três coisas, ainda falta demonstrar algo! Temos um erro sutil mas importantíssimo; *como se fosse* uma possível divisão por zero! Ache o que é, e demonstre o que precisas demonstrar para corrigi-lo. (x11.79 H 0)

▸ **EXERCÍCIO x11.80.**
$\bigcap \mathscr{H} \leq G$. (x11.80 H 0)

▸ **EXERCÍCIO x11.81.**
$A \subseteq \bigcap \mathscr{H}$. (x11.81 H 0)

▸ **EXERCÍCIO x11.82.**
Para cada candidato K com $A \subseteq K \leq G$, temos $\bigcap \mathscr{H} \leq K$. (x11.82 H 1)

▸ **EXERCÍCIO x11.83.**
Demonstre que realmente a condição (ii) acima garanta que se tal conjunto existe, ele é único. (x11.83 H 0)

Θ11.124. Teorema (Top-down, formalmente). *Sejam G grupo e $A \subseteq G$. Logo*

$$\langle A \rangle = \bigcap \{\, H \leq G \mid A \subseteq H \,\}.$$

▸ Esboço. Seja $\mathscr{H} = \{\, H \leq G \mid A \subseteq H \,\}$. Demonstramos cada direção separadamente: Para a $(\subseteq)$, tome um arbitrário membro $\alpha \in \langle A \rangle$ e um arbitrário $H \leq G$ tal que $H \supseteq A$, e mostre que $\alpha \in H$. Para a $(\supseteq)$, tome um α que pertence a todos os subgrupos de G que contêm o A e mostre que ele pode ser escrito na forma desejada (da definição de $\langle A \rangle$). □

Ou seja, temos três definições equivalentes de *subgrupo gerado por A*.

D11.125. Definição (Grupo cíclico). Um grupo G é *cíclico* sse existe $a \in G$ tal que $\langle a \rangle = G$.

▸ **EXERCÍCIO x11.84.**
Quais dos seguintes são grupos cíclicos?

$$(\mathbb{R}\,;+) \quad (\mathbb{Q}\,;+) \quad (\mathbb{Z}\,;+) \quad (\mathbb{R}_{\neq 0}\,;\cdot) \quad (\mathbb{Q}_{\neq 0}\,;\cdot) \quad (\mathbb{Z}_6\,;+_6) \quad (\mathbb{Z}_6 \setminus \{0\}\,;\cdot_6) \quad S_3$$

(x11.84 H 0)

▸ **EXERCÍCIO x11.85.**
Ache todos os membros geradores de $(\mathbb{Z}_6\,;+_6)$. (x11.85 H 1)

▸ **EXERCÍCIO x11.86.**
Ache todos os geradores A de S_3 com tamanho 2. (x11.86 H 0)

§251. Um desvio: bottom-up e top-down

11.126. Bichos e subbichos. As idéias de bottom-up e top-down são tão fundamentais que vale a pena desviar um pouco do nosso estudo de grupos para discutir e generalizar o que acabou de acontecer. Vamos dizer que temos um tipo de coisas que gostamos e estudamos. Aqui esse tipo de coisas foi o grupo, mas queremos ver essas idéias num contexto ainda mais abstrato e geral. Então não vamos especificar esse tipo. Vamos chamar esses objetos de *bichos*. Suponha agora que cada bicho tem "por trás" um associado conjunto. Por exemplo, os grupos e em geral os conjuntos estruturados tem seus carrier sets. Então faz sentido de unir, intersectar, etc., bichos. Suponha também que cada bicho tem algo que faz seu conjunto ser especial: sua estrutura, umas leis, etc. Assim, já temos como definir o que significa *subbicho*: *B_0 é subbicho do bicho B sse $B_0 \subseteq B$ e B_0 também é um bicho*. Agora comece com um bicho B, e considere um subconjunto $S \subseteq B$, que não é necessariamente um subbicho. Queremos definir o *subbicho gerado por S*. Precisamos:

(1) saber que a relação de "subbicho" é uma ordem;
(2) saber que intersecção arbitrária de bichos é bicho.

Agora podemos definir o *subbicho gerado por S* para ser o menor subbicho de B que contem o S, ou seja, a intersecção

$$\langle S \rangle = \bigcap \{\, C \mid C \text{ é subbicho de } B \text{ que contem o } S \,\}.$$

Curtamente: dados $S \subseteq B$, temos

$$\langle S \rangle = \bigcap_{S \subseteq C \leq B} C,$$

onde $(\leq)$ aqui significa "subbicho".

Essas construções aparecem o tempo todo, para vários bichos: espaços topológicos, σ-algebras, espaços vetoriais, relações transitivas, modelos de lógica, etc. Aqui vamos usar como exemplo para ilustrar o processo os *conjuntos convexos* do plano euclideano $\mathbb{R}^2$:

D11.127. Definição (Conjuntos convexos). Seja $C \subseteq \mathbb{R}^2$. Chamamos o C *convexo* sse para todo $P, Q \in C$, o segmento $\overline{PQ} \subseteq C$.

TODO Add figures

▸ **EXERCÍCIO x11.87.**
Desenhe os subconjuntos seguintes de $\mathbb{R}^2$:

(a) $\emptyset$;
(b) $\{\langle 0,0\rangle\}$;
(c) $\{\langle 0,0\rangle, \langle 0,1\rangle\}$;
(d) $\{\langle 0,0\rangle, \langle 0,1\rangle, \langle 1,0\rangle, \langle 1,1\rangle\}$;
(e) $\{\, \langle x,y\rangle \mid x^2+y^2 = 1 \,\}$;
(f) $\{\, \langle x,y\rangle \mid x^2+y^2 \leq 1 \,\}$;
(g) $\{\, \langle x,y\rangle \mid x^2+y^2 < 1 \,\}$;
(h) $\{\, \langle x,0\rangle \mid 0 \leq x < 1 \,\}$;
(i) $\{\, \langle x,y\rangle \mid \max\{|x|, |y|\} < 1 \,\}$.
(j) $\{\, \langle x,y\rangle \mid x+y > 1 \,\}$.

Quais deles são convexos? (x11.87H0)

▸ **EXERCÍCIO x11.88.**
Para cada um dos conjuntos do Exercício x11.87 que não é convexo, desenha seu fecho convexo. (x11.88H0)

▸ **EXERCÍCIO x11.89.**
Demonstre que os conjuntos convexos têm a propriedade de intersecção: se $\mathscr{C}$ é uma família não vazia de conjuntos convexos, então $\bigcap \mathscr{C}$ é um conjunto convexo. (x11.89H0)

Logo, *podemos definir* o *fecho convexo* (ou *convex hull*) dum subconjunto $S \subseteq \mathbb{R}^2$ usando a abordagem top-down.

D11.128. Definição. Seja $S \subseteq \mathbb{R}^2$. Definimos a seqüência de conjuntos $(S_n)_n$ pela recursão:

$$\begin{aligned} S_0 &= S \\ S_{n+1} &= S_n \cup \left\{\, M \in \mathbb{R}^2 \mid \text{existem } P, Q \in S_n \text{ tais que } M \text{ é um ponto no segmento } \overline{PQ} \,\right\}. \end{aligned}$$

Agora definimos o *fecho convexo* (ou *convex hull*) $\langle S\rangle$ de S pela

$$\langle S\rangle \stackrel{\text{def}}{=} \bigcup_{n=0}^{\infty} S_n.$$

▸ **EXERCÍCIO x11.90.**
Demonstre que o convex hull $\langle S \rangle$ dum $S \subseteq \mathbb{R}^2$ merece seu nome: (i) $\langle S \rangle$ é convexo mesmo e contem o S; (ii) qualquer convexo C que contem o S, está contido no $\langle S \rangle$. (x11.90 H 0)

? **Q11.129. Questão.** Como podemos definir o fecho convexo dum conjunto $S \subseteq \mathbb{R}^2$ "top-down"?

!! SPOILER ALERT !!

Resposta. Precisamos ter pelo menos um conjunto convexo que contem o S, verificar que intersecção arbitrária de conjuntos convexos é conjunto convexo, e que a relação "subconjunto convexo" é uma ordem. A última coisa é trivial. As outras duas, deixo como exercícios pra ti (x11.92 e x11.91). Com essas coisas podemos definir o $\langle S \rangle$ como

$$\langle S \rangle = \bigcap \{ C \mid S \subseteq C \leq \mathbb{R}^2 \}$$

onde $(\leq)$ é a relação de "subconjunto convexo". Assim $\langle S \rangle$: (i) é convexo e contem o S; (ii) esta contido em qualquer conjunto que satisfaz a (i). A argumentação é exatamente a mesma com o caso de grupos (Nota 11.123 e os exercícios o seguindo: x11.80; x11.81; x11.82).

▸ **EXERCÍCIO x11.91.**
A intersecção de uma família não vazia de conjuntos convexos é um conjunto convexo. (x11.91 H 0)

▸ **EXERCÍCIO x11.92.**
Seja S um subconjunto do plano. Demonstre que a família de todos os conjuntos convexos que contêm o S não é vazia. (x11.92 H 0)

Chega para agora. No Capítulo 14 vamos revisitar esse assunto num contexto abstrato.

Intervalo de problemas

D11.130. Definição (Centro). Dado um grupo G, definimos seu *centro* $\mathrm{Z}(G)$ como o conjunto de todos os membros de G que "comutam" com todos os membros de G:

$$\mathrm{Z}(G) \stackrel{\text{def}}{=} \{ z \in G \mid \text{para todo } g \in G,\ zg = gz \}.$$

▸ **PROBLEMA Π11.11.**
Mostre que dado um grupo G, seu centro $\mathrm{Z}(G) \leq G$. (Π11.11H0)

▸ **PROBLEMA Π11.12.**
Seja G grupo finito. Existe inteiro $N > 0$ tal que para todo $a \in G$, $a^N = e$. (Π11.12H123)

▸ **PROBLEMA Π11.13.**
No Exercício x11.58 tu demonstraste que para todo $m \in \mathbb{Z}$, $m\mathbb{Z} \leq (\mathbb{Z}\,;+)$. Demonstre que esses são *todos* os subgrupos de $(\mathbb{Z}\,;+)$. Ou seja: para todo $H \leq (\mathbb{Z}\,;+)$, existe $t \in \mathbb{Z}$ tal que $H = t\mathbb{Z}$. (Π11.13H0)

▸ **PROBLEMA Π11.14.**
Seja Q o conjunto de todos os pontos do cíclo com ângulo racional:

$$Q = \{\, \langle \cos\vartheta, \sin\vartheta\rangle \;\;|\;\; \vartheta \in [0, 2\pi) \cap \mathbb{Q} \,\}\,.$$

Considere a seqüência

$$Q = Q_0 \subseteq Q_1 \subseteq Q_2 \subseteq Q_3 \subseteq \cdots$$

obtenida pela bottom-up construção da §251. (i) Qual conjunto é o convex hull $\langle Q\rangle$ do Q? (ii) Descreva o conjunto Q_1. (iii) Tem $Q_i = Q_{i+1}$ para algum $i \in \mathbb{N}$? (Π11.14H0)

▸ **PROBLEMA Π11.15.**
No Problema Π11.14, $Q_1 = Q_2$? (Π11.15H1234)

▸ **PROBLEMA Π11.16.**
O que muda no Problema Π11.14 se definir o Q como $Q = \bigcup_n \{\langle \cos n, \sin n\rangle\}$? (Π11.16H0)

§252. Congruências e coclasses

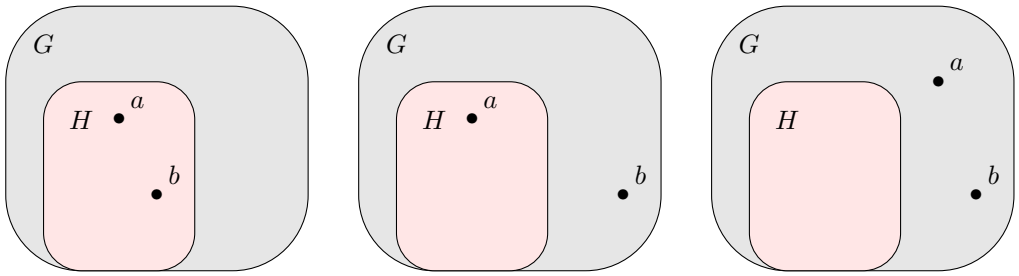
A relação de equivalência que definimos no Exercício x11.68 não é tão desconhecida como talvez apareceu ser. Vamos investigar.

11.131. Congruência módulo subgrupo. Seja G grupo e $H \leq G$. Definimos

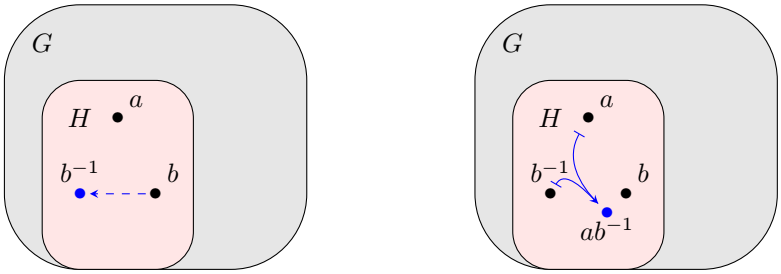
$$a \equiv b \pmod{H} \overset{\text{def}}{\iff} ab^{-1} \in H.$$

Usamos também a notação $a \equiv_H b$.

▸ **EXERCÍCIO x11.93.**
Justifique a notação da Definição D11.144 a comparando com a congruência módulo algum inteiro da Definição D3.155. Ou seja, mostre como a definição nos inteiros é apenas um caso especial da definição nos grupos. (x11.93H1)



Os 3 casos da Investigação 11.132.



Os passos do CASO 1 do 11.132.

11.132. Investigando a congruência. Vamos supor que temos um grupo G e um subgrupo $H \leq G$. Tomamos $a, b \in G$ e queremos ver se $a \equiv b \pmod{H}$. Separamos em casos:

CASO 1: os dois elementos a e b estão no H;
CASO 2: um dos elementos está dentro do H, o outro fora;
CASO 3: os dois estão fora do H.

Para cada caso, queremos decidir se:

(i) podemos concluir que $a \equiv b \pmod{H}$;
(ii) podemos concluir que $a \not\equiv b \pmod{H}$;
(iii) nenhum dos (i)–(ii).

Vamos ver qual dos (i)–(iii) aplica no CASO 1. Temos

$$a \equiv b \pmod{H} \iff ab^{-1} \in H$$

Como $b \in H$ e H é um grupo ($H \leq G$) concluimos que $b^{-1} \in H$. Agora, como $a, b^{-1} \in H$ ganhamos $ab^{-1} \in H$, ou seja, $a \equiv b \pmod{H}$:

▸ **EXERCÍCIO x11.94.**
Decida qual dos (i)–(iii) aplica no CASO 2 do 11.132. (x11.94H12345)

▸ **EXERCÍCIO x11.95.**
Decida qual dos (i)–(iii) aplica no CASO 3 do 11.132. (x11.95H12345)

D11.133. Definição (Coclasses). Seja G grupo e $H \leq G$. Para $a \in G$ definimos

$$aH \stackrel{\text{def}}{=} \{\, ah \mid h \in H \,\} \qquad\qquad Ha \stackrel{\text{def}}{=} \{\, ha \mid h \in H \,\}.$$

Chamamos o aH a *coclasse esquerda* do H através de a, e similarmente o Ha sua *coclasse direita*. Também usamos os termos *coclasse (lateral) à esquerda/direita*, e também chamamos as coclasses de *cosets*.

? **Q11.134. Questão.** O que significa que algum $w \in Ha$? Como podemos usá-lo se é dado? Como podemos matá-lo se é alvo?

!! SPOILER ALERT !!

11.135. Respostas. Pela definição do conjunto Ha com a notação set builder,

$$w \in Ha \iff (\exists h \in H)[\, w = ha \,].$$

Então ganhando $w \in Ha$ como dado, nos permite "sejar" um tal membro de H: *seja $h \in H$ tal que $w = ha$*. E para matar esse alvo precisamos mostrar como escrever nosso w como produto de algum membro do H e do a. Ou seja, procuramos algo que encaixa no $\boxed{?}$:

$$w = \underbrace{\boxed{?}}_{\in H} a.$$

Não esqueça: assim que achar um tal objeto que satisfaz a equação acima, precisa demonstrar que ele pertence ao H.

! **11.136. Aviso (Declare apenas variáveis).** É comum escrever algo do tipo:

> Seja $ha \in Ha$.

Não escreva assim, pois é perigoso roubar sem querer! Em vez disso, podes escrever:

> Seja $w \in Ha$. Logo seja $h \in H$ tal que $w = ha$.

É provável que esse w tem um papel "bobo" aí, e realmente podemos evitá-lo: o conjunto Ha é um conjunto *indexado pelo H*. Então tudo que discutimos no Observação 8.148 aplica, e nesse caso para tomar um arbitrário membro do Ha, basta tomar um arbitrário membro $h \in H$:

> Seja $h \in H$.

...e já temos um arbitrário membro do Ha: o ha.

! **11.137. Aviso.** Vamos supor que temos uns $a, b \in G$ e algum $H = \{h_1, \ldots, h_n\}$. Logo são definidos os

$$\begin{aligned} H &= \{\ h_1,\ h_2,\ h_3,\ \ldots,\ h_n\ \}; \\ Ha &= \{\ h_1a,\ h_2a,\ h_3a,\ \ldots,\ h_na\ \}; \\ Hb &= \{\ h_1b,\ h_2b,\ h_3b,\ \ldots,\ h_nb\ \}. \end{aligned}$$

(1) Agora suponha que sabemos que $Ha = Hb$:

$$\begin{aligned} Ha &= \{\ h_1a,\ h_2a,\ h_3a,\ \ldots,\ h_na\ \} \\ &\| \\ Hb &= \{\ h_1b,\ h_2b,\ h_3b,\ \ldots,\ h_nb\ \}. \end{aligned}$$

É um *erro grave* concluir que

$$\begin{aligned} Ha &= \{\ h_1a,\ h_2a,\ h_3a,\ \ldots,\ h_na\ \} \\ \| &\quad\ \| \quad \| \quad \| \quad\ \| \\ Hb &= \{\ h_1b,\ h_2b,\ h_3b,\ \ldots,\ h_nb\ \}. \end{aligned}$$

A igualdade desses conjuntos nos permite apenas concluir que cada h_ia é igual a um dos h_jb e vice versa. Nada mais!

(2) E agora suponha que queremos demonstrar que $Ha = Hb$. Pela definição de igualdade de conjuntos, precisamos demonstrar $Ha \subseteq Hb$ e $Ha \supseteq Hb$. Mas! Se a gente conseguir demonstrar que realmente para todo i, $h_ia = h_ib$, isso seria ainda mais forte, e obviamente suficiente para concluir que $Ha = Hb$, mas *não necessário*.

▸ **EXERCÍCIO x11.96.**
O que podemos concluir se no (1) acima para *algum* i, $h_ia = h_ib$? (x11.96 H 0)

▸ **EXERCÍCIO x11.97.**
Nenhuma coclasse de H é vazia. (x11.97 H 0)

▸ **EXERCÍCIO x11.98.**
Sejam G grupo, $H \leq G$, e $a \in G$.

$$Ha = H \iff a \in H.$$

(x11.98 H 0)

Uma conseqüência imediata do Exercício x11.98 é que

$$a \notin H \iff Ha \neq H.$$

Mas assim que souber que $a \notin H$ podemos concluir algo bem mais forte que $Ha \neq H$:

▸ **EXERCÍCIO x11.99.**
O quê? Como? (x11.99 H 1)

E se escolher um $b \in G$ fora do H e fora do Ha?

▸ **EXERCÍCIO x11.100.**
Mostre que se $a, b \in G$ tais que $b \notin Ha$ então Hb e Ha são disjuntos. (Que Hb e H são disjuntos já sabemos graças ao Exercício x11.99.) (x11.100H0)

? **Q11.138. Questão.** *Dados um grupo G e $H \leq G$, quantas coclasses tem o H? Ou seja, qual é a cardinalidade do conjunto $\{\, Ha \mid a \in G \,\}$?*

Vamos ver a resposta daqui a pouco (Definição D11.156 e Teorema Θ11.158).

D11.139. Definição. Vamos denotar a família de todas as coclasses esquerdas e direitas do H assim:

$$\mathcal{L}_H \stackrel{\text{def}}{=} \{\, aH \mid a \in G \,\}; \qquad\qquad \mathcal{R}_H \stackrel{\text{def}}{=} \{\, Ha \mid a \in G \,\}.$$

Observe que ambos os $\mathcal{L}_H, \mathcal{R}_H$ são indexados pelo mesmo conjunto G. Como o grupo G é implícito pelo contexto não precisamos especificá-lo na notação; mas caso que não é, escrevemos $\mathcal{L}_H^G$ e $\mathcal{R}_H^G$ respectivamente.

Λ11.140. Lema. *Sejam G grupo e $H \leq G$. A família de todas as coclasses direitas de H é uma partição de G, e a mesma coisa é verdade sobre a família das suas coclasses esquerdas. Ou seja, cada uma das famílias $\mathcal{L}_H$ e $\mathcal{R}_H$ é uma partição do G.*

▸ Esboço. Para a $\mathcal{R}_H$, por exemplo, precisamos demonstrar:

(P1) $\bigcup \mathcal{R}_H \supseteq G$; ou seja: para todo $x \in G$, existe coclasse H' com $x \in H'$;
(P2) as coclasses no $\mathcal{R}_H$ são disjuntas duas-a-duas;
(P3) nenhuma coclasse é vazia ($\emptyset \notin \mathcal{R}_H$).

Para o (P1) tomamos um arbitrário $x \in G$ e achamos uma coclasse de H que o x esteja dentro. O (P3) já demonstramos no Exercício x11.97. Essencialmente demonstramos o (P2) também, no Exercício x11.100. Mas para variar, demonstramos que para todo $a, b \in G$,

$$Ha \cap Hb \neq \emptyset \implies Ha = Hb.$$

Tome um elemento comum $w \in Ha \cap Hb$. Logo

$$h_a a = w = h_b b \qquad \text{para alguns } h_a, h_b \in H.$$

Manipulamos a $h_a a = h_b b$ para mostrar que $Ha = Hb$. □ (Λ11.140P)

Θ11.141. Teorema. *Sejam G grupo e $H \leq G$. A família $\mathcal{R}_H = \{\, Ha \mid a \in G \,\}$ é uma partição do G e sua correspondente relação de equivalência é a congruência $\equiv_H$ módulo-direito H. Equivalentemente:*

$$G/\equiv_H \;=\; \mathcal{R}_H$$

Demonstração. Vamos denotar por $[a]$ a classe de equivalência de $a \in G$ (através da relação $\equiv_H$). Queremos demonstrar que $G/\equiv_H = \mathcal{R}_H$, ou seja

$$\{\, [a] \mid a \in G \,\} = \{\, Ha \mid a \in G \,\}.$$

Esses conjuntos são indexados pelo mesmo conjunto (o G), logo basta demonstrar que para todo $a \in G$, $[a] = Ha$. (Veja o Nota 8.149.)

($\subseteq$): Suponha $x \in [a]$. Logo $x \equiv a \pmod{H}$, ou seja, $xa^{-1} \in H$. Pela definição de Ha então temos

$$Ha \ni \underbrace{\big(xa^{-1}\big)}_{\in H} a = x\big(a^{-1}a\big) = x.$$

($\supseteq$): Suponha que $x \in Ha$. Logo $x = ha$ para algum $h \in H$ e queremos mostrar que $ha \in [a]$, ou seja $ha \equiv a \pmod{H}$. Confirmamos:

$$(ha)a^{-1} = h\big(aa^{-1}\big) = h \in H$$

e pronto. ∎

? **Q11.142. Questão.** Por que as coclasses *direitas?* Tudo até agora na nossa teoria foi justo e simétrico. Nenhuma lei de grupo e nenhum resultado que demonstramos favoreceu um lado ou o outro. Imagine se a gente tivesse conseguido, por exemplo, demonstrar a lei de cancelamento para um lado e não para o outro. Seria bizarro, pois todos os nossos dados trataram os dois lados na mesma maneira. E, até pior, nossa relação de congruência já demonstramos que é simétrica! Como pode ser então que ela favoreceu a família das coclasses direitas? Por que o $G/\equiv_H$ acabou sendo a partição $\mathcal{R}_H$ e não a $\mathcal{L}_H$?

!! SPOILER ALERT !!

Resposta. Na questão acima tem uma mentira! Tem uma coisa que usamos aqui que não tratou os dois lados em maneira igual! É a relação de congruência módulo H! No seu lado *direito* aparece o inverso dum membro do grupo. Por isso não seria justo usar a notação que temos usado! Começando agora, vamos usar a notação justa e própria

$$a \equiv b \pmod{\mathrm{R}\ H} \iff ab^{-1} \in H \iff ba^{-1} \in H.$$

? **Q11.143. Questão.** Como tu definarias (diretamente) a relação de equivalência que corresponde à partição das coclasses esquerdas?

!! SPOILER ALERT !!

D11.144. Definição (Equivalência módulo subgrupo). Seja G grupo e $H \leq G$. Definimos

$$a \equiv b \ (\mathrm{mod}_{\mathrm{L}}\ H) \overset{\text{def}}{\iff} a^{-1}b \in H; \qquad a \equiv b \ (\mathrm{mod}_{\mathrm{R}}\ H) \overset{\text{def}}{\iff} ab^{-1} \in H.$$

Usamos também as notações $a \ {}_H\!\equiv b$ e $a \equiv_H b$.

11.145. Observação. Voltando ao Teorema Θ11.141, simetricamente temos $G/_H\!\equiv = \mathcal{L}_H$, onde $\mathcal{L}_H = \{\, aH \mid a \in G \,\}$.

▸ **EXERCÍCIO x11.101.**
A operação $\langle a, b\rangle \mapsto ab^{-1}$ tá aparecendo mais e mais. Como tu chamaria essa operação binária? (x11.101 H 0)

11.146. Talvez ainda parece estranho: o que a afirmação «$ab^{-1} \in H$» tem a ver com a «os a, b pertencem à mesma coclasse direita de H»? Observe que, se a, b pertencem à mesma coclasse direita de H, então para algum $c \in G$ temos $a, b \in Hc$, e logo $a = h_a c$ e $b = h_b c$ para alguns $h_a, h_b \in H$. Vamo lá:

$$ab^{-1} \in H \iff h_a c(h_b c)^{-1} \in H \iff h_a c c^{-1} {h_b}^{-1} \in H \iff h_a {h_b}^{-1} \in H \quad \text{que é verdade.}$$

Conversamente,

$$ab^{-1} \in H \implies \big(ab^{-1}\big)b \in Hb \implies a\big(b^{-1}b\big) \in Hb \implies a \in Hb$$

e logo a, b pertencem à mesma coclasse de H: $a, b \in Hb$. Espero que ficou mais claro agora.

11.147. Atores. Fixe um $a \in G$. Como tu demonstraste no Problema Π11.1, isso determina duas funções $G \to G$, que no problema chamei de f, g. Vamos relembrá-las e dar um nome e notação especial:

D11.148. Definição (Atores). Sejam G grupo e $a \in G$. Considere as operações de "operar com a pela esquerda" e pela direita

$$\lambda x\,.\,ax \qquad\qquad \lambda x\,.\,xa.$$

que vamos chamar de *a-ator* esquerdo e direito respectivamente. As notações que vamos usar para essas funções são:

$$\begin{aligned} (a_) &: G \to G & (_a) &: G \to G \\ (a_)(x) &= ax & (_a)(x) &= xa. \end{aligned}$$

Ainda mais, para todo par de membros $a, b \in G$ temos um ator definido pela

$$\begin{aligned} (a_b) &: G \to G \\ (a_b)(x) &= axb. \end{aligned}$$

▸ **EXERCÍCIO x11.102.**
$(a_b) = (a_) \circ (_b) = (_b) \circ (a_)$. (x11.102H0)

Λ11.149. Lema. *Todos as funções-atores são bijecções.*

DEMONSTRAÇÃO JÁ FEITA NO PROBLEMA Π11.1. ∎

Λ11.150. Lema. *Todas as coclasses dum finito $H \leq G$ têm a mesma quantidade de elementos com o próprio H (e logo entre si também).*

▸ ESBOÇO. Seja $n \in \mathbb{N} = |H|$, e sejam $h_1, \ldots, h_n$ os membros de H:

$$H = \{h_1, h_2, h_3, \ldots, h_n\}\,.$$

Para qualquer $a \in G$ temos

$$Ha = \{h_1 a, h_2 a, h_3 a, \ldots, h_n a\}\,.$$

Queremos demonstrar que a quantidade dos dois conjuntos acima é a mesma. Primeiramente, como poderia ser diferente? Ambos parecem ter n elementos, mas isso não garanta cardinalidade n pois pode ter repetições no Ha. No H não pode, pois definimos o n para ser a cardinalidade de H. Basta demonstrar então que os

$$h_1 a, h_2 a, h_3 a, \ldots, h_n a$$

são distintos dois-a-dois, e logo, são n também. □ (Λ11.150P)

11.151. Observação. O Lema Λ11.150 é válido até no caso que H é infinito! Mas não se preocupe agora com isso, deixe para o Problema Π11.20.

Vamos agora generalizar a notação que usamos as coclasses de "multiplicação de subgrupo por elemento" para "multiplicação de subgrupo por subgrupo".

D11.152. Definição. Seja G grupo e $H, K \leq G$. Definimos

$$HK \stackrel{\text{def}}{=} \{\, hk \mid h \in H,\ k \in K \,\}\,.$$

▸ **EXERCÍCIO x11.103.**
Demonstre que a operação denotada por justaposição no Definição D11.152 é associativa. (x11.103H0)

? **Q11.153. Questão.** $HK = KH$? $HK \leq G$? $KH \leq G$?

• **EXEMPLO 11.154.**
No grupo S_3, sejam seus subgrupos

$$H := \{\mathrm{id}, \varphi\} \qquad\qquad K := \{\mathrm{id}, \psi\varphi\}\,.$$

Calcule os HK e KH e decida se $HK = KH$ e se HK e KH são subgrupos de S_3.

Resolução. Pela definição

$$\begin{aligned} HK &= \{\, hk \mid h\in H,\ k\in K\,\} & KH &= \{\, kh \mid h\in H,\ k\in K\,\}\\ &= \{\mathrm{id}\circ\mathrm{id}, \mathrm{id}\circ(\psi\circ\varphi), \varphi\circ\mathrm{id}, \varphi\circ(\psi\circ\varphi)\} & &= \{\mathrm{id}\circ\mathrm{id}, \mathrm{id}\circ\varphi, (\psi\circ\varphi)\circ\mathrm{id}, (\psi\circ\varphi)\circ\varphi)\}\\ &= \{\mathrm{id}, \psi\varphi, \varphi, \varphi\psi\varphi\} & &= \{\mathrm{id}, \varphi, \psi\varphi, \psi\varphi^2\}\\ &= \{\mathrm{id}, \psi\varphi, \varphi, \psi^2\} & &= \{\mathrm{id}, \varphi, \psi\varphi, \psi\}\,. \end{aligned}$$

Observamos que $HK \neq KH$ (pois, por exemplo, $\psi \in KH$ mas $\psi \notin HK$). E nenhum deles é subgrupo de S_3.

Então descobrimos que, em geral, nem $HK = KH$, nem $HK \leq G$, nem $KH \leq G$ são garantidos. Pode acontecer que $HK \leq G$ mas $KH \not\leq G$? E o que a igualdade $HK = KH$ tem a ver com a "subgrupidade" dos HK e KH? Vamos responder em todas essas perguntas com o teorema seguinte:

Θ11.155. Teorema. *Seja G grupo e subgrupos $H, K \leq G$. Então:*

$$HK = KH \iff HK \leq G$$

▸ Esboço. Para a direção ($\Rightarrow$), precisamos mostrar que HK é fechado sobre a operação e fechado sobre os inversos. Tomamos aleatórios $h_1k_1, h_2k_2 \in HK$ e aplicando as propriedades de grupo e nossa hipótese, mostramos que $(h_1k_1)(h_2k_2) \in HK$. Similarmente para os inversos: consideramos um arbitrário elemento $hk \in HK$ e mostramos que seu inverso $(hk)^{-1} \in HK$. Aqui, além da hipótese precisamos o Lema Λ11.58. Para a direção ($\Leftarrow$), mostramos as "$\subseteq$" e "$\supseteq$" separadamente, usando idéias parecidas. □ (Θ11.155P)

§253. O teorema de Lagrange

Talvez não é tão óbvio que temos já descoberto um teorema interessante! Ele é conhecido como *teorema de Lagrange*, mesmo que não foi Lagrange que o demonstrou na sua generalidade, mas apenas num caso especifico—mais detalhes nas notas históricas. Vamos formular e demonstrar o teorema, mas primeiro uma definição simples e relevante.

D11.156. Definição (Índice). Sejam G grupo e $H \leq G$. O *índice* de H no G é o número de coclasses direitas de H no G. O denotamos com os símbolos $|G : H|$ ou $i_G(H)$.

11.157. Observação. Escolhemos acima as coclasses direitas, mas isso não é essencial: escolhendo as esquerdas o número ia sempre ser o mesmo, como tu demonstrarás agora:

▸ **EXERCÍCIO x11.104.**
Sejam G grupo, $H \leq G$. Demonstre que o número de coclasses à esquerda de H é o mesmo com o número de coclasses à direita de H:

$$|\mathcal{L}_H| = |\mathcal{R}_H|\,.$$

(x11.104H0)

Θ11.158. Teorema (Lagrange). *Seja G grupo finito e $H \leq G$. Então $o(H) \mid o(G)$.*

Demonstração. Sabemos que o G pode ser particionado pelos right cosets de H, e que cada um deles tem a mesma cardinalidade $o(H)$ com o próprio H. Logo,

$$o(G) = |G : H|\, o(H),$$

e temos o que queremos demonstrar. ∎

11.159. Observação. O teorema de Lagrange então afirma que

$$|G : H| = |G| \,/\, |H| \,.$$

• **EXEMPLO 11.160 (eles não tinham nenhuma chance de ser subgrupos).** No Exemplo 11.154 achamos que

$$HK = \{\mathrm{id}, \psi\varphi, \varphi, \psi^2\} \qquad\qquad KH = \{\mathrm{id}, \varphi, \psi\varphi, \psi\} \,.$$

E afirmamos que nenhum dos dois é subgrupo do G. Por quê? Em vez de fazer o trabalho tedioso e verificar se cada um dos HK, KH é um subgrupo do S_3, observamos que cada um tem 4 elementos—verifique que são *realmente* 4. Mas, graças ao Lagrange (Θ11.158) S_3 não tem subgrupos de ordem 4, pois 4 não divide o 6. Pronto.

11.161. Corolários. Graças ao teorema de Lagrange Θ11.158 ganhamos muitos corolários diretamente, como tu vai verificar agora resolvendo os exercícios seguintes:

▸ **EXERCÍCIO x11.105.** Seja G grupo com $o(G) = p$, onde p primo. Quais são todos os subgrupos de G? (x11.105 H 1)

11.162. Corolário. *Um grupo com ordem primo não tem subgrupos não-triviais.*

Demonstrado no Exercício x11.105. ∎

11.163. Corolário. *Seja G grupo finito e $a \in G$. Então $o(a) \mid o(G)$.*

Demonstrarás no Exercício x11.106. ∎

Já resolveste o Problema Π11.12? O próximo corolário oferece uma resolução mais elegante:

11.164. Corolário. *Seja G grupo finito e $a \in G$. Então $a^{o(G)} = e$.*

Demonstrarás no Exercício x11.107. ∎

▸ **EXERCÍCIO x11.106.** Demonstre o Corolário 11.163. (x11.106 H 1 2 3)

▸ **EXERCÍCIO x11.107.** Demonstre o Corolário 11.164. (x11.107 H 1)

11.165. A idéia atrás do teorema de Lagrange. Temos um grupo finito G, e um subgrupo $H \leq G$. Vamos conseguir arrumar *todos os membros de* G numa tabela:

$$\begin{array}{ccccc} \bullet & \bullet & \bullet & \dots & \bullet \\ \bullet & \bullet & \bullet & \dots & \bullet \\ \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \\ \bullet & \bullet & \bullet & \dots & \bullet \end{array}$$

Sua primeira linha será feita por todos os membros de H. Sabendo que G é finito, temos que H também é, e logo essa primeira linha será finita também. Vamos chamar n a $o(H)$, e logo $h_1, \dots, h_n$ os n membros de H. Então a primeira linha tem tamanho n, e é a seguinte:

$$\begin{array}{lccccc} H: & h_1 & h_2 & h_3 & \dots & h_n \end{array}$$

Vamos mostrar como botar o resto dos membros de G nessa tabela. Na verdade, tem uma chance que não tem mais elementos para botar: isso acontece se $H = G$. Nesse caso não temos mais nada pra fazer, já conseguimos o que queríamos. Mas, no caso geral, existem membros de G fora do H. Seja $a \in G$ um deles, ou seja, $a \notin H$. Agora bota todos os elementos seguintes na tabela:

$$\begin{array}{lccccc} H: & h_1 & h_2 & h_3 & \dots & h_n \\ Ha: & h_1a & h_2a & h_3a & \dots & h_na \end{array}$$

Agora *afirmamos* sobre os elementos novos que:

- eles são realmente n, ou seja, distintos dois-a-dois;
- eles são realmente novos, ou seja, nenhum deles é igual àlgum dos membros que já estava na tabela.

Se demonstrar essas afirmações, saberemos que temos exatamente $2n$ membros de G já arrumados na nossa tabela. E depois? Caso que G não tenha mais elementos, não temos nada mais pra fazer, pois já conseguimos o que queríamos. Caso que tenha membros de G fora deles, seja $a' \in G$ um deles, ou seja, a' não é nenhum dos membros já listados. E agora bota todos os elementos seguintes na tabela:

$$\begin{array}{lccccc} H: & h_1 & h_2 & h_3 & \dots & h_n \\ Ha: & h_1a & h_2a & h_3a & \dots & h_na \\ Ha': & h_1a' & h_2a' & h_3a' & \dots & h_na' \end{array}$$

Novamente, *afirmamos* sobre os elementos novos que:

- eles são realmente n;
- eles são realmente novos.

E por aí vai. Sabemos que o processo vai terminar depois duma quantidade finita de passos, pois o G é finito. Quando terminar então, teriamos conseguido arrumar todos os seus membros numa tabela de largura n e altura igual à quantidade de coclasses direitas do H no G, ou seja, altura $m := |G : H|$.

$$\begin{array}{lccccc} H: & h_1 & h_2 & h_3 & \dots & h_n \\ Ha: & h_1a & h_2a & h_3a & \dots & h_na \\ Ha': & h_1a' & h_2a' & h_3a' & \dots & h_na' \\ \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \\ Ha'': & h_1a'' & h_2a'' & h_3a'' & \dots & h_na'' \end{array}$$

A única coisa que basta fazer então, é demonstrar todas as afirmações que deixamos sem demonstração acima. Mudando os nomes dos $a, a', \dots, a''$ para $a_2, a_3, \dots, a_m$, queremos demonstrar para quaisquer $i, j \in \{2, \dots, m\}$ as seguintes:[84]

(1) $h_1a_i, h_2a_i, \dots, h_na_i$ são realmente n, ou seja, distintos dois-a-dois;
(2) $h_1a_i, h_2a_i, \dots, h_na_i$ são realmente novos, ou seja:
  (2.a) nenhum deles é igual àlgum dos $h_1, h_2, \dots, h_n$;
  (2.b) nenhum deles é igual àlgum dos $h_1a_j, h_2a_j, \dots, h_na_j$ para $j < i$.

Nenhuma delas é difícil pra demonstrar—na verdade, *nos já demonstramos* todas.[85] Mesmo assim, bora demonstrá-las novamente aqui com uns one-liners:

(1) $$h_ua_i = h_va_i \implies h_u = h_v \implies u = v;$$
(2a) $$h_ua_i = h_v \implies a_i = {h_u}^{-1}h_v \implies a_i \in H, \text{ que é absurdo;}$$
(2b) $$h_ua_i = h_va_j \implies a_i = {h_u}^{-1}h_va_j \implies a_i \in Ha_j, \text{ que é absurdo.}$$

Pronto!

! **11.166. Aviso.** Não seja tentado para aplicar o "recíproco"; sabendo que $d \mid o(G)$, *não podemos concluir* que o G possui subgrupos de ordem d (Problema Π11.17)

▸ **EXERCÍCIO x11.108 (dividindo o grupo aditivo dos inteiros).**
Qual é o índice do $(4\mathbb{Z}\,;+) \leq (\mathbb{Z}\,;+)$? Generalize para o $m\mathbb{Z}$. (x11.108 H 0)

▸ **EXERCÍCIO x11.109 (dividindo o grupo aditivo dos reais).**
Qual o $|(\mathbb{Z}\,;+) : (\mathbb{R}\,;+)|$? (x11.109 H 0)

§254. Teoria dos números revisitada

▸ **EXERCÍCIO x11.110.**
Seja p primo e defina $\mathcal{Z}_p = (\overline{p} \setminus \{0\}\,;\cdot)$ onde $(\cdot)$ é a multiplicação módulo p. Mostre que $\mathcal{Z}_p$ é um grupo e ache sua ordem. (x11.110 H 0)

▸ **EXERCÍCIO x11.111.**
Seja $n \in \mathbb{N}$ com $n > 1$ e defina $\mathcal{Z}_n = (\{\, a \in \overline{n} \mid (a, n) = 1 \}\,;\cdot)$ onde $(\cdot)$ é a multiplicação módulo n. Mostre que $\mathcal{Z}_n$ é um grupo e ache sua ordem. (x11.111 H 0)

Já estamos em posição de ganhar o "Fermatinho" (Fermatinho (Θ3.192)) e sua generalização, o teorema de congruências de Euler Θ3.217 como um corolário fácil das nossas novas ferramentas grupoteóricas.

[84] Talvez parece estranha a escolha de índices que começa com $_2$, mas é muito conveniente aqui, pois o índice final $_m$ já seria a própria altura da tabela. Se ficou triste pela falta do a_1, tome $a_1 := e$ e vai dar certo: a primeira coclasse de H (o próprio H), seria o Ha_1 nesse caso. Mas nada disso é necessário!

[85] A (1) é o Lema Λ11.150; a (2) é o (ii) do Λ11.140.

11.167. Corolário (Teorema de Euler). *Sejam $a, m \in \mathbb{Z}$ com $(a, m) = 1$. Então*

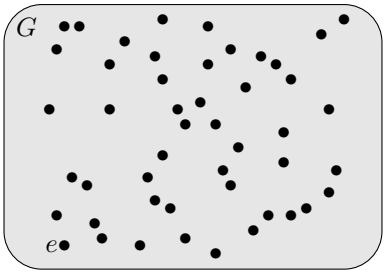
$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

▸ Esboço. Conseqüência do teorema de Lagrange Θ11.158 graças ao Exercício x11.111. □

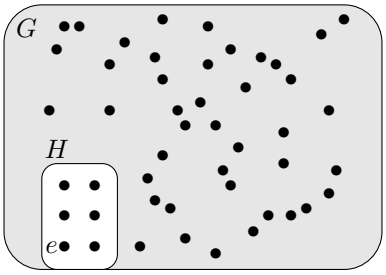
Ainda mais resultados podem ser derivados como corolários do teorema de Lagrange: no Problema Π11.18 por exemplo tu ganhas o fato que tem uma infinidade de primos (teorema de Euclides, Θ3.136).

§255. O grupo quociente

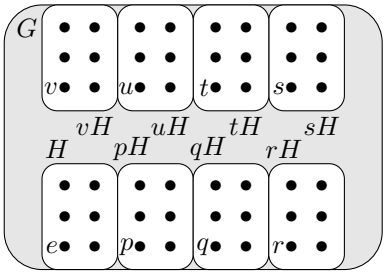
11.168. Assim que tiver um subgrupo.... Vamos começar com um certo grupo G, bagunçado assim:

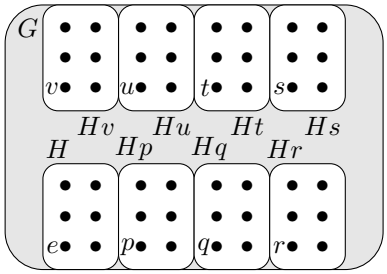


Identificamos nele um subgrupo $H \leq G$:



Assim que fizermos isso, o grupo toda se arruma em dua maneiras, uma a partir das coclasses esquerdas e uma a partir das direitas:

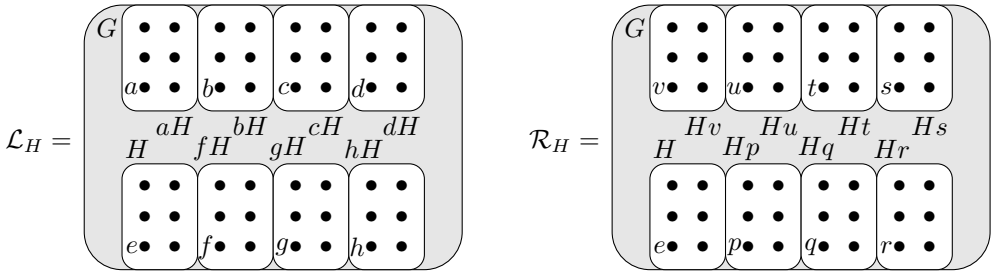
$\mathcal{L}_H =$ 

$\mathcal{R}_H =$ 

? **Q11.169. Questão.** Tem algo errado na figura acima. O que é?

!! SPOILER ALERT !!

Resposta. Não sabemos que cada um dos representantes que desenhamos na partição $\mathcal{L}_H$ vai acabar sendo um representante da correspodente coclasse direita. Pode ser, por exemplo que o $q \in Hp$, e logo $Hp = Hq$. Para formar a partição escolhemos cada vez um membro fora das coclasses que já formamos, mas ninguém garanta que andando pelas coclasses esquerdas e escolhendo os p, q, r, s, t, u, v, vamos conseguir escolher os mesmos como representantes das coclasses direitas. Em geral então, a imagem deve ser alterada para usar nomes diferentes nos representantes, por exemplo:



- **EXEMPLO 11.170.**
  Considere o subgrupo $K \leq S_3$:
  $$K := \{\mathrm{id}, \psi\varphi\}\,.$$
  Calcule todos os left e right cosets de K no S_3, e decida se as duas colecções são iguais. Resolução. Queremos calcular primeiramente todas as coclasses de K. Como $o(K) = 2$, e o G tem 6 membros em total, sabemos que o K tem 3 coclasses esquerdas, e 3 coclasses direitas:

esquerdas:	$K = \{\mathrm{id}, \psi\varphi\}$	$? K = \{?, ?\}$	$? K = \{?, ?\}$
direitas:	$K = \{\mathrm{id}, \psi\varphi\}$	$K ? = \{?, ?\}$	$K ? = \{?, ?\}$

  Vamos escolher o primeiro representante para escrever a primeira coclasse esquerda "própria" de K. Temos 4 opções, pois se escolher qualquer um dos dois membros do K, vamos "cair" na mesma coclasse K. Escolhemos o ψ. Calculamos:
  $$\psi K = \{\psi, \psi\psi\varphi\} = \{\psi, \psi^2\varphi\} = \{\psi, \varphi\psi\}\,.$$
  Observe que seria a mesma coclasse esquerda, se tivemos escolhido o $\varphi\psi$. Vamos calcular a última. Qual seria o represetante agora? Precisamos evitar todos os membros de K e de ψK. Vamos escolher o φ, e bora calular o φK. Ou não? Não precisamos fazer nenhum cálculo, pois so sobraram 2 membros de S_3, então esses 2 formam a última coclasse esquerda:
  $$\varphi K = \{\varphi, \psi^2\}\,.$$

Basta calcular as coclasses direitas agora. Para a primeira, escolhemos de novo o ψ, já que observamos que $\psi \notin K$. Calculamos:

$$K\psi = \{\psi, \psi\varphi\psi\} = \{\psi, \varphi\}\,.$$

Qual seria o representante ta próxima? Aqui não pode ser novamente o φ, pois o φ apareceu no $K\psi$. Escolhemos um dos dois restantes então, vamos tomar o ψ^2, e junto com o último restante ele forma a última coclasse direita:

$$K\psi^2 = \left\{\psi^2, \varphi\psi\right\}.$$

Finalmente achamos todas:

$$\mathcal{L}_K = \left\{ \begin{array}{r} K = \{\mathrm{id}, \psi\varphi\}\,, \\ \psi K = \{\psi, \varphi\psi\}\,, \\ \varphi K = \left\{\varphi, \psi^2\right\} \end{array} \right\} \qquad\qquad \mathcal{R}_K = \left\{ \begin{array}{r} K = \{\mathrm{id}, \psi\varphi\}\,, \\ K\psi = \{\varphi, \psi\}\,, \\ K\psi^2 = \left\{\psi^2, \varphi\psi\right\} \end{array} \right\}.$$

Para responder na pergunta, precisamos comparar as duas *colecções*, ou seja a pergunta é:

$$\{K, \psi K, \varphi K\} \stackrel{?}{=} \left\{K, K\psi, K\psi^2\right\}$$

e facilmente observamos que não são iguais, pois, por exemplo, ψK não é igual a nenhuma das coclasses direitas, algo que verificamos comparando o conjunto ψK com cada um dos conjuntos $K, K\psi, K\psi^2$.

▸ **EXERCÍCIO x11.112.**
Calcule todas as coclasses esquerdas e direitas dos

$$H := \{\mathrm{id}, \varphi\} \qquad\qquad N := \left\{\mathrm{id}, \psi, \psi^2\right\}$$

Quantas coclasses direitas diferentes cada um deles tem? Quantas esquerdas? Explique sua resposta. A família $\mathcal{R}_H$ de todas as coclasses direitas de H é igual à família $\mathcal{L}_H$ de todas as esquerdas? Similarmente para as K e N. (x11.112H0)

D11.171. Notação. Observe que definimos os aH, Ha, e HK, num grupo G para *subgrupos* $H, K \leq G$. Mas não usamos nenhuma propriedade de subgrupo mesmo. Podemos realmente estender essa notação para arbitrários *subconjuntos* de G, e, por que não, até usar notação como a seguinte abominagem:

$$g_1ABg_2Bg_3{}^{-1}Ag_1CB \stackrel{\text{def}}{=} \left\{\, g_1abg_2b'g_3{}^{-1}a'g_1cb'' \;\middle|\; a, a' \in A,\ b, b', b'' \in B,\ c \in C \,\right\}$$

dados $g_1, g_2, g_3 \in G$ e $A, B, C \subseteq G$. Observe primeiramente que *precisamos* usar variáveis diferentes para cada instância de elemento de A, etc. Observe também que todos esses objetos que escrevemos justaposicionando elementos e subconjuntos de G são subconjuntos de G se usamos pelo menos um subconjunto de G na expressão:

$$g_1abg_5ab' \in G \qquad\qquad g_1aBg_5ab' \subseteq G.$$

Finalmente, *confira* que graças à associatividade da operação do grupo G, não precisamos botar parenteses:

$$g_1ABg_2Bg_3{}^{-1}Ag_1CB = g_1A(Bg_2B)g_3{}^{-1}(Ag_1CB) = (g_1A)(Bg_2)(Bg_3{}^{-1})(Ag_1)(CB) = \cdots$$

etc.

D11.172. Definição (Subgrupo normal). Seja G grupo e $N \leq G$. O N é um *subgrupo normal* de G sse a família das suas coclasses esquerdas e a das suas coclasses direitas são iguais. Em símbolos,

$$N \trianglelefteq G \overset{\text{def}}{\iff} \mathcal{L}_N = \mathcal{R}_N.$$

▸ **EXERCÍCIO x11.113.**
Se $H \leq G$ num G abeliano, então $H \trianglelefteq G$. (x11.113H0)

▸ **EXERCÍCIO x11.114.**
Se $H \leq G$ de índice 2, então $H \trianglelefteq G$. (x11.114H0)

11.173. Acabamos de identificar certos subgrupos dum grupo G—que chamamos *normais*—com uma propriedade legal: a colecção de todas as suas coclasses esquerdas é a mesma com a colecção de todas as suas coclasses direitas. (Na verdade a situação é bem mais legal que isso—continue lendo.) Começando então com um $N \trianglelefteq G$, podemos falar *da* partição correspondente de G, sem especificar se estamos considerando a colecção das coclasses esquerdas ou das direitas. Ou seja, nesse caso, as relações de equivalência

$$- \equiv - \pmod{_{\mathrm{L}}\ N} \qquad \text{e} \qquad - \equiv - \pmod{_{\mathrm{R}}\ N}$$

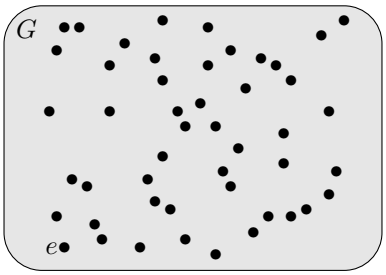
são a *mesma* relação:

D11.174. Definição (congruência módulo subgrupo). Sejam G grupo e $N \trianglelefteq G$. Definimos a relação binária

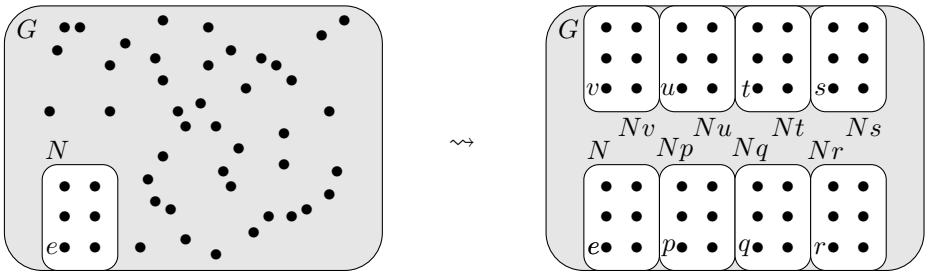
$$- \equiv - \pmod{N}$$

que chamamos de *congruência módulo* N.

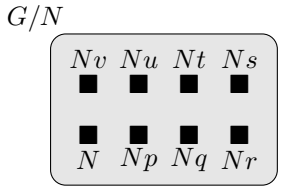
11.175. Assim que tiver um subgrupo normal.... Vamos começar com um certo grupo G:



Agora identificamos nele um subgrupo *normal* $N \trianglelefteq G$. Assim que fizermos isso, todo o G se arruma graças à partição de todas as coclasses de N:



E agora comece se afastar mais e mais, até não dá mais pra ver os pontinhos *dentro* dessas classes, e até as próprias classes viram pontinhos:



Denotamos esse conjunto por G/N:

$$G/N = \{\, Ng \mid g \in G \,\}$$

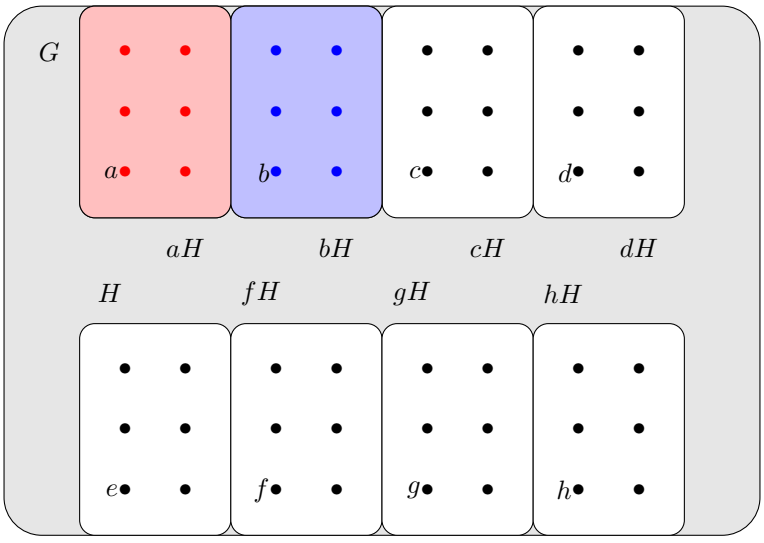
Observe que esse conjunto é o *conjunto quociente* de G através da relação de congruência módulo N.[86]

11.176. E daí?. Isso é válido mesmo se o N não fosse normal: podemos definir os (dois) conjuntos quocientes $G/_N\!\equiv$ e $G/\!\equiv_N$. Mas assim estamos esquecendo *a alma* do G: o G é um *grupo*. Desde o Capítulo 10 (D10.89) sabemos que podemos dividir um *conjunto* (por uma relação de equivalência) e o resultado (quociente) é novamente o mesmo tipo de coisa: *conjunto*. Aqui dividimos um *grupo* e o quociente foi o quê? A melhor coisa que podemos dizer é... *conjunto!* Péssimo! O resultado perdeu seu alma! Por isso os subgrupos normais são *muito* legais: o quociente retenha a alma do grupo original!

11.177. O que exatamente é o problema?. Suponha então que temos um $H \leq G$. Gostariamos de definir a operação $*$ no $G/_H\!\equiv$ em tal forma que

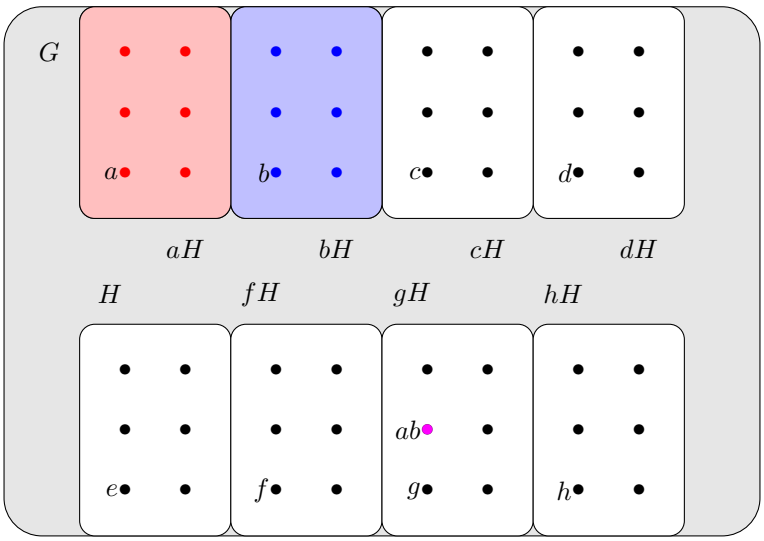
$$aH * bH \overset{\text{"def"}}{=} (a *_G b)H.$$

O problema é que a operação $*$ que estamos tentando definir não tem acesso nos a, b das suas entradas aH, bH respectivamente, e logo o seu valor $aH * bH$ não pode depender das escolhas desses representantes. Ou seja, *não temos como demonstrar que* $*$ *é bem-definida*, e logo *não podemos usar a igualdade acima como definição de operação*—por isso o $\overset{\text{"def"}}{=}$. Voltando no desenho anterior a situação ficará mais clara; vou pintar todos os membros da aH de vermelho e todos os membros da bH de azul:

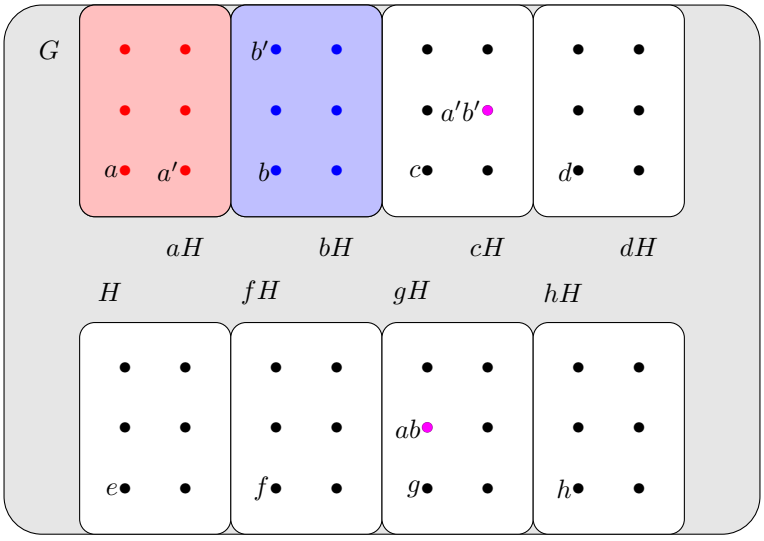


[86] Lembra-se que dada qualquer relação de equivalência num conjunto, definimos seu conjunto quociente? Não?! Corra para a Definição D10.89.

Querendo usar a "definição" da operação $*$ acima escolhemos o $a \in aH$ e o $b \in bH$ e procuramos o $a *_G b$; vamos dizer que achamos aqui no gH:

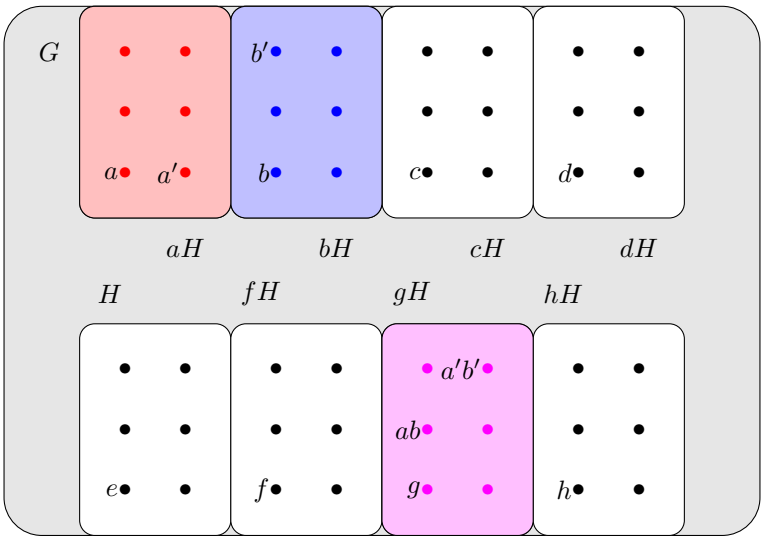


agora escolhendo *outros representantes* a', b' das aH, bH (onde pelo menos uma das $a' \neq a$ e $b' \neq b$ é válida) procuramos o $a' *_G b'$. O que acontece se ele não pertence à mesma coclasse gH? Talvez caiu na cH:



Assim a $*$ *não é bem-definida* (e logo o $G/_{H\equiv}$ não tem nenhuma chance de virar grupo com ela. É exatamente isso que aproveitamos nos subgrupos *normais:* eles não deixam isso acontecer, pois garantam que o produto de quaisquer representantes das aH, bH vai sempre cair dentro da mesma coclasse, e logo apenas a gH será pintada roxa aqui no

nosso desenho



e logo aqui teriamos

$$aH * bH = gH \quad \big(= (ab)H\big).$$

! **11.178. Cuidado.** Caso que o problema de não ser bem-definida não é óbvio, primeiramente volte a re-estudar os: Cuidado 9.53 e Cuidado 9.55. Agora observe que o aH é na verdade um membro a de G *operado* com um subgrupo H de G; e isso resulta num certo subconjunto de G: uma coclasse (esquerda) de H.

Então: as entradas da $*$ são coclasses esquerdas de H, por exemplo podem ser as

$$aH =: \{a, a_1, a_2, a_3, a_4, a_5\} \qquad bH =: \{b, b_1, b_2, b_3, b_4, b_5\}$$

e agora

$$\{a, a_1, a_2, a_3, a_4, a_5\} * \{b, b_1, b_2, b_3, b_4, b_5\} =?$$

Observe que aqui temos

$$aH = a_1H = \cdots = a_5H \qquad bH = b_1H = \cdots = b_5H.$$

Parece então que tentamos definir a $*$ pela

$$A * B = (ab)H, \quad \text{onde } a \text{ é algum membro de } A \text{ e } b \text{ de } B$$

mas para essa ser uma definição de função mesmo temos uma tarefa para fazer: *precisamos demonstrar que seu valor $A * B$ não depende das escolhas desses "representantes" a e b* (Cuidado 9.55). Até conseguir demonstrar isso, não podemos considerar a $*$ uma função *bem-definida*. Vamos voltar se preocupar com o mesmo tipo de coisa logo no Cuidado 11.225.

? **Q11.179. Questão.** Como podemos definir uma operação interessante $*$ nos elementos de G/N, tal que o $(G/N\ ;\ *)$ vira um grupo? Qual seria sua identidade? Para cada um dos seus membros, qual seria o seu inverso? Para cada dois dos seus membros, qual seria o seu produto?

!! SPOILER ALERT !!

D11.180. Definição (Grupo quociente). Sejam G grupo e $N \trianglelefteq G$. O conjunto

$$G/\equiv_N \quad \Big(= \underbrace{\{\, aN \mid a \in G \,\}}_{\mathcal{L}_N} = \underbrace{\{\, Na \mid a \in G \,\}}_{\mathcal{R}_N}\Big)$$

com operação a $*$ definida pela

$$Na * Nb \stackrel{\text{def}}{=} N(ab)$$

é chamado o *grupo quociente de G módulo N*, e é denotado por G/N. ↯

? **Q11.181. Questão.** Tá tudo bem com a Definição D11.180?

!! SPOILER ALERT !!

Resposta. A operação $*$ não é automaticamente "bem-definida" (como discutimos no Cuidado 11.178): precisamos demonstrar que realmente seu valor não depende da escolha dos representantes a e b. Falei "precisamos"? Quis dizer *precisas*. Agora:

▸ **EXERCÍCIO x11.115.**
Demonstre que a $*$ definida acima é bem-definida. (x11.115H123)

TODO Sobre bem-definido por argumento

Λ11.182. Lema. *Sejam G grupo, $N \trianglelefteq G$, e $a, b \in G$.*

$$(Na) * (Nb) = (Na)(Nb) \quad \Big(= \{\, uv \mid u \in Na, v \in Nb \,\}\Big)$$

▸ Esboço. Como $(Na) * (Nb) = N(ab)$, mostramos cada direção da

$$g \in (Na)(Nb) \iff g \in N(ab)$$

separadamente. Sem detalhes, temos

$$\begin{aligned} g \in (Na)(Nb) &\implies g = (n_a a)(n_b b) \\ &\implies g = n_a(a n_b) b \\ &\overset{(\trianglelefteq)}{\implies} g = n_a(n'_b a) b \\ &\implies g = \underbrace{(n_a n'_b)}_{\in N}(ab) \\ &\qquad\qquad \in N(ab) \end{aligned}$$

$$\begin{aligned} g \in N(ab) &\implies g = n(ab) \\ &\implies g = \underbrace{\underbrace{(na)}_{\in Na}\underbrace{b}_{\in Nb}}_{\in (Na)(Nb)} \end{aligned}$$

onde os nomes das variáveis introduzidas devem indicar uns dos detalhes omitidos. □ (Λ11.182P)

Para merecer esse nome, o G/N deve ser um grupo mesmo. Vamos demonstrar isso agora.

Θ11.183. Teorema. *Sejam G grupo e $N \trianglelefteq G$. O G/N é um grupo.*

▸ Esboço. Graças ao Critérion 11.64, basta verificar que G/N com sua operação (Definição D11.180) satisfaz uma definição unilateral de grupo: (G0), (G1), (G2L), (G3L). Observe que o G/N é indexado pelo N, e logo para solicitar um membro arbitrário do G/N, basta tomar um arbitrário membro $a \in N$.
(G0): Sejam $a, b \in N$. Realmente $(Na)(Nb) = N(ab) \in G/N$.
(G1): Sejam $a, b, c \in N$. Calculando verificamos que $((Na)(Nb))(Nc) = (Na)((Nb)(Nc))$.
(G2L): Procuramos um membro de G/N que satisfaz a lei de identidade esquerda. O candidato óbvio é o próprio $N = Ne$. Basta confirmar essa afirmação, ou seja, mostrar que para todo $a \in N$, temos $N(Na) = Na$.
(G3L): Para mostrar que cada um dos membros de G/N tem um inverso esquerdo, seje $a \in N$ e mostre como achar um inverso esquerdo de $Na \in G/N$. Aqui o candidato que faz sentido considerar é o $N(a^{-1})$. □ (Θ11.183P)

Seria importante se convencer que essa coisa legal realmente não é compartilhada por subgrupos não-normais. Faça agora o:

▸ **EXERCÍCIO x11.116.**
Mostre que para qualquer $H \not\trianglelefteq G$ as ${}_H{\equiv}$ e $\equiv_H$ não são congruências e logo nenhum dos $G/{}_H{\equiv}$ $G/{\equiv_H}$ pode virar um grupo com a alma do G. (x11.116H0)

11.184. Congruências. Teve mais algo dessatisfatório com as relações ${}_H{\equiv}$ e $\equiv_H$ baseadas num $H \leq G$, mesmo que ambas são relações de equivalência sim! Eles não são garantidas pra ser... *congruências:*

D11.185. Definição (congruência (em grupo)). Uma relação de equivalência $\sim$ num grupo $\mathcal{G} = (G\,; *, {}^{-1}, e)$ é uma *congruência* de G sse $\sim$ é *compatível com a estrutura* do $\mathcal{G}$:

$$\begin{gathered} (\forall a, b, a', b' \in G)\big[\, a \sim b \;\&\; a' \sim b' \implies a * a' \sim b * b' \,\big] \\ (\forall a, b \in G)\big[\, a \sim b \implies a^{-1} \sim b^{-1} \,\big] \\ e \sim e. \end{gathered}$$

11.186. Observação. Observe que a última linha não oferece absolutamente nada na definição de *congruência* pois a $\sim$ sendo relação de equivalência é reflexiva.

11.187. Corolário. *Se $N \trianglelefteq G$ então $\equiv_N$ é uma congruência.*

Demonstrado no Exercício x11.115. ∎

▸ **EXERCÍCIO x11.117.**
Mostre grupo G e $H \leq G$ tais que ${}_H\!\equiv$ e $\equiv_H$ não são congruências. (x11.117H0)

§256. Subgrupos normais

Na Secção §255 definimos os *subgrupos normais* como aqueles cujas coclasses esquerdas e direitas formam a mesma partição. Aqui encontramos umas definições equivalentes que superficialmente parecem bastante diferentes.

D11.188. Definição (definições de normal). As afirmações seguintes são equivalentes (e logo cada uma pode servir como definição de $N \trianglelefteq G$):

$$N \trianglelefteq G \overset{\text{def}}{\iff} N \leq G \ \&\ \text{qualquer uma das:} \begin{cases} \text{(i)}\ \mathcal{L}_N = \mathcal{R}_N \\ \text{(ii)}\ {}_N\!\equiv = \equiv_N \\ \text{(iii)}\ N \text{ é fechado pelos conjugados} \\ \text{(iv)}\ (\forall g \in G)\big[\, gNg^{-1} \subseteq N \,\big] \\ \text{(v)}\ (\forall g \in G)\big[\, gNg^{-1} = N \,\big] \\ \text{(vi)}\ (\forall g \in G)[\, gN = Ng \,], \end{cases}$$

lembrando que $\mathcal{L}_N$ e $\mathcal{R}_N$ são as colecções de left e right cosets de N respectivamente (Definição D11.139), e ${}_N\!\equiv$ e $\equiv_N$ as equivalências módulo-esquerdo e módulo-direito N respectivamente (Definição D11.144). Se demonstrar tudo isso—algo que vamos fazer junto logo—seria massa pois: cada vez que vamos ter como dado que $N \trianglelefteq G$, a gente vai ganhar *toda* essa afirmação de graça; e dualmente, cada vez que vamos querer demonstrar que $N \trianglelefteq G$, a gente vai ter a liberdade de escolher qualquer uma dessas e pronto!

▸ **EXERCÍCIO x11.118.**
Qual dessas não faria sentido escolher nunca querendo demonstrar que $N \trianglelefteq G$? (x11.118H1)

11.189. Fechado pelos quê?. O que significa *fechado pelos conjugados?* Significa *fechado sob a relação de conjugação*; em símbolos:

$$(\forall n \in N)[\,\text{todos os conjugados do } n \text{ pertencem ao } N\,]$$

ou seja,

$$(\forall n \in N)(\forall g \in G)\big[\, gng^{-1} \in N \,\big].$$

11.190. Observação (trocando a ordem dos quantificadores). Observe que podemos trocar a ordem dos quantificadores pois são do mesmo tipo:

$$(\forall n \in N)(\forall g \in G)\big[\, gng^{-1} \in N \,\big] \iff (\forall g \in G)\underbrace{(\forall n \in N)\big[\, gng^{-1} \in N \,\big]}_{gNg^{-1} \subseteq N}.$$

Vamos dar uma olhada detalhada agora, caso que a parte sublinhada acima pareceu estranha. Lembre-se como tomamos membros arbitrários dum conjunto indexado (Observação 8.148 e Aviso 11.136). Demonstrando a afirmação

$$(\forall n \in N)\big[\,\text{algo sobre o } gng^{-1}\,\big]$$

ganhamos que todos os membros do gNg^{-1} satisfazem esse algo, pois o conjunto gNg^{-1} é indexado por o N. Aqui o algo é o «pertencer ao N». Ou seja:

$$(\forall n \in N)\big[\, gng^{-1} \in N \,\big]$$

afirma que todos os membros de gNg^{-1} pertencem ao N, ou seja, $gNg^{-1} \subseteq N$.

Θ11.191. Teorema. *Sejam G grupo, e $N \leq G$. Os (i)–(vi) da Definição D11.188 são equivalentes.*

Demonstração. (i) ⇔ (ii). Demonstrado no Capítulo 10 (veja Nota 10.97).
(iii) ⇔ (iv). Demonstrado no Observação 11.190.
(iv) ⇔ (v). A (⇐) é trivial, pois o que precisamos demonstrar ($N \trianglelefteq G$) é obviamente uma afirmação mais fraca da nossa hipótese. Para a (⇒), suponha $N \trianglelefteq G$ e seja $g \in G$. Já temos a inclusão $gNg^{-1} \subseteq N$, então só basta demonstrar a $N \subseteq gNg^{-1}$. Seja $n \in N$. Como $n \in N$ e N normal, temos $g^{-1}n\big(g^{-1}\big)^{-1} \in N$. Logo

$$\underbrace{g\Big(g^{-1}n\big(g^{-1}\big)^{-1}\Big)g^{-1}}_{=n} \in gNg^{-1}.$$

(iii) ⇒ (vi) Tome $n \in N$; assim gng^{-1} é um arbitrário membro do gNg^{-1}. Basta mostrar que $gng^{-1} \in N$. Mas $gn \in gN = Ng$ e logo $gn = n'g$ para algum $n' \in N$. Calculamos:

$$gng^{-1} = n'gg^{-1} = n' \in N.$$

As outras implicações são pra ti: Exercício x11.120. ∎

Um corolário bem útil da (vi) é o seguinte:

11.192. Corolário. *Sejam G grupo, $N \trianglelefteq G$. Para todo $A \subseteq G$, $AN = NA$.*

Demonstração. Numa linha só:

$$AN = \bigcup_{a \in A} aN = \bigcup_{a \in A} Na = NA.$$

∎

! **11.193. Cuidado.** Se tivemos $N \trianglelefteq G$ temos sim que $gng^{-1} \in N$ para todo $n \in N$, mas isso *não garanta* que $gng^{-1} = n$ não! Sabemos que para todo $n \in N$, temos $gng^{-1} = n'$ *para algum* $n' \in N$, mas nada nos permite concluir que esse n' é nosso n. Isso quis dizer que em geral não podemos demonstrar que

$$\left(gng^{-1} \mid n \in N \right) = \left(n \mid n \in N \right)$$

como famílias indexadas por o mesmo conjunto N, mas mesmo assim conseguimos demonstrar que os *conjuntos* são iguais sim:

$$\left\{ gng^{-1} \mid n \in N \right\} = \left\{ n \mid n \in N \right\},$$

ou seja,

$$gNg^{-1} = N.$$

Parecidamente, sabendo que $gN = Ng$ e tendo um $n \in N$, *não* podemos concluir que $gn = ng$, mas pelo menos sabemos que

$$gn = n'g, \quad \text{para algum } n' \in N.$$

▸ **EXERCÍCIO x11.119.**
Ache um contraexemplo que mostra que não necessariamente $gng^{-1} = n$, mesmo com $n \in N \trianglelefteq G$. (x11.119H0)

▸ **EXERCÍCIO x11.120.**
Demonstre o que falta para estabelecer que todas as (i)–(vi) do Teorema Θ11.191 são equivalentes. (x11.120H0)

▸ **EXERCÍCIO x11.121.**
Se $S \leq G$ e $N \trianglelefteq G$, então $SN \leq G$. (x11.121H12)

▸ **EXERCÍCIO x11.122.**
Se $S \leq G$ e $N \trianglelefteq G$, então $S \cap N \trianglelefteq S$. (x11.122H1)

Intervalo de problemas

▸ **PROBLEMA Π11.17.**
Justifique o Aviso 11.166: mostre um grupo G e um divisor $d \mid o(G)$ tal que G não possui nenhum subgrupo de ordem d. (Π11.17H0)

▸ **PROBLEMA Π11.18 (Teorema de Euclides).**
Mostre como demonstrar o teorema de Euclides Θ3.136 como um corolário de Lagrange. (Π11.18H123)

▸ **PROBLEMA Π11.19 (Teorema de Wilson).**
Demonstre o teorema de Wilson

$$n \text{ é primo} \iff (n-1)! \equiv -1 \pmod{n}$$

usando o conhecimento da teoria dos grupos até agora. (Π11.19H0)

▸ **PROBLEMA Π11.20.**
Demonstre o Lema Λ11.150 mesmo quando H é infinito. (Π11.20H1234)

▸ **PROBLEMA Π11.21.**
Seja G grupo e $N \leq G$ tal que ${}_N\!\equiv$ ou $\equiv_N$ é uma congruência (Definição D11.185). A afirmação $N \trianglelefteq G$ é correta? Responda «sim» e demonstre; ou «não» e refuta; ou «talvez» e mostre um exemplo e um contraexemplo. (Π11.21H0)

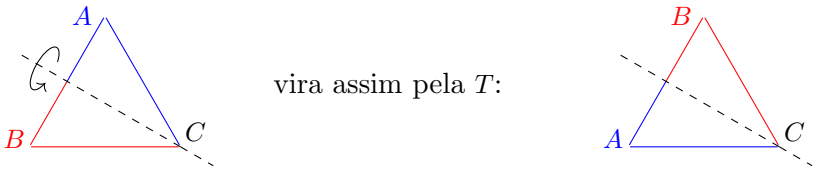
▸ **PROBLEMA Π11.22.**
Sejam G grupo e $N, M \trianglelefteq G$. Afirmação:

$$NM \trianglelefteq G.$$

Se a afirmação é demonstrável demonstre; se é refutável refute; caso contrário mostre que não é nem demonstrável nem refutável. (Π11.22H12)

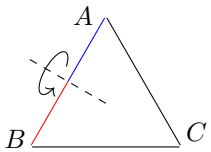
§257. Simetrias

• **EXEMPLO 11.194.**
A transformação T que gira o triangulo por volta do eixo mostrado por um ângulo π, é uma simetria do triangulo.

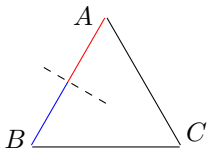


11.195. O que é uma simetria (1). Ok, então «simetria» é uma *transformação* que leva uma forma geométrica para outra, tal que o resultado fica exatamente em cima da forma original: se desenhar a forma-depois em cima da forma-antes, cada ponto da forma-depois vai cair em cima dum ponto da forma-antes. Isso é bem informal, mas nosso objectivo não é estudar simetrias geométricas neste momento, apenas dar uma intuição com "palavras da rua" então essa descripção deve servir para nos guiar. Mas isso *não é suficiente* para chamar uma transformação de simetria.

• **NÃOEXEMPLO 11.196.**
Considere a transformação T' que deixa todos os pontos dos lados AB e AC em paz, mas vira todos os pontos do interior do BC para a outra direção:



vira assim pela T':



? **Q11.197. Questão.** O que tu adicionaria na "definição" de simetria acima para excluir transformações como essa do Nãoexemplo 11.196?

!! SPOILER ALERT !!

11.198. O que é uma simetria (2). Observe que existe uma diferença importante entre a transformação do Exemplo 11.194 e aquela do Nãoexemplo 11.196: a primeira *preserva as distâncias*, a segunda não. Vamos chamar as transformações T e T' respectivamente. Tome quaisquer dois pontos x, y no triângulo, e meça sua distância $d(x, y)$. A transformação T garanta que

$$d(x, y) = d(Tx, Ty)$$

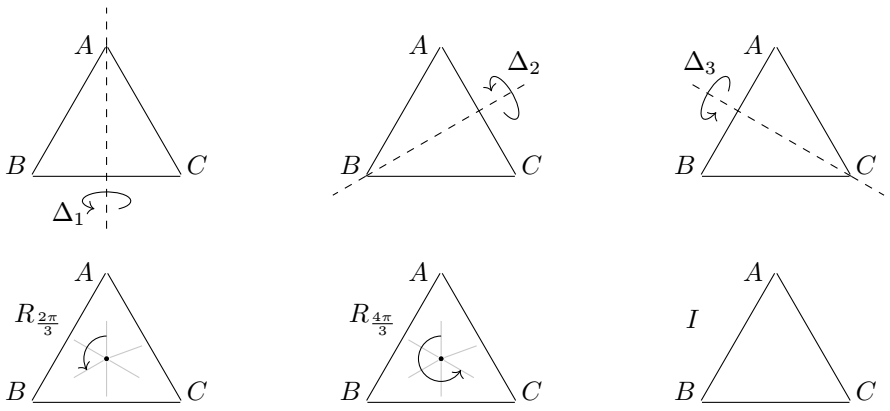
para todos os x, y, mas a T' não: existem x, y tais que $d(x, y) \neq d(T'x, T'y)$. Isso é o que faltou da nossa primeira tentativa de dizer o que é uma simetria: ela tem que *preservar as distâncias*, ou seja, ser uma *isometria*.

▸ **EXERCÍCIO x11.123.**
Demonstre (informalmente no desenho) que a transformação T' do Nãoexemplo 11.196 não é uma simetria. (x11.123 H 1 2)

? **Q11.199. Questão.** Quais são todas as simetrias dum triângulo equilátero?

!! SPOILER ALERT !!

11.200. As simetrias dum triângulo equilátero. Fixa um triângulo equilátero. Aqui todas as suas simetrias:



Tem 6 simetrias então

$$\Delta_1, \Delta_2, \Delta_3, R, R', I$$

onde escrevemos R e R' para as $R_{\frac{2\pi}{3}}$ e $R_{\frac{4\pi}{3}}$ respectivamente.

? **Q11.201. Questão.** Como podemos definir uma operação no conjunto de todas as simetrias dum triângulo equilateral, tal que ele vira um grupo?

!! SPOILER ALERT !!

D11.202. Definição (Os grupos dihedrais). O *grupo dihedral* $\mathcal{D}_n$ (também Dih_n) é o grupo das simetrias dum n-gono regular, com operação a composição $\circ$ (vendo as simetrias como transformações—ou seja, funções): $B \circ A$ é a simetria que criamos aplicando primeiramente a A e depois a B.[87]

▸ **EXERCÍCIO x11.124.**
Verifique que o $\mathcal{D}_n$ realmente é um grupo. (x11.124 H 0)

▸ **EXERCÍCIO x11.125.**
Ache todas as simetrias dum quadrado. (x11.125 H 1)

▸ **EXERCÍCIO x11.126.**
Qual a $o(\mathcal{D}_n)$? (x11.126 H 0)

[87] Alternativamente escrevemos isso como $A\,;B$ (notação diagramática, 9.138). Tendo esclarecido qual das $\circ$ e ; usamos—e com a mesma preguiça notacional que temos elaborado em vários outros casos até agora—escrevemos simplesmente AB, denotando assim a operação do grupo com justaposição.

! **11.203. Aviso.** O que simbolizamos aqui por $\mathcal{D}_n$ em certos textos aparece como $\mathcal{D}_{2n}$. A gente botou a quantidade n de ângulos do n-gono no índice do símbolo, mas tem gente que bota a quantidade de simetrias do n-gono como índice, e como tu acabou de ver no Exercício x11.126, essa quantidade é $2n$. De qualquer forma, nenhuma dessas notações é standard.[88] Então tome cuidado quando tu encontra em outros textos o símbolo $\mathcal{D}_m$.[89]

11.204. Que descoberta! Ou não?. Então, nosso amigo chegou feliz com sua descoberta desse grupo interessante. Mas, mais cedo ou mais tarde, a gente com certeza vai perceber algo: esse grupo $\mathcal{D}_3$ *parece ser* o S_3! Nosso amigo não achou um grupo realmente novo e original, mas apenas re-descobriu o grupo S_3 que conhecemos desde o início desse capítulo! Em qual sentido os dois grupos "são praticamente a mesma coisa"? Esse é o assunto da Secção §258, mas podemos já dar uma primeira resposta informal: *como grupos, eles comportam no mesmo jeito.*

11.205. Então são iguais?. Não! A palavra certa para esse caso é *isómorfos* ou *isomórficos*, que já encontramos no contexto de conjuntos (Definição D9.254). Lembre-se que isómorfos são aqueles que têm a mesma forma (Observação 9.255), mas também que o que significa "forma" depende do contexto. Aqui seria *a estrutura de grupos.* Grupos isómorfos têm exatamente as mesmas *propriedades grupoteóricas.*

11.206. Propriedades grupoteóricas. Essas são propriedades que o grupista consegue enxergar com seus olhos grupoteóricos. Uns exemplos:

- «ele tem membro cuja ordem é 2»;
- «ele é cíclico»;
- «ele tem dois membros que são seus próprios inversos»;
- «ele possui 3 subgrupos normais»;
- «ele tem exatamente 4 membros».

A última talvez não parece ser muito grupoteórica, mas de fato o grupista entende essa afirmação—talvez se reformulá-la como «ele tem ordem 4» não vai parecer estranho. Uns nãœxemplos:

- «seus membros são conjuntos»;
- «seus membros são números»;
- «ele tem membro que é singleton»;

Por outro lado, o conjuntista, com seus olhos conjuntoteóricos consegue enxergar todas as diferenças entre o $\mathcal{D}_3$ e S_3: de fato, ele vai responder que são diferentes—e ainda mais: disjuntos! Os membros do $\mathcal{D}_3$ são transformações dos pontos dum plano; os membros do S_3 são permutações, ou seja, bijecções de $\{1,2,3\}$ para $\{1,2,3\}$.

E para o grupista? *O que são* e *quais são* os membros de grupo é irrelevante. Ele não tá nem aí sobre a natureza dos membros, ou seus nomes, ou sua aparência! O que importa pra ele são suas propriedades grupoteóricas e nada mais: o inverso desse é aquele; o produto desses é aquilo; a identidade é essa; este aqui é um gerador; estes aqui são conjugados; tem tantos com ordem n; etc.

---

[88] Mesmo assim, a nossa notação faz mais sentido, pois: (i) quando definimos o grupo dihedral $\mathcal{D}_n$ já sabemos a quantidade de ângulos (n) mas por enquanto não sabemos quantos membros esse grupo tem (até resolver o Exercício x11.126); (ii) já temos uma notação para a ordem dum grupo, então não perdemos acesso nela optando para o nosso $\mathcal{D}_n$.

[89] Se o m é ímpar, não existe ambigüidade. Óbvio?

• **EXEMPLO 11.207.**
O $\mathcal{D}_4$ não é isómorfo com o S_4.
RESOLUÇÃO. Como $o(\mathcal{D}_4) = 8 \neq 24 = o(S_4)$, já sabemos que os dois grupos não são isomórficos.

▸ **EXERCÍCIO x11.127.**
Explique porque o $\mathcal{D}_4$ não é isómorfo com o grupo aditivo $\mathbb{Z}_8$ dos inteiros com adição módulo 8. (x11.127 H 0)

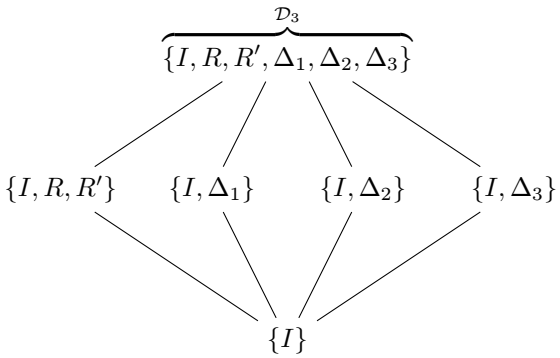
• **EXEMPLO 11.208.**
O $\mathcal{D}_4$ é um grupo cíclico?
RESOLUÇÃO. Para ver se $\mathcal{D}_4$ é um grupo cíclico ou não, conferimos para cada membro a dele, se a pode gerar o grupo inteiro ou não. Calculamos:

$$\begin{aligned} \langle I\rangle &= \{I\} & \langle \Delta_1\rangle &= \{I, \Delta_1\} \\ \langle R\rangle &= \{I, R, R', R''\} & \langle \Delta_2\rangle &= \{I, \Delta_2\} \\ \langle R'\rangle &= \{I, R'\} & \langle H\rangle &= \{I, H\} \\ \langle R''\rangle &= \langle R\rangle & \langle V\rangle &= \{I, V\} \end{aligned}$$

Nenhum desses subgrupos gerados é o próprio $\mathcal{D}_4$, e logo $\mathcal{D}_4$ não é um grupo cíclico.

11.209. Diagramas Hasse. Quando temos uma ordem parcial ($\leq$) definida num conjunto, podemos desenhar os membros do conjunto num diagrama chamado *diagrama Hasse*. Desenhamos os membros do conjunto e botamos uma linha *subindo* dum membro x para outro y sse $x \leq y$ e, ainda mais, não tem nenhum w entre os dois ($x \leq w \leq y$). (Fique lendo até os exemplos e vai fazer sentido.) No Capítulo 14 vamos trabalhar demais com esses diagramas; agora é uma boa oportunidade introduzi-los nesse contexto. Qual contexto exatamente? Qual o conjunto e qual a ordem? Lembre-se que $\leq$ é uma ordem parcial entre grupos (Exercício x11.61), ou seja, o conjunto de todos os subgrupos dum dado grupo é ordenado pela $\leq$. Bora desenhar então!

• **EXEMPLO 11.210 (O Hasse das simetrias do triângulo).**



▸ **EXERCÍCIO x11.128 (O Hasse das simetrias do quadrado).**
Fiz do $\mathcal{D}_3$; faça do $\mathcal{D}_4$. (x11.128 H 1 2)

▸ **EXERCÍCIO x11.129.**
Consegues achar um grupo diferente, que é isomórfico com o $\mathcal{D}_4$? (x11.129H123)

▸ **EXERCÍCIO x11.130.**
Qual é o menor tamanho de gerador $A \subseteq \mathcal{D}_3$, com $\langle A\rangle = \mathcal{D}_3$? Mostre um tal gerador. (x11.130H0)

▸ **EXERCÍCIO x11.131.**
E sobre o $\mathcal{D}_4$? (x11.131H0)

▸ **EXERCÍCIO x11.132 (Simetrias de rectângulo).**
Ache todas as simetrias do rectângulo. (x11.132H0)

▸ **EXERCÍCIO x11.133 (As simetrias do cíclo).**
Ache todas as simetrias do cíclo. (x11.133H0)

§258. Morfismos

11.211. Idéia. Queremos formalizar a idéia de «o grupo $\mathcal{D}_3$ *parece com* o S_3». O que precisa ser satisfeito (ou mostrado) para convencer alguém que, no final das contas, trabalhar com um grupo $\mathcal{A}$ é *essencialmente a mesma coisa* de trabalhar com um grupo $\mathcal{B}$?

D11.212. "Definição" (homomorfismo). Sejam $\mathcal{A}, \mathcal{B}$ grupos. A função $\varphi : A \to B$ é um *homomorfismo* de $\mathcal{A}$ para $\mathcal{B}$ sse ela *preserva a estrutura de $\mathcal{A}$ no $\mathcal{B}$*.

11.213. Preservando a estrutura. Antes de entender o que significa «preservar uma estrutura», vamos lembrar: o que é a estrutura dum grupo? É sua alma: num grupo temos a sua operação (binária), podemos pegar inversos (operação unária), e temos também em cada grupo um membro especial chamado identidade do grupo (constante). Ou seja, *preservar a estrutura* faz sentido significar as três coisas seguintes:

(i)	preservar a operação:	$\varphi(x *_A y) = \varphi(x) *_B \varphi(y)$
(ii)	preservar os inversos:	$\varphi(inv_A(x)) = inv_B(\varphi(x))$
(iii)	preservar a identidade:	$\varphi(e_A) = e_B$.

Também usamos o termo *respeitar*, muitas vezes como sinônimo de preservar mas não sempre—então tome cuidado com as definições, especialmente se a estrutura envolve relações.

11.214. Dois caminhos. Considere que temos uma *função* φ de $\mathcal{A}$ para $\mathcal{B}$. Comece no grupo $\mathcal{A}$ (o domínio de φ) e tome uns membros $a_1, \ldots, a_n$ do seu carrier set A. Faça quaisquer coisas aí que a estrutura de grupo te permite fazer: tome inversos, combine eles com a operação do grupo, etc. Assim tu chega num certo membro x do grupo $\mathcal{A}$. Agora use a φ nesse resultado x, passando assim para um certo membro y do grupo $\mathcal{B}$. Alternativamente, *começando com os mesmos membros* $a_1, \ldots, a_n$ do $\mathcal{A}$, use a φ logo no

início em cada um deles para passar ao grupo $\mathcal{B}$, chegando assim nuns membros $b_1, \ldots, b_n$ do $\mathcal{B}$. Sendo num grupo agora, podes performar exatamente as mesmas operações, na mesma ordem, nos correspondentes membros que tu fez antes (no grupo $\mathcal{A}$), e assim tu chegarás num certo resultado b no $\mathcal{B}$. Vamos chamar a função φ um homomorfismo exatamente quando ela garanta que em qualquer situação como essa, os dois caminhos de $\mathcal{A}$ para $\mathcal{B}$, chegam no mesmo membro, ou seja, $b = y$.

11.215. Diagramas comutativos. Essa idéia é bem melhor desenhada do que escrita, usando diagramas comutativos. Por exemplo, a lei (ii) é equivalente à comutatividade do diagrama seguinte:

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle inv_A}\downarrow & & \downarrow{\scriptstyle inv_B} \\ A & \xrightarrow{\varphi} & B \end{array}$$

► **EXERCÍCIO x11.134.**
Desenhe um diagrama cuja comutatividade é a lei (i). (x11.134H0)

11.216. Diferentes estruturas para grupos. Já vimos como definir "grupo" como conjunto estruturado usando três estruturas diferentes:

$$(A\,;*_A) \qquad (A\,;*_A, e_A) \qquad (A\,;*_A, inv_A, e_A).$$

Então, dependendo na estrutura que escolhemos para nossa definição de grupo, precisamos definir "morfismo" em forma diferente: No caso de estrutura $(A\,;*_A)$ o morfismo deve satisfazer o (i); no caso de $(A\,;*_A, e_A)$, os (i) e (iii), e no caso de $(A\,;*_A, inv_A, e_A)$ todos os (i)–(iii). *Parece então que chegamos no primeiro ponto onde a estrutura escolhida na definição de grupo será crucial.* Felizmente, como nós vamos demonstrar logo após, as leis de grupo são suficientes para garantir que qualquer função φ que satisfaz apenas o (i) acima, obrigatoriamente satisfaz os (ii) e (iii) também! Mesmo assim, vamos botar em nossa definição todos os (i)–(iii), pois isso captura melhor a idéia geral de "homomorfismo". E assim que demonstrar nossa afirmação ganhamos um critérion forte para decidir se alguma função é um homomorfismo.

D11.217. Definição (homomorfismo). Sejam

$$\mathcal{A} = (A\,;*_A, inv_A, e_A), \qquad \mathcal{B} = (B\,;*_B, inv_B, e_B)$$

grupos. A função $\varphi : A \to B$ é um *homomorfismo* do $\mathcal{A}$ para o $\mathcal{B}$ sse ela respeita a operação, os inversos, e a identidade:

$$\begin{array}{ll} \text{para todo } x, y \in A, & \varphi(x *_A y) = (\varphi x) *_B (\varphi y); \\ \text{para todo } x \in A, & \varphi(inv_A x) = inv_B(\varphi x); \\ & \varphi e_A = e_B. \end{array}$$

Às vezes escrevemos $\varphi : \mathcal{A} \to \mathcal{B}$ (em vez de $\varphi : A \to B$) para enfatizar que o φ nos leva do *grupo* $\mathcal{A}$ para o *grupo* $\mathcal{B}$; ou também $\varphi : A \xrightarrow{\text{hom}} B$.

11.218. Quando pelo contexto podemos inferir qual é a operação envolvida, optamos para denotá-la com justaposição como produto mesmo. Por exemplo, escrevemos

$$\varphi(xy) = \varphi(x)\varphi(y)$$

sem ambigüidade nenhuma: o xy que aparece no lado esquerdo, só pode denotar o $x *_A y$, pois $x, y \in A$. E, no outro lado, o $(\varphi x)(\varphi y)$ só pode denotar o $\varphi(x) *_B \varphi(y)$, pois $\varphi(x), \varphi(y) \in B$. A mesma coisa acontece com os inversos: $\varphi(x^{-1})$ só pode denotar "a imagem do inverso (no A) de x", e $(\varphi(x))^{-1}$ só pode denotar "o inverso (no B) de $\varphi(x)$", pois, no primeiro caso o $^{-1}$ é aplicado num membro de A, e no segundo caso num membro de B.

11.219. Critérion (de homomorfismo). *Sejam grupos $\mathcal{A} = (A\ ;\ *_A, inv_A, e_A)$ e $\mathcal{B} = (B\ ;\ *_B, inv_B, e_B)$ e função $\varphi : A \to B$ que preserva a operação, ou seja, tal que*

$$\text{para todo } x, y \in A, \quad \varphi(x *_A y) = (\varphi x) *_B (\varphi y).$$

Então φ é um homomorfismo.

► Esboço. Precisamos demonstrar o que falta:

(iii) $$\varphi e_A = e_B$$

(ii) $$\text{para todo } x \in A, \quad \varphi(x^{-1}) = (\varphi x)^{-1}.$$

Para o (iii), calculamos $\varphi(e_A) = \varphi(e_A)\varphi(e_A)$ para concluir que $e_B = \varphi(e_A)$; para o (ii), mostramos que o $\varphi(x^{-1})$ satisfaz a propriedade característica de ser inverso de φx:

$$\varphi(x^{-1})\varphi(x) \stackrel{?}{=} e_B.$$

□

D11.220. Definição (-morfismos). Sejam grupos $\mathcal{A}$ e $\mathcal{B}$, e $\varphi : \mathcal{A} \to \mathcal{B}$ um homomorfismo. Usamos os termos:

$$\begin{aligned}
\varphi \text{ monomorfismo} &\stackrel{\text{def}}{\iff} \varphi \text{ L-cancelável} \\
\varphi \text{ epimorfismo} &\stackrel{\text{def}}{\iff} \varphi \text{ R-cancelável} \\
\varphi \text{ split monomorfismo} &\stackrel{\text{def}}{\iff} \varphi \text{ L-invertível} \\
&\iff (\exists \varphi' : \mathcal{B} \to \mathcal{A})[\, \varphi'\varphi = \mathrm{id}_A \,] \\
\varphi \text{ split epimorfismo} &\stackrel{\text{def}}{\iff} \varphi \text{ R-invertível} \\
&\iff (\exists \varphi' : \mathcal{B} \to \mathcal{A})[\, \varphi\varphi' = \mathrm{id}_B \,] \\
\varphi \text{ isomorfismo} &\stackrel{\text{def}}{\iff} \varphi \text{ é invertível} \\
&\iff (\exists \varphi' : \mathcal{B} \to \mathcal{A})[\, \varphi'\varphi = \mathrm{id}_A \ \ \& \ \ \varphi\varphi' = \mathrm{id}_B \,] \\
\varphi \text{ endomorfismo} &\stackrel{\text{def}}{\iff} \mathrm{dom}\,\varphi = \mathrm{cod}\,\varphi \\
\varphi \text{ automorfismo} &\stackrel{\text{def}}{\iff} \varphi \text{ endomorfismo \& isomorfismo}
\end{aligned}$$

onde "cancelável" e "invertível" significam com respeito a operação da composição $\circ$.

▸ **EXERCÍCIO x11.135.**
Investigue:

$$\varphi \text{ mono} \overset{?}{\iff} \varphi \text{ split mono} \overset{?}{\iff} \varphi \text{ injectiva}$$

Como a situação compara com os resultados de funções entre conjuntos (veja §222)? (x11.135 H 0)

▸ **EXERCÍCIO x11.136.**
Investigue:

$$\varphi \text{ epí} \overset{?}{\iff} \varphi \text{ split epí} \overset{?}{\iff} \varphi \text{ sobrejectiva}$$

Como a situação compara com os resultados de funções entre conjuntos? (x11.136 H 0)

▸ **EXERCÍCIO x11.137.**
Investigue:

$$\varphi \text{ iso} \overset{?}{\iff} \varphi \text{ mono} + \varphi \text{ epí} \overset{?}{\iff} \varphi \text{ bijectiva}$$

Como a situação compara com os resultados de funções entre conjuntos? (x11.137 H 0)

▸ **EXERCÍCIO x11.138.**
Seja G grupo. Mostre que a $\mathrm{id} : G \to G$ é um homomorfismo (e logo automorfismo). (x11.138 H 0)

▸ **EXERCÍCIO x11.139.**
Seja G grupo. Para todo $g \in G$, o g-conjugador (Definição D11.93) é um automorfismo. (x11.139 H 0)

Finalmente podemos definir o que significa que dois grupos são isómorfos!

D11.221. Definição (Grupos isomórficos). Sejam grupos G e G'. Chamamos o G *isomórfico* (ou *isómorfo*) ao G' sse existe isomorfismo $\varphi : G \to G'$. Nesse caso chamamos o φ *isomorfismo de grupos*. Como introduzimos na Definição D9.254 escrevemos $G \cong G'$ para dizer que «os G, G' são isómorfos», e também $\varphi : G \xrightarrow{\cong} G'$ ou até $\varphi : G \cong G'$ para «φ é um isomorfismo de G para G'».

▸ **EXERCÍCIO x11.140.**
Mostre que $\cong$ é uma relação de equivalência. (x11.140 H 0)

▸ **EXERCÍCIO x11.141.**
Mostre que os $(\mathbb{Z}\,;+)$ e $(\mathbb{Q}\,;+)$ não são isómorfos. (x11.141 H 1)

§259. Kernel, Image

D11.222. Definição (kernel, image). Sejam A, B grupos e $\varphi : A \to B$ um homomorfismo. Definimos

$$\ker \varphi \overset{\text{def}}{=} \varphi_{-1}[\{e_B\}] \quad \left(= \{\, a \in A \mid \varphi(a) = e_B \,\} \right)$$
$$\operatorname{im} \varphi \overset{\text{def}}{=} \varphi[A] \quad \left(= \{\, b \in B \mid (\exists x \in A)[\, \varphi(x) = b \,] \,\} \right)$$

Chamamos o $\ker\varphi$ o *kernel* do φ e o $\operatorname{im}\varphi$ o *image* do φ.

Θ11.223. Teorema. *Sejam A, B grupos e $\varphi : A \to B$ homomorfismo.*

$$\varphi \text{ injetora} \iff \ker\varphi = \{e_A\}\,.$$

▸ Esboço. ($\Rightarrow$): Como $e_A \in \ker\varphi$, basta demonstrar que todos os membros de $\ker\varphi$ são iguais: suponha $x, y \in \ker\varphi$ e mostre que $x = y$.
($\Leftarrow$). Sejam $x, y \in A$ tais que $\varphi(x) = \varphi(y)$. Operando nessa igualdade e usando o fato que φ é homomorfismo, chegamos no $x = y$, ou seja, φ é injetora. □ (Θ11.223P)

▸ **EXERCÍCIO x11.142.**
Sejam A e B grupos e $\varphi : A \to B$ homomorfismo. Demonstre que $\ker\varphi \leq A$. (x11.142H123)

▸ **EXERCÍCIO x11.143.**
Sejam A e B grupos e $\varphi : A \to B$ homomorfismo. Demonstre que $\ker\varphi \trianglelefteq A$. (x11.143H1)

▸ **EXERCÍCIO x11.144.**
Veja a demonstração completa do Exercício x11.143. No seu cálculo, mostre como continuar num caminho diferente depois da terceira igualdade para chegar no mesmo resultado desejado: e_B. (x11.144H1)

▸ **EXERCÍCIO x11.145.**
Sejam A e B grupos e φ um homomorfismo de A para B. Demonstre que $\operatorname{im}\varphi \leq B$. (x11.145H12)

Θ11.224. Teorema (Primeiro teorema de isomorfismo). *Sejam G e G' grupos e $\varphi : G \to G'$ homomorfismo.*

(i) $\ker\varphi \trianglelefteq G$;
(ii) $\operatorname{im}\varphi \leq G'$;
(iii) $G/\ker\varphi \cong \operatorname{im}\varphi$.

▸ Esboço. Acabamos de demonstrar as (i) & (ii) nos x11.143 & x11.145. Para a (iii) precisamos definir uma função

$$\Phi : G/\ker\varphi \to \operatorname{im}\varphi$$

tal que Φ é um isomorfismo. Seja $K := \ker\varphi$. Queremos definir a Φ pela

$$\Phi(Kx) = \varphi(x)$$

para qualquer coclasse Kx do K (essas são as suas entradas).

O problema é que Φ não parece *bem-definida*, pois seu valor pode depender na escolha do representante x da coclasse—veja o Cuidado 11.225 caso que o problema com essa definição não é claro. Precisamos melhorar essa definição e demonstrar que: (a) realmente defina uma *função* Φ; (b) Φ é bijetora; (c) Φ é um homomorfismo (e logo isomorfismo). □

! **11.225. Cuidado.** Caso que o perigo descrito no esboço acima não é óbvio, primeiramente volte re-estudar os Cuidado 11.178, Cuidado 9.53, e Cuidado 9.55.

Agora vamos pensar como um programador querendo definir essa função Φ. Sua função, quando chamada, recebe uma coclasse, ou seja, um conjunto com certos elementos membros. Ela não sabe qual foi o nome que o chamador escolheu para essa coclasse (Cuidado 9.53). Até pior, e para corresponder ainda melhor com nosso caso, observe que o Kx é na verdade uma operação entre um subgrupo K e um membro x que resulta num subconjunto de G. Mas a Φ *não tem acesso nesse* x (Cuidado 9.55).

Mesmo se defini-la pela

$$\Phi(C) = \varphi(c), \quad \text{onde } c \text{ é algum membro de } C$$

temos uma tarefa para fazer: *precisamos demonstrar que seu valor* $\Phi(C)$ *não depende da escolha de* c. Até conseguir demonstrar isso, não podemos considerar a Φ uma função *bem-definida*. Veja bem a demonstração do Teorema Θ11.224.

11.226. Dois lados da mesma moeda. Já demonstramos algo (Exercício x11.143) que, informalmente falando, podemos escrever assim:

$$\text{kernel} \implies \text{normal}.$$

E o converso? Será que também é verdade? O que exatamente é esse converso? Como formalizar? Podemos demonstrar?

Realmente o converso da implicação-informal também é válido:

$$\text{normal} \implies \text{kernel}.$$

Temos então o slogan

$$\text{normal} \iff \text{kernel}.$$

Ou seja, em teoria dos grupos os conceitos de "kernel" e de "subgrupo normal" são apenas dois lados da mesma moeda. Deixo os *detalhes importantes* pra ti, no Problema Π11.29—não pule!

§260. Pouco de cats—categorias e grupos

Temos uns objetos que nos interessam: os grupos. Temos umas setas interessantes entre esses objetos: os morfimos. Será que temos uma categoria (Definição D9.261)?

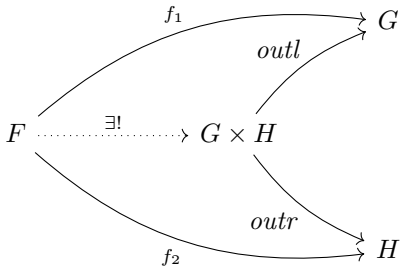
D11.227. Definição. Denotamos por **Group** a categoria dos grupos:

- Obj (**Group**): todos os grupos;
- Arr (**Group**): todos os homomorsfismos de grupos;

onde obviamente os $\operatorname{src}\varphi$ e $\operatorname{tgt}\varphi$ denotam os $\operatorname{dom}\varphi$ e $\operatorname{cod}\varphi$ respectivamente.

▸ **EXERCÍCIO x11.146.**
Demonstre que **Group** realmente é uma categoria. (x11.146 H 0)

• **EXEMPLO 11.228.**
A categoria **Group** possui produtos? (Definição D9.270.)
RESOLUÇÃO. Sim. Dados dois objetos G, H o $(outl, G \times H, outr)$ (D11.33) é um produto dos G, H. Primeiramente precisamos demonstrar que $G \times H$ realmente é um objeto da **Group**, ou seja, um grupo; tu demonstraste isso no Exercício x11.19. Agora falta verificar que dados (f_1, F, f_2),[90]



Defina a ! pela

$$! = \langle f_1, f_2 \rangle.$$

Isso realmente é o único que faz o diagrama comutar—tu já verificaste isso no Exercício x9.128, certo?—então só basta demonstrar uma coisa pra terminar.

▸ **EXERCÍCIO x11.147.**
Qual? Enuncie e demonstre! (x11.147 H 1)

▸ **EXERCÍCIO x11.148.**
A categoria **Group** possui objetos iniciais? Terminais? Quais? (Definição D9.267.) E, esqueci: a **Set** tem? (x11.148 H 0)

D11.229. Definição. Denotamos por **Abel** a categoria dos grupos abelianos:

- $\mathrm{Obj}\,(\mathbf{Abel})$: todos os grupos abelianos;
- $\mathrm{Arr}\,(\mathbf{Abel})$: todos os homomorsfismos de grupos abelianos;

onde novamente os $\mathrm{src}\,\varphi$ e $\mathrm{tgt}\,\varphi$ são as coisas óbvias.

▸ **EXERCÍCIO x11.149.**
Verifique que **Abel** realmente é uma categoria. (x11.149 H 0)

É fácil verificar que a **Abel** também possui produtos: essencialmente o mesmo argumento da **Group** passa aqui também. Mas a situação é bastante diferente olhando para os *coprodutos* (Problema Π9.27).

[90] Sim, isso é uma frase completa, com seu verbo e tudo mais: «... dados (f_1, F, f_2), existe única seta $! : F \to G \times H$ que faz o diagrama seguinte comutar: ...» Mais uma vez que percebemos a veracidade do ditado

1 diagrama comutativo = 1,000 palavras.

11.230. Coprodutos de grupos. Os coprodutos na **Group**... meio complicado. Vamos voltar nesse assunto no Capítulo 15; mas por enquanto observe que o conjunto $G \uplus H$ que usamos para o coproduto $G \amalg H$ na **Set** não possui uma estrutura de grupo óbvia para servir como coproduto dos G, H. Qual seria sua identidade, por exemplo, e, antes de chegar em conseguir perguntar isso, qual seria sua operação? Contudo, é fácil demonstrar que **Abel** possui coprodutos—e tu nem imagina quais são!

▸ **EXERCÍCIO x11.150.**
Dados objetos (grupos abelianos) G, H, ache um coproduto deles. Tu ficarás surpreso. (x11.150 H 1 2)

Problemas

▸ **PROBLEMA Π11.23.**
Pode achar alguma propriedade grupoteórica tal que num grupo G, dentro duma das suas classes de conjugação vai ter membros que satisfazem e membros que não? (Π11.23 H 0)

▸ **PROBLEMA Π11.24.**
Sejam G, G' grupos abelianos. Demonstre que

$$\operatorname{Hom}(G, G') \stackrel{\text{def}}{=} \{\, \varphi : G \to G' \mid \varphi \text{ homomorfismo} \,\}$$

é um grupo abeliano com operação a $(+)$ definida pointwise (Definição D9.203):

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x).$$

com operação a $(+)$ pointwise é um grupo abeliano. Precisas realmente saber que ambos os G, G' são abelianos? (Π11.24 H 0)

▸ **PROBLEMA Π11.25.**
Mostre que dado um grupo G, o conjunto de todos os seus automorfismos

$$\operatorname{Aut} G \stackrel{\text{def}}{=} \{\varphi : G \rightarrowtail G \mid \varphi \text{ é um automorfismo}\}$$

com operação $\circ$ é um grupo. (Π11.25 H 0)

▸ **PROBLEMA Π11.26.**
Sabendo que $\operatorname{Bij} G \stackrel{\text{def}}{=} ((G \rightarrowtail G)\,; \circ)$ é um grupo, mostre que

$$\operatorname{Aut} G \leq \operatorname{Bij} G.$$

(Π11.26 H 1)

D11.231. Definição (Inner autos). Seja G grupo. Definimos o conjunto dos seus *inner automorfismos*

$$\operatorname{Inn}(G) \stackrel{\text{def}}{=} \{\, \sigma_g \mid g \in G \,\}$$

onde σ_g é o g-conjugador (Definição D11.93).

▸ **PROBLEMA Π11.27.**
$\operatorname{Inn} G \trianglelefteq \operatorname{Aut} G$.

(Π11.27 H 1)

▸ **PROBLEMA Π11.28.**
A relação $\trianglelefteq$ é uma ordem?

(Π11.28 H 1 2 3)

▸ **PROBLEMA Π11.29 (kernel = normal).**
Já demonstramos algo que informalmente falando podemos escrever assim:

$$\text{kernel} \implies \text{normal}$$

Formalize e demonstre o converso.

(Π11.29 H 1 2)

▸ **PROBLEMA Π11.30 (Teorema de Cayley).**

TODO Outline Cayley's theorem

(Π11.30 H 0)

▸ **PROBLEMA Π11.31 (Teorema de Cauchy).**

TODO Outline Cauchy's theorem

(Π11.31 H 0)

Leitura complementar

Para practicar com propriedades de operações vale a pena resolver os primeiros 15 problemas do **[Hal95]**.

Livros introdutórios de álgebra abstrata tratam em geral a teoria dos grupos mais profundamente ou extensamente do que podemos tratá-la aqui. **[Pin10]** é um desses livros, bastante acessível, com exemplos de diversas áreas, mostrando várias aplicações. Uma *excelente* introdução em vários tópicos de álgebra é o **[Her75]**, famoso para sua exposição e didáctica.

O assunto da álgebra abstrata foi composto e tratado numa maneira organizada no *Moderne Algebra* de van der Waerden (dois volúmes: 1930, 1931; modernas edições traduzidas: **[vdW03a]**, **[vdW03b]**). Ele foi baseado principalmente em aulas dadas por Artin e Noether. e é um dos livros mais influenciadores e importantes em matemática.

Birkhoff e Mac Lane trazeram o assunto para os currículos de graduação com o clássico **[BM77b]**. Os mesmos autores, no **[MB99]**, apresentam álgebra mais profundamente e com um cheiro categórico (veja Capítulo 15), algo expectado já que Mac Lane é um dos fundadores da teoria das categorias (o outro é o Eilenberg).

Infelizmente, muitos livros (e professores) consideram a teoria das categorias como algo avançado ou difícil para ser introduzido neste nível (e geralmente o primeiro contato com categorias chega bem depois dos primeiros contatos com álgebra abstrata). Felizmente, o bem-legível **[Alu09]** é uma excessão brilhante dessa tradição: começa já introduzindo a linguagem e as idéias das categorias e trata assim todos os assuntos principais de álgebra abstrata. (Essa seria minha maior recomendação para o meu leitor que ficou animado com o conteudo deste capítulo e do próximo.)

Depois de se acostumar com as idéias algébricas em geral, dois livros focados especialmente em teoria dos grupos são os **[Ros13]** e **[Rot99]**.

O convex hull que encontramos *en passant* neste capítulo gera um problema algorítmico muito interessante: *dado um conjunto A de pontos dum espaço euclideano calcule um óptimo $C \subseteq A$ tal que seus pontos são as vértices do convex hull do A.* Para mais sobre isso, veja por exemplo o **[CLRS09:** §33.3**]**.

CAPÍTULO 12

ESTRUTURAS ALGÉBRICAS

§261. Semigrupos

12.1. Esquematicamente:

$$\text{monóide}\left\{\begin{array}{l}\text{semigrupo}\left\{\begin{array}{c}\text{(fechado)}\\ \text{(associatividade)}\\ \text{(identidade)}\\ \text{(inversos)}\\ \text{(comutatividade)}\end{array}\right\}\text{grupo}\end{array}\right\}\text{grupo abeliano}$$

TODO Escrever

§262. Monóides

D12.2. Definição (Monóide). Um conjunto estruturado $\mathcal{M} = (M\,;\cdot,\varepsilon)$ é um *monóide* sse:

(G0) $(\forall a, b \in M)[\,a \cdot b \in M\,]$
(G1) $(\forall a, b, c \in M)[\,a \cdot (b \cdot c) = (a \cdot b) \cdot c\,]$
(G2) $(\forall a \in M)[\,\varepsilon \cdot a = a = a \cdot \varepsilon\,].$

Naturalmente, se a $\cdot$ é comutativa chamamos M de *monóide comutativo*.

- **EXEMPLO 12.3.**
A partir de qualquer exemplo de grupo $\mathcal{G} = (G\,;*_G, {}^{-1}, e_G)$ temos um exemplo de monóide também: o $(G\,;*_G, e_G)$.

Mais interessantes agora seriam exemplos de monóides que não são grupos:

- **EXEMPLO 12.4.**
Os naturais com adição formam um monóide.

- **EXEMPLO 12.5.**
O $(\mathbb{N}_{\neq 0}\,;\cdot)$ é um monóide.

- **EXEMPLO 12.6 (Strings).**
Considere um alfabeto finito Σ e seja $\Sigma^\star$ o conjunto de todos os strings formados por letras do Σ. O $\Sigma^\star$ com a operação a concatenação de strings, é um monóide. Sua identidade é o string vazio.

? **Q12.7. Questão.** Como tu definirias a relação de submonóide?

!! SPOILER ALERT !!

D12.8. Definição (submonóide). Seja $\mathcal{M} = (M\,;\cdot_M, \varepsilon_M)$ monóide e $H \subseteq M$. O H é um submonóide de M sse $\varepsilon_M \in H$ e H é $\cdot_M$-fechado.

12.9. Observação (abusamos como sempre). Literalmente não é o conjunto H que é submonóide, mas o conjunto estruturado

$$\mathcal{H} := (H\,;\cdot_M|_{N\times N}, \varepsilon_M).$$

Eu presumo que tu és acostumado com esses abusos depois que os discutimos nos itens 8.161 e 11.11.

? **Q12.10. Questão.** Como tu definirias o homomorfismo entre monóides?

!! SPOILER ALERT !!

D12.11. Definição (homomorfismo). Sejam $\mathcal{M} = (M\,;\cdot_M, \varepsilon_M)$ e $\mathcal{N} = (N\,;\cdot_N, \varepsilon_N)$ monóides. Uma função $\varphi : M \to N$ é um *homomorfismo* sse:

(i) para todo $x, y \in M$, $\quad \varphi(x \cdot_M y) = \varphi(x) \cdot_N \varphi(y)$.
(ii) $\varphi(\varepsilon_M) = \varepsilon_N$;

- **EXEMPLO 12.12.**
Considere os monóides $\mathcal{N} = (\mathbb{N}\,;+, 0)$ e $\mathcal{B} = (B\,;+\!\!+, \varepsilon)$, onde: B é o conjunto de todos os

strings (finitos) binários, ou seja, $B = \{0,1\}^\star$; ε é o string vazio "“”; $+\!\!+$ a concatenação. A $\varphi : \mathcal{N} \to \mathcal{B}$ definida recursivamente pelas

$$\begin{aligned} \varphi(0) &= \varepsilon \\ \varphi(n+1) &= \varphi(n) +\!\!+ 0 \end{aligned}$$

é um homomorfismo. A *length* : $\mathcal{B} \to \mathcal{N}$ que retorna o tamanho da sua entrada é um homomorfismo.

• **NÃOEXEMPLO 12.13.**
Com o contexto do exemplo anterior, a $\psi : \mathcal{N} \to \mathcal{B}$ definida recursivamente pelas:

$$\begin{aligned} \psi(0) &= \varepsilon \\ \psi(n+1) &= \begin{cases} \psi(n) +\!\!+ 0, & \text{se } \psi(n) \text{ não termina com } 0 \\ \psi(n) +\!\!+ 1, & \text{caso contrário} \end{cases} \end{aligned}$$

não é um homomorfismo.

▸ **EXERCÍCIO x12.1.**
Por quê? (x12.1H0)

! **12.14. Cuidado.** No Capítulo 11 assim que definimos o que significa homomorfismo de grupos (D11.217) demonstramos o Critérion 11.219 que nos permite concluir que uma função entre grupos é homomorfismo assim que souber que ela respeita a operação. Isso quer dizer que temos esse critério nos monóides também? Primeiramente olhamos para a demonstração do Critérion 11.219 para ver se ela "passa" nos monóides também: se ela usou apenas os (G0)–(G2), então passa. Não é o caso: *essa* demonstração necessitou o (G3) pois usou os inversos. Então isso quer dizer que perdemos esse critério nos monóides? *Não!* O que perdemos foi a demonstração; mas talvez existe outra que segura o mesmo teorema, e que não necessita os inversos. Será?

▸ **EXERCÍCIO x12.2.**
Podemos demonstrar um critérion parecido com o Critérion 11.219 para os monóides? Ou seja, se φ preserva a operação do monóide, ela necessariamente preserva a identidade também? (x12.2H12)

12.15. Critérion. *Uma função sobrejetora $\varphi : M \twoheadrightarrow N$ tal que*

$$\text{para todo } x, y \in M, \quad \varphi(x \cdot_M y) = \varphi(x) \cdot_N \varphi(y)$$

é um homomorfismo.

Demonstrarás agora no Exercício x12.3. ∎

▸ **EXERCÍCIO x12.3.**
Demonstre o Critérion 12.15. (x12.3H123456)

§263. Anéis

Vamos estudar pouco a estrutura de *anel*, cuja definição foi dada primeiramente por Fraenkel. Nossa inspiração e guia para os grupos, foram os mapeamentos e as permutações. Para os anéis, nossa guia são os inteiros.

D12.16. Definição (Anel). Seja $\mathcal{R} = (R\,;+,\,\cdot,0,1)$ um conjunto estruturado, onde $+,\cdot$ são operações binárias e $0,1$ são constantes. $\mathcal{R}$ é um *anel* ou *ring* sse

$$\begin{aligned}
&\text{(RA0)} && (\forall a,b\in R)[\,a+b\in R\,]\\
&\text{(RA1)} && (\forall a,b,c\in R)[\,a+(b+c)=(a+b)+c\,]\\
&\text{(RA2)} && (\forall a\in R)[\,0+a=a=a+0\,]\\
&\text{(RA3)} && (\forall a\in R)(\exists y\in R)[\,y+a=0=a+y\,]\\
&\text{(RA4)} && (\forall a,b\in R)[\,a+b=b+a\,]\\
&\text{(RM0)} && (\forall a,b\in R)[\,a\cdot b\in R\,]\\
&\text{(RM1)} && (\forall a,b,c\in R)[\,a\cdot(b\cdot c)=(a\cdot b)\cdot c\,]\\
&\text{(RM2)} && (\forall a\in R)[\,1\cdot a=a=a\cdot 1\,]\\
&\text{(RDL)} && (\forall a,b,c\in R)[\,a\cdot(b+c)=(a\cdot b)+(a\cdot c)\,]\\
&\text{(RDR)} && (\forall a,b,c\in R)[\,(b+c)\cdot a=(b\cdot a)+(c\cdot a)\,]
\end{aligned}$$

Caso que também é satisfeita a

$$\text{(RM4)} \qquad (\forall a,b\in R)[\,a\cdot b=b\cdot a\,].$$

chamamos o $\mathcal{R}$ *anel comutativo*.

▸ **EXERCÍCIO x12.4.**
Acima escolhemos a maneira "intermediaria" de estrutura. Qual seria uma estrutura "mais completa" para definir o conceito de anel, e qual uma estrutura mais pobre? Descreva as aridades dos símbolos usados (a assinatura da estrutura algébrica). (x12.4 H 0)

▸ **EXERCÍCIO x12.5.**
Como podemos definir o que é um anel usando definições de estruturas algébricas que já conhecemos? (x12.5 H 0)

! 12.17. Cuidado (Ring ou Rng?). Na definição de *ring* que usamos aqui necessitamos ter $(\cdot)$-identidade (unidade). Infelizmente isso não é padrão: especialmente em textos antigos (mas também dependendo do objetivo de cada texto) anéis podem necessitar ou não esse axioma, e logo vendo a palavra "anel" num texto, precisamos confirmar qual é a definição usada. Para a gente aqui, quando queremos referir à estrutura que não necessita identidades chamamos de *rng*, a idéia sendo que é como um "ring" sem *i* (dentidade).[91] No outro lado, quem não considera esse axioma como parte de *ser um ring*, refere aos nossos rings como "ring com unidade", "ring com 1", "ring unital" etc. Às vezes o termo

[91] Tentando traduzir "rng" para português, tanto "ael" quanto "anl" funcionam mas não muito bem: na primeira opção perdemos o elemento *n*eutro da $(\cdot)$ e na segunda perdemos o *e* do monóide multiplicativo, mas nenhuma das opções fica boa, então melhor esquecer esses termos e usar *rng* o mesmo.

pseudoring é usado mas este é um termo ainda mais sobrecarregado, então melhor usar "rng" que sempre tem o mesmo significado. No [Poo14] encontrarás mais sobre a escolha da nossa Definição D12.16 mas sugiro não consultá-lo antes de pensar sobre o exercício seguinte primeiro:

▸ **EXERCÍCIO x12.6.**
Tu escolherias incluir o 1 na definição de ring? Por quê? (x12.6H0)

D12.18. Definição. Dado $x \in R$, denotamos com $(-x)$ o objeto garantido pela (RA3). Seguindo nossa experiência com adição e multiplicação de números, adoptamos as mesmas convenções para os anéis: denotamos pela justaposição a "multiplicação" do anel, e consideramos que ela tem precedência contra a "adição". Note também que como não temos alguma operação binária $-$ de subtraição, a expressão $x-y$ num anel não é definida. Definimos a operação *binária* $-$ num anel R pela

$$x - y \overset{\text{sug}}{\equiv} x + (-y).$$

Pelo contexto sempre dará pra inferir a aridade do símbolo '$-$'; então não tem como criar ambigüidade com a operação *unária* $-$, mesmo compartilhando o mesmo símbolo. Continuando, se $n \in \mathbb{N}$, usamos:

$$nx \overset{\text{sug}}{\equiv} \underbrace{x + x + \cdots + x}_{n \text{ vezes}} \qquad\qquad x^n \overset{\text{sug}}{\equiv} \underbrace{xx \cdots x}_{n \text{ vezes}}.$$

Ou seja, lembrando da notação do Definição D11.72:

$$nx \overset{\text{sug}}{\equiv} x^{+n} \qquad\qquad x^n \overset{\text{sug}}{\equiv} x^{\cdot n}.$$

• **EXEMPLO 12.19.**
Todos os seguintes conjuntos são exemplos de anéis:

$$(\mathbb{Z}\,;+,\cdot) \quad (\mathbb{Q}\,;+,\cdot) \quad (\mathbb{R}\,;+,\cdot) \quad (\mathbb{C}\,;+,\cdot) \quad (\mathbb{R}[x]\,;+,\cdot) \quad (C[a,b]\,;+,\cdot) \quad (\mathbb{R}^{n\times n}\,;+,\cdot)$$

onde lembramos que $\mathbb{R}[x]$ é o conjunto de todos os polinómios numa variável x com coeficientes reais, e $\mathbb{R}^{n\times n}$ é o conjunto de todas as matrices reais $n \times n$. Temos também

$$C[a,b] \overset{\text{def}}{=} \{\, f : [a,b] \to \mathbb{R} \mid f \text{ é contínua} \,\}$$

para quaisquer $a, b \in \mathbb{R}$ com $a \leq b$. A adição e multiplicação no $C[a,b]$ são as *operações pointwise*, definidas pelas:

$$f + g = \lambda x \,.\, f(x) + g(x) \qquad\qquad f \cdot g = \lambda x \,.\, f(x) \cdot g(x).$$

(Veja a Definição D9.203.)

• **EXEMPLO 12.20.**
Fez o Problema Π11.24?[92] Quem fez, sabe que se G' é abeliano, então o $(\mathrm{Hom}(G,G)\,;+)$ onde $(+)$ é a operação pointwise baseada no $+_{G'}$. Em particular, para qualquer grupo abeliano G o conjunto

$$\mathrm{End}(G) \overset{\text{def}}{=} \mathrm{Hom}(G,G)$$

vira um grupo abeliano $(\mathrm{End}(G)\,;+)$. Mas no mesmo conjunto uma outra operação interessante é a composição. O $(\mathrm{End}(G)\,;+,\circ)$ é um anel.

[92] Não? Vá lá fazer agora e volte assim que resolver.

▸ **EXERCÍCIO x12.7.**
Demonstre! (x12.7H0)

D12.21. Definição. Se num anel R temos $0_R = 1_R$ chamamos o R de *anel zero*. Caso contrário *anel não-zero*.

Λ12.22. Lema (Zero absorve). *Seja R um anel. Então:*

$$\text{para todo } x \in R, \quad 0x = 0 = x0.$$

Demonstração. Seja $x \in R$. Calculamos:

$$\begin{aligned} 0x &= (0+0)x && \text{(def. 0)} \\ &= 0x + 0x && \text{(pela (RDR))} \end{aligned}$$

Achamos então que $0x$ é uma resolução da $0x + \ ? \ = 0x$. E como o $(R\,;+)$ é um grupo sabemos então que $0x = 0$ (Corolário 11.62) que foi o que queremos demonstrar. ∎

12.23. Corolário. *Se R é um anel zero, R é um singleton.*

Demonstração. Seja $r \in R$. Calculamos:

$$r = r1_R = r0_R = 0_R.$$

∎

▸ **EXERCÍCIO x12.8.**
Para todo $a, b \in R$,

$$-(a-b) = b - a.$$

(x12.8H0)

Λ12.24. Lema (Negação de produto). *Seja R um anel. Logo,*

$$\text{para todo } a, b \in R, \quad (-a)b = -(ab) = a(-b).$$

▸ Esboço. Para demonstrar a primeira igualdade, basta enxergá-la como a afirmação seguinte: *o $(-a)b$ é o $(+)$-inverso do ab*. Verificamos então que $ab + (-a)b = 0$. A outra igualdade é similar. □ (Λ12.24P)

12.25. Corolário. *Em qualquer anel $\mathcal{R}$, para todos $x, y \in \mathcal{R}$ temos:*
(i) $(-x)(-y) = xy$;
(ii) $(-1)x = -x$;
(iii) $(-1)(-1) = 1$;
(iv) $-(x+y) = (-x) + (-y)$.

▸ **EXERCÍCIO x12.9.**
Seja X conjunto. Defina no $\wp X$ duas operações tais que $\wp X$ vira um anel. Identifique quais são os seus $0, 1$ e demonstre que realmente é um anel. (x12.9H123)

? **Q12.26. Questão.** Como tu definirias o conceito de subanel? Pode definir algum critério parecido com os critéria 11.99 ou 11.102 para decidir se algo é subanel dum dado anel? E o homomorfismo de anel? Como definirias isso? E pode definir algum critério parecido com o 11.219?

!! SPOILER ALERT !!

D12.27. Definição (subanel). Seja $\mathcal{R}$ um anel. O $S \subseteq R$ é um *subanel* de $\mathcal{R}$ sse $(S\,;+_R,\cdot_R,0_R,1_R)$ é um anel.

12.28. Critérion (de subanel). *Sejam R anel e $S \subseteq R$. O S é um subanel de R sse:*
(i) *S tem a identidade do R: $1_R \in S$;*
(ii) *S é fechado sob a adição: para todo $a, b \in S$, $a + b \in S$;*
(iii) *S é fechado sob a multiplicação: para todo $a, b \in S$, $ab \in S$;*
(iv) *S é fechado sob negativos: para todo $a \in S$, $-a \in S$.*

D12.29. Definição (homomorfismo). Sejam os anéis $\mathcal{R} = (R\,;+_R,\cdot_R,0_R,1_R)$ e $\mathcal{S} = (S\,;+_S,\cdot_S,0_S,1_S)$. A função $\varphi : R \to S$ é um homomorfismo sse:
(i) $\varphi(0_R) = 0_S$;
(ii) $\varphi(1_R) = 1_S$;
(iii) para todo $x, y \in R$, $\varphi(x +_R y) = \varphi(x) +_S \varphi(y)$;
(iv) para todo $x, y \in R$, $\varphi(x \cdot_R y) = \varphi(x) \cdot_S \varphi(y)$;
(v) para todo $x \in R$, $\varphi(-x) = -(\varphi(x))$.

12.30. Critérion (de homomorfismo). *Se a função $\varphi : \mathcal{R} \to \mathcal{S}$ satisfaz:*

$$\begin{aligned} \varphi(1_R) &= 1_S \\ \varphi(x +_R y) &= \varphi(x) +_S \varphi(y) \quad \text{para todo } x, y \in R \\ \varphi(x \cdot_R y) &= \varphi(x) \cdot_S \varphi(y) \quad \text{para todo } x, y \in R \end{aligned}$$

então ela é um homomorfismo. (Ou seja, podemos apagar os itens (i) e (v) na Definição D12.29.)

Demonstração. Como $(R\,;+_R)$ e $(S\,;+_S)$ são grupos, sabemos que se φ respeita a operação aditiva então ela necessariamente respeita sua identidade e seus inversos também (Critérion 11.219). ∎

▸ **EXERCÍCIO x12.10.**
As leis de anel exigem que sua parte aditiva é um grupo abeliano, e que sua parte multiplicativa é um monóide. Pode ter anel $\mathcal{R} = (R\,;+,\cdot,0,1)$ cuja parte multiplicativa realmente forma um grupo? Ou seja, tal que $(R\,;\cdot,1)$ é um grupo? Se sim, mostre um exemplo de tal anel; se não, demonstre que não existe tal anel. (x12.10H12)

D12.31. Definição (kernel, image). Seja $\varphi : R \to S$ homomorfismo de anéis.

$$\ker \varphi \stackrel{\text{def}}{=} \varphi_{-1}[\{0_S\}] \quad \big(= \{\, r \in R \mid \varphi(r) = 0_S \,\} \big)$$
$$\operatorname{im} \varphi \stackrel{\text{def}}{=} \varphi[R] \quad \big(= \{\, s \in S \mid (\exists r \in R)[\, \varphi(r) = s \,] \,\} \big)$$

Podemos já demonstrar o equivalente do Exercício x11.145 que encontramos nos grupos, para os anéis:

Λ12.32. Lema. *Seja $\varphi : R \to S$ um homomorfismo de anéis. Sua imagem $\operatorname{im}\varphi$ é um subanel de S.*

▸ Esboço. Usamos o Critérion 12.28 e a definição de $\operatorname{im}\varphi$. □ (Λ12.32P)

? **Q12.33. Questão.** Será que o kernel é algo mais-legal-que-subanel na mesma forma que aconteceu nos grupos?

!! SPOILER ALERT !!

▸ **EXERCÍCIO x12.11.**
Seja $\varphi : R \xrightarrow{\text{hom}} S$. O que consegues demonstrar entre o $\ker\varphi$ e o R? (x12.11H0)

§264. Anéis booleanos

D12.34. Definição (Anel booleano). Chamamos o anel $\mathcal{R}$ um *anel booleano* sse sua multiplicação é *idempotente*, ou seja:

$$\text{para todo } a \in \mathcal{R}, \quad a^2 = a.$$

• **EXEMPLO 12.35.**
Dado conjunto X, o $(\wp X\, ; \triangle, \cap)$ é um anel booleano.

▸ **EXERCÍCIO x12.12.**
Seja $\mathcal{R}$ um anel booleano. Demonstre que:

$$\text{para todo } p \in \mathcal{R}, \quad p = -p.$$

(x12.12H1)

▸ **EXERCÍCIO x12.13.**
Seja $\mathcal{R}$ um anel booleano. Demonstre que:

$$\text{para todo } p, q \in \mathcal{R}, \quad pq = -qp$$

e mostre como isso gera mais uma demonstração do Exercício x12.12. (x12.13 H 1)

▸ **EXERCÍCIO x12.14.**
Todo anel booleano é comutativo. (x12.14 H 1)

§265. Domínios de integridade

D12.36. Definição (Divisores de zero). Seja R um anel, e $x, y \in R$. Se $xy = 0_R$ e nem $x = 0_R$ nem $y = 0_R$, chamamos os x, y *divisores de zero* (ou *zerodivisores*) no R.

• **EXEMPLO 12.37.**
No anel $\mathbb{Z}_6$, temos $2 \cdot 3 = 0$. Logo ambos os $2, 3$ são divisores de zero nesse anel. O 4 também é, pois $3 \cdot 4 = 0$ também.

• **EXEMPLO 12.38.**
Considere o anel $C[-1, 1]$ com as operações pointwise (veja Exemplo 12.19). Tome as funções f, g definidas pelas

$$f(x) = \begin{cases} -x, & \text{se } x \leq 0 \\ 0, & \text{se } x > 0 \end{cases} \qquad g(x) = \begin{cases} 0, & \text{se } x \leq 0 \\ x, & \text{se } x > 0. \end{cases}$$

Calculando, achamos

$$f \cdot g = \lambda x \,.\, 0_{C[-1,1]}$$

e logo os f, g são divisores de zero no $C[-1, 1]$.

▸ **EXERCÍCIO x12.15.**
Desenhe os gráficos das funções f, g do Exemplo 12.38, e com um cálculo explique porque $f \cdot g = 0$. (x12.15 H 0)

D12.39. Definição (Domínio de integridade e de cancelamento). Seja $\mathcal{D}$ um anel comutativo. Chamamos o $\mathcal{D}$ *domínio de integridade* sse ele não tem zerodivisores, ou seja, sse:

(NZD) para todo $x, y \in D$, se $xy = 0$ então $x = 0$ ou $y = 0$.

Chamamos o $\mathcal{D}$ *domínio de cancelamento* sse

(RCL) para todo $a, x, y \in D$, $ax = ay \;\&\; a \neq 0 \implies x = y$.

que é equivalente à

(RCR) para todo $a, x, y \in D$, $xa = ya \;\&\; a \neq 0 \implies x = y$.

pois esse anel é comutativo.

12.40. Critérion. *Os termos "domínio de integridade" e "domínio de cancelamento" são sinônimos, ou seja:*

$$D \text{ é um domínio de integridade} \iff D \text{ é um domínio de cancelamento.}$$

Demonstração. ($\Rightarrow$): Sejam $a, x, y \in D$ tais que $a \neq 0$ e $ax = ay$. Logo $ax - ay = 0$. Logo $a(x - y) = 0$. Pela hipótese (NZD) então $x - y = 0$, ou seja $x = y$.
($\Leftarrow$): Sejam $x, y \in D$ tais que $xy = 0$ e $x \neq 0$. Queremos $y = 0$. Temos $xy = 0 = x0$ (pois $0 = 0x$ em todo anel). Ou seja $xy = x0$, e como $x \neq 0$, usando a (RCL) concluimos $y = 0$. ∎

§266. Corpos

D12.41. Definição (Corpo). Seja $\mathcal{K}$ um anel não-zero e comutativo. Chamamos o $\mathcal{K}$ um *corpo* (ou *field*) sse todos os seus membros diferentes de 0 são invertíveis, ou seja sse:

(FM3*) para todo $a \in K_{\neq 0}$, existe $y \in K$, tal que $ay = 1 = ya$.

- **EXEMPLO 12.42.**
Os racionais, os reais, e os complexos, com suas operações canônicas de adição e multiplicação são todos corpos.

- **NÃOEXEMPLO 12.43.**
Os inteiros e os naturais não!

- **EXEMPLO 12.44.**
O $\mathcal{Z}_p = (\mathbb{Z}/p\mathbb{Z}\,; +_p, \cdot_p)$ onde p primo é um corpo.

- **NÃOEXEMPLO 12.45.**
O $\mathcal{Z}_n$ onde $n > 1$ e não primo, não é um corpo.

12.46. Critérion. *Se D é um domínio de integridade finito então D é um corpo.*

Demonstração. Suponha que D é um domínio de integridade finito. Precisamos mostrar que cada $d \neq 0$ no D tem inverso. Seja $d \in D$, $d \neq 0$. Procuro $d' \in D$ tal que $dd' = 1$. Sejam

$$d_1, d_2, \ldots, d_n$$

todos os elementos distintos de $D \setminus \{0\}$. Considere os

$$dd_1, dd_2, \ldots, dd_n.$$

Observe que:

$$dd_i = dd_j \overset{\text{(RCL)}}{\Longrightarrow} d_i = d_j \implies i = j.$$

Ou seja,

$$D \setminus \{0\} = \{dd_1, dd_2, \ldots, dd_n\}.$$

Ou seja, como $1 \in D \setminus \{0\}$,

$$1 = dd_u \quad \text{para algum } u \in \{1, \ldots, n\}$$

que é o que queremos demonstrar. ∎

▸ **EXERCÍCIO x12.16.**
Demonstre que o Exemplo 12.44 realmente é um exemplo de corpo e que o Nãoexemplo 12.45 realmente não é. (x12.16H0)

12.47. Considere um corpo $\mathcal{F}$. Uma coisa que podemos já fazer sem saber nada mais é somar o 1 com o 1 e considerar o elemento $1+1 \in F$. Agora podemos somar mais um 1, e considerar o $1+1+1 \in F$. E por aí vai: sabemos que todos eles são membros do F mesmo pois F é $(+)$-fechado. Agora, existem duas opções: (i) todos esses objetos são diferentes do 0; (ii) existe $k > 0$ tal que a soma de k 1's é 0. Observe que no caso (ii) pelo principio da boa ordem existe um menor tal inteiro m. Chegamos no conceito importante seguinte:

D12.48. Definição (Corpo).

TODO Escrever

▸ **EXERCÍCIO x12.17.**
Um corpo é finito sse tem característica positiva. (x12.17H0)

▸ **EXERCÍCIO x12.18.**
A característica de qualquer corpo finito é um número primo. (x12.18H0)

§267. Ações

TODO Escrever

§268. Modules

TODO Escrever

§269. Espaços vetoriais

Os espaços vetoriais é o exemplo mais conhecido de estrutura algébrica que envolve *dois* conjuntos como carrier sets.

D12.49. Definição. Sejam $F = (F\ ;+,\cdot,-,0,1)$ um corpo e $V = (V\ ;\oplus,\ominus,\mathbf{0})$ um grupo abeliano. Chamamos o $(V,F\ ;*)$ com $* : F \times V \to V$ dum *espaço vetorial sobre o* F sse as leis abaixo são satisfeitas. Chamamos os membros de F de *escalares*, e os membros de V de *vetores*. Se $F = \mathbb{R}$, temos um *espaço vetorial real*; se $F = \mathbb{C}$, um *espaço vetorial complexo*. Usarei $a, b, c, \ldots$ ou letras gregas como metavariáveis para denotar escalares; e para denotar vetores userei $\mathbf{u}, \mathbf{v}, \mathbf{w}, \ldots$ e também $\vec{u}, \vec{v}, \vec{w}, \ldots$. A operação $*$ é chamada *multiplicação escalar* e é sempre denotada por justaposição. Mesmo que denotamos a multiplicação do corpo $(\cdot)$ também por justaposição, isso não gera confusão.

Para diferenciar entre a multiplicação escalar e a multiplicação do corpo chamarei de *scalaplicação* a primeira e *multiplicação* a segunda. Finalmente, as leis:

(VS1) compatibilidade da scalaplicação com a multiplicação;
(VS2) identidade da scalaplicação;
(VS3) distributividade da scalaplicação com a adição dos vetores;
(VS4) distributividade da scalaplicação com a adição dos escalares.

Formulamente:

$$\begin{aligned}
&\text{(VS1)} && a(b\mathbf{v}) = (ab)\mathbf{v}\\
&\text{(VS2)} && 1\mathbf{v} = \mathbf{v}\\
&\text{(VS3)} && a(\mathbf{u} \oplus \mathbf{v}) = a\mathbf{u} \oplus a\mathbf{v}\\
&\text{(VS4)} && (a+b)\mathbf{v} = a\mathbf{v} \oplus b\mathbf{v}.
\end{aligned}$$

Escrevemos $+, -$ em vez dos $\oplus, \ominus$ quando é claro quais são as operações.

- **EXEMPLO 12.50.**
O $\mathbb{R}$ é um espaço vetorial sobre o $\mathbb{R}$.

- **EXEMPLO 12.51.**
O $\mathbb{R}^2$ com

$$\begin{aligned}
(x,y) \oplus (x',y') &= (x+x', y+y')\\
\ominus(x,y) &= (-x,-y)\\
\mathbf{0} &= (0,0)
\end{aligned}$$

é um espaço vetorial real.

O estudo de espações vetorias e seus morfismos (*transformações lineares*) é chamado *algebra linear*.

§270. Teoria de Galois

TODO Escrever

§271. Reticulados

12.52. Leis de reticulado. Num reticulado temos duas operações binárias que chamamos de *join* ($\vee$) e *meet* ($\wedge$). Elas satisfazem as leis de reticulado:

$$\text{associatividade} \begin{cases} a \vee (b \vee c) = (a \vee b) \vee c \\ a \wedge (b \wedge c) = (a \wedge b) \wedge c \end{cases} \quad \begin{cases} a \vee b = b \vee a \\ a \wedge b = b \wedge a \end{cases} \text{comutatividade}$$

$$\text{idempotência} \begin{cases} a \vee a = a \\ a \wedge a = a \end{cases} \quad \begin{cases} a \vee (a \wedge b) = a \\ a \wedge (a \vee b) = a \end{cases} \text{absorpção}$$

Observe que sem as leis de absorpção não temos uma estrutura interessante. Essas leis nos dizem como as duas operações interagem e oferecem à teoria de reticulados sua alma. Formalmente, temos:

D12.53. Definição. Seja $\mathcal{L} = (L\ ;\ \vee, \wedge)$ um conjunto estruturado onde $\vee, \wedge$ são operações binárias que chamamos de *join* e *meet* respectivamente. $\mathcal{L}$ é um *reticulado* (ou *láttice*) sse:

(LJ0) $(\forall a, b \in L)[\, a \vee b \in L\,]$
(LJ1) $(\forall a, b, c \in L)[\, a \vee (b \vee c) = (a \vee b) \vee c\,]$
(LJ2) $(\forall a, b \in L)[\, a \vee b = b \vee a\,]$
(LJ3) $(\forall a \in L)[\, a \vee a = a\,]$
(LM0) $(\forall a, b \in L)[\, a \wedge b \in L\,]$
(LM1) $(\forall a, b, c \in L)[\, a \wedge (b \wedge c) = (a \wedge b) \wedge c\,]$
(LM2) $(\forall a, b \in L)[\, a \wedge b = b \wedge a\,]$
(LM3) $(\forall a \in L)[\, a \wedge a = a\,]$
(LAJ) $(\forall a, b \in L)[\, a \vee (a \wedge b) = a\,]$
(LAM) $(\forall a, b \in L)[\, a \wedge (a \vee b) = a\,]$.

Seja $\mathcal{L} = (L\ ;\ \vee, \wedge, 0, 1)$ um conjunto estruturado onde $\vee, \wedge$ são operações binárias e $0, 1$ constantes, e tal que $\mathcal{L}$ é um *reticulado limitado* (ou *bounded láttice*) sse $(L\ ;\ \vee, \wedge)$ é um reticulado e

(LJB) $(\forall a \in L)[\, a \vee 0 = a\,]$
(LJB) $(\forall a \in L)[\, a \wedge 1 = a\,]$.

12.54. Critérion. *Seja $\mathcal{L} = (L\ ;\ \vee, \wedge)$ conjunto estruturado onde $\vee$ e $\wedge$ satisfazem as leis de: associatividade, comutatividade, absorção. Então $\mathcal{L}$ é um reticulado.*

Demonstração. Exercício x12.19. ∎

▸ **EXERCÍCIO x12.19.**
Demonstre o Critérion 12.54. (x12.19 H 1)

▸ **EXERCÍCIO x12.20.**
Seja $\mathcal{L} = (L\ ;\ \vee, \wedge)$ um reticulado pela Definição D12.53. Demonstre que:

$$a \vee b = b \iff a \wedge b = a.$$

(x12.20 H 0)

D12.55. Definição. Seja $\mathcal{S} = (S\ ;\ \diamond)$ um conjunto estruturado onde $\diamond$ é uma operação binária. $\mathcal{S}$ é um *semirreticulado* (ou *semiláttice*) sse sua operação é associativa, comutativa, e idempotente:

(SL0) $(\forall a, b \in S)[\, a \diamond b \in S\,]$
(SL1) $(\forall a, b, c \in S)[\, a \diamond (b \diamond c) = (a \diamond b) \diamond c\,]$
(SL2) $(\forall a, b \in S)[\, a \diamond b = b \diamond a\,]$
(SL3) $(\forall a \in S)[\, a \diamond a = a\,]$.

Seja $\mathcal{S} = (S\,;\diamond,\ell)$ um conjunto estruturado tal que $(S\,;\diamond)$ é um semirreticulado e ℓ é uma constante. $\mathcal{S}$ é um *semirreticulado limitado* (ou *bounded semiláttice*) sse:

(SLB) $$(\forall a \in S)[\, a \diamond \ell = a\,].$$

12.56. Observação (Definições mais curtas). Com as definições de semirreticulados podemos definir numa maneira mais simples o que é um reticulado:

▸ **EXERCÍCIO x12.21 (Definições mais curtas).**
Defina os conceitos "reticulado" e "reticulado limitado" usando os conceitos "semirreticulado" e "semirreticulado limitado". (x12.21 H 0)

Nosso objectivo aqui é brincar com várias estruturas algébricas, e não aprofundar em nenhuma. Mas se preocupe não: voltamos a estudar reticulados no Capítulo 14.

§272. Estruturas não puramente algébricas

TODO Escrever

D12.57. Definição (Corpo ordenado completo). Um corpo ordenado F é *completo* sse todos os seus subconjuntos bounded above possuem supremum no F

(FC) $$(\forall A \subseteq \mathbb{R})[\, l \text{ cotado por cima } \implies A \text{ tem supremum no } F\,].$$

• **EXEMPLO 12.58.**
Os reais $(\mathbb{R}\,;+,\cdot,-,0,1,<)$.

▸ **EXERCÍCIO x12.22.**
Tem como demonstrar isso? Se sim, o que seria uma demonstração disso? Se não, por que não? (x12.22 H 0)

12.59. Chega!. Vamos revisar pouco a situação com as estruturas que estudamos até agora. Como a gente escolha os axiomas (leis) que botamos nas nossas definições? As mais leis que eu boto, as mais ferramentas que ganho para matar mais teoremas. Minha teoria vai acabar sendo capaz de demonstrar mais coisas, mas o preço que pago para isso são modelos!

Quantos monóides encontramos? Demais! Todos os grupos são monóides, e a gente já encontrou ainda mais monóides que não são grupos (lembra?). E grupos? Menos, mas muitos também! E grupos abelianos? Demonstramos mais teoremas, mas temos menos exemplos de grupos abelianos. E anéis? E anéis comutativos? E domínios de integridade? Cada vez que adicionamos restricções (leis), a teoria correspondente cresce, e a colecção de models diminui. E corpos? Ainda encontramos vários modelos: racionais, reais, complexos, inteiros módulo primo p, ...

E corpos ordenados? Aqui ganhamos muita teoria graças a ordem, mas perdemos os complexos e os inteiros módulo p, mas ainda temos os reais e os racionais e mais uns

modelos, mas já estamos percebendo que fica mais e mais difícil achar modelos *realmente* diferentes que satisfazem todas as leis!

E agora? Adicionamos mais uma lei: o axioma da completude; e assim chegamos nos *corpos ordenados completos*. E agora *chega!* Estamos num ponto onde adicionamos tantos axiomas que nosso conceito foi tão exigente que perdemos todos os modelos exeto um: os reais! Realmente não encontramos outro exemplo, mas isso não significa que não existem outros modelos. Certo? Certo, mas acontece que nessa situação não é o caso: *essencialmente existe apenas um único corpo ordenado completo: os reais!*

? **Q12.60. Questão.** O que significa a palavra «essencialmente» acima?

!! SPOILER ALERT !!

Θ12.61. Teorema (Unicidade). *Se R, R' são corpos ordenados completos então R, R' são isómorfos.*

▸ Esboço. Sejam $(R\,;+,\,\cdot\,,-,0,1,<)$ e $(R'\,;+',\,\cdot'\,,-',0',1',<')$ corpos ordenados completos. Precisamos definir um isomorfismo

$$\varphi\ :\ (R\,;+,\,\cdot\,,-,0,1,<) \xrightarrow{\ \cong\ } (R'\,;+',\,\cdot'\,,-',0',1',<').$$

Obviamente botamos

$$\begin{aligned}\varphi 0 &= 0'\\ \varphi 1 &= 1'\end{aligned}$$

Isso já determina a φ no resto dos "naturais" $N \subseteq R$:

$$\begin{aligned}\varphi 2 = \varphi(1+1) &= \varphi 1 + \varphi 1 = 1' + 1' = 2'\\ \varphi 3 = \varphi(2+1) &= \varphi 2 + \varphi 1 = 2' + 1' = 3'\\ &\vdots\\ \varphi(n+1) &= \varphi n + \varphi 1 = n' + 1'\\ &\vdots\end{aligned}$$

ou seja, a φ (restrita no N) necessariamente embute isomorficamente o $N \subseteq R$ no $\varphi[N] = N' \subseteq R'$:

$$\varphi|_N : N \xrightarrow{\ \cong\ } N'.$$

Agora, como φ é homomorfismo, temos

$$\varphi(-x) = -'(\varphi x) \quad \text{para todo } x \in R,$$

e logo a φ necessariamente embute os "inteiros" $Z \subseteq R$ nos "inteiros" $Z' \subseteq R'$:

$$\varphi|_Z : Z \xrightarrow{\ \cong\ } Z'.$$

Definimos a φ nos "racionais" $Q \subseteq R$ assim:

$$\varphi(m/n) = \varphi(m \cdot n^{-1}) = \varphi m \cdot' (\varphi n)^{-1} = \varphi m \cdot' \varphi(n^{-1}) = \varphi m \,/'\, \varphi n$$

e logo

$$\varphi|_Q : Q \xrightarrow{\cong} Q'.$$

Estamos perto! Basta só definir a φ nos "buracos" (nos "irracionais") de R e pronto! □

12.62. Observação. Infelizmente, por enquanto não temos todo o armamento para matar os detalhes e o que falta no esboço, mas é importante entender pelo menos tudo que tá lá. Voltamos nesse assunto no Capítulo 16 (§327).

! **12.63. Aviso.** Mesmo se aceitar que quaisquer corpos ordenados completos são isomorfos (o Teorema Θ12.61), ainda temos um ponto que roubamos: para existir único, precisamos duas coisas: *pelo menos* um; *no máximo* um. O Θ12.61 realmente ofereceu a segunda coisa; mas a primeira? Qual foi tua resolução do Exercício x12.22 mesmo? Voltamos nesse assunto no Capítulo 16 (§327).

TODO Reorganizar o seguinte

12.64. Calculus, real e oficial. Como começamos a teoria dos grupos no Capítulo 11? Apresentamos os axiomas dos grupos e continumos investigando suas conseqüências. A colecção dessas conseqüências (teoremas) é exatamente o que chamamos de *teoria*. E a *teoria dos anéis* é feita por todos os teoremas que seguem pelos axiomas de anéis; etc. etc. E a *teoria dos corpos ordenados completos?* Ela não é muito famosa por esse nome, mas com certeza tu já ouviste falar dela por uns dos seus apelidos: *calculus*, ou *análise real*, Capítulo 6, etc. Na abordagem axiomática, não nos importa *definir* ou *construir* os objetos que vamos chamar de *números reais*. Começamos aceitando a existência dum certo conjunto que denotamos por $\mathbb{R}$ e umas noções primitivas, e estipulamos uns axiomas sobre eles. A partir de tais noções primitivas e tais axiomas procedemos para definir mais conceitos, e demonstrar mais proposições (os teoremas), elaborando assim a teoria dos corpos ordenados completos.

Problemas

▸ **PROBLEMA Π12.1.**
Considere o conjunto $\mathcal{N}_{00}$ das seqüências infinitas de naturais "eventualmente zero", ou seja

$$\mathcal{N}_{00} \stackrel{\text{def}}{=} \{\, f : \mathbb{N} \to \mathbb{N} \mid (\exists N \in \mathbb{N})(\forall n \geq N)[\, f(n) = 0\,]\,\}\,.$$

Consideramos a operação de *adição pointwise* definida pela:

$$(f + g)(x) = f(x) + g(x).$$

Demonstre que $\mathcal{N}_{00}$ com essa operação forma um monóide isómorfo com o monóide $(\mathbb{N}_{>0}\,;\cdot)$ (com operação a multiplicação usual). (Π12.1H0)

Leitura complementar

[Pin10], [Her75], [BM77b], [MB99]. [Sha87].

Sugiro novamente o [Alu09] como uma introdução completa em algebra.

Dois livros excelentes para uma introdução em algebra linear especificamente são os [Hal93] e [Hal95] (para ser estudados em paralelo). Um primeiro toque dá pra pegar também pelos [Apo67] e [Apo69].

CAPÍTULO 13

O PARAÍSO DE CANTOR

Um pouco de contexto histórico

TODO Terminar as duas histórias

13.1. Números selvágens. 1682: Leibniz demonstra que sin não é uma *função algébrica*. 1700: Euler define os números *transcendentais*; mas não consegue demonstrar se existem ou não. 1768: Lambert demonstra que π é *irracional* e os e^q também, para qualquer $q \in \mathbb{Q}_{\neq 0}$. 1844: Liouville demonstra que existem números transcendentais. Definiu o que hoje chamamos de *números Liouville*, mostrou que todos eles são transcendentais, e no 1851 construiu um número Liouville específico, a *constante Liouville*

$$\sum_{n=1}^{\infty} 10^{-n!} = 0.11000100000000000000000100\ldots$$

que foi (finalmente) um exemplo simples e concreto de um número transcendental. 1870–1872: Cantor; 1873: Hermite demonstrou que e é transcendental. Esse foi o primeiro número transcendental que conhecemos cujo objectivo (cuja definição) não foi feita para ser um tal número. Liouville *definiu* seus números com objectivo de achar transcendentais. O e já era definido e estudado muito, e sua *raison d'être* não tinha nada a ver com os números transcendentais. 1882: von Lindemann demonstra a transcendentalidade dos e^α para $\alpha \neq 0$ algébrico—e logo do π também (Problema II13.10)—e Weierstrass generaliza no 1885 para o teorema conhecido como Lindemann–Weierstrass na teoria de números transcendentais.

13.2. De séries Fourier para o estudo de conjuntos. 1870: Cantor se interessou nas *séries Fourier*. O que são não é importante nesse momento;[93] basta saber que são determinadas por seus *coeficientes* que são duas seqüências de números reais

$$a_1, a_2, a_3, \ldots \qquad\qquad b_1, b_2, b_3, \ldots$$

Cantor demonstrou um teorema impressionante:

[93] Uma série Fourier tem a forma

$$f(x) = a_0 + \sum_{n=1}^{\infty} a_n \cos(nx) + \sum_{n=1}^{\infty} b_n \sin(nx).$$

Os a_n's e b_n's são seus coeficientes.

Θ13.3. Teorema (Cantor, 1870). *Sejam f, f' séries Fourier que convergem pointwise numa função no $[0, 2\pi]$. Então os coeficientes das f, f' são iguais.*

Mas Cantor se perguntou: «E se elas convergem na mesma função em todo o $[0, 2\pi]$ *exceto um conjunto de possíveis excessões* $E \subseteq [0, 2\pi]$? Será que se o E não é grande demais eu ainda consigo demonstrar o mesmo resultado, que os coeficientes são iguais?» E realmente conseguiu, já no próximo ano:

Θ13.4. Teorema (Cantor, 1871). *Sejam f, f' séries Fourier que convergem pointwise na mesma função no $[0, 2\pi] \setminus E$. Se E é finito, então os coeficientes das f, f' são iguais.*

Observe que o teorema de 1870 é um caso especial do teorema de 1871, tomando $E := \emptyset$. No próximo ano, Cantor conseguiu melhorar ainda mais seu teorema:

Θ13.5. Teorema (Cantor, 1872). *Sejam f, f' séries Fourier que convergem pointwise na mesma função no $[0, 2\pi] \setminus E$. Se E é derivável até $\emptyset$, então os coeficientes das f, f' são iguais.*

O que significa *derivável até* $\emptyset$ vamos encontrar no Capítulo 17; por enquanto basta saber que essa condição é satisfeita por muitos conjuntos *infinitos*, e por todos os conjuntos finitos, e logo o teorema de 1871 é um caso especial do teorema de 1872.

Essas aventuras fizeram Cantor se preocupar sobre os conjuntos como objetos matemáticos próprios, como "first-class cítizens" e se preocupar sobre seus tamanhos também. E assim nasceu a *teoria (ingênua) dos conjuntos*. Neste capítulo estudamos as idéias de Cantor sobre conjuntos e sobre infinidade(s); descobertas importantíssimas em matemática, tanto que faz sentido de falar sobre matemática a.C. e d.C. (antes Cantor e depois Cantor).

§273. O que é contar e comparar quantidades?

13.6. Quando queremos *contar* a quantidade de membros dum conjunto A, começamos apontando a cada um deles e, usando *números*, atribuimos um para cada membro. No final das contas—ahem—acabamos com um certo número n e digamos que A tem n membros. A *cardinalidade* de A, é o n. Em símbolos,

$$|A| = n.$$

Essa análise tem varios pontos hipersimplificados e talvez controversiais.

Primeiramente note que, se o conjunto A é infinito, esse processo nunca vai parar, e a gente não vai conseguir atribuir um $n \in \mathbb{N}$ para representar a cardinalidade $|A|$. Além disso, precisamos *ter* os números. Isso talvez parece um ponto bobo, mas vale a pena se perguntar se os humanos sabiam sobre o conceito de *quantidade*, e equivalentemente de *cardinalidade de conjunto*, antes de *ter* os números ou não!

13.7. Precisamos mesmo de números?. Sabemos como contar conjuntos finitos então. E usamos o $\mathbb{N}$ para representar as quantidades possíveis. Agora não queremos contar, mas *comparar* dois conjuntos *com relação à quantidade de elementos*. A discussão sobre contagem acima presuponha a existência dos números que usamos para contar: 1, 2, 3, etc., e dependende da época talvez o 0 também faz parte desses números. Mas, bem antes de ter números para contar, os humanos poderiam comparar quantidades. Talvez um humano prehistórico sabia dizer que ele tem a mesma quantidade de filhos que seu vizinho, sem saber dizer que cada um tem *cinqo* filhos. Como ele sabia então comprarar essas cardinalidades?

§274. Equinumerosidade

D13.8. Definição. Como usamos bastante o conjunto $\{0, 1, \ldots, n-1\}$, vale a pena introduzir uma notação para denotá-lo:

$$\overline{n} \stackrel{\text{"def"}}{=} \{0, \ldots, n-1\}\,.$$

▸ **EXERCÍCIO x13.1.**
Defina o $\overline{n}$ usando a notação set builder. (x13.1 H 1)

▸ **EXERCÍCIO x13.2.**
Defina o operador $\overline{\bullet} : \mathbb{N} \to \wp\mathbb{N}$ recursivamente. (x13.2 H 1)

D13.9. Definição (Equinúmeros). Chamamos os conjuntos A e B *equinúmeros* sse existe bijecção $f : A \rightarrowtail\!\!\!\!\twoheadrightarrow B$. Escrevemos:

$$A =_{\mathrm{c}} B \iff^{\mathsf{def}} (\exists f)[\, f : A \rightarrowtail\!\!\!\!\twoheadrightarrow B\,].$$

Continuamos em definir mais relações para comparar os tamanhos de conjuntos:

D13.10. Definição. Sejam A e B conjuntos. Definimos

$$A \leq_{\mathrm{c}} B \iff^{\mathsf{def}} (\exists B_0 \subseteq B)[\, A =_{\mathrm{c}} B_0\,]$$
$$A <_{\mathrm{c}} B \iff^{\mathsf{def}} A \leq_{\mathrm{c}} B \;\&\; A \neq_{\mathrm{c}} B$$

Seguindo nossa práctica comum, usamos também $A >_{\mathrm{c}} B$ como sinónimo de $B <_{\mathrm{c}} A$, $A \not\geq_{\mathrm{c}} B$ para significar que não é o caso que $B \leq_{\mathrm{c}} A$, etc.

▸ **EXERCÍCIO x13.3.**
Verifique que

$$A \subseteq B \implies A \leq_{\mathrm{c}} B.$$

Mostre que, em geral,

$$A \subsetneq B \not\Longrightarrow A <_{\mathrm{c}} B.$$

(x13.3 H 0)

▸ **EXERCÍCIO x13.4.**
Demonstre ou refute a afirmação que podemos usar a seguinte definição como alternativa:

$$A <_{\mathrm{c}} B \stackrel{?}{\iff} (\exists B_0 \subsetneq B)[\, A =_{\mathrm{c}} B_0 \,].$$

(x13.4 H 1)

▸ **EXERCÍCIO x13.5.**
Demonstre ou refute a afirmação que podemos usar a seguinte definição como alternativa:

$$A \leq_{\mathrm{c}} B \stackrel{?}{\iff} (\exists f)[\, f : A \rightarrowtail B \,].$$

(x13.5 H 1)

▸ **EXERCÍCIO x13.6.**
Podemos usar a seguinte definição como alternativa?:

$$A \leq_{\mathrm{c}} B \stackrel{?}{\iff} (\exists f)[\, f : B \twoheadrightarrow A \,].$$

(x13.6 H 0)

▸ **EXERCÍCIO x13.7.**
A $=_{\mathrm{c}}$ é uma relação de equivalência. Ou seja:

reflexiva:	para todo conjunto A, $A =_{\mathrm{c}} A$;
transitiva:	para todo conjunto A, B, C, $A =_{\mathrm{c}} B \;\&\; B =_{\mathrm{c}} C \implies A =_{\mathrm{c}} C$;
simétrica:	para todo conjunto A, B, $A =_{\mathrm{c}} B \implies B =_{\mathrm{c}} A$.

(x13.7 H 0)

Λ13.11. Lema. *$A \leq_{\mathrm{c}}$ é:*

reflexiva:	$A \leq_{\mathrm{c}} A$;
transitiva:	$A \leq_{\mathrm{c}} B \;\&\; B \leq_{\mathrm{c}} C \implies A \leq_{\mathrm{c}} C$;
não antissimétrica:	$A \leq_{\mathrm{c}} B \;\&\; B \leq_{\mathrm{c}} A \not\implies A = B$;
"equiantissimétrica":	$A \leq_{\mathrm{c}} B \;\&\; B \leq_{\mathrm{c}} A \implies A =_{\mathrm{c}} B$.

▸ Esboço. Para as duas primeiras usamos a identidade e a composição respectivamente. Para a próxima tomando $A := \mathbb{N}$ e $B := \mathbb{Z}$ serve. Para ver que não é antissimétrica basta achar um contraexemplo: tente os $\{0\}$ e $\{1\}$. A última é realmente difícil para demonstrar: é um corolário direto do teorema Schröder–Bernstein (Teorema Θ13.45). □

▸ **EXERCÍCIO x13.8.**
$A =_{\mathrm{c}} A' \;\&\; B =_{\mathrm{c}} B' \implies A \times B =_{\mathrm{c}} A' \times B'$. (x13.8 H 0)

▸ **EXERCÍCIO x13.9.**
$A =_{\mathrm{c}} A' \implies \wp A =_{\mathrm{c}} \wp A'$. (x13.9 H 0)

▸ **EXERCÍCIO x13.10.**
$A =_{\mathrm{c}} A' \;\&\; B =_{\mathrm{c}} B' \implies (A \to B) =_{\mathrm{c}} (A' \to B')$. (x13.10 H 0)

▸ **EXERCÍCIO x13.11.**
$A =_{\mathrm{c}} A' \;\&\; B =_{\mathrm{c}} B' \implies A \uplus B =_{\mathrm{c}} A' \uplus B'$. (x13.11 H 0)

▸ **EXERCÍCIO x13.12.**
Quais das operações $\bigcup$, $\bigcap$, respeitam a equinumerosidade? (x13.12 H 1)

▸ **EXERCÍCIO x13.13.**
$((A \times B) \to C) =_{\mathrm{c}} (A \to (B \to C))$. (x13.13 H 1 2)

§275. O que é cardinalidade?

13.12. A dupla abstracção de Cantor. Cantor definiu a cardinalidade numa maneira informal, mas sua descripção é bastante indicativa e serve como uma guia para chegar numa definição formal. A cardinalidade dum conjunto A é o que fica, se a gente mentalmente esquecer a ordem que pensamos os membros de A e também os seus nomes. Assim o A parece uma colecção de pontinhos abstratos e distintos. Cantor denotou a cardinalidade de A

$$\overline{\overline{A}}$$

usando as duas barras para indicar essa "dupla abstracção".

13.13. Mas o que é um número cardinal?. Vamos voltar pouco ao passado, e seguindo os passos do livro clássico de Hausdorff ([**Hau78**]) não vamos preocupar com a *natureza* dos cardinais. Vamos deixar isso «para os filósofos», como ele disse, pois na época que ele escreveu seu texto ninguém tinha conseguido dar uma definição satisfatória de *número cardinal*. Uns anos depois, von Neumann conseguiu definir formalmente os números cardinais, algo que vamos encontrar no Secção §332. Mas sem saber o que são, já podemos usá-los deixando claro quais são as propriedades que exigimos que eles satisfaçam. Um operador de cardinalidade $|-|$ deve satisfazer pelo menos a:

$$A =_{\mathrm{c}} B \iff |A| = |B|$$

e possivelmente mais condições ainda. Vamos voltar para estudar os detalhes no Capítulo 16.

§276. Finitos e infinitos; contáveis e incontáveis; jogos para imortais

D13.14. Definição. O conjunto A é *finito* sse existe $n \in \mathbb{N}$ tal que $A =_{\mathrm{c}} \overline{n}$. O conjunto A é *infinito* sse A não é finito.

D13.15. Definição. O conjunto A é *contável* sse A é finito ou $\mathbb{N} =_c A$. Usamos os termos *enumerável* e *denumerável* como sinónimos de contável. O conjunto A é *incontável* sse A não é contável.

! 13.16. Aviso. Em muitos textos as palavras "contável" e "(d)enumerável" não são exatamente sinónimas: uma delas pode insistir que o conjunto seja infinito, e a outra relaxar essa restricção para permitir os finitos também. As duas palavras, etimologicamente e semanticamente falando, parecem ser sinônimos no mundo matemático, e por isso nesse texto eu vou usar as duas como sinônimos mesmo. Mas cuidado lendo textos diferentes, pois podem significar coisas diferentes no caso que o conjunto em questão é finito. (Sobre conjuntos infinitos os dois termos sempre concordam.)

D13.17. Definição. Uma *enumeração* dum conjunto A é qualquer surjecção $\pi : \mathbb{N} \twoheadrightarrow A$. Assim temos:

$$A = \pi[\mathbb{N}] = \{\pi(0), \pi(1), \pi(2), \dots\}$$

13.18. O jogo de enumeração de Smullyan. Smullyan criou o seguinte jogo que ajuda em entender o conceito de conjunto enumerável. Seja S um conjunto que chamaremos de *conjunto-segredo*. Tu, o jogador, e eu, o inimigo, começamos o jogo e nos dois sabemos qual é o conjunto S desse jogo. Eu jogo primeiro, escolhendo um membro $w \in S$. Teu objectivo é adivinhar o w. Todo dia tu tens um palpite, e eu vou responder "sim" ou "não". No dia i então, tu escolhe um membro $s_i \in S$ como um palpite fazer exatamente um palpite na forma equacional:

$$w = s_i?$$

onde s_i é teu i-ésimo palpite, ou seja, o palpite do dia i. Tu ganhas se um belo dia tu conseguir adivinhar a minha escolha: o w que selecionei no inicio do jogo. Um exemplo de jogo então com $S = \mathbb{N}$ parece assim:

- Eu escolhi meu membro $w \in \mathbb{N}$.
- (Dia 0:) É o 42?
- Não.
- (Dia 1:) É o 28?
- Não.
- (Dia 2:) É o 8?
- Não.
- (Dia 3:) É o 1024?
- Não.
- (Dia 4:) É o 1024?
- Não!
- (Dia 5:) É o 12?
- Sim.

Quantas tentativas tu tens? Um para cada dia, pra sempre! Pois é, um detalhe pequeno: vamos supor que nós dois somos imortais. E o inimigo não tem o direito de mudar seu palpite! O jogo então é baseado no conjunto-segredo S. O teu objectivo como jogador é adivinhar o w que eu, teu inimigo, escolhi.

O teu objectivo como matemático é achar uma *estratégia vencedora*, ou seja, *uma estratégia que garanta vitória* para o jogador. Se tal estratégia existe para esse jogo, dizemos que o S é *enumerável*. Observe que uma estratégia nesse jogo não é nada mais que uma *seqüência*

$$s_0, s_1, s_2, s_3, s_4, \dots$$

de membros de S, que o jogador vai seguir, jogando s_i no i-ésimo dia. Ela é vencedora sse

$$(\forall w \in S)(\exists i \in \mathbb{N})[\, s_i = w \,].$$

Pensando em seqüências do S como funções $s : \mathbb{N} \to S$ isso quis dizer que s é sobrejetora.

13.19. Conjunto-segredo: de easy para nightmare. Vamos ver se (e como!) tu jogaria nesse jogo com uns S variando em dificuldade:

$$S = \{12, -2, 0\}\,.$$

Espero que é óbvio como garantir vitória aqui:

$$0, 12, -2;$$

ou seja, no primeiro dia jogue o 0; se não foi o escolhido, jogue o 12; se nem isso foi o escolhido, jogue o -2 que com certeza será o certo pois não tem outros membros o S.

$$S = \mathbb{N}.$$

Aqui a situação é pouco mais complicada, mais ainda múito fácil:

$$0, 1, 2, 3, 4, \ldots ;$$

ou seja: no dia i, escolha o i! Não importa quão grande foi o número segredo w que escolhi, um belo dia (no w-ésimo dia mesmo) tu acertás! Próximo!

$$S = \mathbb{Z}.$$

Aqui eu vou adivinhar qualquer inteiro. O que farás? Observe que a última estratégia não funciona mais. Se eu escolher qualquer número negativo, tu nunca adivinharás, pois tu "ficarás preso" eternamente adicionando apenas os inteiros não-negativos. *O fato que uma estratégia não é vencedora não quer dizer que não existem vencedoras!* Aqui realmente existe!

? **Q13.20. Questão.** Tem como garantir vitória nesse jogo com $S = \mathbb{Z}$?

!! SPOILER ALERT !!

▸ **EXERCÍCIO x13.14.**
A união $C \cup D$ de dois conjuntos contáveis C, D é contável. (x13.14H0)

? **Q13.21. Questão.** Para cada um dos conjuntos seguintes, tu jogaria nesse jogo? Ou seja, tem estratégia vencedora?

$$
\begin{aligned}
I &= \{\, x \in \mathbb{R} \mid x \text{ é irracional} \,\} \\
A &= \{\, x \in \mathbb{R} \mid x \text{ é algébrico} \,\} \\
T &= \{\, x \in \mathbb{R} \mid x \text{ é transcendental} \,\} \\
C &= \{\, z \in \mathbb{C} \mid |z| = 1 \,\} \\
P_L &= \{\, p \mid p \text{ é um programa da linguagem de programação } L \,\} \\
G &= \operatorname{graph}(f), \quad \text{onde } f : \mathbb{R} \to \mathbb{R} \text{ definida pela } f(x) = x^2 \\
D &= (\mathbb{N} \to \{0, 2\}) \\
S &= (\mathbb{N} \to \mathbb{N}) \\
P &= (\mathbb{N} \rightarrowtail \mathbb{N}) \\
Z &= \{\, f : \mathbb{N} \to \mathbb{N} \mid (\exists n_0 \in \mathbb{N})(\forall n \geq n_0)[\, f(n) = 0 \,] \,\}
\end{aligned}
$$

E as respostas?. Pense nisso agora, meio-adivinhando, e até o fim desse capítulo tu vai saber a resposta para cada um deles!

Λ13.22. Lema. *Seja A conjunto. O.s.s.e.:*
(1) *A é contável*
(2) *$A \leq_{\mathrm{c}} \mathbb{N}$*
(3) *$A = \emptyset$ ou A possui enumeração.*

▸ Esboço. As direcões (1) ⇒ (2) ⇒ (3) são conseqüências fáceis das definições. Para "fechar o round-robin" ((3) ⇒ (1)), precisamos definir uma *bijecção* $f : \mathbb{N} \rightarrowtail A$ ou $f : \overline{n} \rightarrowtail A$, dados uma *surjecção* $\pi : \mathbb{N} \twoheadrightarrow A$. Usamos recursão e o princípio da boa ordem. □ (Λ13.22P)

13.23. O que ganhamos?. Suponha que um conjunto A é contável. O que ganhamos realmente com essa informação? Como podemos usar essa hipótese? Já sabemos, por exemplo, que o fato "$C \neq \emptyset$" nos permite escrever "Seja $c \in C$.". O que o fato "A é contável" nos permite fazer? Bem, podemos escrever: "seja a_n uma *enumeração* de A", ou, escrever: "Suponha $A = \{a_0, a_1, a_2, \dots\}$.".

! **13.24. Cuidado.** É um erro comum escrever "Suponha $A = \{a_0, a_1, a_2, \dots\}$." mesmo quando não sabemos que A é contável. Talvez A é *grande demais* para poder ser escrito nessa forma. Como o $\mathbb{R}$, por exemplo, que sabemos que não pode ser escrito como $\mathbb{R} = \{r_0, r_1, r_2, \dots\}$, pois é um conjunto incontável!

§277. O primeiro argumento diagonal de Cantor

13.25. E os racionais?. O fato que $\mathbb{Z}$ é contável não deixou ninguém muito surpreso. Mas na maneira que contamos os membros do $\mathbb{Z}$, existe essa idéia de "próximo número" meio incorporada no próprio conjunto pela sua ordem. *«Primeiramente tome o* 0*. Depois tome o próximo positívo, e depois o próximo negativo, e por aí vai.»* Mas o $\mathbb{Q}$ com sua ordem padrão é um conjunto *denso*: entre quaisquer racionais x, y com $x < y$, existe

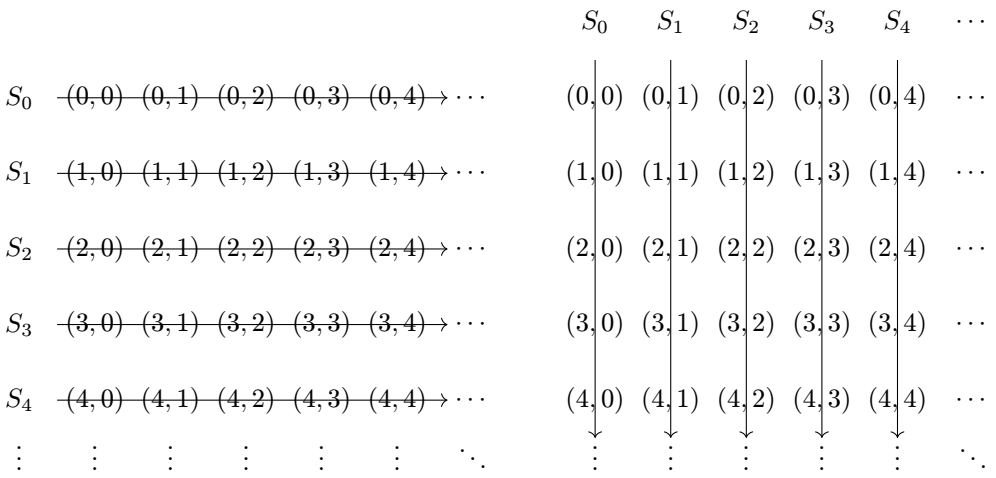
racional w tal que $x < w < y$. Vamos dizer que começou no 0. Quem vai depois? Não existe "próximo" para nenhuma direção! Em vez de contar os membros de $\mathbb{Q}$, vamos contar os membros de $\mathbb{N}^2$. E isso já vai resolver o problema de enumerar o $\mathbb{Q}$ facilmente.

13.26. Contando os pares de naturais. Naturalmente pensamos no $\mathbb{N}^2$ numa forma bidimensional (até pronunciando o conjunto usamos a palavra "quadrado"). Vamos arrumar então os naturais numa tabela bidimensional e infinita assim:

$$\begin{array}{ccccccc}
(0,0) & (0,1) & (0,2) & (0,3) & (0,4) & \cdots \\
(1,0) & (1,1) & (1,2) & (1,3) & (1,4) & \cdots \\
(2,0) & (2,1) & (2,2) & (2,3) & (2,4) & \cdots \\
(3,0) & (3,1) & (3,2) & (3,3) & (3,4) & \cdots \\
(4,0) & (4,1) & (4,2) & (4,3) & (4,4) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Naturalmente, influenciados por nossos hábitos talvez gostariamos de contar os membros linha por linha, ou coluna por coluna—só que...

Expectativa:



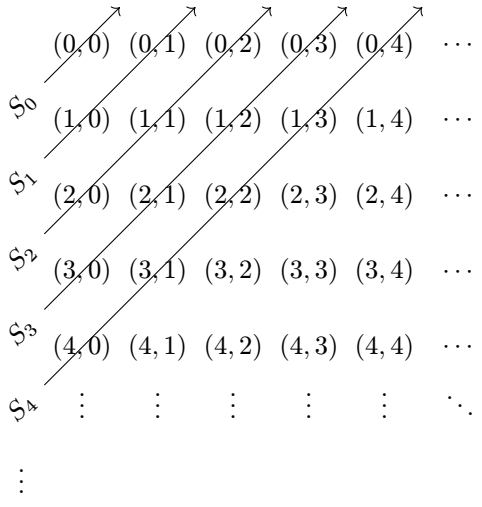
Realidade:

							S_0	S_1	S_2	S_3	S_4	$\cdots$
S_0	~~$(0,0)$~~	~~$(0,1)$~~	~~$(0,2)$~~	~~$(0,3)$~~	~~$(0,4)$~~	$\cdots$	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$	$\cdots$
S_1	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$	$\cdots$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$	$\cdots$
S_2	$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$	$(2,4)$	$\cdots$	$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$	$(2,4)$	$\cdots$
S_3	$(3,0)$	$(3,1)$	$(3,2)$	$(3,3)$	$(3,4)$	$\cdots$	$(3,0)$	$(3,1)$	$(3,2)$	$(3,3)$	$(3,4)$	$\cdots$
S_4	$(4,0)$	$(4,1)$	$(4,2)$	$(4,3)$	$(4,4)$	$\cdots$	$(4,0)$	$(4,1)$	$(4,2)$	$(4,3)$	$(4,4)$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

O que aconteceu? Stratificando nosso espaço nessa maneira, *ficaremos presos* no S_0 pra sempre! Se o inimigo no jogo escolher qualquer um dos membros fora do S_0 a gente nunca vai ganhar!

13.27. Strata finita. Stratificando nosso espaço precisamos tomar cuidado para qualquer stratum ser um conjunto *finito*. Usando a analogia do jogo isso garanta vitória, pois ficaremos no primeiro stratum para uma quantidade finita de dias, e um belo momento depois de ter contado todos os membros do primeiro stratum vamos começar o segundo, que (sendo também finito) sabemos que um belo dia já vamos começar contar o terceiro; etc., etc.

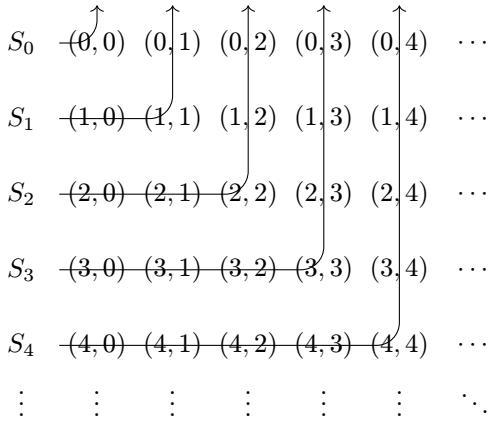
13.28. O primeiro argumento diagonal de Cantor. Cantor conseguiu stratificar esse espaço apenas virando sua cabeça num ângulo $\pi/4$:



Observe que na stratificação de Cantor, *cada stratum é finito*. Com sua método de diagonalização Cantor conseguiu algo maravilhoso: contou todos dos *racionais*, algo muito chocante, pois a maneira que visualizamos esse conjunto é *muito* mais populosa

daquela dos inteiros ou dos naturais. Mas chega Cantor e nos ilumina: *o $\mathbb{Q}$ parece tão mais populoso porque tu não tá fazendo essa dupla abstração, deixando a natureza e ordem te confundir!*

13.29. A stratificação de Gödel. Gödel muitos anos depois preferiu uma stratificação diferente:



Observe que aqui também cada stratum é finito, e logo serve para contar todos os membros do conjunto.

▸ **EXERCÍCIO x13.15.**
Defina formalmante as stratificações de Cantor (13.28) e de Gödel (13.29). Observe que cada stratum, sendo finito, pode ser representado por um conjunto (e não uma tupla) sem problema nenhum. Defina curtamente então, usando a notação set builder, os S_n's de ambas as stratificações. (x13.15 H 1)

13.30. Observação. Para corresponder numa bijecção mesmo, o jogo do 13.18 tem que ser modificado, para proibir repetições do mesmo palpite. Observamos que se o jogador tem uma estratégia para ganhar num jogo que permite repetições de palpites, ele já pode adaptá-la para ganhar no jogo com a restricção: ele apenas segue a estratégia do jogo "livre" e quando aparecem palpites que ele já adivinhou, ele pula para o próximo, até chegar num palpite que ele não tentou ainda, para tentá-lo. Por exemplo, para enumerar os racionais sabendo uma enumeração dos pares de inteiros, copiamos a estratégia do $\mathbb{Z}^2$, pulando pares que ou não correspondem em racionais (como o $(0,0)$ por exemplo), ou que são iguais com palpites anteriores (como o $(2,4)$ que pulamos por causa do $(1,2)$ que já adivinhamos).

Θ13.31. Teorema. *Seja $\mathcal{C}$ uma colecção contável de conjuntos contáveis. Logo $\bigcup\mathcal{C}$ é contável. Em outras palavras: união contável de contáveis é contável.*

▸ Esboço. Seja $(C_n)_n$ uma enumeração dos membros do $\mathcal{C}$:

$$\mathcal{C} = \{C_0, C_1, C_2, \dots\}\,.$$

Sabemos que todos os C_n's são contáveis; logo seja $\left(c_n^i\right)_i$ uma enumeração do C_n:

$$\begin{aligned} C_0 &= \left\{c_0^0, c_0^1, c_0^2, c_0^3, \dots\right\} \\ C_1 &= \left\{c_1^0, c_1^1, c_1^2, c_1^3, \dots\right\} \\ C_2 &= \left\{c_2^0, c_2^1, c_2^2, c_2^3, \dots\right\} \\ &\vdots \end{aligned}$$

e agora é óbvio como usar o primeiro argumento diagonal de Cantor e obtenir uma enumeração do $\bigcup \mathcal{C} = \bigcup_{n=0}^{\infty} C_n$. □

13.32. Tem incontáveis?. Até este momento podemos sentir uns dos sentimentos de Cantor investigando essas infinidades. Até talvez uma frustração, pois, por enquanto, todos os conjuntos infinitos que testamos acabaram sendo contáveis. Será que todos são? Os reais estão resistindo ainda, mas antes de pensar no primeiro argumento diagonal, os racionais também estavam! Agora tu demonstraras que bem mais conjuntos são realmente contáveis.

► **EXERCÍCIO x13.16.**
Demonstre ou refute: o conjunto de todos os strings feitos por qualquer alfabeto finito é contável. (x13.16H0)

Intervalo para hackear

► **CODE-IT c13.1 (EnumPairs).**
Implemente uma estratégia para ganhar no jogo sem repetições com conjunto-segredos o $\mathbb{N}^2$. Ou seja, escreva um programa que imprime (pra sempre) os palpites do jogador na sua ordem. (c13.1H0)

► **CODE-IT c13.2 (EnumRatsReps).**
Modifique o EnumPairs para o caso com conjunto-segredos o conjunto de racionais não-negativos, mas permitindo repetições. Represente cada palpite como fracção, imprimindo por exemplo o racional $\frac{1}{3}$ como o string "`1/3`". (c13.2H0)

► **CODE-IT c13.3 (EnumRats).**
Modifique o EnumRats para o caso que o jogo proibe repetições (mas para o mesmo conjunto $\mathbb{Q}_{\geq 0}$). Use teu código para responder na pergunta: *dada a escolha do inimigo, em qual dia o jogador vai adivinhá-la?* (c13.3H0)

► **EXERCÍCIO x13.17 (Jogador amnésico).**
Ache uma estratégia para ganhar no jogo com conjunto-segredos o conjunto dos racionais não-negativos, se o jogador tem memória que o permite lembrar apenas seu último palpite! (x13.17H0)

▸ **EXERCÍCIO x13.18.**
Defina uma função nextPair : $\mathbb{N}^2 \to \mathbb{N}^2$ tal que para cada entrada (n, m) ela retorna o próximo palpite do jogador que acabou de tentar o (n, m), no jogo com conjunto-segredos o $\mathbb{N}^2$. Considera que sua estratégia começa com o palpite $(0, 0)$. Assim, a enumeração representada pela estratégia do jogador seria a:

$$(0,0), f(0,0), f^2(0,0), f^3(0,0), \ldots,$$

ou seja, a seqüência $\{f^n(0,0)\}_n$. (x13.18H0)

▸ **CODE-IT c13.4 (NextPair).**
Implemente função do Exercício x13.18. (c13.4H0)

§278. O segundo argumento diagonal de Cantor

Vamos finalmente atacar a cardinalidade dos reais, começando com seu subconjunto $[0, 1] \subseteq \mathbb{R}$. Vamos ver que realmente isso é um conjunto *incontável*. Não tem como enumerar seus membros! Como podemos demonstrar isso? Lembrando a definição, basta demonstrar que não existe enumeração

$$[0,1] = \{a_0, a_1, a_2, \ldots\}.$$

Vamos começar com um esboço que tem um erro para entender a idéia básica—e para ver se tu perceberás o erro, claro.

13.33. Um esboço pouco errado. Suponha que alguém chegou feliz pra ti, afirmando que conseguiu enumerar todos os reais no $[0, 1]$, a apresenta sua enumeração pra ti:

$$a_0, a_1, a_2, a_3, \ldots$$

Tu pega sua lista e escreva a expansão decimal de cada número, um número por linha; por exemplo:

$$\begin{aligned}
a_0 &= 0 \,.\, 3\ 6\ 4\ 8\ 8\ 5\ 0\ \ldots\\
a_1 &= 0 \,.\, 2\ 1\ 8\ 9\ 8\ 0\ 5\ \ldots\\
a_2 &= 0 \,.\, 0\ 8\ 9\ 8\ 5\ 8\ 8\ \ldots\\
a_3 &= 0 \,.\, 9\ 2\ 6\ 6\ 8\ 6\ 6\ \ldots\\
a_4 &= 0 \,.\, 2\ 3\ 4\ 6\ 0\ 5\ 7\ \ldots\\
&\vdots
\end{aligned}$$

Nosso objectivo é mostrar um certo número $w \in [0, 1]$ que não está nessa lista. Vamos definir esse w construindo sua expansão decimal:

$$w \stackrel{\text{def}}{=} 0 \,.\, ?\ ?\ ?\ ?\ ?\ ?\ ?\ \ldots$$

E a idéia é a seguinte: traversa a tabela acima diagonalmente, mudando o dígito, construindo assim um novo número. Os primeiros três passos aqui podem ser os seguintes:

$$\begin{aligned}
w &\stackrel{\text{def}}{=} 0 \,.\, 4\ ?\ ?\ ?\ ?\ ?\ \ldots\\
a_0 &= 0 \,.\, 3\ 6\ 4\ 8\ 8\ 5\ \ldots\\
a_1 &= 0 \,.\, 2\ \underline{1}\ 8\ 9\ 8\ 0\ \ldots\\
a_2 &= 0 \,.\, 0\ 8\ \underline{9}\ 8\ 5\ 8\ \ldots\\
a_3 &= 0 \,.\, 9\ 2\ 6\ \underline{6}\ 8\ 6\ \ldots\\
a_4 &= 0 \,.\, 2\ 3\ 4\ 6\ \underline{8}\ 5\ \ldots\\
&\vdots
\end{aligned}
\qquad
\begin{aligned}
w &\stackrel{\text{def}}{=} 0 \,.\, 4\ 2\ ?\ ?\ ?\ ?\ \ldots\\
a_0 &= 0 \,.\, \underline{3}\ 6\ 4\ 8\ 8\ 5\ \ldots\\
a_1 &= 0 \,.\, 2\ 1\ 8\ 9\ 8\ 0\ \ldots\\
a_2 &= 0 \,.\, 0\ 8\ \underline{9}\ 8\ 5\ 8\ \ldots\\
a_3 &= 0 \,.\, 9\ 2\ 6\ \underline{6}\ 8\ 6\ \ldots\\
a_4 &= 0 \,.\, 2\ 3\ 4\ 6\ \underline{8}\ 5\ \ldots\\
&\vdots
\end{aligned}
\qquad
\begin{aligned}
w &\stackrel{\text{def}}{=} 0 \,.\, 4\ 2\ 0\ ?\ ?\ ?\ \ldots\\
a_0 &= 0 \,.\, \underline{3}\ 6\ 4\ 8\ 8\ 5\ \ldots\\
a_1 &= 0 \,.\, 2\ \underline{1}\ 8\ 9\ 8\ 0\ \ldots\\
a_2 &= 0 \,.\, 0\ 8\ 9\ 8\ 5\ 8\ \ldots\\
a_3 &= 0 \,.\, 9\ 2\ 6\ \underline{6}\ 8\ 6\ \ldots\\
a_4 &= 0 \,.\, 2\ 3\ 4\ 6\ \underline{8}\ 5\ \ldots\\
&\vdots
\end{aligned}$$

onde para mudar cada dígito, eu fui para o "próximo". Foi construido assim o

$$w \stackrel{\text{def}}{=} 0 \ . \ 4 \ 2 \ 0 \ 7 \ 9 \ \ldots$$

que não está na lista $a_0, a_1, a_2, \ldots$. ↯

? **Q13.34. Questão.** Por que w não está na lista?

!! SPOILER ALERT !!

Pois pela sua construção, o w discorda com todos os membros da lista em pelo menos uma posição: ele discorda com o a_0 na primeira posição, com o a_1 na segunda, etc. É fácil demonstrar que

$$\text{para todo } n \in \mathbb{N}, \quad w \neq a_n.$$

Seja $n \in \mathbb{N}$. Agora observe que o $w \neq a_n$ pois pela sua construção, ele discorda com o a_n no n-ésimo dígito. ↯

? **Q13.35. Questão.** Qual o problema com essa argumentação?

!! SPOILER ALERT !!

Resposta. O argumento é baseado numa hipótese falsa para concluir que o número w construido é diferente de todos os números da lista: que duas expansões de números reais que discordam no dígito duma certa posição representão reais distintos, que tá simplesmente errado:

$$0.4999\ldots = \frac{1}{2} = 0.5000\ldots$$

as expansões são distintas, não temos reais distintos aqui!

E agora?. Em vez de desistir e jogar a idéia brilhante fora, podemos (i) perceber que já temos nas nossas mãos uma demonstração da incontabilidade dum certo conjunto, só que não é o conjunto $[0, 1]$ e (ii) proceder para concertar o probleminha da argumentação para virar uma demonstração correta da incontabilidade do $[0, 1]$ mesmo! Faça ambos agora.

▸ **EXERCÍCIO x13.19 ((i)).**
Sobre qual conjunto podemos já afirmar que é incontável, usando a argumentação bugada que não deu certo para o $[0,1]$? (x13.19 H 1)

Θ13.36. Teorema (Cantor). *O conjunto de todas as seqüências feitas por dois símbolos distintos é incontável.*

DEMONSTRAÇÃO. Cantor escolheu os 'm' e 'w' como símbolos distintos, vamos seguir seu gosto então. Denotamos $\mathbf{2} = \{m, w\}$. Seja $\{f_n\}_n \subseteq (\mathbb{N} \to \mathbf{2})$. Basta construir um membro de $(\mathbb{N} \to \mathbf{2})$ que não é nenhum dos membros de $\{f_n\}_n$. Definimos a $g : \mathbb{N} \to \mathbf{2}$ então pela

$$g(x) = \begin{cases} w, & \text{se } f(x) = m; \\ m, & \text{se } f(x) = w. \end{cases}$$

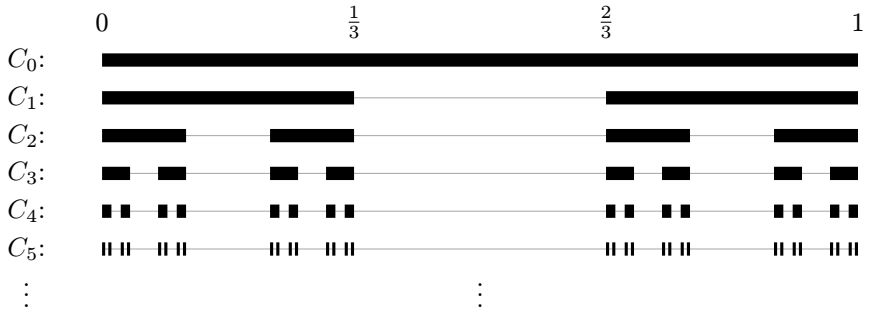
Basta verificar que para todo $n \in \mathbb{N}$, $g \neq f_n$. Seja $n \in \mathbb{N}$ então. Pela definição da g temos que g, f_n discordam no ponto n e logo $g \neq f_n$. ∎

▸ **EXERCÍCIO x13.20 ((ii)).**
Conserta o problema. (x13.20 H 1 2)

▸ **EXERCÍCIO x13.21.**
Por que não podemos usar o mesmo argumento para concluir que o $\{\, q \in \mathbb{Q} \mid 0 \leq q \leq 1 \,\}$ também é incontável? (x13.21 H 1)

§279. O conjunto de Cantor

13.37. O conjunto de Cantor.



TODO Terminar

§280. Umas aplicações importantes da teoria de Cantor

13.38. Corolário. *Os irracionais são incontáveis.*

Demonstração. Os racionais são contáveis. Os reais incontáveis. Logo, os irracionais são incontáveis, pois $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$ e logo se $\mathbb{R} \setminus \mathbb{Q}$ fosse contável teriamos a contradição do $\mathbb{R}$ ser contável também (Exercício x13.14). ∎

13.39. E os transcendentais?. Os transcendentais parecem ainda mais selvagens que os irracionais. E neste momento temos poquíssimos exemplos: os números de Liouville que foram contruidos exatamente com esse propósito; o e que Hermite acabou de demonstrar que é transcendental (1873) e a transcendentalidade do π demorou uns anos. Como encontramos transcendentais tão raramente em comparação com os algébricos faz sentido pensar que eles são contáveis.[94]

Λ13.40. Lema (Dedekind). *Os algébricos são contáveis.*

▸ Esboço. Basta observar que $\mathbb{Q}[x] =_c \mathbb{Q}^\star$, com a correspondência

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n \leftrightarrow (a_0, a_1, a_2, \ldots, a_{n-1}, a_n)\,.$$

Seja $f_0, f_1, f_2, \ldots$ uma enumeração do $\mathbb{Q}[x]$. Stratificamos então os números algébricos onde o i-ésimo stratum é o conjunto de todas as raízes reais de f_i:

$$S_i = \{\, \alpha \in \mathbb{R} \mid f_i(\alpha) = 0 \,\}\,.$$

Pelo teorema fundamental da Álgebra agora, sabemos que cada f_i tem no máximo $\deg(f_i)$ raízes, ou seja, todos os strata são finitos e pronto! □

13.41. Corolário (Cantor). *Os transcendentais são incontáveis.*

Demonstração. Como os algébricos são contáveis (Lema Λ13.40), os transcendentais são incontáveis com o mesmo argumento da demonstração do Corolário 13.38. ∎

13.42. Céu de estrelas. Sem as descobertas de Cantor, alguém pensaria que isso é uma coincidência muito grande e bizarra: como aconteceu que a gente definiu um número bem importante como o π ou o e e aconteceu que ele tem essa propriedade estranha de ser transcendental? Mas, graças ao Cantor, sabemos melhor: *de fato, seria bizarro se fosse o contrário!* Pois sabemos agora que, na verdade, as excessões são os algébricos e não os transcendentais. O estranho seria descobrir que e aconteceu que é racional! Como piada considere o princípio seguinte:

13.43. Piada (Princípio de transcendentalidade). Seja $x \in \mathbb{R}$ com $x \neq 0, 1$. Se x é profundamente interessante em matemática, então x é transcendental.

13.44. Liouville vs Cantor. É comum encontrar argumentos favorecendo o teorema de Liouville contra o teorema de Cantor, sobre a existência de transcendentais. Normalmente escutamos algo do tipo «Liouville construiu e mostrou transcendentais, Cantor apenas demonstrou que existem sem constriur ou mostrar nenhum». Essa afirmação é completamente errada!

[94] Na verdade, a única razão que temos nesse momento de acreditar que o conjunto de transcendentais é infinito são os números Liouville: ele realmente conseguiu contruir uma infinidade (incontável) de transcendentais.

▸ **EXERCÍCIO x13.22.**
Explique o porquê. (x13.22H0)

▸ **CODE-IT c13.5 (CantorCon).**
Escreva um programa que compute irracionais e transcendentais. Considere que teu usuário vai querer determinar quantos números construir, e também até que precisão (quantos dígitos). (c13.5H0)

Intervalo de problemas: Cantor vs. Reais

O conjunto dos reais é incontável. Cantor não deu apenas uma demonstração para esse teorema seu. A demonstração que já encontramos aqui, que envolve seu argumento diagonal, é a mais importante e elegante (exatamente por causa da diagonalização e suas diversas aplicações).[95] Mas essa foi nem a primeira, nem a segunda, mas sim a terceira demonstração dele! As outras duas foram bem diferentes. Cantor que o $\mathbb{R}$ é incontável foi bem diferente. Dado quaisquer reais a, b com $a < b$ e qualquer seqüência de reais no $[a, b]$ ele mostrou um certo membro do $[a, b]$ que a seqüência "esqueceu de contar". Redescobrir essa demonstração é o objetivo do Problema Π13.1.

▸ **PROBLEMA Π13.1 (Cantor vs. Reais: 1874).**
Sejam $a, b \in \mathbb{R}$ com $a < b$ e $(x_n)_n$ seqüência de reais no $[a, b]$. Demonstre que existe $w \in [a, b]$ tal que $w \notin \{x_n\}_n$, seguindo o esboço seguinte. O plano é construir uma cadeia de intervalos fechados

$$[a, b] = I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$$

e escolher o w na sua intersecção. Para conseguir isso, vamos definir duas subseqüências $(a_n)_n$ e $(b_n)_n$ da seqüência $(x_n)_n$ tais que a primeira começa no a e é ascendente e a segunda no b e é descendente tais que os intervalos $[a_n, b_n]$ vão assumir o papel dos I_n. (Π13.1H0)

▸ **PROBLEMA Π13.2.**
Por que não podemos usar o mesmo argumento para concluir que o $\{\, q \in \mathbb{Q} \mid a \leq q \leq b \,\}$ também é incontável? (Π13.2H0)

§281. Procurando bijecções

Vamos ver como as transformações de esticar/encolher (stretch/shrink) e de deslocar (shift) nos intervalos de reais, sendo bijecções levam suas entradas para saídas equinúmeras.

[95] Cantor terminou seu artigo **[Can91]** onde publicou sua demonstração com a frase profética *"Die weitere Erschließung dieses Feldes ist Aufgabe der Zukunft."* que significa: *desenvolver essa área mais é a tarefa do futuro.*

▸ **EXERCÍCIO x13.23.**
Mostre as seguintes equinumerosidades entre os seguintes intervalos de reais:

(a) $(0,1) =_{\mathrm{c}} (0,2)$;
(b) $(0,2) =_{\mathrm{c}} (3,5)$;
(c) $[0,1) =_{\mathrm{c}} (0,1]$;
(d) $(a,b) =_{\mathrm{c}} (c,d)$;
(e) $[a,b) =_{\mathrm{c}} [c,d)$;
(f) $[a,b) =_{\mathrm{c}} (c,d]$;
(g) $[a,b] =_{\mathrm{c}} [c,d]$;

(onde $a < b$ e $c < d$). (x13.23 H 1)

▸ **EXERCÍCIO x13.24.**
Mostre as seguintes equinumerosidades entre os seguintes intervalos de reais,

$$(\alpha,\beta) =_{\mathrm{c}} (0,1)$$

onde $\alpha,\beta \in \mathbb{R} \cup \{-\infty,+\infty\}$ com $\alpha < \beta$. (x13.24 H 1 2 3)

§282. O teorema Cantor–Schröder–Bernstein

Esse teorema que demonstramos aqui é conhecido como "Cantor–Schröder–Bernstein" ou "Schröder–Bernstein", mas vamos referir a ele nessas notas apenas com o nome de Bernstein, pois foi o primeiro que demonstrou sua veracidade numa forma correta.[96] Vamos começar atacando esse problema com uma abordagem amorosa, de Smullyan (veja **[Smu14]**).

▸ **EXERCÍCIO x13.25 (Abordagem amorosa).**
Suponha que num universo seus habitantes são divididos em dois conjuntos *infinitos*: o conjunto A de homens e B de mulheres. Suponha também que os seguintes são fatos sobre esse universo:

(1) Cada homem ama exatamente uma mulher.
(2) Nenhuma mulher é amada por dois homens.
(3) Cada mulher ama exatamente um homem.
(4) Nenhum homem é amado por duas mulheres.

(Essas condições já deixam esse universo bem bizarro.) Mostre que tem como casar todos os habitantes desse universo em casamentos monogâmicos e heterosexuais, em tal modo que em cada casal é garantido amor (mas não necessariamente reciprocal), ou seja: se $a \in A$ é casado com $b \in B$, *pelo menos uma* das duas condições acontece: a ama b; b ama a. (x13.25 H 1)

[96] E sua demonstração não precisou o *axioma da escolha* (§333), algo que vamos apreciar mais no Capítulo 16.

Voltando dessa versão antropomórfica do problema, observe que a condição (1) garanta a existência duma função $f : A \to B$, que graças à (2) é injetora. Similarmente, a condição (3) garanta a existência duma função $g : B \to A$, que graças à (4) é injetora também. Essas são as hipotéses do Teorema Θ13.45. Observe também que se resolver o problema amoroso do Exercício x13.25 tu já forneceu uma função *bijetora* $F : A \to B$, definida pela

$$F(x) = \text{a pessoa casada com } x.$$

Vamos ver isso agora sem amor.

Θ13.45. Teorema (Bernstein). *Sejam conjuntos A e B e funções injetoras $f : A \rightarrowtail B$ e $g : B \rightarrowtail A$. Então existe bijecção $\varphi : A \rightarrowtail\!\!\!\!\twoheadrightarrow B$.*

§283. Procurando injecções

Agora é *bem* mais fácil demonstrar o seguinte e ganhar o corolário embaixo. Sem Bernstein, precisamos resolver o Problema Π13.4.

▸ **EXERCÍCIO x13.26.**
Usando o teorema de Schröder–Bernstein Θ13.45 demonstre que $(a, b) =_{\mathrm{c}} (a, b] =_{\mathrm{c}} [a, b]$. (x13.26 H 0)

13.46. Corolário. *Qualquer intervalo não-trivial (vazio ou singleton) de reais, tem a mesma cardinalidade com o próprio $\mathbb{R}$.*

▸ **EXERCÍCIO x13.27.**
Usando o teorema de Schröder–Bernstein Θ13.45 demonstre que $\mathbb{R} =_{\mathrm{c}} \wp\mathbb{N}$. (x13.27 H 0)

§284. Codificações

13.47. Encodings. Uma maneira de pensamento para construir injecções seria através de codificações (ou *encodings*). Uma *codificação* de A no B é qualquer injecção de A para B.

• **EXEMPLO 13.48.**
Para demonstrar que $\mathbb{Q} \leq_{\mathrm{c}} \mathbb{N}$ basta achar uma maneira de codificar cada racional como um natural. Aqui um jeito fácil: dado um racional $q \in \mathbb{Q}$ sejam m, n tais que $q = m/n$ e m/n irredutível; codificamos

$$m/n \mapsto 1\underbrace{00\cdots0}_{m \text{ vezes}}1\underbrace{00\cdots0}_{n \text{ vezes}}1.$$

Assim,

$$\begin{aligned} 1/2 &\mapsto 101001 \\ 10/6 = 5/3 &\mapsto 10000010001 \\ 22/7 &\mapsto 1000000000000000000000100000001 \end{aligned}$$

etc. Observe que para qualquer $n \in \mathbb{N}$, existem dois casos: ou ele serve como codificação para algum $q \in \mathbb{Q}$ (como o 101001 acima) ou não (como o 1, o 2, o 1011, etc.). Caso que sim, podemos facilmente extrair a informação codificada no n, voltando para o racional q:

$$10001001 \rightsquigarrow 3/2.$$

A mesma idéia serve para codificar o $\mathbb{N}^\star$:

► **EXERCÍCIO x13.28.**
Demonstre usando codificação que $\mathbb{N}^\star \leq_{\mathrm{c}} \mathbb{N}$. (x13.28 H 0)

► **EXERCÍCIO x13.29.**
Demonstre usando codificação que $\wp\mathbb{N} \leq_{\mathrm{c}} [0,1)$. (x13.29 H 0)

► **EXERCÍCIO x13.30.**
Demonstre demonstrando duas codificações que $[0,1) =_{\mathrm{c}} (\mathbb{N} \to \mathbb{N})$. (x13.30 H 0)

§285. O teorema de Cantor e suas conseqüências

Até agora temos encontrado apenas duas quantidades infinitas diferentes: aquela do $\mathbb{N}$, e aquela do $\mathbb{R}$. Essa situação está prestes a mudar drasticamente..

13.49. O teorema de Cantor. Cantor demonstrou que para todo conjunto A, seu powerset $\wp A$ tem cardinalidade estritamente maior que do A:

$$A <_{\mathrm{c}} \wp A.$$

Primeiramente observe que para conjuntos finitos já sabemos disso, e é fácil demonstrar:

$$|\wp A| = 2^{|A|} > |A|$$

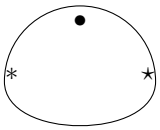
pois para todo $n \in \mathbb{N}$, realmente temos $2^n > n$. Cantor conseguiu demonstrar que $A <_{\mathrm{c}} \wp A$ para qualquer A. Lembrando a definição de $<_{\mathrm{c}}$, precisamos demonstrar duas coisas:

$$A \leq_{\mathrm{c}} \wp A \qquad\qquad A \neq_{\mathrm{c}} \wp A.$$

A primeira é fácil: faça agora!

► **EXERCÍCIO x13.31.**
Para todo conjunto A, $A \leq_{\mathrm{c}} \wp A$. (x13.31 H 1)

13.50. A linda idéia da sua demonstração. Suponha que temos um conjunto A, e uma função $A \xrightarrow{\pi} \wp A$. Vamos demonstrar que a π não pode ser sobrejetora—e logo, nem bijetora. Para entender a idéia melhor, vamos desenhar um exemplo. Imagina então que o A parece como no desenho abaixo, e seu powerset tá no seu lado, onde eu desenhei apenas uns dos seus membros, pois o desenho ficaria bagunçado demais se eu tivesse desenhado todos. Mas todos estão lá mesmo: o $\wp A$, pela sua definição, é o conjunto de *todos* os subconjuntos de A.



A π então mapeia cada membro de A com um membro de $\wp A$. Por exemplo, pode ser assim:

desenho com π aqui

Vamos dar um toque antropomórfico agora: vamos considerar os membros de A como pessoas, e a π como uma função de *amor*, que mapeia cada $x \in A$ para o conjunto de todas as pessoas que x ama:

$$\pi(x) = \{\, y \in A \mid x \text{ ama } y \,\}.$$

Lembre-se que nosso objectivo é achar um membro de $\wp A$ que não pertence na imagem da π. Chame *depressivo* um $x \in A$ sse x não se ama. Ou seja,

$$x \text{ é depressivo} \overset{\text{def}}{\iff} x \notin \pi(x)$$

pois $\pi(x)$ são todas as pessoas que x ama.[97] Assim, cada $x \in A$ ou é depressivo, ou não. Condiseramos o conjunto D de todos os depressivos membros de A:

$$D \overset{\text{def}}{=} \{\, x \in A \mid x \text{ é depressivo} \,\} = \{\, x \in A \mid x \notin \pi(x) \,\}.$$

Observe que $D \subseteq A$, ou seja, D é um membro do $\wp A$. Esse D é o testemunha que estamos procurando: um membro do codomínio da π, garantido para não pertencer na imagem $\pi[A]$. Por quê? Para chegar num absurdo, suponha o contrário: que para algum $d \in A$, temos $\pi(d) = D$. Faz sentido agora perguntar: *esse d é depressivo?* Dois casos existem, e os dois chegam em absurdo:

$$\begin{aligned}
d \text{ depressivo} &\implies d \notin \pi(d) && \text{(def. depressivo)}\\
&\implies d \notin D && \text{(pela escolha de } d\text{)}\\
&\implies d \text{ não depressivo} && \text{(def. } D\text{)}\\
&\implies \text{absurdo!}
\end{aligned}$$

e no outro lado,

$$\begin{aligned}
d \text{ não depressivo} &\implies d \in \pi(d) && \text{(def. depressivo)}\\
&\implies d \in D && \text{(pela escolha de } d\text{)}\\
&\implies d \text{ depressivo} && \text{(def. } D\text{)}\\
&\implies \text{absurdo!}
\end{aligned}$$

[97] Outros exemplos de definições razoáveis nessa interpretação seriam chamar o x *misántropo* se $\pi(x) = \emptyset$, *egoista* se $\pi(x) = \{x\}$, etc., mas aqui só vamos precisar dos depressivos mesmo.

Logo, para nenhum $d \in A$ temos $\pi(d) = D$, ou seja, $D \notin \pi[A]$ e logo π não é sobrejetora. Em palavras antropomórficas, com essas definições ninguém pode amar *somente todos* os depressivos. Note bem que em lugar nenhum usamos os desenhos do A e da π nessa demonstração. Desenhei apenas para ilustrar. Podemos então demonstrar formalmente o teorema de Cantor, sem nada depressivo!

Θ13.51. Teorema (Cantor). *Seja A conjunto. Então $A <_c \wp A$.*

Demonstração. Seguindo a definição de $<_c$, precisamos demonstrar duas coisas:
demonstração de $A \leq_c \wp A$: feita no Exercício x13.31; um testemunha é a $\lambda x\,.\,\{x\}$, que "obviamente" (Exercício x13.32) é injetiva.
demonstração de $A \neq_c \wp A$. Basta demonstrar que não existe função sobrejetora de A para $\wp A$. Seja $\pi : A \to \wp A$. Queremos demonstrar que a π não pode ser sobrejetora, ou seja, mostrar um elemento C do seu codomínio que não pertence na imagem da π (ou seja: tal que $C \notin \pi[A]$). Observe que para qualquer $x \in A$, temos $\pi(x) \in \wp A$, ou seja $\pi(x) \subseteq A$. Considere o conjunto

$$D = \{\, x \in A \mid x \notin \pi(x) \,\}\,.$$

Pela definição de D, temos $D \subseteq A$. Ou seja, $D \in \wp A$, que é o codomínio da π. Precisamos demonstrar que para todo $x \in A$, $\pi(x) \neq D$. Para chegar num absurdo, seja $d \in A$ tal que $\pi(d) = D$. Agora nos perguntamos: $d \in \pi(d)$? Como $\pi(d) = D$, a pergunta reduza em: $d \in D$? Ambas as alternativas (*sim* e *não*) são impossíveis:

$$d \in D \iff d \notin D$$

pela definição de D e pela escolha de d. Absurdo! Logo π não mapeia nenhum membro de A para o $D \in \wp A$, ou seja, π não é sobrejetora. ∎

▸ **exercício x13.32.**
Demonstre em detalhe que a função $(x \mapsto \{x\})$ na demonstração de Teorema Θ13.51 realmente é injetora. (x13.32 H 1)

13.52. Corolário. *Existe uma infinidade (contável) de cardinalidades infinitas:*

$$\mathbb{N} <_c \wp\mathbb{N} <_c \wp\wp\mathbb{N} <_c \wp\wp\wp\mathbb{N} <_c \wp\wp\wp\wp\mathbb{N} <_c \dots$$

13.53. Corolário. *Não existe cardinalidade máxima: para qualquer conjunto M, o conjunto $\wp M$ tem cardinalidade maior.*

D13.54. Definição. Denotamos a cardinalidade de $\mathbb{N}$ por $\aleph_0$ (*aleph 0*), e a cardinalidade de $\wp\mathbb{N} =_c \mathbb{R}$ por $\mathfrak{c}$. Chamamos o $\mathfrak{c}$ o *continuum*.

13.55. Considere os conjuntos

$$\emptyset <_c \wp\emptyset <_c \wp\wp\emptyset <_c \wp\wp\wp\emptyset <_c \wp\wp\wp\wp\emptyset <_c \cdots$$

Observe que cada conjunto nessa seqüência (infinita) de conjuntos é finito. Mas, quais

são suas cardinalidades? Calculamos:

$$\begin{aligned} |\emptyset| &= 0 \\ |\wp\emptyset| &= 1 \\ |\wp\wp\emptyset| &= 2 \\ |\wp\wp\wp\emptyset| &= 4 \\ |\wp\wp\wp\wp\emptyset| &= 16 \\ &\vdots \end{aligned}$$

Observamos que a seqüência dessas cardinalidades "tem burácos". Por exemplo, nenhum desses conjuntos tem cardinalidade 3, mesmo que realmente tem conjuntos com essa cardinalidade (por exemplo o $\overline{3} = \{0, 1, 2\}$). Ou seja, existe conjunto C com

$$\wp\wp\emptyset <_{\mathrm{c}} C <_{\mathrm{c}} \wp\wp\wp\emptyset.$$

Similarmente achamos conjuntos "estritamente entre" os conjuntos que aparecem depois nessa seqüência.

13.56. Umas questões aparecem imediatamente:

(1) Será que tem conjuntos "estritamente entre" alguns dos conjuntos infinitos da seqüência anterior?
(2) Será que tem algum conjunto com cardinalidade maior que qualquer uma dessas cardinalidades?
(3) Será que tem algum conjunto incomparável com todos eles?
(4) Até pior: tem conjuntos incomparáveis em cardinalidade?)

§286. As menores infinidades

Então. Já sabemos que tem uma quantidade infinita de infinidades diferentes graças ao teorema de Cantor. Já encontramos as cardinalidades dos primeiros beths

$$\beth_0 < \beth_1 < \beth_2 < \beth_3 < \cdots$$

que são os nomes das cardinalidades dos conjuntos

$$\mathbb{N} <_{\mathrm{c}} \wp\mathbb{N} <_{\mathrm{c}} \wp\wp\mathbb{N} <_{\mathrm{c}} \wp\wp\wp\mathbb{N} <_{\mathrm{c}} \cdots$$

13.57. As equinumerosidades até agora. Temos então demonstrado as:

$$\mathbb{N} =_{\mathrm{c}} \mathbb{Z} =_{\mathrm{c}} \mathbb{Q} =_{\mathrm{c}} \mathbb{A} =_{\mathrm{c}} C \cup C' =_{\mathrm{c}} \bigcup_{n=0}^{\infty} C_n =_{\mathrm{c}} C^n =_{\mathrm{c}} C^\star$$

onde C, C', etc. denotam conjuntos contáveis. E tambem temos:

$$\Delta =_{\mathrm{c}} \mathfrak{C} =_{\mathrm{c}} \wp\mathbb{N}$$
$$(\alpha, \beta) =_{\mathrm{c}} [\alpha, \beta) =_{\mathrm{c}} (\alpha, \beta] =_{\mathrm{c}} [\alpha, \beta] =_{\mathrm{c}} \mathbb{R}.$$

onde $\alpha, \beta \in \mathbb{R} \cup \{-\infty, +\infty\}$ tais que $\alpha < \beta$. Como $\mathfrak{C} \subseteq [0, 1]$ concluimos que

$$\Delta =_{\mathrm{c}} \mathfrak{C} =_{\mathrm{c}} \wp\mathbb{N} \leq_{\mathrm{c}} (a, b) =_{\mathrm{c}} [a, b) =_{\mathrm{c}} (a, b] =_{\mathrm{c}} [a, b] =_{\mathrm{c}} (0, 1) =_{\mathrm{c}} \mathbb{R}.$$

§287. Duas grandes hipoteses

13.58. A hipótese da comparabilidade de cardinais.

TODO Escrever

13.59. Hipótese. *Para todo conjunto A, B, $A \leq_{\mathrm{c}} B$ ou $B \leq_{\mathrm{c}} A$.*

13.60. A hipótese do continuum. [CH]

TODO Escrever

13.61. Hipótese (CH). *Não existe subconjunto de reais com cardinalidade estritamente entre as cardinalidades de $\mathbb{N}$ e de $\mathbb{R}$:*

$$(\forall X \subseteq \mathbb{R})[\, X \leq_{\mathrm{c}} \mathbb{N} \vee X =_{\mathrm{c}} \mathbb{R}\,].$$

13.62. Hipótese (GCH). *Para todo conjunto infinito A, não existe conjunto com cardinalidade estritamente entre as cardinalidades de A e de $\wp A$.*

$$(\forall A)[\, A \text{ infinite} \implies (\forall X \subseteq \wp A)[\, X \leq_{\mathrm{c}} A \vee X =_{\mathrm{c}} \wp A\,]\,].$$

§288. Os números transfinitos

13.63. Ordinais vs. cardinais. Na língua natural temos os números *cardinais*

um, dois, três, quatro, cinco, ...

e os números *ordinais*

primeiro, segundo, terceiro, quarto, quinto, ...

Cantor generalizou esses números finitos para os casos finitos, que chamou de *números transfinitos* (veja **[Can55]**). Os cardinais representam *quantidades* e os ordinais *ordens*. Abusando pouco a lingua, podemos dizer que o cardinal dum conjuno A mostra *quantos membros ele tem*, e o ordinal dum conjunto ordenado $\mathcal{B}$ *mostra quão longo ele é*.

13.64. Aritmética transfinita. Bem mais que isso, Cantor conseguiu definir e elaborar uma *aritmética transfinita:* definiu operações de adição, multiplicação, e exponenciação nesses números e sua aritmética realmente—além de ser linda—é muito útil e interessante. Neste capítulo não vamos nos preocupar com isso—paciência até o Capítulo 16 (Teoria dos conjuntos) (Secção §321 (Os cardinais) e Secção §332 (Os ordinais)).

§289. Um toque de teoria da medida

13.65. Assim que Cantor, Dedekind, e seus seguidores desenvolveram essa primeira teoria de conjuntos, os matemáticos da época ganharam uma ferramenta poderosa e útil que nos liberou e guiou para desenvolvemento de bem mais teorias interessantes, como: *teoria de espaços métricos*, *topologia geral*, e *teoria da medida*. Nesse texto vamos dedicar um capítulo para a primeira (Capítulo 17) e um para a segunda (Capítulo 18), e apenas uma secção (esta!) para a terceira.

13.66. Vários matemáticos, principalmente Borel, Baire, Lebesgue, Frechét, Hausdorff, desenvolveram a teoria da medida. Podemos pensar em medida como uma generalização do comprimento dum intervalo (a, b) de reais, em tal jeito que podemos atribuir um "comprimento" (ou seja, *medir*) conjuntos bem mais complicados que intervalos, e equivalentemente para dimensões maiores, generalizando assim as idéias de área, volume, etc. Isso nos leva para uma *teoria de integração* bem mais poderosa que a primeira que encontramos (integral Riemann), e também serve como base para fundar a *teoria de probabilidade*, graças ao Kolmogorov (1933, [Kol56]). Nosso interesse aquí tem a ver com probabilidade mesmo, pois queremos responder na pergunta seguinte.

? **Q13.67. Questão.** Escolhemos *aleatoriamente* um número real $r \in [0, 1]$. Qual a probabilidade de r ser... (i) o número $1/2$? (ii) um número real no (a, b) com $0 \leq a < b \leq 1$? (iii) um número racional? (iv) um número algébrico?

! **13.68. Aviso («Tende ao»).** É um erro comum afirmar certas coisas sobre probabilidades, números, funções, limites, etc., especialmente usando frases como a *«tende ao»*, então vou deixar certas coisas claras aqui antes de começar nosso pequeno estudo.

(1) A probabilidade dum evento especifico acontecer, se é definida, é um número real no $[0, 1]$. E números não mexem. Números não tendem a lugar nenhum. Números ficam quetinhos nos seus lugares.

(2) O limite duma função também não tende a lugar nenhum. Se é definido, é apenas um número real; talvez *estendido* para incluir os $\pm\infty$ (Nota 6.60). Por exemplo, temos

$$\lim_{x\to+\infty} 1/x = 0.$$

Tá vendo essa igualdade aí? Esse limite *é* o número zero. O limite *não tende ao* zero. O limite *é o próprio* zero! Podemos sim dizer (corretamente) que $1/x$ *tende ao* 0 *quando* x *tende ao* $+\infty$.

§290. Conseqüências em computabilidade e definabilidade

13.69. Áristos vs Blammenos.

Cena 1.

Segunda-feira, madrugada.
Dois amigos, Áristos e Blammenos,
estão estudando para a prova de Fundamentos Matemáticos.
Eles estão tentando resolver o problema seguinte:

«O conjunto P de todos os programas de tipo $\mathsf{Nat} \to \mathsf{Nat}$ *é contável?»*

Áristos: O conjunto P é contável, e aqui minha demonstração: o conjunto S de todos os strings feitos por um alfabeto finíto é contável, e todos os programas possíveis correspondem em apenas um subconjunto próprio de S (pois todo programa é um string, mas tem strings que não são programas). Logo, o P é contável.

Blammenos: Então tu tá afirmando que existe enumeração do P? Eu vou chegar num absurdo com essa hipótese. Suponha $p_0, p_1, p_2, \ldots$ uma enumeração de P. Eu defino o programa p_* com o algoritmo bem simples:

$$p_*(n) = p_n(n) + 1.$$

Agora temos $p_* \notin P$, pois para todo $n \in \mathbb{N}$, $p_* \neq p_n$.

Á: Por quê?

B: Seja $n \in \mathbb{N}$. Eu vou lhe mostrar que $p_* \neq p_n$. Calculamos

$$\begin{aligned} p_*(n) &= p_n(n) + 1 \qquad \text{(pela def. } p_*\text{)} \\ &\neq p_n(n) \end{aligned}$$

que mostra que $p_* \neq p_n$. Ou seja, p_* não é nenhum dos $p_0, p_1, \ldots$ que a gente supôs que esses são todos os membros do P. Cheguei assim num absurdo, logo P é incontáv—

Á: Peraí, tu tá roubando! Como teu programa usou essa enumeração $p_0, p_1, \ldots$? Se tu tivesse um algoritmo (programa) que gera essa seqüência, tu teria razão.

B: Hmmm... Mas é fácil programar esse algoritmo! Concordas que podemos gerar facilmente todos os strings no S?

Á: Sim, esse programa que gera os strings, a gente já encontrou na aula.

B: Bem, então meu algoritmo é o seguinte: gere todos os strings $s_0, s_1, s_2, \ldots \in S$, mas para cada string que não é um programa, pula para o próximo. Esse programa gera sim a seqüência $p_0, p_1, p_2, \ldots$ de todos os programas!

Á: Pqp, faz sentido! Não consigo achar um erro na tua demonstração, mas nem na minha!

B: Eu também não consigo achar um erro na tua demonstração!

? **Q13.70. Questão.** Um conjunto não pode ser contável e incontável, então pelo menos um dos dois alunos tá errado. Quais são o(s) erro(s)? Seguindo as suas idéias o que podemos concluir mesmo?

!! SPOILER ALERT !!

Resposta. O Blammenos tá errado. O problema é que seu programa em algum momento tem que decidir se um string aleatório é um programa válido, e ainda mais, se termina ou não para alguma dada entrada. Também não podemos chamar a

$$p_*(n) \neq p_n(n)$$

verdadeira para todo $n : \mathsf{Nat}$, pois existe a possibilidade de algum programa não terminar. Nesse caso os dois lados são $\perp$ ("bottom"). Podemos então concluir que é impossível criar tal programa!

TODO Quantos programas?
TODO Quantas funções?
TODO Gödel numbers e lista de todos os programas

§291. Problemas no paraíso de Cantor: o paradoxo de Russell

13.71. O paradoxo de Russell. Russell, no ano 1902, observou que o conjunto

$$\mathbb{V} \stackrel{\text{def}}{=} \{\, x \mid x \text{ é conjunto} \,\}$$

tem uma peculiaridade, uma propriedade estranha: *ele pertence nele mesmo*, ou seja, $\mathbb{V} \in \mathbb{V}$. Os conjuntos que encontramos em matemática normalmente não têm essa propriedade: $\mathbb{N} \notin \mathbb{N}$, pois o $\mathbb{N}$ não é um número natural! Similarmente $\{0, 1, \{1, 2\}\} \notin \{0, 1, \{1, 2\}\}$, pois $\{0, 1, \{1, 2\}\} \neq 0$, $\{0, 1, \{1, 2\}\} \neq 1$, e $\{0, 1, \{1, 2\}\} \neq \{1, 2\}$. Também $\emptyset \notin \emptyset$ pois nada pertence ao $\emptyset$. Tudo bem, nenhum problema com isso, mas faz sentido definir o conjunto de todos os conjuntos "tranqüilos", ou seja, aqueles que não têm essa propriedade estranha de pertencer neles mesmo. Russell definiu então o conjunto seguinte:

$$\begin{aligned} R &\stackrel{\text{def}}{=} \{\, x \mid x \text{ é conjunto } \& \; x \text{ é tranqüilo} \,\} \\ &= \{\, x \mid x \text{ é conjunto } \& \; x \notin x \,\}. \end{aligned}$$

E se perguntou: *o conjunto R é tranqüilo, ou tem essa propriedade estranha?* Consideramos os dois casos: Se $R \in R$ então pela definição de R temos que R é tranquilo, ou seja, $R \notin R$, então esse caso é impossível. Se $R \notin R$ então R não pertence nele mesmo (ou seja, R é tranqüilo) e logo pela definição de R temos $R \in R$; e assim esse caso também é impossível! Sem muitas palavras:

$$\begin{aligned} R \in R &\implies R \text{ tranqüilo} && \text{(def. } R\text{)} \\ &\implies R \notin R && \text{(def. } R \text{ tranqüilo)} \\ R \notin R &\implies R \text{ não tranqüilo} && \text{(def. } R\text{)} \\ &\implies R \in R && \text{(def. } R \text{ tranqüilo)} \end{aligned}$$

Ou seja, concluimos que:

$$R \in R \iff R \notin R$$

e naturalmente queremos escrever um grande *"absurdo"* neste momento, mas... De onde chegamos nesse absurdo? Todas as vezes que chegamos num absurdo até agora, foi tentando demonstrar algo: *supondo uma hipótese H*, chegamos num absurdo, então

concluimos que sua negação $\neg H$ é verdadeira, ou vice-versa, usando o "reductio ad absurdum", querendo demonstrar que a H é verdadeira supomos sua negação $\neg H$, achamos um absurdo e concluimos que nossa suposição não pode ser correta, logo H. Mas aqui não começamos supondo algo aleatoriamente. Qual vai ser nossa conclusão agora? Parece que chegamos num absurdo apenas com lógica sem supor nada "extra". Será que lógica ou matemática é quebrada?

13.72. Princípio (Comprehensão geral). *Seja $P(-)$ uma condição definitiva. Existe um conjunto*

$$\{\, x \mid P(x) \,\}$$

cujos membros são exatamente todos os objetos x que satisfazem a condição: $P(x)$.

13.73. Corolário (Russell). *O princípio da comprehensão geral não é válido.*

Demonstração. Supondo que é, chegamos no absurdo que achamos no 13.71. ∎

13.74. Observação (O paradoxo de Russell geral). O paradoxo de Russell que encontramos fala de conjuntos e de pertencer, mas facilmente identificamos que seu paradoxo é apenas um caso duma verdade mais geral. Considere uma relação R. A fórmula

$$\neg\exists x\forall y(R(x,y) \leftrightarrow \neg R(y,y))$$

é um tautologia; um teorema da FOL. Suponha que tal x existe, e o chame de x_0. Como $R(x_0,y) \leftrightarrow \neg R(y,y)$ para todos os y, então tomando $y := x_0$ chegamos na contradição

$$R(x_0,x_0) \leftrightarrow \neg R(x_0,x_0).$$

Observe que tomando como R a relação $\in$ e como universo o universo matemático comum, chegamos no paradoxo de Russell.

§292. As soluções de Russell e de Zermelo

13.75. Teoria dos tipos (Russell).

TODO Escrever

13.76. Teoria axiomática dos conjuntos (Zermelo).

TODO Escrever

13.77. Créditos. A teoria axiomática de conjuntos que estudamos neste capítulo é conhecida como "Zermelo–Fraenkel set theory". Mesmo assim, mais foram envolvidos na sua evolução, sua definição, e seu amadurecimento, como os Mirimanoff, Skolem, e von Neumann, entre outros.

Problemas

▸ **PROBLEMA Π13.3 (Uma carta de Cantor para Dedekind).**
Dia 20 de junho, 1877. Cantor manda uma carta para Dedekind onde ele defina a função $f : [0,1]^2 \to [0,1]$ pela

$$f(a,b) = 0.a_1b_1a_2b_2a_3b_3\ldots \quad \text{onde} \quad \begin{cases} a =: 0.a_1a_2a_3\ldots \\ b =: 0.b_1b_2b_3\ldots \end{cases}$$

são as expansões decimais *que não terminam em 0's repetidos*, exceto para o proprio 0 que só tem essa representação mesmo.[98] Afirmando que ela é bijetora ele ficou surpreso que tinha conseguido demonstrar que $[0,1]^2 =_{\mathrm{c}} [0,1]$. Ansioso, está esperando a resposta de Dedekind.

Dia 22 de junho, 1877. Cantor recebe a carta-resposta:[99] Dedekind percebeu um erro na demonstração!

Dia hoje. Tendo lido tudo isso, tu respondes nas perguntas seguintes: (1) Por que Cantor botou a restricção «que não terminam em 0's repetidos»? (2) Qual o erro de Cantor?[100] (Π13.3H1)

▸ **PROBLEMA Π13.4 (Sem Bernstein).**
Mostre pela definição a equinumerosidade

$$(a,b) =_{\mathrm{c}} [a,b) =_{\mathrm{c}} [a,b];$$

onde $a, b \in \mathbb{R}$ e tais que os intervalos não são nem vazios nem singletons. (Π13.4H123)

▸ **PROBLEMA Π13.5 (Ainda sem Bernstein).**
Cantor demonstrou direitamente (pela sua definição) que

$$[0,1] =_{\mathrm{c}} [0,1] \setminus \mathbb{Q}.$$

Faça o mesmo. (Π13.5H1234)

▸ **PROBLEMA Π13.6.**
No $(\mathbb{N} \to \mathbb{N})$ sejam as relações $\overset{\mathrm{e}}{=}$ e $\overset{\mathrm{o}}{=}$ como no Problema Π10.11:

$$f \overset{\mathrm{e}}{=} g \overset{\text{def}}{\iff} f(2n) = g(2n) \text{ para todo } n \in \mathbb{N}$$
$$f \overset{\mathrm{o}}{=} g \overset{\text{def}}{\iff} f(2k+1) = g(2k+1) \text{ para todo } k \in \mathbb{N}.$$

Qual é a cardinalidade do $[f]_{\overset{\mathrm{e}}{=}} \cap [f]_{\overset{\mathrm{o}}{=}}$? (Π13.6H0)

---

[98] Na verdade esta definição é um caso especial da definição de Cantor; sua função foi do "cubo n-dimensional" para o $[0,1]$.

[99] sim, foi tão rapido; e sim, foi pelos correios mesmo!

[100] Cantor, corrigiu sua demonstração e mandou numa nova carta-resposta, onde também incluiu sua demonstração que $(0,1] =_{\mathrm{c}} [0,1]$ (Problema Π13.4). Dedekind essa vez não respondeu tão rápidamente, e Cantor mandou um lembrete com a frase *je le vois, mais je ne le crois pas* referindo à sua descoberta. Ele escreveu essa frase em francês mesmo, mesmo que a comunicação entre eles foi em alemão. Traduzindo: "eu o vejo, mas eu não o acredito".

▸ **PROBLEMA Π13.7.**
No conjunto dos reais $\mathbb{R}$, defina três relações de equivalência $\sim_1$, $\sim_2$, $\sim_3$, diferentes da igualdade $=_{\mathbb{R}}$, da vazia, e da trivial True, tais que:

$$\mathbb{R}/\!\sim_1 <_{\mathrm{c}} \mathbb{N} \qquad \mathbb{R}/\!\sim_2 =_{\mathrm{c}} \mathbb{N} \qquad \mathbb{R}/\!\sim_3 >_{\mathrm{c}} \mathbb{N}.$$

Para cada uma, descreva seu conjunto quociente. (Π13.7 H 1)

▸ **CODE-IT c13.6 (RatApprox).**
Usando uma implementação de enumeração $\{q_n\}_n$ do $\mathbb{Q}$ (com ou sem repetições), implemente uma função $a : \mathbb{R} \times \mathbb{R} \to \mathbb{N}$ que, dados $x \in \mathbb{R}$ e $\varepsilon > 0$ retorna o primeiro $n \in \mathbb{N}$ com a propriedade $|q_n - x| < \varepsilon$:

$$a(x, \varepsilon) = \min \{\, n \in \mathbb{N} \mid |q_n - x| < \varepsilon \,\}.$$

Se tua linguagem de programação suporta funções de ordem superior, considere que seu primeiro argumento deve ser a própria enumeração q:

$$\begin{aligned} &\mathit{ratApprox} : (\mathbb{N} \to \mathbb{Q}) \to \mathbb{R} \to \mathbb{R} \to \mathbb{N} \\ &\mathit{ratApprox}\; q\; x\; \varepsilon = \min \{\, n \in \mathbb{N} \mid |q_n - x| < \varepsilon \,\} \end{aligned}$$

Alternativamente, pode representar uma enumeração de racionais como uma lista (infinita) de racionais. Considere retornar o primeiro racional suficientemente próximo além de apenas seu índice. Improvise e teste sua função, vendo quanto "demora" uma enumeração para chegar suficientemente perto de um número pre-determinado, sendo racional ou não. Por exemplo, use $x = \sqrt{2}$ ou e ou π, e $\varepsilon = 1, 1/2, 1/4, \ldots$. Assim, para qualquer real x, tu pode *construir*—mesmo não muito "eficientemente"—uma seqüência de racionais que converge em x, apenas aplicando a função $\lambda\varepsilon\,.\,\mathit{ratApprox}\; q\; x\; \varepsilon$ em argumentos que formam qualquer seqüência que convirja no zero! (c13.6 H 0)

D13.78. Definição (Jogo terminante). Consideramos jogos entre 2 jogadores. Chamamos um jogo *terminante* sse não tem partidas infinitas. Ou seja, seguindo suas regras cada partida termina depois um finíto número de turnos.

D13.79. Definição (Hypergame (Zwicker)). Considere o jogo seguinte $\mathcal{H}$, chamado *hypergame*: O $\mathcal{H}$ começa com o Player I que escolha um jogo terminante G. O Player II começa jogar o jogo G contra o Player I. Quem ganha nesse jogo G é o vencedor do jogo $\mathcal{H}$.

• **EXEMPLO 13.80.**
Por exemplo, sendo um bom jogador de "jogo da velha" e um pessimo jogador de xadrez, se eu for o Player I num hypergame, meu primeiro movimento seria escolher o jogo terminante "jogo da velha" para jogar. Meu oponente, se for o Player I duma partida de hypergame, seu primeiro movimento seria escolher o jogo terminante "xadrez". Depois desse movimento eu viro o Player I no xadrez. Quem vai ganhar nesse xadrez, vai ser o vencedor dessa partida de hypergame.

13.81. O paradoxo de hypergame. Zwicker percebeu o seguinte paradoxo, se perguntando se o próprio Hypergame é um jogo terminante ou não. Claramente tem que ser, pois a primeira regra do jogo obriga o PLAYER I escolher um jogo terminante. Logo, depois de $n \in \mathbb{N}$ turnos, esse jogo termina, e junto com ele termina a partida do hypergame (em $n+1$ turnos). Então hypergame é terminante. Logo, numa partida de hypergame, o PLAYER I pode escolher o próprio hypergame. Assim começamos uma sub-partida de hypergame, onde o PLAYER II toma o papel de PLAYER I. Se ele escolher, por exemplo, "jogo de velha", a partida parece assim:

P : Escolho "Hypergame"
O : Escolho "Jogo de velha"
P :
⋮ ⋮
O :
P :

Onde denotamos os dois jogadores com P e O (de "Player" e "Opponent"). Mas, agora a partida seguinte é possível:

P : Escolho "Hypergame"
O : Escolho "Hypergame"
P : Escolho "Hypergame"
O : Escolho "Hypergame"
⋮ ⋮

e achamos uma partida infinita do hypergame! Logo o hypergame não é terminante.

▸ **PROBLEMA Π13.8.**
Seja conjunto A e suponha que existe injecção $\varphi : A \rightarrowtail \wp A$. Para todo $x \in A$, denota com A_x o $\varphi(x)$, ou seja, A_x é o subconjunto de A associado com o x. Seja $a \in A$. Chame um *caminho* de a qualquer seqüência finita ou infinita $\{a_i\}_i$ de elementos de A que satisfaz:

$$a_0 = a$$
$$a_{n+1} \in A_{a_n}.$$

Finalmente, chame um $a \in A$ *terminante* se todos os caminhos de a são finítos. Use o paradoxo do Hypergame para demonstrar que a φ não pode ser sobrejetora, achando assim uma nova demonstração do teorema de Cantor Θ13.51. (Π13.8 H 1 2 3)

▸ **PROBLEMA Π13.9 (Agora é fácil).**
Para resolver o Problema Π11.15 demonstramos um certo "buraco" que o Q_1 tem: o $(0,0)$. Tem outro(s)? Quantos? (Π13.9 H 1)

Θ13.82. Teorema (von Lindemann). *Para todo $\alpha \neq 0$ algébrico, e^α é transcendental.*

▸ **PROBLEMA Π13.10.**
Dado o teorema de von Lindemann Θ13.82 demonstre que π é transcendental. (Π13.10H1)

▸ **PROBLEMA Π13.11.**
Responda com 'T' ou 'F' quando possível:[101]

(a) o conjunto dos números transcendentais é contável:
(b) existe irracional α tal que α^α é racional:
(c) nas questões do Problema Π13.11 tem mais afirmações falsas do que verdadeiras:
(d) o conjunto $(\mathbb{N} \to \{0,1\})$ é contável:
(e) o segmento $[0,1]$ é equinúmero com o cubo $[0,1]^3$:

(Π13.11H0)

Leitura complementar

Sobre a teoria de conjuntos de Cantor. [Kle52], [Mos05].
Um livro muito divertido que trata bem essas idéias de infinito que encontramos aqui é o [Smu92: Part VI].

Sobre teoria da medida. [Bar14], [Hal13], [Tay12].

Sobre os passos que levaram Cantor nas suas descobertas. [Sri14]. Mais sobre a construtividade e os ataques injustos contra a demonstração de Cantor no [Gra94]. Cantor conheceu Dedekind na Suiça no 1872 e desde então e até 1899 trocaram muitas cartas entre si comunicando suas idéias que acabaram gerando as teorias que conhecemos aqui neste capítuo e que vão muito além disso! A colecção dessas cartas foi publicada no [CD37]. O [Gou11] é artigo curto e bem escrito que resuma a historia entre Cantor e Dedekind, oferecendo também uma análise na situação, nos posicionamentos, e até nos possíveis sentimentos envolvidos dos dois homens. O [Fer93] é uma análise mais extensa, defendendo bastante a contribuição de Dedekind nos resultados que geralmente atribuimos apenas ao Cantor.

[101] A terceira questão fez parte *mutatis mutandis* duma prova final de Rondogiannis (infelizmente muitos anos depois de tê-lo como professor).

CAPÍTULO 14

POSETS; RETICULADOS

§293. Conceito, notação, propriedades

TODO Conceito

D14.1. Definição (poset). Chamamos o conjunto estruturado $\mathcal{P} = (P\,;\leq)$ um *poset* (ou conjunto parcialmente ordenado), sse $(\leq)$ é uma relação de ordem parcial:

$$\begin{gathered} x \leq x \\ x \leq y \;\&\; y \leq z \implies x \leq z \\ x \leq y \;\&\; y \leq x \implies x = y \end{gathered}$$

14.2. Abusos notacionais. Extendemos o "tipo" do predicado $- \leq -$ de elementos de P para elementos e/ou subconjuntos de P, definindo:

$$\begin{aligned} a \leq Y &\overset{\text{def}}{\iff} a \leq y, \quad \text{para todo } y \in Y; \\ X \leq b &\overset{\text{def}}{\iff} x \leq b, \quad \text{para todo } x \in X; \\ X \leq Y &\overset{\text{def}}{\iff} x \leq y, \quad \text{para todo } x \in X \text{ e } y \in Y. \end{aligned}$$

Nas definições seguintes nosso contexto é um poset $(P\,;\leq)$.

D14.3. Definição. Se $x \not\leq y$ e $y \not\leq x$ chamamos x e y *incomparáveis*. Denotamos assim:

$$x \parallel y \overset{\text{def}}{\iff} x \not\leq y \;\&\; y \not\leq x.$$

D14.4. Definição. Seja $X \subseteq P$. Chamamos o X uma *cadeia* sse todos os seus elementos são comparáveis. No caso oposto, onde todos são comparáveis apenas com eles mesmo, chamamos o X *anticadeia*. Simbolicamente:

$$\begin{aligned} \text{cadeia:} &\quad x, y \in X \implies x \leq y \text{ ou } y \leq x; \\ \text{anticadeia:} &\quad x, y \in X \;\&\; x \leq y \implies x = y. \end{aligned}$$

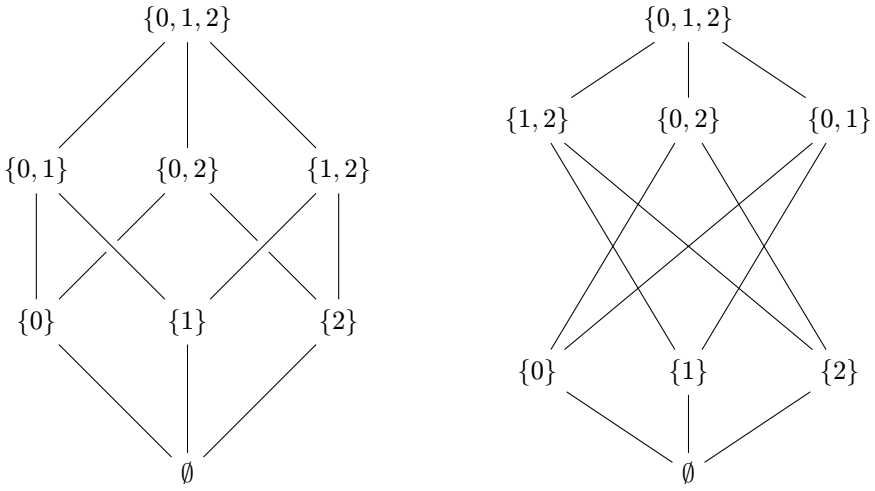
D14.5. Definição. Se $x \leq y$ e não existe nenhum z estritamente entre os x e y falamos que y *cobre* o x. Simbolicamente:

$$x \prec y \overset{\text{def}}{\iff} x < y \;\&\; \neg\exists z(x < z < y).$$

14.6. Diagramas Hasse. Já encontramos diagramas Hasse no Capítulo 11 (11.209, 11.210, x11.128) onde desenhamos os Hasse duns posets de subgrupos.

! **14.7. Cuidado.** Diagramas Hasse podem aparecer bastante diferentes mesmo sendo do mesmo poset.

• **EXEMPLO 14.8.**
Aqui duas formas de desenhar diagramas Hasse para o $(\wp\{0,1,2\}\,;\subseteq)$:



Esse poset é chamado *cubo:* por motivos óbvios se olhar no seu primeiro diagrama, e não-tão-óbvios olhando para o segundo!

D14.9. Definição. Sejam $A \subseteq P$. Chamamos o m de *mínimo* de A sse $m \in A$ e $m \leq a$ para todo $a \in A$. *Dualmente* m é o *máximo* de A sse $m \in A$ e $a \leq m$ para todo $a \in A$. Denotamos o mínimo de A, se existe, por $\min A$; e seu máximo, se existe, por $\max A$. ↯

▸ **EXERCÍCIO x14.1.**
Qual o erro na definição acima? O ache e o corrija. (x14.1H0)

▸ **EXERCÍCIO x14.2.**
Seja U um conjunto unitário ordenado. Demonstre que ele tem mínimo. Quais propriedades da $(\leq)$ tu precisas aqui? (x14.2H0)

▸ **EXERCÍCIO x14.3.**
Demonstre que qualquer conjunto finito, não vazio, e linearmente ordenado é bem ordenado. (x14.3H1)

D14.10. Definição. Se o próprio $P \subseteq P$ possui elemento mínimo, o chamamos de *bottom* de P, e se possui máximo, o chamamos de *top* de P. Usamos as notações $\bot_P$ e $\top_P$ respectivamente, esquecendo o $_P$ quando é implícito pelo contexto. Sinônimos de bottom e top são os *zero* e *um* respectivamente, usando as notações 0_P e 1_P. Se um poset possui bottom, ele é chamado *bounded por baixo*, e se ele possui top, ele é chamado *bounded por cima*. Caso que seja bounded por cima e por baixo, o chamamos apenas de *bounded*.

D14.11. Definição. Chamamos o x um elemento *minimal* de P sse nenhum elemento está embaixo dele, e, *dualmente* chamamos o x *maximal* de P sse nenhum elemento está acima dele. Simbolicamente:

$$x \text{ minimal de } P \stackrel{\text{def}}{\iff} (\forall y \in P)[\, y \leq x \implies x = y\,];$$
$$x \text{ maximal de } P \stackrel{\text{def}}{\iff} (\forall y \in P)[\, x \leq y \implies x = y\,].$$

D14.12. Definição. Sejam $A \subseteq P$ e $p \in P$. O p é uma *cota superior* (ou *upper bound*) de A sse $p \geq A$. Dualmente, o p é uma *cota inferior* (ou *lower bound*) de A sse $p \leq A$. Usamos a notação

$$(A \leq) \stackrel{\text{def}}{=} \operatorname{ubs} A \stackrel{\text{def}}{=} \{\, p \in P \mid A \leq p \,\}$$
$$(\leq A) \stackrel{\text{def}}{=} \operatorname{lbs} A \stackrel{\text{def}}{=} \{\, p \in P \mid p \leq A \,\}.$$

• **EXEMPLO 14.13.**
No $\mathbb{R}$, considere seu subconjunto $(1, 2]$. Uns upper bounds dele são os reais $2, 5, \sqrt{12}, 8000$; uns lower bounds dele são os $-400, -\pi, 0, 1/2, 0.8, 1$.

D14.14. Definição. Se os $\operatorname{ubs} A$ e $\operatorname{lbs} A$ tem elemento mínimo e máximo respectivamente, definimos

$$\operatorname{lub} A \stackrel{\text{def}}{=} \min \operatorname{ubs} A$$
$$\operatorname{glb} A \stackrel{\text{def}}{=} \max \operatorname{lbs} A.$$

Naturalmente chamamos o $\operatorname{lub} A$ o *least upper bound* de A, e o $\operatorname{glb} A$ o *greatest lower bound* de A. Usamos *muitos* sinônimos, resumidos aqui:

$\sup A$ (supremum)	$\operatorname{lub} A$ (least upper bound)	$\bigvee A$ (join)
$\inf A$ (infimum)	$\operatorname{glb} A$ (greatest lower bound)	$\bigwedge A$ (meet)

• **EXEMPLO 14.15.**
O $A = (1, 2]$ do Exemplo 14.13 tem $\inf A = 1$ e $\sup A = 2$. Observe que $\sup A \in A$ mas $\inf A \notin A$.

▸ **EXERCÍCIO x14.4.**
O que podemos concluir quando $\operatorname{glb} A \in A$ e quando $\operatorname{lub} A \in A$? (x14.4H0)

D14.16. Definição. Chamamos o $A \subseteq P$ um *downset* no P sse o A é "fechado para baixo", e *dualmente*, o chamamos *upset* sse ele é "fechado para cima". Formalmente,

$$A \text{ downset} \stackrel{\text{def}}{\iff} (\forall a \in A)(\forall x \leq a)[\, x \in A\,];$$
$$A \text{ upset} \stackrel{\text{def}}{\iff} (\forall a \in A)(\forall x \geq a)[\, x \in A\,].$$

Dado um poset P, usamos $\mathcal{O}(P)$ para denotar o conjunto de todos os seus downsets. Simbolicamente,

$$\mathcal{O}(P) \stackrel{\text{def}}{=} \{\, D \subseteq P \mid D \text{ é um downset de } P\,\}.$$

D14.17. Definição. Definimos para qualquer $a \in P$ os conjuntos

$$\downarrow a \stackrel{\text{def}}{=} \{\, x \in P \mid x \leq a \,\}$$
$$\uparrow a \stackrel{\text{def}}{=} \{\, x \in P \mid a \leq x \,\}$$

e generalizamos essas operações de elementos $a \in P$ para subconjuntos $A \subseteq P$ assim:

$$\downarrow A \stackrel{\text{def}}{=} \{\, x \in P \mid x \leq a \text{ para algum } a \in A \,\}$$
$$\uparrow A \stackrel{\text{def}}{=} \{\, x \in P \mid a \leq x \text{ para algum } a \in A \,\}.$$

Observe que $\downarrow x = \downarrow\{x\}$ e $\uparrow x = \uparrow\{x\}$. Diretamente pelas definições também temos:

$$\downarrow A = \bigcup_{a \in A} \downarrow a \qquad\qquad \uparrow A = \bigcup_{a \in A} \uparrow a$$

▸ **EXERCÍCIO x14.5.**
Sejam P poset e $A \subseteq P$. Demonstre que $\downarrow A$ é um downset e $\uparrow A$ um upset. (x14.5H0)

▸ **EXERCÍCIO x14.6.**
Sejam P um poset, $x, y \in P$. Demonstre que as afirmações

(i) $x \leq y$;
(ii) $\downarrow x \subseteq \downarrow y$;
(iii) para todo downset D de P com $y \in D$, temos $x \in D$;

são equivalentes. (x14.6H0)

§294. Posets de graça: operações e construções

TODO elaborar

D14.18. Definição (discreto). Qualquer conjunto X equipado com a igualdade vira um poset, que chamamos de *discreto*.

D14.19. Definição (dual). Dado qualquer poset $(P\,; \leq_P)$ definimos o seu poset *dual* que denotamos por P^∂ apenas virando o P "de cabeça pra baixo"; ou seja, usando como ordem do P^∂ a $\geq_P$:

$$x \leq_{P^\partial} y \iff y \leq_P x.$$

D14.20. Definição (números).

TODO Escrever

D14.21. Definição (lift). Para qualquer poset P definimos seu *lifting* $P_\perp$ botando um novo membro abaixo do P.

▸ **EXERCÍCIO x14.7.**
Formalize a Definição D14.21. (x14.7H0)

D14.22. Definição (flat). Um poset P é chamado *flat* sse possui mínimo $\bot$ e

$$x \leq y \iff x = \bot \text{ ou } x = y.$$

D14.23. "Definição" (soma). Dados posets disjunos P, Q definimos sua *soma* $P \oplus Q$ para ser o poset botando cada membro de Q para ser maior de cada membro de P; fora disso, consultamos as ordens dos P e Q.

▸ **EXERCÍCIO x14.8.**
Defina formalmente a soma de posets $P \oplus Q$ numa maneira que é capaz de lidar até com posets cujos carrier sets não são necessariamente disjuntos. (x14.8H0)

▸ **EXERCÍCIO x14.9.**
Defina o $P_\bot$ como somatório. (x14.9H0)

D14.24. "Definição" (união). Dados P e Q posets disjuntos definimos sua *união* $P \uplus Q$ para ser o poset botando o P e o Q um no lado do outro.

▸ **EXERCÍCIO x14.10.**
Defina formalmente a união de posets $P \uplus Q$ numa maneira que é capaz de lidar até com posets cujos carrier sets não são necessariamente disjuntos. (x14.10H0)

? **Q14.25. Questão.** Dados posets P, Q, como tu definaria (formalmente) uma ordem nos membros de $P \times Q$ para ele virar um poset também?

!! SPOILER ALERT !!

Resposta. Tem duas ordens bem diferentes e importantes que podemos definir no $P \times Q$: a "coordinatewise" e a "(anti)lexicográfica":

D14.26. Definição (produto componentwise). Sejam P, Q posets. Definimos a relação $(\leq_{P\times Q})$ no $P \times Q$ pela:

$$(p, q) \leq_{P\times Q} (p', q') \overset{\text{def}}{\iff} p \leq_P p' \ \&\ q \leq_Q q'.$$

Chamamos essa ordem de *componentwise* ou *coordinatewise*.

D14.27. Definição (produto (anti)lexicó). Sejam P, Q posets. Definimos a *ordem lexicográfica* no $P \times Q$ pela

$$(p,q) \leq_{P\times Q} (p',q') \iff^{\text{def}} p <_P p' \text{ ou } (p = p' \ \&\ q \leq_Q q').$$

A ordem é chamada assim pois é a ordem seguida nos diccionários (e "lexicó" significa "diccionário"). Similarmente definimos a ordem *antilexicográfica* começando as comparações no lado oposto:

$$(p,q) \leq'_{P\times Q} (p',q') \iff^{\text{def}} q <_Q q' \text{ ou } (q = q' \ \&\ p \leq_P p').$$

14.28. Observação. A ordem padrão que vamos considerar em produtos de posets é a coordinatewise. Observe que ela generaliza tranqüilamente para famílias indexadas por qualquer conjunto de índices $\mathcal{I}$; porém, para generalizar a (anti)lexicográfica, o $\mathcal{I}$ necessita uma ordem também.

▸ **EXERCÍCIO x14.11.**
Generalize a ordem componentwise para o produto cartesiano de família indexada de posets. (x14.11 H 0)

▸ **EXERCÍCIO x14.12.**
Generalize a ordem (anti)lexicográfica para o produto cartesiano de família indexada de posets. (x14.12 H 0)

? **Q14.29. Questão.** Dado poset P e conjunto A, como definarias uma ordem no espaço $(A \to P)$?

!! SPOILER ALERT !!

D14.30. Definição (pointwise). Sejam P poset e A conjunto. Definimos a ordem *pointwise* no espaço de funções $(A \to P)$ pela

$$f \leq g \iff^{\text{def}} (\forall x \in A)[\, fx \leq_P gx \,].$$

▸ **EXERCÍCIO x14.13.**
A mesma ordem ordena o $(A \rightharpoonup P)$? (x14.13 H 0)

§295. Dualidade

TODO escrever

§296. Mapeamentos

D14.31. Definição. Sejam $(P\,;\leq_P)$ e $(Q\,;\leq_Q)$ posets e $\varphi : P \to Q$. Definimos

$$\begin{aligned}
\varphi \text{ monótona} &\stackrel{\text{def}}{\iff} x \leq_P y \implies \varphi(x) \leq_Q \varphi(y) \\
\varphi \text{ order-embedding} &\stackrel{\text{def}}{\iff} \varphi \text{ injetora } \&\ x \leq_P y \iff \varphi(x) \leq_Q \varphi(y) \\
\varphi \text{ order-isomorfismo} &\stackrel{\text{def}}{\iff} \varphi \text{ bijetora } \&\ x \leq_P y \iff \varphi(x) \leq_Q \varphi(y)
\end{aligned}$$

14.32. Critério. *Se $\varphi : P \to Q$ tal que*

$$x \leq_P y \iff \varphi(x) \leq_Q \varphi(y)$$

então φ é um order-embedding. Segue que se φ é sobrejetora, ela é um order-isomorfismo.

Demonstração. Basta demonstrar que φ é injetora. Tome $x, y \in P$. Temos

$$\begin{aligned}
\varphi(x) = \varphi(y) &\implies \varphi(x) \leq_Q \varphi(y) \ \&\ \varphi(y) \leq_Q \varphi(x) && \text{(Exercício x14.14)} \\
&\implies x \leq_P y \ \&\ y \leq_P x && \text{(pela hipótese)} \\
&\implies x = y. && \text{(antissimetria)}
\end{aligned}$$

∎

▸ **EXERCÍCIO x14.14 (Converso de antissimetria).**
Justifique a primeira implicação na demonstração do Critério 14.32. (x14.14H0)

▸ **EXERCÍCIO x14.15.**
Defina um $\varphi : \mathcal{O}(P) \cong \mathcal{O}(P^\partial)$. (x14.15H0)

▸ **EXERCÍCIO x14.16.**
Defina um $\psi : \mathcal{O}(P_1 \uplus P_2) \cong \mathcal{O}(P_1) \times \mathcal{O}(P_2)$. (x14.16H0)

▸ **EXERCÍCIO x14.17.**
Para $n \in \mathbb{N}$, definimos o poset $\mathcal{D}_n \stackrel{\text{def}}{=} (D_n\,;|)$ onde $D_n \stackrel{\text{def}}{=} \{\, d \in \mathbb{N} \mid d \mid n \,\}$.
(i) Desenhe o diagrama Hasse de $\mathcal{D}_{30}$.
(ii) Ache conjunto A tal que $\mathcal{D}_{30} \cong (\wp A\,;\subseteq)$ e defina um isomorfismo $\varphi : D_{30} \to \wp A$.
(iii) Existe conjunto B tal que $\mathcal{D}_0 \cong (\wp B\,;\subseteq)$? Se sim, ache o B e defina um isomorfismo $\varphi : D_0 \to \wp B$; se não, demonstre que é impossível. (x14.17H0)

§297. Direções

§298. Reticulados como posets

D14.33. Definição. Um poset $\mathcal{L} = (L\ ;\leq)$ é um *lattice* (ou *reticulado*) sse para todo $x, y \in L$, os $\sup\{x, y\}$ e $\inf\{x, y\}$ existem.

§299. Reticulados como estruturas algébricas

No Capítulo 12 introduzimos reticulados como uma estrutura algébrica.[102] Aqui a definição novamente:

D14.34. Definição. Seja $\mathcal{L} = (L\ ;\vee,\wedge)$ conjunto estruturado onde $\vee,\wedge$ são operadores binários no L. Chamamos o L um *lattice* (ou *reticulado*) sse as operações $\vee,\wedge$ são associativas, comutativas, e idempotentes, e satisfazem as leis seguintes *de absorção*:

$$a \vee (b \wedge a) = a$$
$$a \wedge (b \vee a) = a$$

TODO place the following somewhere

14.35. Conselho. Vamos supor que tu tá tentando demonstrar

$$(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z).$$

Os $(\wedge)$ e $(\vee)$ sendo glb e lub, fornecem duas maneiras de visualizar esse alvo. Primeiramente esqueça o $(\wedge)$ à direita: considera toda a $x \wedge (y \vee z)$ como uma coisa só, e perceba qua a parte esquerda é um $(\vee)$, um join, um l.u.b.:

$$(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z).$$

Ou seja precisamos demonstrar que o *azul* é $(\geq)$ que um l.u.b.; basta então mostrar que é *um* u.b.:

$$\frac{\bullet \geq \bullet \qquad \bullet \geq \bullet}{\bullet \geq (\bullet \vee \bullet)}$$

Alternativamente enxergue a parte esquerda como uma coisa só e perceba que a parte direita é um $(\wedge)$, um meet, um g.l.b.:

$$(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z).$$

Assim precisamos demonstrar que o *azul* é $(\leq)$ que um g.l.b.; basta então mostrar que é *um* l.b.:

$$\frac{\bullet \leq \bullet \qquad \bullet \leq \bullet}{\bullet \leq (\bullet \wedge \bullet)}$$

[102] Leia a Secção §271 se não tá ligado.

§300. Reticulados completos

D14.36. Definição. Um reticulado L é um *reticulado completo* sse para todo $S \subseteq L$ ambos os $\bigvee S$ e $\bigwedge S$ são definidos.

▸ **EXERCÍCIO x14.18.**
Todo reticulado completo é bounded. (x14.18H0)

14.37. Observação. Já demonstramos que num reticulado L os joins e meets existem para qualquer subconjunto *não vazio e finito* dele. Então num reticulado *completo*, sabemos disso para o vazio e para os subconjuntos infinitos também.

TODO generalize o Definição D8.168 para qualquer reticulado completo

§301. Fixpoints

D14.38. Definição. Seja $f : X \to X$. Usamos a notação

$$\operatorname{Fix} f \stackrel{\text{def}}{=} \{\, x \in X \mid x \text{ é um fixpoint de } f \,\}$$

e se X é um poset e $\operatorname{Fix} F$ tem mínimo e máximo botamos

$$\operatorname{lfp} f \stackrel{\text{def}}{=} \min(\operatorname{Fix} f) \qquad \text{o } \textit{menor fixpoint} \text{ de } f$$
$$\operatorname{gfp} f \stackrel{\text{def}}{=} \max(\operatorname{Fix} f). \qquad \text{o } \textit{maior fixpoint} \text{ de } f$$

D14.39. Definição (prefixpoints, postfixpoints). Sejam P poset e $F : P \to P$ e seja $p \in P$. Chamamos o p de *prefixpoint da* F sse $Fp \leq p$. Dualmente p é um *postfixpoint da* F sse $p \leq Fp$.

Θ14.40. Teorema (Knaster–Tarski). *Seja L reticulado completo e $F : L \to L$ monótona. Então F tem um fixpoint.*

▸ Esboço. Sejam

$$D := \{\, x \in L \mid x \leq Fx \,\} \qquad\qquad U := \{\, x \in L \mid Fx \leq x \,\}.$$

os conjuntos de todos os postfixpoints e prefixpoints da F respecitivamente. Considere o conjunto $\operatorname{Fix} F$. Observe que $\operatorname{Fix} F = D \cap U$. Vamos demonstrar que o $\bigvee D$ é um fixpoint de F. (O $\bigwedge U$ é similar.) Precisamos $\bigvee D = F(\bigvee D)$. Vamos demonstrar $\bigvee D \leq F(\bigvee D)$ primeiro e depois $F(\bigvee D) \leq \bigvee D$. $\bigvee D \leq F(\bigvee D)$: Como $\bigvee D$ é o least upper bound de D, basta demonstrar $F(\bigvee D)$ é um upper bound de D. $F(\bigvee D) \leq \bigvee D$: Aqui como $\bigvee D$ é um upper bound de D, basta mostrar que $F(\bigvee D)$ é um membro de D. (Nessa parte podemos e vamos usar a $\bigvee D \leq F(\bigvee D)$ que acabamos de demonstrar!) □ (Θ14.40P)

14.41. Observação. O teorema Knaster–Tarski fala ainda mais: o $\operatorname{Fix} F \subseteq L$ é um reticulado completo (Problema Π14.4).

TODO explicar e desenhar

14.42. Corolário. *Sejam $a, b \in \mathbb{R}$ com $a \leq b$, e função $f : [a, b] \to [a, b]$ monótona. Logo f tem um máximo e um mínimo fixpoint.*

14.43. Observação. Observe que no Corolário 14.42 não precisamos da f ser contínua.

14.44. Nova demonstração de Schröder–Bernstein. Ganhamos também como corolário o teorema Schröder–Bernstein (Θ13.45)! Os detalhes estão no Problema Π14.6.

D14.45. "Definição" (órbita). Seja $a \in A$ e $f : A \to A$. Chamamos a seqüência

$$a, fa, f^2a, \dots$$

de *f-órbita* de a, omitindo o prefixo 'f-' quando o mapa é implícito pelo contexto.

▸ **EXERCÍCIO x14.19.**
Sejam P um poset com $\bot$ e f um endomapa no P. Defina formalmente a f-órbita do $\bot$. (x14.19 H 0)

D14.46. Definição. Um poset P é chamado *chain-completo* sse todo chain $C \subseteq P$ possui lub.

▸ **EXERCÍCIO x14.20.**
Todo poset chain-completo possui bottom. (x14.20 H 0)

D14.47. Definição. Sejam P, Q posets indutivos. Um mapa $f : P \to Q$ é chamado *contavelmente continuo* sse f respeita os lubs de todas as *cadeias habitadas e contáveis:* $f(\bigvee C) = \bigvee f[C]$.

Θ14.48. Teorema (Kleene). *Sejam P poset chain-completo e $\pi : P \to P$ endomapa monótono e contavelmente continuo. Logo π possui exatamente um strongly least fixpoint x^*:*

$$\text{(i)} \qquad \pi(x^*) = x^*$$
$$\text{(ii)} \qquad (\forall y \in P)[\,\pi(y) \leq y \implies x^* \leq y\,]$$

▸ Esboço. A idéia é tomar como x^* o lub dos elementos da órbita do $\bot$ e demonstrar que ele é o único strongly least fixpoint. □ (Θ14.48P)

▸ **EXERCÍCIO x14.21.**
Para qualquer π monótona a π-órbita de $\bot$ é uma cadeia. (x14.21 H 0)

▸ **EXERCÍCIO x14.22.**
O x^* da demonstração do Teorema Θ14.48 é um fixpoint. (x14.22 H 0)

▸ **EXERCÍCIO x14.23.**
O x^* da demonstração do Teorema Θ14.48 é o strongly least fixpoint. (x14.23H0)

§302. Elementos irredutíveis

§303. Álgebras booleanas

§304. Álgebras Heyting

§305. Pouco de cats—categorias e posets

§306. Teoria de domínios

Problemas

▸ **PROBLEMA Π14.1.**
Demonstre que o $\mathbb{Q}$ com sua ordem padrão é denso. (Π14.1H0)

D14.49. Definição. Chamamos um $A \subseteq \mathbb{N}$ *cofinito* sse seu complemento $\mathbb{N} \setminus A$ é finito.

▸ **PROBLEMA Π14.2.**
Mostre que as famílias

$$\mathscr{L}_1 := \{\, A \subseteq \mathbb{N} \mid A \text{ é cofinito} \,\}$$
$$\mathscr{L}_2 := \{\, A \subseteq \mathbb{N} \mid A \text{ é finito ou cofinito} \,\}$$

são *reticulados de conjuntos*, ou seja, reticulados com relação de ordem $(\subseteq)$. (Π14.2H0)

▸ **PROBLEMA Π14.3.**
Mostre que nenhum dos $\mathscr{L}_1, \mathscr{L}_2$ do Problema Π14.2 é completo. (Π14.3H1)

▸ **PROBLEMA Π14.4 (Teorema Knaster–Tarski completo).**
No contexto do Teorema Θ14.40, demonstre que o subconjunto $\operatorname{Fix} F \subseteq L$ é um reticulado completo. (Π14.4H0)

▸ **PROBLEMA Π14.5 (Teorema de decomposição de Banach).**

TODO escrever

(Π14.5H0)

▸ **PROBLEMA Π14.6 (Teorema de Schröder–Bernstein).**
Sejam $f : A \rightarrowtail B$ e $g : B \rightarrowtail A$ funções injetoras. Usando o teorema fixpoint de Knaster–Tarski Θ14.40 demonstre que existe função bijetora $h : A \rightarrowtail\!\!\!\!\twoheadrightarrow B$. (Π14.6H1234)

Leitura complementar

[DP02], [Grä09], [Grä11].
[Mos05: Cap. 6].
[CL00: Cap. 2], [BM77a: Cap. 4], [Hal63].

CAPÍTULO 15

TEORIA DAS CATEGORIAS

§307. O que é uma categoria?

TODO Escrever

§308. Exemplos e nãœxemplos

TODO Adicionar desenhos

- **EXEMPLO 15.1 (Um).**
  Aqui a categoria $\mathbb{1}$. Ela possui exatamente um objeto (não importa qual) que denotarei por $\star$, uma seta (não importa qual). Necessariamente tal seta deve ter como source e target o único objeto disponível. Devo também esclarecer qual é a identidade desse objeto, mas eu tenho uma única opção para ela: só pode ser a única seta do $\star$ para ele mesmo.

- **EXEMPLO 15.2 (Dois).**
  E aqui a categoria $\mathbb{2}$. Ela possui exatamente dois objetos (não importa quais) que denotarei por $\star$ e $\bullet$, uma seta de $\star$ para $\bullet$ e (necessariamente) mais duas setas (quais?). Devo também esclarecer qual é a identidade desse objeto, mas eu tenho uma única opção para ela: só pode ser a única seta do $\star$ para ele mesmo.

§309. Primeiras definições

TODO Escrever

Problemas

Leitura complementar

[LS09], [AM75], [LR03].

[Gol06].

[Awo10], [BW90], [AHS09], [Bor94].

[Rie16], [Mac13].

Sobre teoria dos grafos, já que foram mencionados neste capítulo: umas introduções extensas são os [BM76] e [CZ12]. Depois continua com [Die05] e [BM11]. Finalmente, um nível ainda mais avançado, [Bol98].

CAPÍTULO 16

TEORIA DOS CONJUNTOS

Quando "protoencontramos" conjuntos no Capítulo 8, prometi que eles têm um papel importante para a *fundação de matemática*. Chegou a hora para ver o porquê! Podemos traduzir todas as definições e relações matemáticas nessa linguagem. Nesse sentido, parece como uma assembly: uma linguagem low-level onde podemos "compilar" toda a matemática, em tal modo que cada definição, cada afirmação, cada teorema que demonstramos, no final das contas, todos podem ser traduzidos para definições, afirmações, teoremas e demonstrações, que envolvem apenas conjuntos e a relação primitiva de *pertencer*. E *nada* mais!

P16.1. Noção primitiva (conjunto). Aceitamos apenas duas *noções primitivas* (§12): [redacted]

ser conjunto	pertencer
$\mathrm{Set}(-)$	$- \in -$

Escrevemos '$x \in A$' e pronunciamos «(o objeto) x é um membro do (conjunto) A», ou simplesmente «x pertence ao A».

§310. O princípio da puridade

D16.2. Definição (urelemento). Chamamos de *átomos* ou de *urelementos*, os objetos que não são conjuntos (mas podem pertencer a conjuntos). Números, funções, pessoas, sapos, planetas, etc.

16.3. Princípio de Puridade. *Tudo é conjunto.*

16.4. Seria ruim assumir o princípio da puridade. Como assim «só tem conjuntos»? É pra jogar fora os objetos de todos os outros tipos que temos estudado até agora? E os números, as funções, os grupos? E as pessoas? Eu com certaza existo, e meu leitor também, não é assim? Se nosso universo é para ter apenas conjunto só vamos conseguir falar de conjuntos. E em matemática mesmo que os conjuntos são importantes per se, temos muitas coisas também importantes que não são conjuntos. Então não faz sentido nos limitar. Ou talvez faz:

16.5. Seria bom assumir o princípio da puridade. Alguém falando sobre computadores e programação falou:

«Tudo é 0's e 1's. Não tem nada mais que isso.»

Primeiramente temos que apreciar a simplicidade dum mundo onde *só tem bits*. Porém, meu computador tem este texto que tô escrevendo aqui pra ti; e umas músicas, fotos, vídeos—e mais coisas que não são da tua conta. Os programas que programamos e que usamos manipulam números, conexões, documentos, ou até outros programas. O que o rapaz acima quis dizer com sua afirmação então? Bem, com certeza esse documento *não é* uma seqüência de 0's e 1's, mas *pode ser representado fielmente* por uma. E é assim que meu computador o representa mesmo. Pensando na mesma maneira, quando optamos para assumir o princípio da puridade parece que vamos perder tudo que não é conjunto como algo primitivo; mas se conseguirmos *representá-lo fielmente* dentro do mundo dos conjuntos não vamos perder nada essencialmente. Vamos voltar nesse assunto daqui a pouco na §315.

16.6. O que Zermelo faria?. Zermelo não assumiu o princípio da puridade, nem sua negação. Ou seja, talvez o universo tem urelementos, talvez não. Como nenhum teorema dependeu na existência deles, então tudo continua válido mesmo se escolher assumí-lo, *algo que vamos fazer aqui*, comentando às vezes o que teria que mudar caso que não tivemos esse princípio. Assim não vamos precisar do predicado $\mathrm{Set}(-)$ que teriamos de carregar em muitas definições e demonstrações.

§311. Traduções de e para a FOL de conjuntos

16.7. A FOL da teoria de conjuntos. Nessa linguagem de primeira ordem temos apenas um predicado não-constante: o $\in$, de aridade 2, cuja interpretação canônica é "__ pertence ao __". Nosso universo aqui consiste (apenas) em conjuntos, ou seja assumimos o princípio da puridade (16.3).

▸ **EXERCÍCIO x16.1.**
Traduza as frases seguintes para a FOL da teoria de conjuntos.

(1) Existe conjunto sem membros.
(2) O conjunto x não tem membros.
(3) O conjunto y tem membros.
(4) Existe conjunto com membros.
(5) O x é um singleton.
(6) Existe conjunto com exatamente um membro.
(7) Existe conjunto com pelo menos dois membros.
(8) Os x e y têm exatamente um membro em comum.
(9) Todos os conjuntos tem o x como membro.
(10) Existe conjunto que pertence nele mesmo.
(11) O y consiste em todos os subconjuntos de x com exatamente 2 elementos.
(12) Existe conjunto com exatamente dois membros.
(13) Para todos conjuntos a e b sua intersecção é conjunto.
(14) A união de a e b é um conjunto.
(15) O x não pertence em nenhum conjunto.
(16) Existem conjuntos tais que cada um pertence no outro.
(17) Existe conjunto que não é igual com ele mesmo.

(x16.1 H 0)

16.8. Apenas escrever algo não o torna verdade. O fato que podemos expressar uma afirmação numa linguagem não quer dizer que essa afirmação é válida. Isso não é nada profundo: em português também podemos escrever a frase "a lua não é feita de queijo", mas isso não quis dizer que realmente não é—todos sabemos que é, certo? Infelizmente existe um hábito de confundir as duas noções e usar como "prova de veracidade de algo" o fato que apenas esse algo foi escrito, ou dito.[103] A afirmação da fórmula que tu achou para a última frase do Exercício x16.1 por exemplo é falsa em nosso mundo de conjuntos e ainda mais: é falsa em cada mundo possível, com qualquer interpretação do símbolo $\in$!

16.9. Um padrão útil. Muitas vezes queremos dizer que existe um certo conjunto *determinado por uma propriedade característica*, ou seja, um conjunto s que consiste em exatamente todos os objetos que satisfazem um certo critério.

Como podemos dizer isso na FOL da teoria de conjuntos? Fácil! Assim:

$$\exists s \forall x \big(x \in s \leftrightarrow \underbrace{_____}_{\text{critério}} \big).$$

Na maioria das vezes queremos afirmar a existência dum certo conjunto dados conjuntos $a, b, c, \ldots$. Nesse caso usamos apenas o

$$\forall a \forall b \forall c \cdots \exists s \forall x \big(x \in s \leftrightarrow _____ \big).$$

Esse padrão vai aparecer em muitos dos axiomas abaixo.

16.10. Abreviações e açúcar sintáctico. Assim que conseguirmos descrever um conceito interessante com uma fórmula, faz sentido introduzir uma notação, um novo predicado. Por exemplo, nas (2) e (5) de Exercício x16.1, tu achou fórmulas que afirmam que x é vazio, e que x é um singleton. Faz sentido definir como abreviações então os predicados seguintes:

$$\begin{aligned} \mathsf{Empty}(x) &\overset{\text{sug}}{\equiv} \neg \exists w (w \in x) \\ \mathrm{Singleton}(x) &\overset{\text{sug}}{\equiv} \exists w \big(w \in x \wedge \forall u (u \in x \to u = w) \big) \end{aligned}$$

e os símbolos:

$$\begin{aligned} a \subseteq b &\overset{\text{sug}}{\equiv} \forall x (x \in a \to x \in b) \\ a \subsetneq b &\overset{\text{sug}}{\equiv} a \subseteq b \wedge a \neq b. \end{aligned}$$

Lembre-se também nossa práctica onde usamos

$$\begin{aligned} x \neq y &\overset{\text{sug}}{\equiv} \neg\, x = y, \\ x \notin y &\overset{\text{sug}}{\equiv} \neg\, x \in y, \end{aligned}$$

etc.

[103] Veja por exemplo argumentações de várias igrejas de várias religiões.

§312. Classes vs. Conjuntos (I)

16.11. O que é uma classe?. Sem dúvida, a notação $\{\, x \mid ____ \,\}$ que temos usado até agora é natural e útil. Ela denota a colecção de todos os objetos x que satisfazem a condição (ou "passam o filtro") que escrevemos no $____$. Dada uma condição definitiva P então consideramos a colecção

$$\{\, x \mid P(x) \,\}$$

de todos os objetos que a satisfazem. Provavelmente você já percebeu que eu evitei usar a palavra *conjunto*, pois reservamos essa palavra para apenas os conjuntos-objetos do nosso universo.

D16.12. Definição (Classe). Dada uma condição definitiva $P(-)$ definimos a *classe*

$$\boldsymbol{\{}\, x \mid P(x) \,\boldsymbol{\}}$$

como um sinónimo da própria condição P! Chamamos a classe P *própria* sse não existe *conjunto* S que satisfaz a propriedade:

$$x \in S \iff P(x).$$

- **EXEMPLO 16.13.**
Dados conjuntos a e b, das classes

$$\underbrace{\boldsymbol{\{}\, x \mid x = a \,\boldsymbol{\}}}_{\{a\}} \qquad \underbrace{\boldsymbol{\{}\, x \mid x \in a \wedge x \in b \,\boldsymbol{\}}}_{a \cap b} \qquad \underbrace{\boldsymbol{\{}\, x \mid x \neq x \,\boldsymbol{\}}}_{\emptyset} \qquad \boldsymbol{\{}\, x \mid x = x \,\boldsymbol{\}}$$

apenas a última é própria. As outras são conjuntos mesmo!

! 16.14. Aviso (abuso notacional). É muito comum abusar o símbolo $\in$, escrevendo

$$x \in C$$

mesmo quando C é uma classe própria! Nesse caso consideramos o $x \in C$ apenas como uma abreviação do $C(x)$. Em outras palavras, esse $\in$ não é um símbolo de relação da nossa FOL de teoria de conjuntos, mas sim uma abreviação em nossa *metalinguagem*, no mesmo jeito que $\iff$ também não é, mas o $\leftrightarrow$ é. Quando precisamos enfatizar essa diferença vamos usar um símbolo diferente:

D16.15. Notação. Usamos o símbolo $\Coloneqq$ na metalinguagem como "pertence" quando possivelmente o lado direito é uma classe própria.[104] Com essa notação:

$$x \Coloneqq P \overset{\text{def}}{\iff} \begin{cases} P(x) & \text{se } P \text{ é uma classe própria} \\ x \in P & \text{se } P \text{ é um conjunto.} \end{cases}$$

[104] Seguimos aqui o exemplo dos símbolos de equivalência na metalinguagem ($\iff$) e na linguagem-objeto de lógica ($\leftrightarrow$).

§313. Os primeiros axiomas de Zermelo

α16.16. Axioma (Extensionalidade). *Todo conjunto é determinado por seus membros.*

(ZF1) $$\forall a \forall b (\forall x (x \in a \leftrightarrow x \in b) \to a = b)$$

Qual o efeito disso em nosso mundo? Ainda nem podemos garantir a existência de nada, mas pelo menos sabemos dizer se duas coisas são iguais ou não. Vamos logo garantir a existência dum conjunto familiar:

α16.17. Axioma (Emptyset). *Existe conjunto sem membros.*

(ZF2) $$\exists s \forall x (x \notin s)$$

E já nosso mundo mudou completamente: ganhamos nossa primeira peça, uma coisa para brincar: *um conjunto sem membros!* E já estamos em posição de demonstrar nosso primeiro teorema, seguido pela nossa primeira definição:

Θ16.18. Teorema (Unicidade do conjunto vazio). *O conjunto sem membros garantido pelo axioma (ZF2) é único.*

Demonstração. Suponha que e, o são conjuntos ambos satisfazendo a propriedade:

$$\forall x (x \notin e) \qquad \forall x (x \notin o).$$

Então a equivaléncia

$$x \in e \iff x \in o$$

é válida para todo x, pois ambos lados são falsos. Logo, pelo axioma (ZF1), $e = o$. ∎

D16.19. Definição (Conjunto vazio). Denotamos por $\emptyset$ o *conjunto vazio* com a propriedade característica

$$\forall x (x \notin \emptyset).$$

. . . e agora parece que não podemos fazer muita coisa mais. Precisamos novos axiomas:

α16.20. Axioma (Pairset). *Dado um par de conjuntos, existe conjunto que consiste em exatamente os conjuntos do par.*

(ZF3) $$\forall a \forall b \exists s \forall x \big(x \in s \leftrightarrow (x = a \vee x = b)\big)$$

D16.21. Definição (Doubleton). Dados a e b quaisquer, o conjunto que consiste nos a e b é chamado o *doubleton* de a e b, e denotado por $\{a, b\}$. Definimos assim o operador $\{-, -\}$.

16.22. Efeitos. Como isso muda nosso mundo? Quais novas peças ganhamos em nosso xadrez? Para ganhar a existência de algo usando o Pairset precisamos dar a ele dois objetos, pois começa com dois quantificadores universais ($\forall$) antes de chegar no seu primeiro existencial ($\exists$): "$\forall a \forall b \exists \ldots$". Quais objetos vamos escolher para dá-lo? Nosso mundo está tão pobre que é fácil responder nessa pergunta: *vamos usar como a e como b a única peça que temos: o $\emptyset$.* Ganhamos então que:

$$\exists s \forall x \big(x \in s \leftrightarrow (x = \emptyset \vee x = \emptyset) \big)$$

ou seja, $\exists s \forall x \big(x \in s \leftrightarrow x = \emptyset \big)$, ou seja, existe o conjunto

$$\{\, x \mid x = \emptyset \,\}$$

que acostumamos a denotá-lo por $\{\emptyset\}$. Uma nova peça![105] E teoremas?

Θ16.23. Teorema (Singleton). *Dado conjunto a, existe um único conjunto cujo membro único é o a. Formalmente,*

$$\forall a \exists s \forall x \big(x \in s \leftrightarrow x = a \big).$$

Demonstração. Bote $a := a$ e $b := a$ no Pairset (ZF3):

$$\exists s \forall x \big(x \in s \leftrightarrow x = a \big).$$

O conjunto cuja existência está sendo afirmada tem como membro único o a, e graças ao (ZF1), ele é o único conjunto com essa propriedade. ∎

D16.24. Definição. Dado qualquer conjunto a, o conjunto cujo único membro é o a é chamado o *singleton* de a, e denotado por $\{a\}$. Definimos assim o operador $\{-\}$.

▸ **EXERCÍCIO x16.2.**
Mostre como construir uma infinidade de singletons e uma infinidade de doubletons usando apenas os axiomas (ZF1), (ZF2), e (ZF3). (x16.2 H 1 2)

▸ **EXERCÍCIO x16.3.**
Considere a tentativa seguinte de resolver o Exercício x16.2.

«Para conseguir uma infinidade de doubletons $\mathcal{D}$ botamos:

$$\begin{aligned} D_0 &\stackrel{\text{def}}{=} \{\emptyset, \{\emptyset\}\} \\ D_{n+1} &\stackrel{\text{def}}{=} \{\, \{s\} \mid s \in D_n \,\} \end{aligned}$$

assim construimos o

$$\begin{aligned} \mathcal{D} &= \{D_0,\ D_1,\ D_2,\ \ldots\} \\ &= \{\{\emptyset, \{\emptyset\}\},\ \{\{\emptyset\}, \{\{\emptyset\}\}\},\ \{\{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}\},\ \ldots\} \end{aligned}$$

que possui uma infinidade de doubletons como membros.»

Ache todos os problemas com essa resolução. (x16.3 H 0)

[105] Agora temos duas opções para cada usar nos $\forall$ do Pairset: $\emptyset$, $\{\emptyset\}$.

Agora mesmo que nosso mundo mudou drasticamente—sim, ganhamos uma infinidade de objetos—ele ainda tá bem limitado.

▸ **EXERCÍCIO x16.4.**
Será que podemos garantir a existência de conjuntos com qualquer cardinalidade finita que desejamos? (x16.4 H 1 2)

O próximo axioma não vai nos permitir—por enquanto—definir novos conjuntos. Mas é a versão "bug-free" do princípio da comprehensão geral. Com isso, o paradoxo de Russell se torna teorema!

α16.25. Axioma (Separation (schema)). Para cada propriedade $\varphi(-)$, o seguinte: *para todo conjunto, a colecção de todos os seus membros que têm a propriedade φ é um conjunto.*

(ZF4) $$\forall w \exists s \forall x \big(x \in s \leftrightarrow (x \in w \wedge \varphi(x)) \big)$$

▸ **EXERCÍCIO x16.5.**
Quantos axiomas temos listado até este momento? (x16.5 H 1 2)

16.26. Axiomas vs. esquemas axiomáticos. Usamos o termo *esquema axiomático*, pois para cada fórmula $\varphi(-)$, ganhamos um novo axioma pelo (ZF4). Para enfatizar isso podemos até citá-lo como $(\text{ZF4})_\varphi$. Antes de usá-lo então precisamos primeiramente escolher nossa fórmula φ, assim passando do *esquema* (ZF4) para o *axioma* $(\text{ZF4})_\varphi$. Agora como o axioma começa com $\forall w \exists \ldots$, precisamos escolher em qual conjunto w nós vamos aplicá-lo, para ganhar finalmente um novo conjunto.

D16.27. Definição. Denotamos por

$$\{\, x \in W \mid \varphi(x) \,\}$$

o conjunto único (pelo (ZF1)) garantido pelo (ZF4) quando o aplicamos com uma fórmula $\varphi(x)$ para um conjunto W.

▸ **EXERCÍCIO x16.6.**
Mostre que os conjuntos garantidos pelos (ZF1)–(ZF3) são os mesmos com os conjuntos garantidos pelos (ZF1)–(ZF4). (x16.6 H 1 2)

16.28. Como usar o Separation. Queremos mostrar que uma certa classe C de objetos realmente é um conjunto. Para conseguir isso com o (ZF4), precisamos construir (pelos axiomas!) um *conjunto* W que contem todos os objetos da nossa classe C. Em geral o W vai ter mais elementos, um certo "lixo", que precisamos nos livrar. E é exatamente com o (ZF4) que jogamos fora esse lixo, usando uma apropriada fórmula φ como "tesoura" para cortar o W e ficar só com o C, garantido agora de ser conjunto. Vamos ver uns exemplos desse uso, enriquecendo nosso mundo com uns operadores conhecidos.

• **EXEMPLO 16.29.**
Defina o operador $- \cap -$.
RESOLUÇÃO. Dados conjuntos a e b, precisamos achar um conjunto W que contenha todos os membros da intersecção desejada. Assim vamos conseguir definir o $a \cap b$ usando o (ZF4) com filtro a fórmula

$$\varphi(x) := x \in a \wedge x \in b$$

Observe que todos os elementos da $a \cap b$ são elementos tanto de a, quanto de b. Temos então duas opções. Vamos escolher a primeira e construir o

$$\{\, x \in a \mid x \in a \wedge x \in b \,\}$$

Observamos que com essa escolha nem precisamos a parte "$x \in a$" em nosso filtro. Chegamos assim em duas soluções para nosso problema:

$$\{\, x \in a \mid x \in b \,\} \qquad\qquad \{\, x \in b \mid x \in a \,\}$$

D16.30. Definição (Intersecção binária). Sejam conjuntos a, b. Usando o (ZF4) definimos

$$a \cap b \stackrel{\text{def}}{=} \{\, x \in a \mid x \in b \,\}.$$

▸ **EXERCÍCIO x16.7.**
Defina o operador $- \setminus -$. (x16.7 H 1)

▸ **EXERCÍCIO x16.8.**
Tente definir os operadores $- \cup -$ e $- \triangle -$. (x16.8 H 1 2)

16.31. Blammenos strikes back. Estudamos o paradoxo de Russell, e a resolução do problema por Zermelo: *o princípio de comprehensão geral não é válido; usando o separation axiom evitamos cair no paradoxo.* Mas o aluno Blammenos pensou:

Blammenos: Ok, eu vou trabalhar na teoria de Zermelo então. Seja A um conjunto. Defino o

$$r(A) \stackrel{\text{def}}{=} \{\, x \in A \mid x \notin x \,\}$$

que realmente é um conjunto, graças ao Separation (que o usei com a fórmula $\varphi(x) := x \notin x$). Mas agora faço a mesma pergunta que Russell fez: $r(A) \in r(A)$? Assim consigo cair no mesmo paradoxo:

$$r(A) \in r(A) \iff r(A) \notin r(A).$$

Então Zermelo não resolveu o problema não!

▸ **EXERCÍCIO x16.9.**
Qual o erro do Blammenos essa vez? (x16.9 H 0)

Com o axioma da separação no lugar do princípio da comprehensão geral, o paradoxo de Russell vira-se um teorema muito útil que nos permite definir o operador $\mathbf{r}(-)$ que "escolhe definitivamente um objeto fora da sua entrada". Vamos?

Θ16.32. Teorema. *Dado qualquer conjunto existe algo que não pertence nele. Ainda mais, pelo menos um dos seus subconjuntos não pertence nele.*

▸ Esboço. Tome um conjunto A. Usamos a mesma idéia do paradoxo de Russell, só que essa vez não consideramos *todos* os conjuntos que não pertencem neles mesmo, mas apenas aqueles que pertencem ao A:

$$\mathbf{r}(A) \stackrel{\text{def}}{=} \{\, x \in A \mid x \notin x \,\}.$$

Concluimos que $\mathbf{r}(A) \notin A$ pois o caso $\mathbf{r}(A) \in A$ chega no mesmo absurdo de Russell. □

Destacamos agora o operador que definimos no Teorema Θ16.32:

D16.33. Definição. Seja a conjunto. Definimos o operador $\mathbf{r}(-)$ pela

$$\mathbf{r}(a) \stackrel{\text{def}}{=} \{\, x \in a \mid x \notin x \,\}.$$

Chamamos o $\mathbf{r}(-)$ de *operador Russell*.

16.34. Propriedade. *O operador Russell retorna um objeto (um conjunto) que não pertence à sua entrada:*

$$(\forall a)[\, \mathbf{r}(a) \notin a \,].$$

Demonstrado no Teorema Θ16.32. ▮

16.35. Corolário. *O universo $\mathbb{V}$ não é um conjunto.*

Demonstração. Se $\mathbb{V}$ fosse um conjunto, aplicando o teorema teriamos um conjunto $\mathbf{r}(\mathbb{V})$ com $\mathbf{r}(\mathbb{V}) \notin \mathbb{V}$, absurdo pela definição do $\mathbb{V}$. ▮

α16.36. Axioma (Powerset). *Para cada conjunto a colecção de todos os seus subconjuntos é um conjunto.*

(ZF5) $$\forall a \exists s \forall x (x \in s \leftrightarrow x \subseteq a)$$

D16.37. Definição. Dado conjunto a, escrevemos $\wp a$ para o conjunto garantido pelo Powerset (ZF5), que é único graças ao Extensionality (ZF1). Definimos assim o operador $\wp -$.

▸ **exercício x16.10.**
Seja a conjunto. Mostre que a classe

$$\big\{\, \{x\} \mid x \in a \,\big\}$$

de todos os singletons de elementos de a é conjunto. (x16.10 H 0)

▸ **exercício x16.11.**
Usando os (ZF1)+(ZF2)+(ZF3)+(ZF5), podemos construir conjunto com cardinalidade finita, arbitrariamente grande? (x16.11 H 0)

▸ **EXERCÍCIO x16.12.**
Usando os (ZF1)+(ZF2)+(ZF3)+(ZF5), podemos construir conjunto com cardinalidade finita qualquer? (x16.12 H 1 2)

16.38. Jogos. Como descobrimos no Exercício x16.12 não existe estratégia vencedora num jogo onde nosso oponente joga primeiro escolhendo um número $n \in \mathbb{N}$, e nosso objectivo é construir pelos axiomas um conjunto com cardinalidade n. Se ele escolher como n um dos

$$0, 1, 2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \ldots$$

temos como ganhar, mas caso contrário, não.

Por outro lado, num jogo onde nosso objectivo é construir pelos axiomas um conjunto com cardinalidade *pelo menos* n, como vimos no Exercício x16.11, temos uma estratégia vencedora sim: comece com uma aplicação do Emptyset (ZF2) para ganhar o $\emptyset$ e aplique iterativamente o Powerset (ZF5) construindo assim conjuntos de cardinalidades 0 (do próprio $\emptyset$), 1, 2, 2^2, 2^{2^2}, etc., até chegar num conjunto com cardinalidade maior-ou-igual ao n escolhido por nosso oponente.

▸ **EXERCÍCIO x16.13.**
Quantas iterações precisamos para conseguir conjunto com cardinalidade $n \in \mathbb{N}$? (x16.13 H 0)

▸ **EXERCÍCIO x16.14.**
Usando os (ZF1)+(ZF2)+(ZF4)+(ZF5), podemos construir conjunto com cardinalidade finita qualquer? (x16.14 H 1)

α16.39. Axioma (Unionset). *Para cada conjunto, sua união (a colecção de todos os membros dos seus membros) é um conjunto.*

(ZF6) $$\forall a \exists s \forall x \big(x \in s \leftrightarrow \exists w (x \in w \wedge w \in a) \big)$$

D16.40. Definição. Dado conjunto a, escrevemos $\bigcup a$ para o conjunto garantido pelo Unionset (ZF6), que é único graças ao Extensionality (ZF1). Definimos assim o operador da *união arbitrária* $\bigcup -$.

▸ **EXERCÍCIO x16.15.**
Defina os operadores binários $\cup$ e $\triangle$. (x16.15 H 1 2)

▸ **EXERCÍCIO x16.16.**
Como podemos definir o operador unitário $\cdot^{\mathsf{c}}$ de *complemento*, tal que a^{c} é o conjunto de todos os objetos que não pertencem ao a? (x16.16 H 1)

▸ **EXERCÍCIO x16.17.**
Defina o operador unário $\bigcap$, aplicável em qualquer conjunto não vazio. Precisamos o Unionset (ZF6)? (x16.17 H 0)

Θ16.41. Teorema. *Dados $a_1, a_2, \ldots, a_n$ (onde $n \in \mathbb{N}$) existe conjunto único cujos membros são exatamente os a_1, a_2, …, a_n.*

DEMONSTRARÁS NO PROBLEMA Π16.6. ∎

16.42. Observação. Pelo Teorema Θ16.41 ganhamos para qualquer $n \in \mathbb{N}$ o operador n-ário

$$\{-, -, \ldots, -\}.$$

§314. Árvores de construção

Um jeito bem econômico e claro para descrever uma construção e usando árvores. Os exemplos seguintes servem para explicar essa idéia.

- **EXEMPLO 16.43.**
Queremos demonstrar que $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$ é um conjunto, ou seja, construí-lo. Escrevemos: Pelo Emptyset (ZF2), $\emptyset$ é um conjunto. Pelo Pairset (ZF3) aplicado com $a, b := \emptyset$ temos que $\{\emptyset, \emptyset\}$ também é conjunto. Mas, pelo Extensionality (ZF1), $\{\emptyset, \emptyset\} = \{\emptyset\}$. Agora, novamente pelo Pairset (ZF3) essa vez aplicado com $a := \emptyset$ e $b := \{\emptyset\}$ temos que $\{\emptyset, \{\emptyset\}\}$ é um conjunto. Aplicando uma última vez o Pairset (ZF3) com $a := \emptyset$ e $b := \{\emptyset, \{\emptyset\}\}$, conseguimos construir o conjunto $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$. Podemos representar essa construção em forma de árvore:

$$\dfrac{\dfrac{\dfrac{}{\emptyset}\,(\text{ZF2}) \qquad \dfrac{\dfrac{}{\emptyset}\,(\text{ZF2}) \qquad \dfrac{}{\emptyset}\,(\text{ZF2})}{\{\emptyset\}}\,(\text{ZF3})}{\{\emptyset, \{\emptyset\}\}}\,(\text{ZF3})}{\{\emptyset, \{\emptyset, \{\emptyset\}\}\}}\,(\text{ZF3})$$

onde pulamos ou deixamos alguns passos implícitos, como o uso de Extensionality (ZF1) nesse caso. (As vezes indicamos com uma dupla linha tais omissões mas seu uso pode ter outros significados também.) Usamos agora essa construção para construir um conjunto de cardinalidade 3:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\emptyset}\,\textsc{Emptyset} \qquad \dfrac{\dfrac{}{\emptyset}\,\textsc{Emptyset} \qquad \dfrac{}{\emptyset}\,\textsc{Emptyset}}{\{\emptyset\}}\,\textsc{Emptyset}}{\{\emptyset, \{\emptyset\}\}}\,\textsc{Pairset}}{\{\emptyset, \{\emptyset, \{\emptyset\}\}\}}\,\textsc{Pairset}}{\{\emptyset, \{\emptyset\}, \{\{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}\}}\,\textsc{Powerset}}{\{\{\emptyset\}, \{\{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}\}}\,\textsc{Separation}, \varphi(x) := \exists w(w \in x)$$

Observe que para usar o Separation (ZF4) precisamos especificar qual é a fórmula–filtro.

- **EXEMPLO 16.44.**
Sejam a, b conjuntos. Mostre que $\{b, \{\emptyset, \{a\}\}\}$ é conjunto.
RESOLUÇÃO.

$$\dfrac{\dfrac{\dfrac{}{\emptyset}\,\textsc{Empty} \qquad \dfrac{a}{\{a\}}\,\textsc{Singleton}}{\{\emptyset, \{a\}\}}\,\textsc{Pair}}{\{b, \{\emptyset, \{a\}\}\}}\,\textsc{Pair}$$

Onde deixamos as "folhas" da árvore a, b "sem fechar", pois correspondem realmente em nossas hipotéses: os conjuntos a, b são dados! Observe também que "Singleton" se-refere no Teorema Θ16.23.

▸ **EXERCÍCIO x16.18.**
Sejam a, b, c, d conjuntos. Mostre pelos axiomas que os seguintes também são:

$$A = \{a, b, c, d\}$$
$$B = \{a, b, \{c, d\}\}$$
$$C = \{\, x \mid x \subseteq a \cup b \cup c \cup d \;\&\; x \text{ tem exatamente 2 membros} \,\}$$

Use a método de árvores para umas construções e outras faça escrevendo em texto mesmo. É bom practicar os dois jeitos. (x16.18 H 0)

§315. Fundações de matemática

16.45. Uma linguagem "low-level" para matemática. Fazendo uma analogia entre matemática e programação, dizemos que a teoria de conjuntos pode servir como uma certa low-level linguagem em qual podemos "compilar" (traduzir, representar, ...) todos os high-level conceitos que nos interessam em matemática! As "definições" (assim entre aspas) que temos usado até agora para os vários tipos e conceitos que encontramos não foram formais. Nossa tarefa então aqui é tirar essas aspas. Dar uma definição formal dum conceito significa defini-lo dentro da teoria de conjuntos. No final das contas, tudo vai ser representado dentro da FOL da teoria de conjuntos, pegando como noções primitívas *apenas* os "Set(−)" de "ser conjunto" e o "$- \in -$" de "pertencer". Já temos uma primeira biblioteca construida até agora, um certo *açúcar sintáctico*. E cada vez que conseguimos compilar algo dentro da teoria de conjuntos, ganhamos não apenas o próprio algo para seus usos e suas aplicações, mas também algo mais para usar para nossas próximas compilações.

16.46. Nosso inventório até agora. Vamos resumir todos os operadores e predicados que temos já definido dentro da teoria de conjuntos, usando apenas os axiomas que encontramos até agora. Temos:

$$\emptyset\,;$$
$$\{-\}\,;\quad \{-,-\}\,;\quad \{-,\dots,-\}\,;\quad \{\, x \in - \mid \varphi(x) \,\}\,;$$
$$-\cap -\,;\quad -\cup -\,;\quad -\setminus -\,;\quad -\triangle -\,;\quad \bigcup -\,;\quad \wp -$$

e com o proviso de a conjunto com $a \neq \emptyset$ também o

$$\bigcap a\,.$$

Observe-se então que de todos esses operadores, o $\bigcap -$ é o único operador *parcial*. Mas isso não é nada novo como conceito: no final das contas, estamos usando operadores parciais o tempo todo trabalhando com números reais: o $-/-$ por exemplo não é definido quando seu segundo argumento é o 0, e a mesma coisa sobre a operação (unária) de inverso: o 0^{-1} também não é definido.

16.47. De especificação para implementação. Quando queremos representar algum *tipo* de coisa dentro do nosso mundo de conjuntos, precisamos esclarecer qual é a *especificação* desse tipo. Quais propriedades desejamos dos objetos desse tipo? O que precisamos para construir um objeto desse tipo? Quando identificamos dois objetos desse tipo e os consideramos iguais? Como podemos usar os objetos desse tipo? Qual é a "interface" deles? Talvez ajuda pensar que nossa tarefa é semelhante à de um "vendedor de implementações matemáticas". Nossos clientes são os próprios matemáticos que desejam usar certos tipos de objetos matemáticos, e nos seus pedidos eles estão esclarecendo quais são as propriedades que eles precisam. Nosso trabalho então será: *implementar* essa especificação, ou seja, *representar fielmente* esses tipos e conceitos como conjuntos. Para conseguir isto: (1) *definimos* os conceitos e objetos como conjuntos; (2) *demonstramos* que nossa implementação realmente atende as especificações. Muitas vezes vamos até oferecer uma *garantia de unicidade* para mostrar para nosso cliente-matemático que ele não precisa procurar outras implementações alternativas da nossa concorrência, pois *essencialmente* nem tem!

Nosso próximo trabalho será representar as tuplas, e por isso vamos analisar em muito detalhe essa especificação. Depois relaxamos um pouco deixando uns detalhes tediosos como "óbvios".

§316. Construindo as tuplas

16.48. Especificação. Vamos começar com o trabalho de implementar tuplas de tamanho 2, ou seja *pares ordenados*. Precisamos então definir *um* operador $\langle -, - \rangle$ que atende as especificações. Primeiramente:

(TUP1) $$\langle x, y\rangle = \langle x', y'\rangle \implies x = x' \ \&\ y = y'.$$

Mas precisamos mais que isso. Dados conjuntos A e B queremos que

(TUP2) a *classe* $A \times B = \{\, z \mid (\exists x \in A)(\exists y \in B)[\, z = \langle x, y\rangle \,]\,\}$ é um *conjunto*.

Lembrando a idéia de tupla como black box, a interface que desejamos consiste em duas operações, as *projecções outl* e *outr* tais que

$$\mathit{outl}\,\langle x, y\rangle = x \qquad \text{e} \qquad \mathit{outr}\,\langle x, y\rangle = y.$$

Queremos definir também um predicado $\mathrm{Pair}(-)$ para afirmar que um certo objeto representa um par ordenado. Isso é facil:

$$\mathrm{Pair}(z) \overset{\text{def}}{\iff} \exists x \exists y (z = \langle x, y\rangle)$$

Finalmente, precisamos e confirmamos:

$$\mathrm{Pair}(z) \iff z = \langle \mathit{outl}(z), \mathit{outr}(z)\rangle\,.$$

Anotamos também que assim que definir *funções* dentro da teoria de conjuntos, vamos mostrar a existência das funções

$$\begin{aligned} \mathit{outl} &: A \times B \to A & \qquad \mathit{outr} &: A \times B \to B \\ \mathit{outl}\,\langle x, y\rangle &= x & \qquad \mathit{outr}\,\langle x, y\rangle &= y \end{aligned}$$

para todos os conjuntos A e B.

▸ **EXERCÍCIO x16.19.**
No (TUP1) botamos '$\Longrightarrow$' em vez de '$\Longleftrightarrow$'. Por quê? O que acontece com a '$\Longleftarrow$'? (x16.19 H 1)

▸ **EXERCÍCIO x16.20.**
Demonstre que a operação

$$\langle x, y\rangle \stackrel{\text{def}}{=} \{x, y\}$$

satisfaz uma das (TUP1) & (TUP2) mas não a outra, então essa *não* é uma implementação de par ordenado (x16.20 H 0)

Nossa primeira tentativa não deu certo. Mesmo assim é realmente possível implementar pares ordenados como conjuntos! Como?

!! SPOILER ALERT !!

D16.49. Definição (par de Kuratowski). Sejam x, y objetos. Definimos

$$\langle x, y\rangle \stackrel{\text{def}}{=} \{\{x\}, \{x, y\}\}.$$

▸ **EXERCÍCIO x16.21.**
Mostre pelos axiomas que o operador $\langle -, -\rangle$ de Kuratowski é bem-definido, ou seja: dados objetos x, y, o $\langle x, y\rangle$ é conjunto. (x16.21 H 0)

16.50. Propriedade. *O operador $\langle -, -\rangle$ de Kuratowski satisfaz a (TUP1).*

▸ Esboço. Suponha $\langle x, y\rangle = \langle x', y'\rangle$. Logo

$$\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}.$$

Precisamos deduzir que $x = x'$ e $y = y'$ mas ainda não é claro. O que temos é apenas igualdade desses dois conjuntos, que não garanta o que queremos imediatamente. Não podemos concluir nem que

$$\{x\} = \{x'\} \qquad \& \qquad \{x, y\} = \{x', y'\},$$

pois pela definição de igualdade de conjuntos (ZF1) sabemos apenas que cada membro do conjunto no lado esquerdo é algum membro do conjunto no lado direito e vice-versa. Então, talvez

$$\{x\} = \{x', y'\} \qquad \& \qquad \{x, y\} = \{x'\}.$$

Precisamos então separar em casos: $x = y$ ou não. Em cada caso argumentamos usando o (ZF1) e a cardinalidade dos conjuntos para progressar até chegar nos desejados $x = x'$ e $y = y'$. □

16.51. Propriedade. *O operador $\langle -,-\rangle$ de Kuratowski satisfaz a (TUP2).*

Demonstração. Sejam A, B conjuntos. Precisamos mosrar que a classe

$$A \times B = \{\, z \mid (\exists x \in A)(\exists y \in B)[\, z = \langle x, y\rangle \,]\,\}$$

é um conjunto. Como já temos escrita a classe nessa forma, basta achar um conjunto W que contem todos os pares que queremos, e aplicar esse mesmo filtro para ficar apenas com eles mesmo. Como parece o aleatório $\langle a, b\rangle \in A \times B$?

$$a \in A \;\&\; b \in B \implies \langle a, b\rangle = \{\{a\}, \{a, b\}\} \in \,?$$

Vamos ver:

Suponha $a \in A$ e $b \in B$.
Logo $a, b \in A \cup B$. $(A, B \subseteq A \cup B)$
Logo $\{a\}, \{a, b\} \subseteq A \cup B$.
Logo $\{a\}, \{a, b\} \in \wp(A \cup B)$.
Logo $\{\{a\}, \{a, b\}\} \subseteq \wp(A \cup B)$.
Logo $\{\{a\}, \{a, b\}\} \in \wp\wp(A \cup B)$.
Logo $\langle a, b\rangle \in \wp\wp(A \cup B)$.

Tome então $W := \wp\wp(A \cup B)$ e defina

$$A \times B \stackrel{\text{def}}{=} \{\, z \in \wp\wp(A \cup B) \mid (\exists x \in A)(\exists y \in B)[\, z = \langle x, y\rangle \,]\,\}$$

que é conjunto graças ao Separation (ZF4). ∎

16.52. Sendo agnósticos. Acabamos de encontrar *um* operador de par ordenado: do Kuratowski. Ele não é o único possível, mas para continuar com nossa teoria, precisamos apenas mostrar que existe um. Vamos usar o símbolo $\langle -,-\rangle$ sem esclarecer se realmente é a implementação de Kuratowski que usamos, ou alguma outra implementação. Tomando cuidado, sobre esse operador nos permitimos usar *apenas as propriedades da sua especificação e nada mais*: as (TUP1) & (TUP2) da 16.48. Falamos então que estamos sendo $\langle\,,\rangle$-*agnósticos*. Por exemplo, não podemos afirmar que $\{x\} \in \langle x, y\rangle$. Sim, isso é válido com a implementação de Kuratowski, mas é uma *coincidência* e não uma *conseqüência* da especificação de par ordenado. Talvez outra implementação não tem essa propriedade, como tu vai descobrir agora demonstrando que o $\langle -,-\rangle$ de Wiener também é uma implementação de par ordenado.

▸ **EXERCÍCIO x16.22 (par de Wiener).**
Mostre pelos axiomas que a operação $\langle -,-\rangle$ definida pela

$$\langle x, y\rangle \stackrel{\text{def}}{=} \big\{\{\emptyset, \{x\}\}, \{\{y\}\}\big\}$$

é uma implementação bem-definida de par ordenado (ou seja, dados x, y o $\langle x, y\rangle$ é um conjunto sim) que satisfaz as (TUP1) & (TUP2).[106] (x16.22 H 1)

[106] Wiener definiu essa operação uns anos *antes* da definição de Kuratowski.

▸ **EXERCÍCIO x16.23 (par de Hausdorff).**
Considere 0 e 1 dois objetos distintos (algo que nossos axiomas garantam). Para ser especifico, tome $0 := \emptyset$ e $1 := \{\emptyset\}$. Demonstre que a operação

$$\langle x, y\rangle \stackrel{\text{def}}{=} \big\{\{0, x\}, \{1, y\}\big\}$$

também é uma implementação de par ordenado. (x16.23 H 1 2)

▸ **EXERCÍCIO x16.24 (Bad pair).**
Demonstre que não podemos usar a operação

$$\langle x, y\rangle \stackrel{\text{def}}{=} \big\{x, \{y\}\big\}$$

como uma implementação de par ordenado. (x16.24 H 1)

▸ **EXERCÍCIO x16.25 (Spooky pair).**
Considere a operação

$$\langle x, y\rangle \stackrel{\text{def}}{=} \big\{x, \{x, y\}\big\}$$

como uma implementação de par ordenado. Demonstre que ela satisfaz a (TUP2). Sobre a (TUP1), a situação é mais complicada. Nesse momento não podemos demonstrar que ela é satisfeita, mas nem construir um contraexemplo! Mesmo assim, vale a pena pensar: que conjunto (spooky!) serviria? Deixo isso para o Problema Π16.14. (x16.25 H 1)

§317. Construindo a união disjunta

16.53. Especificação. Queremos definir a operação binária da *união disjunta*.

TODO Especificação: mention coproduct

D16.54. Definição (União disjunta). Fixamos dois objetos distintos como os $\mathrm{L} := \emptyset$ e $\mathrm{R} := \{\emptyset\}$ e definimos:

$$A \uplus B \stackrel{\text{def}}{=} (\{\mathrm{L}\} \times A) \cup (\{\mathrm{R}\} \times B).$$

▸ **EXERCÍCIO x16.26.**
Uma escolha de "tags" para os membros dos conjuntos A e B seria os próprios conjuntos A e B em vez dos $\emptyset$ e $\{\emptyset\}$ que usamos. Qual é o problema com essa idéia? (x16.26 H 0)

▸ **EXERCÍCIO x16.27.**
Generalize a construção de união disjunta binária para o operador "grande" de união disjunta indexada por algum conjunto de índices I. (x16.27 H 0)

§318. Construindo as relações

16.55. Especificação. O que precisamos de algum objeto R que merece o nome de *implementação de relação de A para B*? Bem, primeiramente, dados $a \in A$ e $b \in B$ queremos ter como "perguntar" esse objeto R se o a está relacionado com o b. Dados quaisquer conjuntos c e d queremos também que a classe de todas as relações de c para d seja um conjunto. Nossa definição tem que ser feita em tal jeito que facilita as demais definições de operações em relações, por exemplo a composição, os vários fechos que encontramos, etc.

Praticamente, *nossa especificação é o Capítulo 10!*

D16.56. Definição (Relação). Sejam A, B conjuntos. Qualquer subconjunto $R \subseteq A \times B$ é uma relação de A para B. Em outras palavras:

$$R \text{ relação de } A \text{ para } B \overset{\text{def}}{\iff} R \subseteq A \times B.$$

Introduzimos as notações

$$x \mathrel{R} y \overset{\text{sug}}{\iff} \langle x, y\rangle \in R$$
$$R(x, y) \overset{\text{sug}}{\iff} \langle x, y\rangle \in R.$$

Formalmente definimos o predicado

$$\text{Relation}(r, a, b) \overset{\text{sug}}{\iff} r \subseteq (a \times b).$$

16.57. Observação. No final das contas, já tivemos definido esse conceito. Seu nome foi *o gráfico da R*. Lembra? Se não, veja o Definição D10.13. Em outras palavras, dentro da teoria de conjuntos, com nossa Definição D16.56, *identificamos as relações com seus gráficos:* $R = \operatorname{graph} R$.

! **16.58. Aviso.** Enfatizamos mais uma vez que isso não quis dizer que uma relação *é* o seu gráfico (que é um conjunto)! Mas que isso é apenas um jeito de *representar fielmente* o conceito de *relação* dentro da teoria de conjuntos, ou seja: "*como se fosse* conjunto".

? **Q16.59. Questão.** Agora precisamos definir as demais noções e termos que encontramos no Capítulo 10? Por exemplo: precisamos definir os termos "transitiva", "reflexiva", etc.?

!! SPOILER ALERT !!

Resposta. Não! Voltando no Capítulo 10 podes verificar que todas as outras definições dependem apenas na noção de relação mesmo (que acabamos de definir formalmente na Definição D16.56).

• **EXEMPLO 16.60.**
Seja A um conjunto. O conjunto

$$\{\, \langle x, x\rangle \in A^2 \mid x \in A \,\}$$

é uma relação, pois realmente é um subconjunto de $A \times A$. Qual relação é essa? Ela merece seu próprio nome e sua própria notação.

D16.61. Definição. Dado conjunto A, a relação de *igualdade no* A é a relação

$$=_A \stackrel{\text{def}}{=} \{\, \langle x, x\rangle \in A^2 \mid x \in A \,\}.$$

Logo temos

$$x =_A y \iff x = y \;\&\; x, y \in A.$$

16.62. Proposição. *Dados conjuntos a, b, a classe*

$$\operatorname{Rel}(a, b) \stackrel{\text{def}}{=} \{\, R \mid R \text{ é uma relação de } a \text{ para } b \,\}$$

é um conjunto.

Demonstração. Basta achar um conjunto onde todas as relações de a para b pertencem. Pela definição de relação, todas pertencem ao $\wp(a \times b)$. De fato, ainda mais é verdade:

$$\operatorname{Rel}(a, b) = \wp(a \times b)$$

e logo é um conjunto graças aos operadores (totais) $\wp$ e $\times$. ∎

• **EXEMPLO 16.63.**
Seja $R \subseteq A \times A$. Então temos

$$\begin{aligned} R \text{ reflexive} &\iff =_A \subseteq R \\ R \text{ irreflexive} &\iff =_A \cap R = \emptyset \end{aligned}$$

etc.

‣ **EXERCÍCIO x16.28.**
Mostre que podemos definir o operador de composição de relações $- \diamond -$ em tal modo quando é aplicado em conjuntos a, b que são relações (compatíveis), o conjunto $a \diamond b$ também é uma relação, e a correta: a composição de a com b. (Lembre-se a Definição D10.31.) (x16.28 H 0)

‣ **EXERCÍCIO x16.29.**
Defina formalmente e diretamente como conjuntos os fechos que encontramos no Capítulo 10: reflexivo (D10.56), simétrico (D10.57), transitivo (D10.59). Tente dar a definição mais curta, elegante, e flexível possível! (x16.29 H 0)

§319. Construindo as funções

16.64. Especificação. Como nas relações, aqui também nossa especificação deve ser clara: *traduzir todo o Capítulo 9 na teoria de conjuntos!*

D16.65. Definição (Função). Sejam A, B conjuntos. Uma relação f de A para B é chamada *função de A para B* sse

$$(\forall a \in A)(\exists! b \in B)[\, \langle a, b\rangle \in f \,].$$

Equivalentemente (e para ficar mais perto das Condições 9.11 do Capítulo 9) podemos separar essa condição em duas:

$$\text{(TOT)} \qquad (\forall a \in A)(\exists b \in B)[\, \langle a, b\rangle \in f \,]$$
$$\text{(DET)} \qquad (\forall a \in A)(\forall b, b' \in B)[\, \langle a, b\rangle, \langle a, b'\rangle \in f \implies b = b' \,].$$

Escrevemos

$$f(a) = b \overset{\text{def}}{\iff} \langle a, b\rangle \in f$$

e também usamos

$$f(a) \overset{\text{def}}{=} \text{aquele único } b \in B \text{ tal que } \langle a, b\rangle \in f.$$

Lembre-se que escrevemos $f : A \to B$ ou $A \xrightarrow{f} B$ para dizer que f é uma função de A para B, etc. (Veja Definição D9.3.) Formalmente definimos o predicado

$$\text{Function}(f, a, b) \overset{\text{sug}}{\iff} \text{Relation}(f, a, b) \wedge (\forall x \in a)(\exists! y \in b)[\, \langle x, y\rangle \in f \,].$$

16.66. Propriedade. *Dados conjuntos a, b, a classe*

$$(a \to b) \overset{\text{def}}{=} \{\, f \mid f : A \to B \,\}$$

é um conjunto.

Demonstração. Fácil:

$$(a \to b) = \{\, f \in \text{Rel}\,(a, b) \mid f : A \to B \,\}$$

que é conjunto graças ao operador $\text{Rel}\,(-,-)$ (Proposição 16.62) e ao axioma da separação (ZF4). ∎

16.67. Observação. Como as definições de "injetora", "sobrejetora", e "bijetora" do Capítulo 9 dependem apenas da definição de "função" (que acabamos de definir), já temos essas definições na teoria de conjuntos! Simlarmente os operadores $(- \rightarrowtail -)$, $(- \twoheadrightarrow -)$, e $(- \rightarrowtail\!\!\!\!\twoheadrightarrow -)$ são facilmente definidos graças à Propriedade 16.66 e o axioma da separação (ZF4).

- **EXEMPLO 16.68.**
Uma definição alternativa e formal do $=_{\text{c}}$ é a seguinte:

$$a =_{\text{c}} b \overset{\text{def}}{\iff} (a \rightarrowtail b) \neq \emptyset.$$

► **EXERCÍCIO x16.30.**
Defina formalmente as operações e construções de funções que encontramos no Capítulo 9: composição (D9.137); restricção (D9.161); produto (D9.199). (x16.30 H 0)

► **EXERCÍCIO x16.31.**
Descreva curtamente as funções identidades, características, e constantes como conjuntos. Esses conjuntos representam outras coisas (de outros tipos)? (x16.31 H 0)

! **16.69. Cuidado.** Tem um conceito do Capítulo 9 que *não* definimos em termos de "função", e logo precisamos defini-lo formalmente aqui: a *função parcial*.

D16.70. Definição (Função parcial). Uma relação f de A para B é uma *função parcial* sse

$$\text{(DET)} \qquad (\forall a \in A)(\forall b, b' \in B)[\, \langle a, b\rangle, \langle a, b'\rangle \in f \implies b = b' \,].$$

► **EXERCÍCIO x16.32.**
Dados conjuntos a, b, a classe

$$(a \rightharpoonup b) \stackrel{\text{def}}{=} \{\, f \mid f : A \rightharpoonup B \,\}$$

é um conjunto. (x16.32 H 0)

► **EXERCÍCIO x16.33.**
Ache um outro jeito para definir funções parciais como funções. (Talvez tu já pensou nisso no Problema Π9.18.) Verifique que dados conjuntos a, b a classe $(a \rightharpoonup b)$ também é um conjunto. (x16.33 H 1 2)

D16.71. Definição (Compatibilidade). Sejam A, B conjuntos e $\mathscr{F}$ uma família de funções parciais de A para B: $\mathscr{F} \subseteq (A \rightharpoonup B)$. Chamamos a $\mathscr{F}$ *compatível* sse $\bigcup \mathscr{F} \in (A \rightharpoonup B)$. Digamos que $\mathscr{F}$ tem *conflito* no $a \in A$ sse existem $y, y' \in B$ com $y \neq y'$ e $\langle a, y\rangle, \langle a, y'\rangle \in \mathscr{F}$; equivalentemente

$$|\{\, \langle a, y\rangle \mid y \in B \,\}| > 1.$$

D16.72. Definição (Aproximação). Seja $F : A \to B$. Chamamos qualquer $f \subseteq F$ uma aproximação (parcial) da F. Ela é *própria* se $f \subsetneq F$.

► **EXERCÍCIO x16.34.**
Seja $F : A \to B$. Demonstre que a classe

$$\{\, f \mid f \text{ é uma aproximação da } F \,\}$$

é um conjunto. (x16.34 H 0)

▸ **EXERCÍCIO x16.35.**
Seja $F : A \to B$. (i) Demonstre que:

$$F = \bigcup \mathscr{F}$$

onde $\mathscr{F}$ é o conjunto de todas as aproximações da F. (ii) É também verdadeiro que

$$F = \bigcup \mathscr{F}_{\mathrm{f}}$$

onde $\mathscr{F}_{\mathrm{f}}$ é o conjunto de todas as aproximações finitas da F? (x16.35 H 0)

§320. Construindo mais tipos familiares

▸ **EXERCÍCIO x16.36 (famílias indexadas).**
Construa as famílias indexadas na teoria dos conjuntos. (x16.36 H 0)

▸ **EXERCÍCIO x16.37.**
«Como podemos implementar cada seqüência como uma família indexada pelo conjunto de indices $\mathcal{I} := \mathbb{N}$, e como acabamos de construir as famílias indexadas por qualquer conjunto de indices $\mathcal{I}$, logo já temos construido as seqüências também dentro da teoria dos conjuntos.» Concordas? (x16.37 H 1)

? **Q16.73. Questão.** Ainda falta muita coisa: grupos, monóides, anéis, corpos, etc. Como podemos construí-los na teoria dos conjuntos?

!! SPOILER ALERT !!

▸ **EXERCÍCIO x16.38.**
Construa o conceito de conjunto estruturado na teoria dos conjuntos. (x16.38 H 1)

§321. Os cardinais

Tem mais uma coisa muito legal que conseguimos definir sem introduzir nenhum axioma ainda: a *aritmética dos cardinais*. Infelizmente não podemos ainda definir mesmo os cardinais mas podemos brincar suficientemente com umas idéias e entender como funciona sua aritmética ao ponto de aplicá-la para conseguir uns resultados interessantes.

D16.74. Definição (atribuidor de cardinalidade). Um operador unário $|-|$ é chamado *atribuidor (forte) de cardinalidade* sse ele satisfaz:

TODO Escrever

§322. Classes vs. Conjuntos (II)

Pelas nossas definições de relação e de função, observe que nem $- \subseteq -$ é uma relação unária, nem $\wp -$ é uma função unária.

▸ **EXERCÍCIO x16.39.**
Por que não? (x16.39 H 0)

Então certas coisas que *parecem como* relações na verdade são "grandes demais" para ser relações mesmo (segundo nossa definição de relação dentro da teoria dos conjuntos), e similarmente sobre funções. Vamos chamá-las de predicados ou relações-classes, e de operadores ou funções-classes:

D16.75. Definição (relação-classe). Qualquer fórmula com n buracos determina um *predicado* n-ário, que chamamos também de *relação-classe* n-ária.

D16.76. Definição (function-like, função-classe). Uma fórmula $\Phi(x, y)$ é *function-like*, sse:

$$\forall x \exists! y \Phi(x, y) \qquad \text{ou seja,} \qquad \forall x \exists y \big(\Phi(x, y) \wedge \forall y' (\Phi(x, y') \to y = y')\big).$$

Nesse caso, também usamos os termo *função-classe*, *operador*, e a notação comum

$$\Phi(x) = y \qquad \text{como sinónimo de} \qquad \Phi(x, y).$$

Seguindo essa linha denotamos por $\Phi(x)$ o único objeto y tal que $\Phi(x, y)$. Assim o $\Phi(x)$ denota um *objeto*, mas o $\Phi(x, y)$ uma *afirmação*.

Intervalo de problemas

▸ **PROBLEMA Π16.1 (Someset is the new Emptyset).**
Considere o axioma seguinte:
Someset. *Existe algo.*

(ZF2*) $$\exists s (s = s)$$

Mostre que no sistema axiomático (ZF1)+(ZF2*)+(ZF3)+(ZF4)+(ZF5)+(ZF6), existe o $\emptyset$.[107] (Π16.1 H 0)

[107] Dependendo do uso e do contexto, podemos considerar como parte da lógica que o universo não é vazio, ou seja, existe algo. Nesse caso nem precisamos o Someset (ZF2*), pois seria implícito.

▸ **PROBLEMA Π16.2 (Triset is the new Pairset).**
Considere o axioma seguinte:
Triset. *Dados tres objetos distintos existe conjunto com exatamente esses membros.*

$$\text{(ZF3*)} \qquad \forall a \forall b \forall c \Big(\big(a \neq b \wedge b \neq c \wedge c \neq a\big) \to \exists s \forall x \big(x \in s \leftrightarrow x = a \vee x = b \vee x = c\big)\Big)$$

(0) No sistema (ZF1)+(ZF2)+(ZF3)+(ZF4)+(ZF5)+(ZF6) construa conjunto de cardinalidade 3.
(1) Demonstre que no mesmo sistema podemos substituir o axioma Pairset (ZF3) pelo axioma Triset (ZF3*) "sem perder nada". Em outras palavras, demonstre que no sistema (ZF1)+(ZF2)+(ZF3*)+(ZF4)+(ZF5)+(ZF6) *para todos os* a, b *existe o conjunto* $\{a, b\}$.
(2) Podemos demonstrar a mesma coisa no (ZF1)+(ZF2)+(ZF3*)+(ZF4)+(ZF6)?

(Π16.2H1)

▸ **PROBLEMA Π16.3.**
Considere o axioma seguinte:

$$\text{(CONS)} \qquad \forall h \forall t \exists s \forall x \big(x \in s \leftrightarrow x = h \vee x \in t\big).$$

(1) No sistema (ZF1)+(ZF2)+(CONS) demonstre o (ZF3).
(2) Mostre que não tem como demonstrar o (CONS) no sistema (ZF1)+(ZF2)+(ZF3).
(3) No sistema (ZF1)+(ZF2)+(ZF3)+(ZF4)+(ZF5)+(ZF6) demonstre o (CONS). (Π16.3H0)

▸ **PROBLEMA Π16.4.**
Sejam a, b conjuntos. Mostre pelos axiomas (ZF1)–(ZF6) que:
(i) a classe $\big\{\, \{x, \{y\}\} \mid x \in a \wedge y \in b \,\big\}$ é conjunto;
(ii) a classe $\big\{\, \{x, y\} \mid x, y \text{ conjuntos com } x \neq y \,\big\}$ é própria. (Π16.4H1)

▸ **PROBLEMA Π16.5.**
Sejam a, b conjuntos. Mostre pelos axiomas (ZF1)–(ZF6) que as classes

$$C = \big\{\, \{x, \{x, y\}\} \mid x \in a \wedge y \in b \,\big\}$$
$$D = \Big\{\, \{x, y\} \mid \Big(x \in a \vee x \in \bigcup a\Big) \wedge (y \in b \vee y \subseteq b) \,\Big\}$$

são conjuntos, mas a classe

$$Z = \Big\{\, \bigcap \bigcap z \mid z \neq \emptyset \wedge \bigcap z \neq \emptyset \,\Big\}$$

não é. (Π16.5H0)

▸ **PROBLEMA Π16.6.**
Demonstre o Teorema Θ16.41. (Π16.6H1)

▸ **PROBLEMA Π16.7.**
Demonstre que para todo conjunto a, o $\wp_{\mathrm{f}} a$ também é conjunto. Ganhamos assim mais um construtor (unário) de conjuntos: $\wp_{\mathrm{f}} -$. (Π16.7H1)

§323. O axioma da infinidade

16.77. Com todos os nossos axiomas até agora, mesmo tendo conseguido representar tanta matemática fielmente dentro da teoria de conjuntos, ainda *não é garantida* a existência de nenhum conjunto infinito. Mesmo assim, a noção de "ser infinito" pode sim ser expressada em nossa dicionário, num jeito genial graças ao Dedekind, que deu a primeira definição de infinito que não presupõe a definição dos números naturais. Como?

!! SPOILER ALERT !!

D16.78. Definição (Dedekind-infinito). Seja A conjunto. Chamamos o A *Dedekind-infinito* sse ele pode ser "injetado" para um subconjunto próprio dele, ou seja, sse existem $X \subsetneq A$ e $f : A \rightarrowtail X$. Definimos então o predicado

$$\text{Infinite}(a) \overset{\text{def}}{\iff} \exists x(x \subsetneq a \wedge (a =_{\text{c}} x)).$$

16.79. Conjunto-sucessor.

TODO Escrever

D16.80. Definição (Zermelo, von Neumann). Definimos o *conjunto-sucessor* dum conjunto x ser o

(Zermelo) $$x^+ \overset{\text{def}}{=} \{x\}$$

(von Neumann) $$x^+ \overset{\text{def}}{=} x \cup \{x\}\,.$$

Como não existe ambigüidade, omitimos parenteses escrevendo por exemplo x^{+++} em vez de $((x^+)^+)^+$.

α16.81. Axioma (Infinity). *Existe um conjunto que tem o $\emptyset$ como membro e é fechado sob a operação $\lambda x\,.\,x^+$.*

(ZF7) $$\exists s\big(\emptyset \in s \wedge \forall x\big(x \in s \to x^+ \in s\big)\big)$$

▸ **EXERCÍCIO x16.40.**
Verdadeiro ou falso? Com o axioma Infinity (ZF7) é garantida a existência *do* conjunto

$$\big\{\emptyset, \emptyset^+, \emptyset^{++}, \emptyset^{+++}, \dots\big\}\,.$$

(Escrevemos "do" em vez de "dum" pois o axioma Extensionality (ZF1) garanta que se existe, existe único.) (x16.40 H 1)

D16.82. Definição. Seja I o conjunto cuja existência é garantida pelo axioma Infinity (ZF7). Ou seja, o conjunto que satisfaz a condição:

$$\emptyset \in I \wedge \forall x\big(x \in I \to x^+ \in I\big).$$

↯

▸ **EXERCÍCIO x16.41.**
Qual o problema com a Definição D16.82? (x16.41 H 1)

16.83. Efeitos e efeitos colaterais. O axioma Infinity (ZF7) é o segundo dos nossos axiomas que garanta diretamente a existência dum certo objeto; o primeiro foi o Emptyset (ZF2).[108] Assim que aceitamos o Emptyset, nós definimos o símbolo $\emptyset$ para ser *o* conjunto vazio. Para poder fazer isso precisamos *demonstrar* a unicidade do conjunto vazio (Teorema Θ16.18). Mas a condição que aparece no (ZF7) não é suficientemente forte para ganhar unicidade pelo (ZF1)! Possivelmente (e realmente, como nós vamos ver) nosso mundo tem muitos conjuntos com essa propriedade!

▸ **EXERCÍCIO x16.42.**
Mostre que já é garantida uma infinidade de conjuntos infinitos. (x16.42 H 1)

16.84. Como parece esse conjunto infinito?. Bem; sabemos que I é infinito e tal, mas quais são os elementos dele? É tentador pensar que I é o conjunto

$$I_* \stackrel{\text{"def"}}{=} \{\emptyset, \emptyset^+, \emptyset^{++}, \emptyset^{+++}, \dots\}.$$

No final das contas, vendo o (ZF7), *o que mais poderia estar no I?* Nada. Certo? Não. Bem o oposto! *Absolutamente tudo* pode pertencer nesse I, pois a única informação que temos sobre ele não tira nenhum objeto como possível membro dele! Realmente, os únicos elementos *garantidos* no I são aqueles que escrevemos acima como membros do I_*, mas o I pode ter mais: pode ter "lixo", como este:

$$I_{\spadesuit,\heartsuit} \stackrel{\text{"def"}}{=} \{\emptyset, \spadesuit, \heartsuit, \emptyset^+, \emptyset^{++}, \emptyset^{+++}, \dots\}.$$

Aqui os ♠ e ♡ denotam dois objetos do nosso universo, talvez nem são conjuntos, talvez denotam os próprios símbolos "♠" e "♡", talvez somos nos, eu e tu, etc. Para a gente, é o lixo.[109]

Na verdade, esse último conjunto não pode ser o nosso I, pois ele não satisfaz a condição do (ZF7) pois

$$\spadesuit \in I \qquad \text{mas} \qquad \spadesuit^+ \notin I.$$

Podemos então entender melhor nosso I. Ele é um superconjunto do I_*—isto é garantido pelo (ZF7) mesmo. O que mais ele tem? Não sabemos dizer, mas sabemos que *se tem* outros objetos, ele obrigatoriamente tem uma infinidade de conjuntos para cada um deles:

$$\{\emptyset, \spadesuit, \heartsuit, \emptyset^+, \spadesuit^+, \heartsuit^+, \emptyset^{++}, \spadesuit^{++}, \heartsuit^{++}, \emptyset^{+++}, \spadesuit^{+++}, \heartsuit^{+++}, \dots\}.$$

Vamos revisar esse I então. Sabemos que ele parece assim:

$$I = \left\{\emptyset, \vdots, \emptyset^+, \vdots, \emptyset^{++}, \vdots, \emptyset^{+++}, \vdots, \emptyset^{++++}, \vdots, \dots\right\}$$

[108] Pois todos os outros começam com quantificadores universais.
[109] Sem ofensa.

onde os $\vdots$ representam o lixo, e nosso próximo trabalho será achar um jeito para nos livrar desse lixo!

§324. Construindo os números naturais

16.85. Especificação. Primeiramente precisamos esclarecer o que precisamos implementar. Qual é o "pedido" do cliente que queremos atender? Quais são as leis (suficientes e necessárias) que os números naturais devem respeitar?

!! SPOILER ALERT !!

D16.86. Definição (Sistema Peano). Um *sistema Peano* é um conjunto estruturado $\mathcal{N} = (\mathbf{N}\,;\,\mathsf{O},\mathsf{S})$ que satisfaz as leis:

(P1)	Zero é um número natural:	$\mathsf{O} \in \mathbf{N}$
(P2)	O sucessor é uma operação unária nos naturais:	$\mathsf{S} : \mathbf{N} \to \mathbf{N}$
(P3)	Naturais diferentes tem sucessores diferentes:	$\mathsf{S} : \mathbf{N} \rightarrowtail \mathbf{N}$
(P4)	Zero não é o sucessor de nenhum natural:	$\mathsf{O} \notin \mathsf{S}[\mathbf{N}]$
(P5)	Os naturais satisfazem o princípio da indução:	

Princípio da indução: *para todo* $X \subseteq \mathbf{N}$*,*

$$\big(\mathsf{O} \in X \wedge \forall n(n \in X \to \mathsf{S}n \in X)\big) \to X = \mathbf{N}.$$

Observe que graças às (P3) e (P4) temos

$$\mathsf{S}n = \mathsf{S}m \implies n = m$$
$$\mathsf{S}n \neq \mathsf{O}$$

para todos os $n, m \in \mathbf{N}$. Os axiomas (P1)–(P5) são conhecidos como *axiomas Dedekind–Peano*.

16.87. Definindo um sistema Peano. Então o que precisamos implementar é um conjunto estruturado $\mathcal{N} = (\mathbf{N}\,;\,\mathsf{O},\mathsf{S})$. Isso é fácil: nosso $\mathcal{N}$ vai ser uma tripla $\langle \mathbf{N}, \mathsf{O}, \mathsf{S}\rangle$, onde seus membros $\mathbf{N}$, O, e S são tais objetos que as leis (P1)–(P5) são satisfeitas. Sabemos que o $\mathbf{N}$ precisa ser infinito, então temos que o procurar entre os conjuntos infinitos da nossa teoria. Uma primeira idéia seria botar $\mathbf{N} \stackrel{\text{def}}{=} I$, mas essa não parece uma idéia boa—será difícil "vender" uma implementação com lixo! O que realmente queremos botar como $\mathbf{N}$ é o I_* (que não conseguimos ainda defini-lo). Mas vamos supor

que o I_* realmente é um conjunto; ele vai representar os números naturais, mas quais serão nossos O e S? Pela especificação dos naturais, O tem que ser um dos membros do I_*, e bem naturalmente escolhemos o $\emptyset$ como o zero. E o S? Obviamente queremos botar $\mathsf{S} = \lambda x \,.\, x^+$, mas para realmente definir o S como função, lembramos que em nosso dicionário "função" é um certo tipo de conjunto de pares. Botamos então

$$\mathsf{S} \overset{\text{"def"}}{=} \{\!\!\{ \langle n, m\rangle \mid m = n^+ \}\!\!\}$$

e agora só basta achar um conjunto que tem todos esses pares como membros. Fácil:

$$\mathsf{S} \overset{\text{def}}{=} \{ \langle n, m\rangle \in \mathbf{N} \times \mathbf{N} \mid m = n^+ \}\,.$$

Então falta só definir esse I_*.

16.88. Jogando fora o lixo. Queremos definir o I_* como conjunto; construí-lo pelos axiomas. Uma primeira tentativa seria começar com o próprio I, e usar o Separation (ZF4) para filtrar seus elementos, separando os quais queremos do lixo, assim botando

$$I_* = \{ x \in I \mid \varphi(x) \}\,.$$

para algum certo filtro $\varphi(-)$. Qual fórmula vamos usar?

!! SPOILER ALERT !!

16.89. Uma abordagem top-down. Não podemos descrever um filtro em nossa linguagem de lógica (FOL de teoria de conjuntos)! (Lembra-se, uma fórmula não pode ter tamanho infinito.) Precisamos então alguma outra idéia para nos livrar dos elementos "extra" do I. *Vamos definir o conjunto I_* com a abordagem top-down!* Sabemos que nosso I_* desejado é um subconjunto de I. Então vamos começar com a colecção de todos os subconjuntos de I que satisfazem a condição do Infinity:

$$\mathscr{I} \overset{\text{def}}{=} \{ i \in \wp I \mid \emptyset \in i \wedge \forall x\big(x \in i \to x^+ \in i\big) \}\,.$$

Queremos agora selecionar o "menor" elemento dessa família $\mathscr{I}$. Menor no sentido de "aquele que está contido em todos". Sim, nosso I_* é o $(\subseteq)$-menor elemento do $\mathscr{I}$! Para defini-lo basta tomar a intersecção da família $\mathscr{I}$, que podemos pois $\mathscr{I} \neq \emptyset$ (Exercício x16.43):

$$I_* \overset{\text{def}}{=} \bigcap \mathscr{I}\,.$$

► **EXERCÍCIO x16.43.**
Por que $\mathscr{I} \neq \emptyset$? (x16.43 H 0)

Θ16.90. Teorema (Existência dos naturais). *Existe pelo menos um sistema Peano* $\mathcal{N} = (\mathbf{N}\,;\,\mathsf{O},\mathsf{S})$.

▸ Esboço. Definimos

$$\mathcal{N} \stackrel{\text{def}}{=} \langle \mathbf{N}, \mathsf{O}, \mathsf{S}\rangle\,,$$

onde:

$$\begin{aligned}\mathbf{N} &\stackrel{\text{def}}{=} \bigcap \big\{\, i \in \wp I \;\mid\; \emptyset \in i \wedge \forall x\big(x \in i \to x^+ \in i\big)\,\big\}\\ \mathsf{O} &\stackrel{\text{def}}{=} \emptyset\\ \mathsf{S} &\stackrel{\text{def}}{=} \big\{\, \langle m, n\rangle \in \mathbf{N}\times\mathbf{N} \;\mid\; n = m^+\,\big\}\,.\end{aligned}$$

Temos já justificado que cada objeto que aparece nessa definição é conjunto pelos axiomas. Basta só verificar que as (P1)–(P5) são satisfeitas. □ (Θ16.90P)

▸ **EXERCÍCIO x16.44 (P1).**
Demonstre que $\mathsf{O} \in \mathbf{N}$. (x16.44H0)

▸ **EXERCÍCIO x16.45 (P2).**
Demonstre que S é uma função. (x16.45H0)

▸ **EXERCÍCIO x16.46 (P3).**
Demonstre que $\mathsf{S} : \mathbf{N} \rightarrowtail \mathbf{N}$. (x16.46H0)

▸ **EXERCÍCIO x16.47 (P4).**
Demonstre que $\mathsf{O} \notin \mathsf{S}[\mathbf{N}]$. (x16.47H0)

▸ **EXERCÍCIO x16.48 (P5).**
Seja $X \subseteq \mathbf{N}$ tal que:
(1) $\mathsf{O} \in X$;
(2) para todo $k \in \mathbf{N}$, se $k \in X$ então $\mathsf{S}k \in X$.
Demonstre que $X = \mathbf{N}$. (x16.48H0)

Θ16.91. Teorema (Unicidade dos naturais). *Se* $\mathcal{N}_1 = (\mathbf{N}_1\,;\,\mathsf{O}_1,\mathsf{S}_1)$ *e* $\mathcal{N}_2 = (\mathbf{N}_2\,;\,\mathsf{O}_2,\mathsf{S}_2)$ *são sistemas Peano, então são isomorfos:* $\mathcal{N}_1 \cong \mathcal{N}_2$.

▸ Demonstração errada. Precisamos definir um isomorfismo $\varphi : \mathcal{N}_1 \cong \mathcal{N}_2$. Definimos a função $\varphi : \mathbf{N}_1 \to \mathbf{N}_2$ usando recursão:

$$\begin{aligned}\varphi(\mathsf{O}_1) &= \mathsf{O}_2\\ \varphi(\mathsf{S}_1 n) &= \mathsf{S}_2\varphi(n).\end{aligned}$$

Pela sua definição, a φ é um homomorfismo. Basta só verificar que a φ é bijetora, algo que tu vai fazer agora nos exercícios x16.49 & x16.50. ↯ ↯

▸ **EXERCÍCIO x16.49.**
Demonstre que a $\varphi : \mathbf{N}_1 \to \mathbf{N}_2$ definida no Teorema Θ16.91 é um monomorfismo. (x16.49H0)

▸ **EXERCÍCIO x16.50.**
Demonstre que a $\varphi : \mathbf{N}_1 \to \mathbf{N}_2$ definida no Teorema Θ16.91 é um epimorfismo. (x16.50 H 1 2 3)

▸ **EXERCÍCIO x16.51.**
Qual o erro na demonstração do Teorema Θ16.91? (x16.51 H 1)

§325. Teoremas de recursão

Θ16.92. Teorema da Recursão. *Sejam $\mathcal{N} = (\mathbf{N} ; \mathsf{O}, \mathsf{S})$ um sistema Peano, A conjunto, $a \in A$, e $h : A \to A$. Então existe única função $F : \mathbf{N} \to A$ que satisfaz as equações:*

$$F(\mathsf{O}) = a \tag{1}$$
$$F(\mathsf{S}n) = h(F(n)), \quad \text{para todo } n \in \mathbf{N}. \tag{2}$$

▸ Esboço. Nosso plano é

(i) construir o objeto F como conjunto;
(ii) mostrar que $F : \mathbf{N} \to A$;
(iii) mostrar que F satisfaz as (1)–(2);
(iv) unicidade.

(i) Vamos construir o F *bottom-up*, juntando umas das suas aproximações finitas: funções parciais $f : \mathbf{N} \rightharpoonup A$ onde a idéia é que elas "concordam" com a F desejada onde elas estão definidas. Nem vamos considerar todas elas: para nossa conveniência queremos apenas aquelas cujo domínio é algum $\overline{n}$. Por exemplo, as primeiras aproximações seriam as seguintes:

$$\begin{aligned} f_0 &= \emptyset \\ f_1 &= \{\langle 0, a\rangle\} \\ f_2 &= \{\langle 0, a\rangle, \langle 1, h(a)\rangle\} \\ f_3 &= \{\langle 0, a\rangle, \langle 1, h(a)\rangle, \langle 2, h(h(a))\rangle\}, \\ &\vdots \end{aligned}$$

Definimos o conjunto $\mathscr{A}$ de todas as aproximações aceitáveis:

$$\mathscr{A} \stackrel{\text{def}}{=} \{\, f \in (\mathbf{N} \rightharpoonup A) \mid f \text{ é aproximação aceitável} \,\}$$

onde falta descrever com uma fórmula nossa idéia de "ser aproximação aceitável" (Exercício x16.53). (Das aproximações acima a f_0 não é aceitável.) Agora podemos já definir o F:

$$F \stackrel{\text{def}}{=} \bigcup \mathscr{A}.$$

(ii) Precisamos mostrar a compatibilidade da $\mathscr{A}$ e a totalidade da F, ou seja: que não existem *conflitos* (em outras palavras: que a família de funções parciais $\mathscr{A}$ é *compatível*); e que $\operatorname{dom} F = \mathbf{N}$. Esses são os exercícios Exercício x16.54 & Exercício x16.55 respectivamente.

(iii) Precisamos verificar a corretude da F, que ela atende sua especificação. Essa parte deve seguir da definição de "aproximação aceitável". Confirmamos isso no Exercício x16.56.

(iv) Para a unicidade da F, precisamos mostrar que se $G : \mathbf{N} \to A$ tal que satisfaz as (1)–(2), então $F = G$. Isso é o Exercício x16.57, e com ele terminamos nossa demonstração. □ (Θ16.92P)

▸ **EXERCÍCIO x16.52.**
Desenhe um diagrama comutativo que expressa o Teorema da Recursão Θ16.92. (x16.52 H 1 2)

▸ **EXERCÍCIO x16.53.**
No contexto do Teorema da Recursão Θ16.92 defina formalmente a afirmação «f é uma aproximação aceitável». (x16.53 H 1)

▸ **EXERCÍCIO x16.54 (Compatibilidade).**
No contexto do Teorema da Recursão Θ16.92 mostre que $\mathscr{A}$ é compatível. (x16.54 H 0)

▸ **EXERCÍCIO x16.55 (Totalidade da F).**
No contexto do Teorema da Recursão Θ16.92 mostre que $\operatorname{dom} F = \mathbf{N}$. (x16.55 H 1)

▸ **EXERCÍCIO x16.56 (Corretude da F).**
No contexto do Teorema da Recursão Θ16.92 mostre que F atende sua especificação, ou seja:

(1) $$F(\mathsf{O}) = a$$
(2) $$F(\mathsf{S}n) = h(F(n)), \quad \text{para todo } n \in \mathbf{N}.$$

(x16.56 H 0)

▸ **EXERCÍCIO x16.57 (Unicidade da F).**
No contexto do Teorema da Recursão Θ16.92 demonstre a unicidade da F, ou seja: se $G : \mathbf{N} \to A$ tal que

(1) $$G(\mathsf{O}) = a$$
(2) $$G(\mathsf{S}n) = h(G(n)), \quad \text{para todo } n \in \mathbf{N}.$$

então $F = G$. Em outras palavras, as equações (1)–(2) *determinam* a função no $\mathbf{N}$. (x16.57 H 1)

§326. Conseqüências de indução e recursão

Na §83 definimos recursivamente umas operações nos naturais. Graças ao Teorema da Recursão Θ16.92, ganhamos todas essas operações em qualquer sistema Peano. Vamos lembrar como, e também demonstrar que não importa *em qual* sistema Peano calculamos: os resultados serão os correspondentes!

16.93. Operações e ordem. Para qualquer sistema Peano $\mathscr{N} = (\mathbf{N} ; \mathsf{O}, \mathsf{S})$, definimos as operações de adição e de multiplicação

(a1)	$n + \mathsf{O} = n$	$n \cdot \mathsf{O} = \mathsf{O}$	$(\cdot).1$
(a2)	$n + \mathsf{S}m = \mathsf{S}(n + m)$	$n \cdot \mathsf{S}m = (n \cdot m) + n$	$(\cdot).2$

e a relação de ordem no $\mathbf{N}$

$$n \leq m \overset{\text{def}}{\iff} (\exists k \in \mathbf{N})[n + k = m].$$

Sejam dois sistemas Peano $\mathcal{N}_1 = (\mathbf{N}_1 \,;\, \mathsf{O}_1, \mathsf{S}_1)$ e $\mathcal{N}_2 = (\mathbf{N}_2 \,;\, \mathsf{O}_2, \mathsf{S}_2)$, e suas operações de adição $+_1$ e $+_2$, e suas relações de ordem $\leq_1$ e $\leq_2$. Seja $\varphi : \mathbf{N}_1 \rightarrowtail \mathbf{N}_2$ o isomorfismo definido pelas

$$(\varphi 1) \qquad \varphi(\mathsf{O}_1) = \mathsf{O}_2$$
$$(\varphi 2) \qquad \varphi(\mathsf{S}_1 n) = \mathsf{S}_2(\varphi(n)).$$

16.94. Propriedade. *A φ respeita a adição, ou seja:*

$$\text{para todo } n, m \in \mathbf{N}_1, \quad \varphi(n +_1 m) = \varphi(n) +_2 \varphi(m)$$

Demonstração. Por indução no $m \in \mathbf{N}_1$: Base ($m := \mathsf{O}_1$): *para todo* $n \in \mathbf{N}_1$, $\varphi(n +_1 \mathsf{O}_1) = \varphi(n) +_1 \varphi(\mathsf{O}_1)$. Seja $n \in \mathbf{N}_1$. Calculamos:

$$\begin{aligned} \varphi(n +_1 \mathsf{O}_1) &= \varphi(n) && \text{(pela (a1)}_1\text{)} \\ &= \varphi(n) +_2 \mathsf{O}_2 && \text{(pela (a1)}_2\text{)} \\ &= \varphi(n) +_2 \varphi(\mathsf{O}_1) && \text{(pela } (\varphi 1)\text{)} \end{aligned}$$

Passo indutivo: Seja $k \in \mathbf{N}_1$ tal que

$$\text{(H.I.)} \qquad \text{para todo } n \in \mathbf{N}_1,\ \varphi(n +_1 k) = \varphi(n) +_1 \varphi(k).$$

Vamos demonstrar que

$$\textit{para todo } n \in \mathbf{N}_1,\ \varphi(n +_1 \mathsf{S}_1 k) = \varphi(n) +_1 \varphi(\mathsf{S}_1 k).$$

Seja $n \in \mathbf{N}_1$. Calculamos:

$$\begin{aligned} \varphi(n +_1 \mathsf{S}_1 k) &= \varphi(\mathsf{S}_1(n +_1 k)) && \text{(pela (a1)}_2\text{)} \\ &= \mathsf{S}_2(\varphi(n +_1 k)) && \text{(pela } (\varphi 2)\text{)} \\ &= \mathsf{S}_2(\varphi(n) +_2 \varphi(k)) && \text{(pela (H.I.), com } n := n\text{)} \\ &= \varphi(n) +_2 \mathsf{S}_2 \varphi(k) && \text{(pela (a2)}_2\text{)} \\ &= \varphi(n) +_2 \varphi(\mathsf{S}_1 k) && \text{(pela } (\varphi 2)\text{)} \end{aligned}$$

∎

► **EXERCÍCIO x16.58.**
Mostre que φ respeita a multiplicação, ou seja:

$$\text{para todo } n, m \in \mathbf{N}_1, \quad \varphi(n \cdot_1 m) = \varphi(n) \cdot_2 \varphi(m).$$

(x16.58 H 1)

▸ **EXERCÍCIO x16.59.**
Mostre que φ respeita a ordem também, no sentido de:

$$\text{para todo } n, m \in \mathbf{N}_1, \quad n \leq_1 m \iff \varphi(n) \leq_2 \varphi(m).$$

(x16.59 H 1)

§327. Construindo mais números

Tendo construido já os naturais, vamos construir seus parentes também: os inteiros, os racionais, os reais, e os complexos.

16.95. Os inteiros. Provavelmente a primeira idéia para implementar um inteiro x é usar uma 2-tupla $x \stackrel{\text{def}}{=} \langle s, m\rangle$ onde s é um objeto para indicar o sinal do x e $m \stackrel{\text{def}}{=} |x|$. Essa resolução, mesmo tecnicamente possível, não é legal. Dependendo de se teriamos 2 ou 3 sinais podemos acabar com duas distintas representações de 0, números $x \neq 0$ com sinal 0, ou outros problemas similares. Além disso, como vamos definir as operações? Vão acabar sendo definições por casos no sinal s, na ordem dos argumentos, etc. Nenhum desses problemas é difícil corrigir; mas tudo isso deve aparecer coisa com cheiro de "ugly hack". E é mesmo. A idéia é representar os inteiros como diferenças de naturais. O inteiro 5 então pode ser visto como a diferença $12-7$; e o inteiro -5 como a $7-12$. Como podemos formalizar isso numa maneira elegante?

!! SPOILER ALERT !!

D16.96. Definição (Números inteiros). Seja $Z = \mathbb{N} \times \mathbb{N}$. Defina no Z a relação $\approx$ pela

$$\langle a, b\rangle \approx \langle c, d\rangle \iff a + d = c + b.$$

Sendo uma relação de equivalência (Exercício x16.60), definimos

$$\mathbf{Z} \stackrel{\text{def}}{=} Z/\!\approx.$$

▸ **EXERCÍCIO x16.60.**
Mostre que $\approx$ é uma relação de equivalência. (x16.60 H 0)

▸ **EXERCÍCIO x16.61.**
Defina o que falta para o $\mathbf{Z}$ virar uma representação de inteiros útil para o *matemático trabalhador*. (Parte desses exercícios é decidir o que falta mesmo.) (x16.61 H 0)

16.97. Os números racionais. Essa construção é bem interessante—e simples!—pois usa um conceito nosso que deve ser familiar já: sim, novamente o conjunto quociente. Queremos identificar o racional $1/2$ com o par $\langle 1,2\rangle$, mas não podemos identificar o próprio $\mathbb{Q}$ com o $\mathbb{Z}\times\mathbb{Z}_{\neq 0}$, pois $\langle 1,2\rangle \neq \langle 2,4\rangle$ mesmo que $1/2 = 2/4$. Duas idéias parecem razoáveis: (1) escolher um representante específico para cada racional, trabalhando assim num subconjunto próprio do $\mathbb{Z}\times\mathbb{Z}_{\neq 0}$; (2) definir a relação $\approx$ de *equivalência* no $\mathbb{Z}\times\mathbb{Z}_{\neq 0}$, e representar os racionais *não como* membros desse conjunto, mas *sim como* classes de equivalência, ou seja, membros do conjunto quociente $\mathbb{Z}\times\mathbb{Z}_{\neq 0}/\!\approx$. Vamos seguir essa segunda idéia, pois é mais símples e elegante.

D16.98. Definição (Números racionais). Seja $Q = \mathbb{Z}\times\mathbb{Z}_{\neq 0}$. Defina no Q a relação $\approx$ pela

$$\langle a,b\rangle \approx \langle c,d\rangle \stackrel{\text{def}}{\iff} ad = bc.$$

Sendo uma relação de equivalência (Exercício x16.62), definimos

$$\mathbf{Q} \stackrel{\text{def}}{=} Q/\!\approx.$$

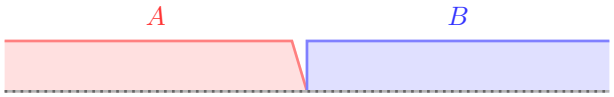
▸ **EXERCÍCIO x16.62.**
Mostre que $\approx$ é uma relação de equivalência. (x16.62 H 0)

▸ **EXERCÍCIO x16.63.**
Defina o que falta para o $\mathbf{Q}$ virar uma representação de racionais útil para o *matemático trabalhador*. (x16.63 H 0)

16.99. Os números reais. Existem várias maneiras de construir os reais com o que temos até agora. Neste texto encontramos as duas "principais": de Dedekind, que usa *Dedekind cuts*, e de Cantor, que usa *seqüências Cauchy*. Ambas as maneiras são baseadas na idéia que a linha dos racionais tem buracos (certos pontos estão fazendo falta) e a construção dos reais precisa adicionar esses buracos. Para a metodo de Dedekind, visualizamos os buracos como suprema que estão em falta de certos conjuntos; para o Cantor, os buracos são limites de seqüências que *querem converger mas não conseguem* pois seus limites desejados não estão presentes! Vamos seguir Dedekind agora; a abordagem de Cantor fica para o Problema Π16.16.

TODO Elaborar/terminar

16.100. Dedekind cut. Seja $\alpha\in\mathbb{R}$. O Dedekind cut que corresponde (representa) o α parece assim:

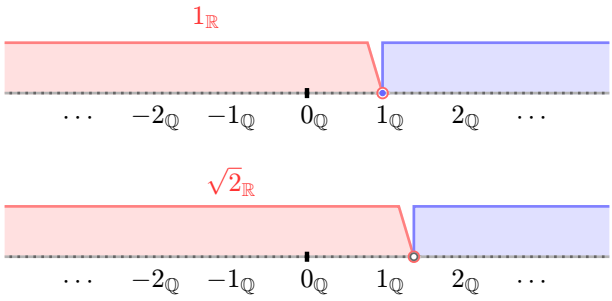


onde

$$A = \{\, r\in\mathbb{Q} \mid r < \alpha \,\} \qquad\qquad B = \{\, r\in\mathbb{Q} \mid r \geq \alpha \,\}.$$

A idéia é que podemos definir o real α para ser esse Dedekind cut. Observe que definindo o A, determinamos o B também, pois $B = \mathbb{Q}\setminus A$. Só que já temos um problema: na definição do A usamos o real α, ou seja, nossa definição presupõe que já temos os reais na nossa disposição; mas os reais são o que estamos tentando construir, então obviamente

não podemos usá-los para construí-los! Mesmo assim, podemos usar nossa intuição da reta real e da reta dos racionais no nosso rascunho para nos ajudar resolver esse problema. Note que caso que α é um racional a parte B possui mínimo (o próprio α); no outro lado, os B's que correspondem em irracionais não possuem mínimo. Por exemplo, aqui os $1_{\mathbb{R}}$ e $\sqrt{2}_{\mathbb{R}}$ como Dedekind cuts:



Agora basta achar uma maneira que descreva todos os subconjuntos do $\mathbb{Q}$ que podem ser usados como A's num Dedekind cut, para construir o $\mathbb{R}$ como o conjunto de todos eles:

$$\mathbf{R} \stackrel{\text{def}}{=} \{\, A \subseteq \mathbb{Q} \mid A \text{ parece como no desenho acima} \,\}.$$

? **Q16.101. Questão.** Como descreverias formalmente esses A's?

!! SPOILER ALERT !!

D16.102. Definição (Dedekind cuts). Chamamos A de *Dedekind cut* sse:

(i) A é "fechado pra baixo": $(\forall a \in A)(\forall q \in \mathbb{Q})[\, q < a \implies q \in A\,]$;
(ii) A não possui máximo: $(\forall a \in A)(\exists a' \in A)[\, a < a'\,]$;
(iii) $A \neq \emptyset$;
(iv) $A \neq \mathbb{Q}$.

Visualmente parece melhor chamar de *Dedekind cut* a partição $\{A, B\}$ ou o par $\langle A, B\rangle$. As vezes fazemos isso, algo que nunca gera confusão graças ao contexto.

▸ **EXERCÍCIO x16.64.**
Defina o que falta para o $\mathbf{R}$ virar uma representação de reais útil para o *matemático trabalhador*. (x16.64H0)

Θ16.103. Teorema (Existência dos reais). *Existe um corpo ordenado competo.*

Demonstração. Seja $\mathcal{R} \stackrel{\text{def}}{=} (\mathbf{R}\,;\, +_{\mathcal{R}}, \cdot_{\mathcal{R}}, -_{\mathcal{R}}, 0_{\mathcal{R}}, 1_{\mathcal{R}}, P_{\mathcal{R}})$ um conjunto estruturado, onde todos os componentes devem estar já definidos no Exercício x16.64. Falta só demonstrar que o $\mathcal{R}$ realmente satisfaz os axiomas de corpo ordenado completo, que deixo para o Problema Π16.9. ∎

▸ **EXERCÍCIO x16.65.**
O que acontece se apagar os (iii) e (iv) da Definição D16.102? (x16.65 H 0)

16.104. Mais numeros. Podemos construir mais mas nosso objetivo aqui não é formalizar e implementar tudo; apenas apreciar as possibilidades e o poder da teoria dos conjuntos nesse quesito, e obter pelo menos o que precisamos aqui: naturais, inteiros, racionais, reais. Como exercício, deixo pra ti a construção dos complexos (que raramente aparecem aqui como *cameo*). Se quiser implementar ainda mais, sinta-se a vontade aprofundar.

▸ **EXERCÍCIO x16.66.**
Construa os complexos. (x16.66 H 0)

Intervalo de problemas

▸ **PROBLEMA Π16.8 (Multisets).**
Alguém te deu a seguinte especificação de multiset e tu queres implementá-la dentro da teoria de conjuntos. (Veja também Secção §191 no Capítulo 8.)
"Definição". Lembre (Secção §191) que um *multiset* (ou *bag*) M é como um conjunto onde um elemento pode pertencer ao M mais que uma vez (mas não uma infinidade de vezes). Ou seja, a ordem não importa (como nos conjuntos), mas a "multiplicidade" importa sim.

Queremos tres operações em multisets, exemplificadas assim:

$$\begin{aligned}
&\wr x,y,y,z,z,z,w\wr \Cup \wr x,y,z,z,u,v,v\wr = \wr x,y,y,z,z,z,u,v,v,w\wr\\
&\wr x,y,y,z,z,z,w\wr \Cap \wr x,y,z,z,u,v,v\wr = \wr x,y,z,z\wr\\
&\wr x,y,y,z,z,z,w\wr \oplus \wr x,y,z,z,u,v,v\wr = \wr x,x,y,y,y,z,z,z,z,z,u,v,v,w\wr
\end{aligned}$$

Também queremos um predicado de "pertencer" ε e uma relação de "submultiset" $\Subset$ tais que:

$$\begin{aligned}
&x \varepsilon \wr x,y,y,z,z,z,w\wr && \wr x,y,z,z\wr \Subset \wr x,x,y,y,z,z\wr\\
&z \varepsilon \wr x,y,y,z,z,z,w\wr && \wr x,y,z,z\wr \not\Subset \wr x,x,y,y,z\wr\\
&u \not\varepsilon \wr x,y,y,z,z,z,w\wr && \wr x,y,z,z\wr \Subset \wr x,y,z,z\wr\\
&x \not\varepsilon \wr\wr \quad \text{para todo } x && M \Subset M \quad \text{para todo multiset } M\\
& && \wr\wr \Subset M \quad \text{para todo multiset } M.
\end{aligned}$$

(MS1) Para os multisets A e B temos $A = B$ sse eles têm os mesmos membro com as mesmas multiplicidades. Por exemplo,

$$\wr x,y,z,z,y\wr = \wr x,y,y,z,z\wr \neq \wr x,y,z\wr.$$

(MS2) Para cada conjunto A, a classe

$$\{\, M \mid M \text{ é multiset e } \forall x(x \varepsilon M \to x \in A) \,\}$$

de todos os multisets formados por membros de A é um conjunto.

(i) Defina formalmente (em teoria de conjuntos) o termo "multiset" e mostre (como exemplos) como são representados os multisets seguintes:

$$\wr\wr \qquad \wr 0,1,2,2,1\wr \qquad \wr 1,2,2,3,3,3,4,4,4,4,\ldots\wr.$$

(ii) Defina as operações de multisets $(\Cup, \Cap, \oplus)$ e os predicados $(\varepsilon, \Subset)$.

(iii) Demonstre pelos axiomas ZF que tua definição satisfaz as (MS1)–(MS2). (Π16.8 H 1)

▸ **PROBLEMA Π16.9.**
Demonstre que o $\mathcal{R}$ do Teorema Θ16.103 satisfaz mesmo as leis e corpo ordenado completo. (Π16.9 H 0)

§328. Mais axiomas (ZF)

16.105. Créditos. Todos os axiomas que temos visto até agora são essencialmente os axiomas de Zermelo, e falta apenas um dos seus axiomas originais (o axioma da escolha que encontramos na §333). Sobre o axioma Separation (ZF4), Zermelo usou o termo "propriedade definitiva", que temos usado também sobre o "filtro", mas foram Fraenkel e Skolem que consideraram definir isso como uma fórmula da linguagem da FOL com $(=)$ e $(\in)$.

16.106. Uma carta de Fraenkel para Zermelo. Fraenkel percebeu (e comunicou no 1921 para Zermelo) que com os seus axiomas não é possível demonstrar a existência duns certos conjuntos interessantes, como por exemplo o

$$\{\mathbf{N}, \wp\mathbf{N}, \wp\wp\mathbf{N}, \wp\wp\wp\mathbf{N}, \ldots\}.$$

Sim, podemos construir cada um dos seus elementos, mas não a colecção deles como conjunto!

α16.107. Axioma (Replacement (schema)). Para cada função-classe $\Phi(-)$, o seguinte: *Para todo conjunto a, a classe $\Phi[\,a\,] \stackrel{\text{def}}{=} \{\, \Phi(x) \mid x \in a \,\}$ é um conjunto.*

(ZF8) $$\forall a \exists b \forall y \big(y \in b \leftrightarrow (\exists x \in a)[\, \Phi(x) = y \,] \big)$$

▸ **EXERCÍCIO x16.67.**
Resolve o Exercício x16.10 sem usar o Powerset (ZF5). (x16.67 H 1)

16.108. Um jogo mortal. Teu oponente escolha um conjunto (e ele não participa mais no jogo): esse é o "conjunto da mesa". Em cada rodada do jogo tu tem que escolher um dos membros do conjunto da mesa, e ele se vira o novo conjunto da mesa. O objectivo é simples: *continuar jogando pra sempre.* (Imagine que se o jogo acabar, tu morre—e que tu queres viver—ou algo desse tipo.) Então uma partida onde o oponente escolheu o conjunto

$$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$$

seria a seguinte (sublinhamos as escolhas do jogador onde possível):

Rodada	Conjunto	Movimento
1	$\{\emptyset,\ \{\emptyset\},\ \underline{\{\emptyset,\{\emptyset\}\}},\ \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}\}$	$\{\emptyset,\{\emptyset\}\}$
2	$\{\emptyset,\underline{\{\emptyset\}}\}$	$\{\emptyset\}$
3	$\{\underline{\emptyset}\}$	$\emptyset$
4	$\emptyset$	☹

Talvez esse jogador não foi o mais esperto, mas facilmente confirmamos que qualquer possível estratégia dele é condenada com morte certa depois dum finito número de rodadas. *E se o próprio jogador começa escolhendo qual é o conjunto da mesa inicial?* Qual conjunto tu escolheria? Pode *imaginar* algum conjunto que seria uma boa opção que porderia garantir vitória?

!! SPOILER ALERT !!

► **EXERCÍCIO x16.68.**
Considere os conjuntos da mesa seguintes:

- o conjunto x, onde
$$x = \{\emptyset,\ \mathbf{N},\ \{\emptyset,\{\{\emptyset\}\}\},\ x\};$$
- o conjunto a, onde
$$a = \{\emptyset,\ b\} \qquad b = \{\{\emptyset\},\ c\} \qquad c = \{\{\emptyset\},\ \{\{a\},\{\{\{\emptyset\}\}\}\}\};$$
- o conjunto Ω, onde
$$\Omega = \{\Omega\}.$$

Como tu jogaria nesses jogos? (x16.68 H 0)

16.109. Podemos ganhar?. Talvez. Nossos axiomas *não garantam a existência* de nenhum conjunto que nos permitaria ganhar; contudo, *nem garantam a ausência* de conjuntos como os x, a, b, c, Ω do Exercício x16.68. O axioma seguinte resolve essa questão, afirmando que qualquer partida desse jogo seria realmente mortal.

α16.110. Axioma (Foundation). *Todo conjunto não vazio tem membro disjunto com ele mesmo.*

(ZF9) $$(\forall a \neq \emptyset)(\exists z \in a)[\, z \cap a = \emptyset \,]$$

Vamos agora pesquisar umas conseqüências desse axioma, também conhecido como *Regularity*.

▸ **EXERCÍCIO x16.69.**
Demonstre diretamente que para todo conjunto x, $x \notin x$. Quais axiomas tu precisou? (x16.69 H 1)

16.111. Corolário. $\mathbb{V} \notin \mathbb{V}$, *ou seja,* $\mathbb{V}$ *não é um conjunto.*

▸ **EXERCÍCIO x16.70.**
Demonstre que é impossível para dois conjuntos x, y ter $x \in y$ e também $y \in x$. (x16.70 H 0)

▸ **EXERCÍCIO x16.71.**
Demonstre que não existe seqüência infinita de conjuntos

$$x_0 \ni x_1 \ni x_2 \ni x_3 \ni \cdots$$

e mostre que assim ganhamos os exercícios x16.69 & x16.70 como corolários. (x16.71 H 0)

▸ **EXERCÍCIO x16.72 (Spooky pair agora).**
Demonstre que com o axioma Foundation podemos sim usar a operação do Exercício x16.25

$$\langle x, y \rangle \stackrel{\text{def}}{=} \{x, \{x, y\}\}$$

como uma implementação de par ordenado. (x16.72 H 0)

16.112. ZF. A teoria dos axiomas (ZF1)–(ZF9) junto com o Princípio de Puridade 16.3 é conhecida como ZF: Zermelo–Fraenkel (without Choice). O *working mathematician* típico—sendo pouco mimado—tá querendo mais do que a ZF oferece como fundação! Falta um ingrediente só, que é nosso próximo assunto: o axioma da escolha.

TODO Arrumar/espalhar as próximas 4 seções

§329. Wosets

O termo *wellorder* (ou *well-order*) de inglês tem sido traduzido como *boa ordem* em português. Aqui eu uso o termo *bem-ordem*. Além de ficar mais perto no termo internacional, a palavra "bem" tem um significado *bem* mais usado em português do que em inglês, onde não é muito *well* known, exemplificado aqui:[110]

> Uma ordem é uma relação legal.
> Uma *bem*-ordem é uma relação *bem* legal—vamos descobrir isso nesta secção.

D16.113. Definição (Bem-ordem). Seja $(A\ ;<)$ um conjunto totalmente ordenado. Sua ordem $(<)$ é uma *bem-ordem*, sse *cada subconjunto* $S \subseteq A$ *possui um elemento mínimo*. Nesse caso chamamos o A *bem-ordenado* ou *woset* (de *well-ordered set*).

TODO Elaborar

▸ **EXERCÍCIO x16.73.**
Quais dos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}_{>0}$, $\mathbb{Q}_{\geq 0}$, $\mathbb{R}$, são bem ordenados por sua ordem? (x16.73 H 0)

[110] e com certeza *well* beyond nossos interesses aqui

▸ **EXERCÍCIO x16.74.**
Seja $a \in \mathbb{R}$. Quais dos $\mathbb{Q}_{\geq a}$, $\mathbb{R}_{\geq a}$, e $\{\, 2^{-n} \mid n \in \mathbb{N}, n \leq a \,\}$ satisfázem a propriedade de boa ordem? (x16.74 H 0)

§330. Indução transfinita

§331. Recursão transfinita

§332. Os ordinais

▸ **EXERCÍCIO x16.75.**
O $\omega^2 + 1$ é bem ordenado. (x16.75 H 1)

▸ **EXERCÍCIO x16.76.**
O que podes concluir sobre os ordinais α e β se...:

(i) $\omega + \alpha = \omega$
(ii) $\alpha + \omega = \omega$
(iii) $\omega \cdot \alpha = \omega$
(iv) $\alpha \cdot \omega = \omega$
(v) $\alpha + \beta = \omega$
(vi) $\alpha \cdot \beta = \omega$

(x16.76 H 0)

§333. Axiomas de escolha (ZFC)

Finalmente encontramos aqui o último axioma de Zermelo, o mais infame, seu *axioma de escolha*. Mas, primeiramente, umas definições.

D16.114. Definição (Conjunto-escolha). Seja $\mathscr{A}$ uma família de conjuntos. Chamamos o E um *conjunto-escolha* da $\mathscr{A}$ sse (1) $E \subseteq \cup\mathscr{A}$, e (2) para todo $A \in \mathscr{A}$, a intersecção $E \cap A$ é um singleton.

• **EXEMPLO 16.115.**

Aqui umas famílias de conjuntos e um exemplo de conjunto-escolha para cada uma:

$\mathscr{A}_1 = \{[0,2],[1,4],[3,5]\}$	$\{0,\ 5/2,\ 5\}$
$\mathscr{A}_2 = \{\{a,b\},\{b,c\},\{d\}\}$	$\{a,c,d\}$
$\mathscr{A}_3 = \{\{a,b\},\{b,c\},\{c,a\}\}$	não tem conjunto-escolha
$\mathscr{A}_4 = \{\emptyset,\{\emptyset\},\{\{\emptyset\}\},\{\{\{\emptyset\}\}\},\{\{\{\{\emptyset\}\}\}\},\dots\}$	não tem conjunto-escolha
$\mathscr{A}_5 = \{\{\emptyset\},\{\{\emptyset\}\},\{\{\{\emptyset\}\}\},\{\{\{\{\emptyset\}\}\}\},\dots\}$	$\mathscr{A}_4$
$\mathscr{A}_6 = \{\overline{1},\overline{2},\overline{3},\dots\}$	não tem conjunto-escolha

D16.116. Definição (Função-escolha). Seja A conjunto. Chamamos a $\varepsilon : \wp A \setminus \{\emptyset\} \to A$ uma *função-escolha do conjunto* A sse $\varepsilon(X) \in X$ para todo $X \in \operatorname{dom}\varepsilon$.

Seja $\mathscr{A}$ família de conjuntos. Chamamos a $\varepsilon : \mathscr{A} \to \bigcup\mathscr{A}$ uma *função-escolha da família de conjuntos* $\mathscr{A}$ sse $\varepsilon(A) \in A$ para todo $A \in \mathscr{A}$.

α16.117. Axioma (Choice (AC)). *Seja $\mathscr{A}$ família de conjuntos não vazios. Então*

(AC) existe $\varepsilon : \mathscr{A} \to \bigcup\mathscr{A}$, tal que para todo $A \in \mathscr{A}$, $\varepsilon(A) \in A$.

α16.118. Axioma (Choice (forma disjunta)). *Seja $\mathscr{D}$ família disjunta de conjuntos não vazios. Então*

(ACdis) existe $\varepsilon : \mathscr{D} \to \bigcup\mathscr{D}$, tal que para todo $D \in \mathscr{D}$, $\varepsilon(D) \in D$.

α16.119. Axioma (Choice (forma powerset)). *Seja M conjunto não vazio. Então*

(ACpow) existe $\varepsilon : \wp M \setminus \{\emptyset\} \to M$, tal que para todo $\emptyset \neq A \subseteq M$, $\varepsilon(A) \in A$.

▸ **EXERCÍCIO x16.77.**
Todas as "formas" do axioma de escolha (AC) que vimos até agora são logicamente equivalentes. Demonstre isso seguindo o "round-robin" seguinte:

$$\text{(AC)} \implies \text{(ACdis)} \implies \text{(ACpow)} \implies \text{(AC)}.$$

(x16.77 H 0)

16.120. ZFC. Finalmente chegamos na fundação mais popular entre matemáticos, a teoria dos conjuntos ZFC (Zermelo–Fraenkel with Choice) composta por todos os axiomas da ZF junto com o AC:

$$\mathsf{ZFC} = \mathsf{ZF} + \mathsf{AC}$$

O *working mathematician* típico provavelmente afirmaria que trabalha dentro da ZFC, mas em geral não vai saber citar nem quais são seus próprios axiomas, tanto como um programador típico não sabe dizer quais são os comandos primitivos da linguagem primitiva nem da sua própria máquina que tá usando para escrever e/ou executar seus programas. Existem outras fundações interessantes, usadas, e investigadas; voltarei nisso daqui a pouco (§339).

16.121. Pra que tantos axiomas?. Sabemos desde o Exercício x16.5 que estamos usando uma quantidade infinita de axiomas, por causa dos usos de esquemas axiomáticos (veja Nota 16.26). Já que a ZFC é tão importante e usada, faz sentido nos perguntar se alguém poderia achar outra maneira de axiomatizar a mesma teoria usando apenas uma quantidade finita de axiomas, ou seja, se a teoria ZFC é *finitamente axiomatizável*. Não é o caso: Montague demonstrou na sua tese [Mon57] que isso é impossível:

Θ16.122. Teorema (Montague). *A teoria* ZFC *não é finitamente axiomatizável.*

§334. Conseqüências desejáveis e controversiais

TODO Terminar

Vamos ver aqui umas conseqüências do axioma da escolha (AC). Muitas delas na verdade são logicamente equivalentes a ele! Certos desses teoremas são realmente desejáveis para os matemáticos, mas outros parecem tão parádoxos que o assunto acaba sendo controversial.

Θ16.123. Teorema (Banach–Tarski). *Podemos decompor a bola sólida unária*

$$B = \left\{ \langle x, y, z\rangle \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 \leq 1 \right\}$$

em 5 subconjuntos $S_1, S_2, S_3, S_4, S_5 \subseteq S$, rodar e transladar eles, criando duas cópias sólidas de B.

Θ16.124. Teorema (Bem-ordenação (Zermelo)). *Todo conjunto A pode ser bem ordenado.*

Θ16.125. Teorema (Comparabilidade de cardinais). *Para todos conjuntos A, B, temos $A \leq_{\mathrm{c}} B$ ou $B \leq_{\mathrm{c}} A$.*

§335. Escolhas mais fracas

§336. Outras axiomatizações

§337. Um outro ponto de vista

TODO Terminar

16.126. Linguagem bugada (I): teoria dos quais?!. Considere o que chamamos de *teoria dos grupos*, que encontramos estudar no Capítulo 11. E agora pense no que

chamamos de *teoria dos conjuntos* e estudamos neste capítulo. Os dois estudos têm umas diferenças gritantes que vamos identificar e analisar agora. Olhe nos axiomas de grupos: cada um *afirma algo sobre o que acontece dentro dum grupo*. São do tipo:

- para qualquer objeto g, tal coisa existe;
- existe um objeto que faz aquilo;
- para quaisquer objetos g, h, tal coisa acontece;

etc. Podemos vê-los como uma definição de quando uma tal estrutura merece ser chamada de *grupo*.

Observe que existem dois "razoaveis" interpretações do termo *universo* na teoria dos grupos:

(i) um seria o carrier set $|G|$, assim supondo que *estamos vivendo dentro dum grupo especifico* G;
(ii) o outro seria a classe de todos os grupos.

Os axiomas da teoria dos grupos estão usando a idéia da primeira interpretação. Axiomas do segundo tipo seriam proposições como as seguintes:

- Para todo grupo G, existe um group G' tal que bla blu...
- Existe grupo com exatamente dois membros.
- Para quaisquer grupos G, H, existe grupo A tal que blu bla...

Em vez disso, os axiomas da teoria dos grupos estão referindo ao que acontece "dentro" dum grupo. (Observe que as proposições em cima não são nem *enunciáveis* dentro dum grupo!) Podemos vê-los como definição do que significa *ser um grupo*. Tome aqui um conjunto talmente estruturado. Satisfaz as leis de grupo? Beleza então, vamos chamá-lo de grupo. Não satisfaz as leis de grupo? Também beleza, não vamos chamá-lo de grupo e vida que segue.

Vida que segue sim, pois não estamos usando a teoria dos grupos como fundação de matemática! Por outro lado, se encontrar algo que viola os axiomas da teoria dos conjuntos... morte que segue sim![111]

Os axiomas da teoria dos conjuntos então não estão falando nada sobre o que acontece *dentro dum conjunto*—pelo que eles saibam nem existe o conceito de interior dum conjunto!—e não pode ser vista como definição do que significa *ser conjunto* no sentido que falei sobre as leis dos grupos.

Infelizmente a linguagem e terminologia usada não é consistente e contribui na possível confusão criada na tua cabeça lendo este texto neste momento. Estamos usando os nomes inconsistentemente escolhidos «teoria dos grupos» e «teoria dos conjuntos». Felizmente a inconsistência é *apenas mais uma* da linguagem natural que já temos aceitado (e aproveitado) tais "features" dela, então não é tão problemático para os acostumados.[112] Para ficar consistentes, alguém precisaria renomear exatamente uma das duas frases: ou a «teoria dos grupos» para «teoria dos membros-de-grupo», ou a «teoria dos conjuntos» para «teoria dos universos». Seguindo a maioria dos usos da frase «teoria dos ...» a segunda alternativa parece melhor.

A primeira coisa que fazemos em grupos é procurar *modelos dos axiomas*, ou seja, grupos! Em teoria dos conjuntos não fizemos isso *aqui*. Meio que deixamos subentendido que tem um modelo só, "a colecção dos verdadeiros conjuntos" ou sei-lá-o-que e ficamos procurando ver «o que mais tem por aqui?»... «ah, olha, descobrimos um novo membro do nosso universo», etc. Mas, podemos—e devemos!—tratar a teoria dos conjuntos como *teoria dos universos* também e procurar ver quantos universos temos, quais são eles,

[111] OK, *talvez* ninguém vai morrer por causa disso mas com certeza a fundação vai cair todinha, ou seja, não vai ser mais uma fundação. E quem quer viver sem fundações matemáticas?

[112] os falantes nativos duma linguagem não percebem as inconsistências gramáticas da sua própria linguagem até encontrar um gringo que reclama delas.

achar novos, compará-los, etc. E teoristas dos conjuntos a tratam nessa forma também; o Exercício x16.78 é um brinquedo para ajudar visualizar a idéia num nível elementar.

Mas vamos voltar na treta principal deste momento: o que chamamos de *grupo* na primeira teoria? Qualquer *modelo* cujos membros são os objetos referidos pelos axiomas. Os *objetos* então não são os grupos; mas seus membros (e não demos um nome especial para eles). E chamamos essa coisa de *teoria dos ...* dos quais mesmo? Dos *grupos*, ou seja, escolhemos o termo do nosso universo para usar como nome da teoria. Mas o que chamamos de *conjunto* na segunda teoria? Agora não é o universo, mas os objetos! E qual nome escolhemos para esse estudo? *Teoria dos conjuntos*, ou seja, agora usamos o nome dos nossos objetos e não do universo para chamar a disciplina.

▸ **EXERCÍCIO x16.78.**
Escolhe ~~subconjuntos~~ *subcolecções* dos axiomas ZF1–ZF6 e tente criar modelos diferentes para cada uma delas. Dê cada modelo em forma dum desenho dum grafo direcionado: o gráfico da relação $\in$ onde os vértices são os objetos (os *sets*, os *conjuntos*), e botamos aresta (seta) de a para b quando «a possui b como membro». Tecnicamente isso seria o gráfico da $\ni$, mas ajuda mais desenhar assim modelos-universos. (x16.78 H 0)

16.127. Linguagem bugada (II): Colecção vs. conjunto. Mais um desafio criado apenas pela terminologia e linguagem que usamos: o termo *conjunto* faz parte da nossa metalinguagem, e lá é usado como um sinónimo dos termos *colecção*, *classe*, *aglomerado*, *grupo*, etc. Mas aqui precisamos separar os dois conceitos diferentes e logo faz sentido adoptar palavras distintas para cada uso. Chamamos então de *conjunto* (ou de *set*) um objeto do universo duma teoria dos conjuntos e reservamos o termo *colecção* para referir à idéia intuitiva. Se for necessário precuramos salientar tal distinção na notação matemática pois ela aparece na nossa metalinguagem também. O mais que nossa maturidade aumenta, o menos que procuramos tais distincções—pois o contexto elimina possíveis confusões para o versado—e o mais que acabamos abusando notações e termos.

A distinção é importante pois não existe necessariamente uma correspondencia entre os dois (aliás, já vimos que na colecção de todos os objetos dum universo, não corresponde um objeto-membro na ZF).

Mas é bem mais que isso. Por exemplo, entendemos o $\wp A$ como «o conjunto de todos os subconjuntos de A». Certo? Sim e não: tanto o *conjunto* quanto o *subconjunto* nessa frase foram usados com o sentido formal da teoria mesmo, como certos objetos que satisfazem certas coisas (tudo isso dentro dum universo).

Olha uma conclusão importante disso:

> «Seja A conjunto.»

traduzindo para a terminologia mais fria de ZF:

> «Seja A objeto.»

e traduzindo para um desenho daqueles que desenhou no Exercício x16.78 isso vira

> «Seja A um vértice no desenho do universo.»

E agora: o que é o $\wp A$? Pensando com nossa meta-cabeça nas meta-palavras *conjunto* e *subconjunto* podemos nos confundir que $\wp A$ seria a colecção de todas as subcolecções de A, entendo também aqui o A como a colecção dos seus membros. Mas na verdade, nosso universo/desenho *pode faltar de certas colecções*, que na nossa meta-cabeca existem, mas no universo não! Mas observe que tal falta não seria perceptível dentro do universo, pois: a palavra *conjunto* significa *objeto* e não *colecção*; similarmente *subconjunto* significa o que foi definido significar e não *subcolecção*; etc.

Isso parece que pode criar uns problemas, quebrando uns teoremas e tal. Por exemplo, o que acontece se umas relações de cardinalidade entre conjuntos ($=_c$ ou $<_c$) que deveriam ser num jeito, parecem não ser? O problema vai embora assim que perceber que a palavra *função* também sofre o mesmo abuso linguístico: temos as funções do nosso meta-mundo, e temos o que definimos para significar *função* dentro dum universo. No caso, entao, as funções que iam criar o problema que tememos com nossos meta-olhos simplesmente não existem no nosso universo! Ou seja, não sao *funções-objetos* mas *metafunções* e logo as definições que demos referindo às funções na teoria dos conjuntos não estão referindo a elas!

Qual o moral da estoria? É uma boa prática no começo reservar uma palavra diferente para o «objeto que satisfaz os axiomas ZF» e outra para a noção intuitiva de «colecção de coisas» (como entendo desde que me lembro de ser humano). Aqui então chamamos a primeira de *conjunto* ou de *set* e a segunda de *colecção* mesmo. E similarmente sobre todos os outros termos que usamos tanto no mundo formal dos objetos quanto na metalinguagem. Usamos os termos *função* para os objetos e *mapeamento* ou *mapa* para o conceito intuitivo. Novamente: abusamos tais coisas com mais experiência e quando o contexto é suficiente para eliminar confusões.

16.128. O paradoxo de Skolem.

TODO Escrever

§338. Outras teorias de conjuntos

TODO Terminar

16.129. Quais axiomas?. Uma outra diferença entre as disciplinas da teoria dos grupos e da teoria dos conjuntos encontra-se na ambiguïdade do segundo termo. Quando encontrar um *teorista dos grupos* trabalhando num outro canto, num outro país, pergunte e veja: o que ele chama de grupo será o que chamamos de grupo aqui também: qualquer coisa que satisfaz os (G0)–(G3) é um grupo e pronto.[113] Porém, não existe *a* teoria dos conjuntos. Os *teoristas dos conjuntos*, têm como um objeto do seu estudo varias teorias diferentes. Em tal teoria dos conjuntos acontece isso, naquela teriamos essa outra coisa, basta substituir tal axioma dela por esses dois, e teremos construido um tal bicho aqui, etc. Isso não acontece em teoria dos grupos!

O que estudamos então na disciplina teoria dos conjuntos poderia ter comecado com: «chamamos de *modelo-ZF1–ZF6* qualquer colecção de objetos com uma relação '$\in$' que satisfaz tais coisas: ...» E depois: «se um modelo-ZF1–ZF6, satisfaz tambem o (ZF7), o chamamos de *modelo-ZF1–ZF7*», etc. Isso é para lembrar das frases como a «se um grupo (isto é, modelo-G0–G3) satisfaz o (G4), chamamos de *grupo abeliano* (isto é, modelo-G0–G4)».

E todas essas teorias de conjuntos são equivalentes? Umas são, mas em geral não—ainda bem, pois não teria graça assim! Observe que já encontramos várias que não são (todas baseadas nos ZF) simplesmente adicionando ou não algum dos próximos axiomas; e, alem disso, podemos adicionar *negações* de tais axiomas e acabar com teorias *equiconsistentes:* se uma é consistente, entao a outra também é e vice versa.

[113] Pequenas diferenças podem aparecer como já mencionamos em outras disciplinas, como a teoria dos anéis—tem 1 ou não?—mas mesmo assim não chegam ser algo tão assumidamente (e propositadamente) diverso.

16.130. ZF, ZFC, NBG, NF, MK. Tem outras teorias dos conjuntos mais diferentes, as mais famosas seriam as: *NBG* (von Neumann–Bernays–Gödel); *NF* (New Foundations, de Quine); e *MK* (Morse–Kelley). NBG e MK têm a noção de *classe* dentro delas (lembre se que ZF não possui classes formalmentes, ficaram por fora, e apareceram só no meta-mundo). NF possui um objeto-universo dentro dela e mesmo assim não permite Russell explodir o mundo: em vez de limitar a parte esquerda do set builder, limita a parte direita (o filtro).

§339. Outras fundações

TODO ETCS, MLTT, HoTT

TODO connection with unityped vs. statically typed languages

Problemas

▸ **PROBLEMA Π16.10.**
Seja a conjunto. *Sem usar* o Separation (ZF4), mostre pelo resto dos axiomas que as classes seguintes são conjuntos:

$$E = \left\{ \left\{ x, \bigcup x, \wp x \right\} \;\middle|\; x \in a \right\}; \qquad F = \{\, x \mid x \subsetneq a \,\}; \qquad G = \left\{ x \mid x \neq \emptyset \wedge x = \bigcap x \right\}.$$

(Π16.10 H 0)

▸ **PROBLEMA Π16.11 (Replacement is the new Separation—or is it?).**
Podemos tirar o Separation scheme (ZF4) dos nossos axiomas "sem perder nada", se temos o Replacement scheme (ZF8) no lugar dele? (Π16.11 H 1 2)

▸ **PROBLEMA Π16.12 (Replacement is the new Pairset—or is it?).**
Podemos tirar o Pairset (ZF3) dos nossos axiomas "sem perder nada", se temos o Replacement scheme (ZF8) no lugar dele? (Π16.12 H 1 2)

▸ **PROBLEMA Π16.13.**
Na resolução do Exercício x16.24, tem um roubo. Ache e explique. (Π16.13 H 0)

▸ **PROBLEMA Π16.14.**
No Exercício x16.25 demonstraste que a operação binária definida pela

$$\langle x, y \rangle \stackrel{\text{def}}{=} \{x, \{x, y\}\}$$

satisfaz a propriedade (TUP2). Depois, no Exercício x16.72, usando o (ZF9) conseguimos demonstrar que satisfaz a propriedade (TUP1) também. Mostre que o (ZF9) é necessário para conseguir isso, mostrando um contraexemplo: conjuntos a, b, a', b' tais que

$$\langle a, b \rangle = \langle a', b' \rangle$$

mas mesmo assim pelo menos uma das $a = a'$ e $b = b'$ não é válida. (Π16.14 H 1 2 3)

▸ **PROBLEMA Π16.15.**
Mostre que o Choice (AC) é equivalente com o seguinte axioma:
Choice (Rel). *Se uma relação $R \in \mathrm{Rel}\,(A, B)$ tem a propriedade de totalidade, então existe função $f : A \to B$ com $x\ R\ f(x)$ para todo $x \in A$.*

(ACrel) $$\big(R \in \mathrm{Rel}\,(A,B) \wedge \mathrm{dom}\,R = A\big) \to \big((\exists f : A \to B)(\forall x \in A)[\,x\ R\ f(x)\,]\big)$$

(Π16.15 H 0)

▸ **PROBLEMA Π16.16 (Reais como seqüências Cauchy).**

TODO Enunciar o problema

(Π16.16 H 0)

Leitura complementar

[VH67], [Hal60], [Mos05], [Kun09]. [Kun11], [Coh12], [Kun80], [Kri71], [Jec13], [Kan03].
Sobre teoria dos conjuntos construtiva: [AR10].

CAPÍTULO 17

ESPAÇOS MÉTRICOS

Logo depois do desenvolvemento da teoria de conjuntos de Cantor, no ano 1906 Fréchet introduziu os *espaços métricos* na sua tese de doutorado **[Fré06]**. Neste capítulo estudamos as primeiras idéias básicas.

§340. Distáncias

D17.1. "Definição" (espaço métrico). Um *espaço métrico* é um conjunto equipado com uma noção de *distância* entre quaisquer dois membros dele em tal forma que:

- a distância de cada ponto para ele mesmo é 0;
- a distância entre pontos distintos é positiva;
- a distância de x para y é a mesma da de y para x;
- as distâncias satisfazem a desigualdade triangular.

Bora formalizar:

D17.2. Definição (espaço métrico). Seja X conjunto. Uma função $d : X^2 \to \mathbb{R}$ é chamada *métrica* no X sse:

$$
\begin{aligned}
&d(x,y) \geq 0 && \text{não-negatividade}\\
&d(x,x) = 0 \\
&d(x,y) = d(y,x) && \text{simetria}\\
&d(x,y) \leq d(x,w) + d(w,y). && \text{triangular}\\
&d(x,y) = 0 \implies x = y
\end{aligned}
$$

Chamamos a última *desigualdade triangular*, e dados pontos $x, y \in X$ chamamos o valor $d(x,y)$ de *d-distância* entre os x, y, omitindo o prefixo '*d-*' quando a métrica é implicita pelo contexto. Um conjunto estruturado $(X\,;\,d)$ onde d é uma métrica no X é chamado *espaço métrico*.

D17.3. Definição (pré-métrica). Uma função $d : X^2 \to \mathbb{R}$ que satisfaz as primeiras 4 propriedades da Definição D17.2 é chamada *pré-métrica* (ou *pseudométrica*).

► **EXERCÍCIO x17.1.**
Justifique o nome «pré-métrica». (x17.1 H 0)

• **EXEMPLO 17.4.**
Os reais $(\mathbb{R}\,;\,d)$ onde

$$d(x,y) = |x-y|\,.$$

• **EXEMPLO 17.5.**
O plano euclideano $(\mathbb{R}^2\,;\,d)$ onde

$$d(\langle x_1, x_2\rangle\,,\langle y_1, y_2\rangle) = \sqrt{(x_1-y_1)^2+(x_2-y_2)^2}.$$

• **EXEMPLO 17.6.**
Seja X um conjunto e defina a função $d : X^2 \to \mathbb{R}$ pela

$$d(x,y) = \begin{cases} 0, & \text{se } x = 0 \\ 1, & \text{caso contrário.} \end{cases}$$

O $(X\,;\,d)$ é um espaço métrico.

Esse espaço é bastante importante e merece seu próprio nome:

D17.7. Definição (discreto). Dado conjunto X, a *métrica discreta* nele é a função $d : X^2 \to \mathbb{R}$ definida pela

$$d(x,y) = \begin{cases} 0, & \text{se } x = y \\ 1, & \text{caso contrário.} \end{cases}$$

O $(X\,;\,d)$ é chamado *espaço métrico discreto*.

▸ **EXERCÍCIO x17.2.**
Donde chegou essa d do Exemplo 17.5? (x17.2H1)

▸ **EXERCÍCIO x17.3.**
Qual seria a métrica "standard" do $\mathbb{R}^3$? (x17.3H0)

Em qualquer espaço métrico, podemos definir a noção de ε-perto:

D17.8. Definição (ε-perto). Sejam $x, y \in X$ e $\varepsilon > 0$. Dizemos que

$$x, y \text{ são } \varepsilon\text{-perto} \overset{\text{def}}{\iff} d(x,y) < \varepsilon.$$

Assim temos de graça a definição de limite. Literalmente copiamos a Definição D6.83:

D17.9. Definição (limite). Seja $(a_n)_n$ uma seqüência num espaço métrico $(X\,;\,d)$. Dizemos que $(a_n)_n$ *tende ao limite* ℓ sse a partir dum membro a_N, todos os seus membros ficam ε-perto do ℓ. Ou seja:

$$(a_n)_n \to \ell \overset{\text{def}}{\iff} (\forall \varepsilon > 0)(\exists N \in \mathbb{N})(\forall i \geq N)[\,a_i \text{ é } \varepsilon\text{-perto de } \ell\,].$$

Escrevemos

$$\lim_n a_n = \ell$$

como sinônimo de $(a_n)_n \to \ell$. ↯

! **17.10. Cuidado.** Lembra do erro da Definição D6.83 que descobreste no x6.104? Pois é, junto com a definição, copiamos seu errinho também, mas não ganhamos de graça sua resolução, pois a demonstração de unicidade de limites (Teorema Θ6.90) usou a definição de *ε-perto* dos reais, e aqui isso mudou. Então sim, tu tens um trabalho pra fazer agora:

▸ **EXERCÍCIO x17.4 (Unicidade de limites (espaços métricos)).**
Demonstre a unicidade dos limites. (x17.4H1)

§341. Exemplos e nãœxemplos

§342. Conjuntos abertos e fechados

D17.11. Definição. Um conjunto $A \subseteq X$ é *aberto* (ou *open*) sse todo $a \in A$ tem bola contida no A:

$$A \text{ aberto} \overset{\text{def}}{\iff} (\forall a \in A)(\exists \varepsilon > 0)[\, \mathcal{B}_\varepsilon(a) \subseteq A \,].$$

▸ **EXERCÍCIO x17.5.**
Em todo espaço métrico $(X\,;d)$, X e $\emptyset$ são abertos. (x17.5H0)

▸ **EXERCÍCIO x17.6.**
Cada bola $\mathcal{B}_\varepsilon(x)$ é um conjunto aberto. (x17.6H0)

D17.12. Definição. Sejam $N \subseteq X$ e $a \in X$. Dizemos que A é uma *vizinhança* (ou *neighborhood*, ou *nbhd*) de x sse N contenha uma bola de a:

$$N \text{ vizinhança de } a \overset{\text{def}}{\iff} (\exists \varepsilon > 0)[\, \mathcal{B}_\varepsilon(a) \subseteq N \,]$$

▸ **EXERCÍCIO x17.7.**
Demonstre ou refute a afirmação: «cada vizinhança é um conjunto aberto». (x17.7H1)

▸ **EXERCÍCIO x17.8.**
Intersecção binária de abertos é aberto. (x17.8H0)

▸ **EXERCÍCIO x17.9.**
Intersecções finitas de abertos são abertos. (x17.9H0)

▸ **EXERCÍCIO x17.10.**
Uniões arbitrárias de abertos são abertos. (x17.10H0)

D17.13. Definição (puncturados). Chamamos a $\mathcal{B}_\varepsilon(a) \setminus \{a\}$ de *bola puncturada* do a. Similarmente, se e N é uma vizinhança de a, chamamos o $N \setminus \{a\}$ de *vizinhança puncturada* de a.

D17.14. Definição (limit point, conjunto derivado). Sejam $A \subseteq X$ e $\ell \in X$. Chamamos o ℓ um *limit point* de A sse existe seqüência $(a_n)_n \subseteq A \setminus \{\ell\}$ que tende ao ℓ:

$$(a_n)_n \to \ell.$$

Usamos o termo *ponto de acumulação* como sinônimo. Chamamos o conjunto de todos os limit points de A de *conjunto derivado de* A e o denotamos por A'.

17.15. Critérion. *Sejam $A \subseteq X$ e $\ell \in X$.*

$$\ell \text{ limit point de } A \iff \text{toda bola puncturada de } \ell \text{ intersecta o } A.$$

D17.16. Definição. Um conjunto $A \subseteq X$ é *fechado* sse A é fechado sob a operação de limites, ou seja, sse todos os limit points do A estão no A, ou seja:

$$A \text{ fechado} \overset{\text{def}}{\iff} (\forall \ell \in X)[\,\ell \text{ limit point de } A \implies \ell \in A\,].$$

17.17. Critérion. *Um conjunto $A \subseteq X$ é fechado sse seu complemento $X \setminus A$ é aberto.*

§343. Continuidade

D17.18. Definição. Sejam $f : (X\,;\,d) \to (Y\,;\,\rho)$ e $x_0 \in X$. Chamamos a f de *contínua no* x_0 sse:

$$(\forall \varepsilon > 0)(\exists \delta > 0)(\forall x \in X)[\,x_0, x \text{ são } \delta\text{-perto} \implies fx_0, fx \text{ são } \varepsilon\text{-perto}\,];$$

ou, equivalentemente:

$$(\forall \varepsilon > 0)(\exists \delta > 0)[\,f[\mathcal{B}_\delta(x_0)] \subseteq \mathcal{B}_\varepsilon(fx_0)\,].$$

Chamamos f de *contínua* sse f é contínua em cada $x \in X$.

§344. Completude

D17.19. Definição (complete). Um espaço metrico em qual todas as seqüências Cauchy convergem é chamado *completo*.

§345. Compacidade

D17.20. Definição. Um espaço métrico é chamado *compacto* sse é totalmente limitado e completo.

§346. Pouco de cats—categorias e espaços métricos

Problemas

Leitura complementar

[Sim68], [KF99], [Car00].

"Baby Rudin" [Rud76].

CAPÍTULO 18

TOPOLOGIA

§347. O que é uma topologia

18.1. Vocabulário topológico. Num espaço topológico podemos falar de conjuntos *abertos* e de conjuntos *fechados*; para qualquer conjunto podemos falar so seu *fecho*, seu *interior*, e seu *derivado*; e falar de *pontos de acumulação*, de *vizinhanças*, de *compacidade*, *conexividade*, *separabilidade*, e por aí vai. O conceito mais fundamental que queremos capturar com a introdução de espaços topológicos é da *continuidade*. Sim, o vocabulário topológico é bem grande mesmo; mas é aplicável em tantas situações diferentes que aprendê-lo, e se acostumar com as noções envolvidas acaba sendo um investimento numa ferramenta versátil não apenas de comunicação mas de pensamento também: na mesma maneira que temos elaborado pensamento algébrico, analítico, categorial, vamos elaborar um *pensamento topológico*.

TODO Relacionar com vocabulário categórico

§348. Especificações equivalentes

Queremos estabelecer logo as noções seguintes: conjunto *aberto*, conjunto *fechado*, *vizinhança* de ponto, *pontos de acumulação* de um conjunto, *fecho* de conjunto, *interior* de conjunto, função *contínua*. Cada especificação que encontramos aqui considera uma dessas como noção primitiva, e logo procede para obter o resto como definidas. Nesta secção estabelecemos a equivalência entre essas especificações através de qual ganhamos nossa primeira experiência com as idéias elementares de topologia. E a partir da próxima seção começamos o estudo das demais noções dos espaços topológicos; tentando trabalhar numa maneira agnóstica, ou seja, sem escolher uma especificação especifica.

S18.2. Especificação (Espaço de opens). Chamamos o $(X\,;\mathcal{O})$ de *espaço de opens* onde $\mathcal{O}$ é uma coleção de subconjuntos de X

$$\mathcal{O} : \wp\wp X$$

e onde as leis seguintes são satisfeitas:

$\mathcal{O}$ é fechado sob interseções finitas;
$\mathcal{O}$ é fechado sob uniões (arbitrárias).

Chamamos os membros da $\mathcal{O}$ de *opens* (abertos).

S18.3. Especificação (Espaço de hoods). Chamamos o $(X\,;\mathcal{N})$ de *espaço de vizinhanças* (neighborhoods, ou hoods, ou nbhds) onde $\mathcal{N}$ é uma coleção de subconjuntos de X

$$\mathcal{N} : \wp\wp X$$

e onde as leis seguintes são satisfeitas:

$$\begin{aligned}&\text{todo ponto mora em alguma nbhd;}\\ &p \in N_1 \cap N_2 \implies (\exists N)[\, p \in N \subseteq N_1 \cap N_2\,].\end{aligned}$$

Chamamos os membros da $\mathcal{N}$ de *nbhds* ou de *vizinhaças*.

S18.4. Especificação (Espaço de hoodsystems). Chamamos o $(X\,;(\mathcal{N}_x \mid x \in X))$ de *espaço de hood-systems* onde $(\mathcal{N}_x)_x$ é uma X-família de coleçoẽs de subconjuntos de X, ou seja, para cada $x \in X$,

$$\mathcal{N}_x : \wp\wp X$$

e onde para cada $x \in X$ as leis seguintes são satisfeitas:

$$\begin{aligned}&x \in \bigcap \mathcal{N}_x\\ &\mathcal{N}_x \text{ é um filtro no } \wp X\\ &(\forall N \in \mathcal{N}_x)(\exists N \supseteq M \in \mathcal{N}_x)(\forall m \in M)[\, M \in \mathcal{N}_m\,].\end{aligned}$$

Chamamos o $\mathcal{N}_x$ de *sistema de x-nbhds*, e seus membros de *x-nbhds*.

S18.5. Especificação (Espaço de closure). Chamamos o $(X\,;\operatorname{clos}_{_})$ de *espaço de closure* onde

$$\operatorname{clos}_{_} : \wp X \to \wp X$$

e onde para cada $A, B \subseteq X$ as leis seguintes são satisfeitas:

$$\begin{aligned}&\operatorname{clos}\emptyset = \emptyset;\\ &A \subseteq \operatorname{clos} A;\\ &\operatorname{clos}\operatorname{clos} A = \operatorname{clos} A;\\ &\operatorname{clos} A \cup B = \operatorname{clos} A \cup \operatorname{clos} B.\end{aligned}$$

Chamamos o $\operatorname{clos} A$ de *fecho de A*.

D18.6. Definição (topologia). Dado um espaço $\mathcal{S} \equiv (S\,;\ldots)$ onde a noção de conjunto aberto é disponível (primitiva ou definida), chamamos de *topologia de $\mathcal{S}$* a coleção de todos os conjuntos abertos de $\mathcal{S}$:

$$\mathcal{O}\mathcal{S} \stackrel{\text{def}}{=} \{\, O \subseteq S \mid O \text{ aberto}\,\}.$$

Escrevemos apenas $\mathcal{O}$ se o espaço é implícito pelo contexto.

▸ **EXERCÍCIO x18.1.**
Dualize a Especificação S18.2 para chegar na especificação que tem como noção primitiva os *fechados*. (x18.1 H 0)

▸ **EXERCÍCIO x18.2.**
Dualize a Especificação S18.5 para chegar na especificação que tem como noção primitiva a operação de *interior*. (x18.2H0)

§349. Uns espaços topológicos

18.7. Sierpinski. O espaço de Sierpiński possui só dois pontos: $\bot, \top$, e sua topologia considera o $\{\top\}$ de aberto além dos $\emptyset$ e $\{\bot, \top\}$, que é obrigada a considerar abertos também:

$$\mathcal{O} \stackrel{\text{def}}{=} \{\emptyset, \{\top\}, \{\bot, \top\}\}.$$

§350. Noções topológicas

Já temos acesso a todas as noções de: *aberto*, *fechado*, *vizinhança*, *vizinhança de ponto*, *topologia*; foram estabelecidas na secção anterior ou como primitivas ou como definidas (dependendo da especificação). Aqui investigamos mais noções topológicas para introduzir, agora em termos do que já temos. *pontos de acumulação* de um conjunto, *fecho* de conjunto, *interior* de conjunto. Em tudo que segue, X é um espaço topológico, p um ponto dele, e A um subconjunto dele.

D18.8. Definição (ponto de acumulação). Dizemos que p é um *ponto de acumulação* de A sse qualquer vizinhança $N_p \in \mathcal{N}(p)$ interseta o A em maneira essencial, ou seja, possui outros pontos de A. Sinônimos: *ponto de limite* de A, *ponto de cluster* de A.

D18.9. Definição (derivado). Denotamos por $\operatorname{deriv} A$ o conjunto de todos os pontos de acumulação de A:

$$\operatorname{deriv} A \stackrel{\text{def}}{=} \{\, x \mid x \text{ é um ponto de acumulaçào de } A \,\}.$$

D18.10. Definição (ponto isolado). Dizemos que p é um *ponto isolado* de A sse $p \in A$ e existe p-vizinhança que interseta A apenas no p:

$$N \cap A = \{p\}.$$

D18.11. Notação. Escrevemos aplicações repetidas em forma de expoentes sem parenteses, entendendo por exemplo que

$$A^{\circ-\flat\mathsf{c}\prime} \equiv ((((A^{\circ})^{-})^{\flat})^{\mathsf{c}})'.$$

Essa forma de escrever é conveniente quando queremos enfatisar uma ordem *diagramática* ou *imperativa* que descreve como chegar no conjunto descrito em passos. Pelo contrário escrevendo assim:

$$((((\operatorname{inte}(A))^{-})^{\flat})^{\mathsf{c}})'$$

o mesmo conjunto é descrito em ordem *composicional* ou *declarativa*, que enfatisa o que o (mesmo) conjunto *é*, no sentido contrário.

D18.12. Definição (fecho).

TODO Escrever

D18.13. Definição (denso). O conjunto A é chamado *denso* sse $A^- = X$.

D18.14. Definição (separável). Chamamos o espaço X de *separável* sse existe conjunto denso e contável.

D18.15. Definição (ponto interior). Chamamos p de *ponto interior* de A sse A é uma vizinhança de p.

D18.16. Definição (interior). O *interior de* A, denotado por A°, é o conjunto de todos os pontos de interior de A:

$$A^\circ \stackrel{\text{def}}{=} \{\, x \mid x \text{ é ponto interior de } A \,\}.$$

▸ **EXERCÍCIO x18.3.**
A aberto $\iff A = A^\circ$. (x18.3H0)

▸ **EXERCÍCIO x18.4.**
A° é o *melhor* aberto contido no A. (x18.4H0)

D18.17. Definição (boundary). Dizemos que p é ponto de fronteira de A sse toda p-vizinhança interseta ambos os A e $A^\complement$. Chamamos de *fronteira* (ou *boundary*) de A o conjunto de todos eles e denotamos por

$$A^\flat \stackrel{\text{def}}{=} \{\, x \mid x \text{ é ponto de fronteira de } A \,\}.$$

▸ **EXERCÍCIO x18.5.**
Os pontos de fronteira de A são exatamente os pontos que não são interiores nem de A nem de $A^\complement$. (x18.5H0)

▸ **EXERCÍCIO x18.6.**
Complete as equações em forma interessante, e demonstre:

(1) $(A^\complement)^\flat = ?$;
(2) $A^\flat = A^- \cap ?$;
(3) $A^\flat = A^- \setminus ?$;
(4) $(A^\flat)^\complement = ?$;
(5) $A \cup A^\flat = ?$;
(6) $A \setminus A^\flat = ?$.

(x18.6H0)

!! SPOILER ALERT !!

▸ **EXERCÍCIO x18.7.**
Demonstre:

(1) $A^\flat = (A^\complement)^\flat$;
(2) $A^\flat = A^- \cap (A^\complement)^-$;
(3) $A^\flat = A^- \setminus A^\circ$;
(4) $(A^\flat)^\complement = A^\circ \cup (A^\complement)^\circ$;
(5) $A^- = A \cup A^\flat$;
(6) $A^\circ = A \setminus A^\flat$.

(x18.7H1)

§351. Continuidade

18.18. Cadê as setas?. Chega! Todo esse tempo falando de espaços topológicos (os objetos-ilhas desse mundo) sem falar ainda quais são as setas-transportes que nos levam de um para outro! Finalmente as conhecemos: *são as funções contínuas*— só que precisamos definir o que isso significa, já que as definições que temos encontrado até agora todas dependem de algo não necessariamente presente num espaço topológico: uma noção de distância. Antes de continuar lendo, tente definir em forma compatível: tua definição, quando aplicada a um espaço métrico, deveria concordar com a definição que já temos.

D18.19. Definição (contínua em ponto). Sejam $p \in X \xrightarrow{f} Y$. Dizemos que f é *contínua no p* sse para toda vizinhança E de $f\,p$, existe vizinhança D de p tal que $f[D] \subseteq E$.

Um imaginaria que tendo definido o que significa *contínua num ponto do domínio* definiríamos *contínua* para significar *contínua em cada ponto do seu domínio*. Conseguimos uma definição melhor que nem precisa olhar para os pontinhos dos espaços envolvidos:

D18.20. Definição (contínua). Sejam $X \xrightarrow{f} Y$. Dizemos que f é *contínua no t* sse f reflete os abertos, ou seja: para qualquer Y-aberto $V \ni f\,t$, $f_{-1}[V]$ é X-aberto.

▸ **EXERCÍCIO x18.8.**
Sejam $X \xrightarrow{f} Y$.

$$f \text{ contínua} \iff (\forall x \in X)[\, f \text{ contínua no } x\,].$$

(x18.8 H 0)

▸ **EXERCÍCIO x18.9.**
Sejam $X \xrightarrow{f} Y$. Os seguintes são equivalentes:
(i) f contínua;
(ii) para todo $A \subseteq X$, $f[A^-] \subseteq \operatorname{clos}(f[A])$;
(iii) f reflete os fechados.

(x18.9 H 0)

▸ **EXERCÍCIO x18.10.**
Mostre que as funções continuas servem como setas. (x18.10 H 1)

O erro mais comum sobre a definição de continua é pensar que ela *preserva* em vez de *refletir* os opens. De fato, esse conceito tem seu próprio nome:

D18.21. Definição (mapa aberto). Sejam $X \xrightarrow{f} Y$. Dizemos que f é um *mapa aberto* sse f preserva os abertos, ou seja: para qualquer X-aberto $U \ni t$, $f[U]$ é Y-aberto.

§352. Bases

D18.22. Definição (base local (de ponto)). Sejam X um espaço topológico e p um ponto dele. Chamamos uma coleção $\mathcal{B}_p$ de p-vizinhanças de *base local no p* sse qualquer p-vizinhança contem um membro de $\mathcal{B}_p$:

$$\mathcal{B} \text{ base local no } p \iff (\forall N_p \in \mathcal{N}(p))(\exists B_p \in \mathcal{B}_p)[\, B_p \subseteq N_p \,]$$

Também chamamos a $\mathcal{B}_p$ de uma *base para o sistema de vizinhanças de p*.

D18.23. Definição (base de espaço). Seja X um espaço topológico e $\mathcal{B}$ uma coleção de abertos. Chamamos a $\mathcal{B}$ de *base para a topologia de X* sse para qualquer ponto p e qualquer p-vizinhança N_p, existe membro $B \in \mathcal{B}$ tal que

$$(\forall p \in X)(\forall N_p \in \mathcal{N}(p))(\exists B \in \mathcal{B})[\, p \in B \subseteq V_p \,]$$

18.24. Critérion. *Seja X um espaço topológico e $\mathcal{B}$ uma coleção de abertos.*

$$\mathcal{B} \text{ base} \iff \text{todo } X\text{-aberto é união de membros de } \mathcal{B}.$$

Demonstrarás agora no Exercício x18.11. ∎

▸ **EXERCÍCIO x18.11.**
Demonstre o Critérion 18.24. (x18.11 H 0)

18.25. Contabilidades. Olhando na cardinalidades de bases chegamos em duas propriedades destacáveis de certos espaços topológicos, com os nomes (infelizes) primeiro-contável e segundo-contável:

D18.26. Definição (primeiro-). Um espaço topológico é *primeiro-contável* sse todo ponto possui uma base local contável.

D18.27. Definição (segundo-). Um espaço topológico é *segundo-contável* sse ele possui uma base contável.

▸ **EXERCÍCIO x18.12.**
Seja X espaço topológico.

$$X \text{ segundo-contável} \implies X \text{ primeiro-contável.}$$

(x18.12H0)

▸ **EXERCÍCIO x18.13 (Lindelöf).**
Sejam X segundo-contável, e $G = \bigcup_\alpha G_\alpha$ um aberto que é união de abertos. Logo G pode ser escrito como união contável desses G_α's. (x18.13H0)

▸ **EXERCÍCIO x18.14.**
Qualquer espaço métrico separável é segundo-contável. (x18.14H0)

§353. Construções

18.28. Dois extremos: discreta e indiscreta. Qualquer topologia num conjunto X é obrigada considerar os $\emptyset$ e X abertos. Quando esses são os únicos abertos, chamamos a topologia *indiscreta*:

$$\{\emptyset, X\}.$$

Por outro lado extremo, a topologia que considera *todos* os conjuntos abertos é a *discreta*:

$$\wp X.$$

Ass

18.29. Subbase.
TODO Escrever

18.30. Soma.
TODO Escrever

18.31. Produto.
TODO Escrever

▸ **EXERCÍCIO x18.15 (Box).**

TODO Escrever

(x18.15 H 0)

18.32. Soma.

TODO Escrever

18.33. Quociente.

TODO Escrever

18.34. Poset.

TODO Escrever

18.35. Ordem.

TODO Escrever

§354. Compacidade

D18.36. Definição (compacto). Sejam X espaço topológico e $K \subseteq X$. Dizemos que K é *compacto* sse cada cobertura aberta de K possui subcobertura aberta finita.

! **18.37. Cuidado (O que compacidade não é).** É comum pensar que o desafio é encontrar uma cobertura finita. Isso seria trivial: dá para achar cobertura não apenas finita, mas usando só um aberto até: a $\{X\}$ é de fato uma cobertura aberta de K (qualquer que seja esse K), feita por um conjunto aberto só. O desafio é conseguir achar uma *subcobertura finita* de uma dada *cobertura* (escolhida por teu inimigo). O jogo então é o seguinte: eu escolho uma cobertura, e tu escolha uma subcobertura da minha. Para defender que um conjunto é compacto então, precisa achar uma estratégia vencedora para esse jogo.

• **EXEMPLO 18.38.**
Considere a reta dos reais $\mathbb{R}$, com sua topologia comum. Se eu escolher

Relaxando o finito para contável chegamos no conceito de espaço de Lindelöf:

D18.39. Definição (Lindelöf). Sejam X espaço topológico e $L \subseteq X$. Dizemos que L é *Lindelöf* sse cada cobertura aberta de L possui subcobertura aberta contável.

§355. Conexidade

D18.40. Definição (conexo). Seja X espaço topológico. Dizemos que X é *conexo* sse X não pode ser escrito como união de dois conjuntos disjuntos, abertos, e habitados.

► **EXERCÍCIO x18.16.**
Para qualquer espaço topológico X,

$$X \text{ conexo} \iff \text{os únicos clopens de } X \text{ são os: } \emptyset, X.$$

(x18.16 H 0)

D18.41. Definição (caminho). Sejam a, b pontos de um espaço topológico X. Chamamos de *caminho de a para b* qualquer função continua $f : \mathbb{I} \to X$ que satisfaz:

$$f\ 0 = a; \qquad\qquad f\ 1 = b.$$

Costumamos visualizar tais caminhos como um ponto móvel num intervalo de tempo onde $f\ t$ representa a posição do ponto no tempo t e onde tal movimento começa no $a = f\ 0$ e termina no $b = f\ 1$.

D18.42. Definição (conexo por caminho). Seja X espaço topológico. Dizemos que X é *conexo por caminhos* sse para quaisquer $a, b \in X$, existe *caminho* de a para b no X.

► **EXERCÍCIO x18.17.**
Para qualquer espaço topológico X,

$$X \text{ conexo por caminhos} \implies X \text{ conexo.}$$

(x18.17 H 0)

§356. Separações

Pelos olhos de um espaço topológico podemos enxergar conjuntos e pontos mas o quão bem podemos distingüi-los e separá-los varia. Considere o espaço indiscreto com 2 pontos $0, 1$. A topologia deste espaço não permite perceber nenhuma diferença (topológica) entre os dois: aqui só tem dois conjuntos abertos: o vazio, a qual nenhum dos dois pontos pertence, e o espaço inteiro, a qual ambos pertencem. Por outro lado, no espaço de Sierpinski os dois pointos são distingüíveis, já que temos um aberto a qual $\top$ pertence e $\bot$ não. Há muitas maneiras de *separar* coisas dum espaço topológico e, dependendo do nível e da maneira que estamos querendo separar, chegamos em conceitos diferentes. Nesta seção vamos conhecer uns deles.

Os primeiros axiomas estão se referindo à separação entre dois pontos do espaço.

D18.43. Definição (Kolmogorov). Dizemos que X é um espaço de *Kolmogorov*, sse para quaisquer dois pontos distintos de X existe vizinhança de um a qual não pertence o outro.

D18.44. Definição (Frechet). Dizemos que X é um espaço de *Fréchet*, sse para quaisquer dois pontos distintos de X existem vizinhanças de cada um a qual não pertence o outro.

▸ **EXERCÍCIO x18.18.**
Seja X um espaço topológico.

$$X \text{ Fréchet} \iff \text{todo } p \in X \text{ é fechado.}$$

(x18.18 H 0)

D18.45. Definição (Hausdorff). Dizemos que X é um espaço de *Hausdorff*, sse para quaisquer pontos $p \neq q$ de X existem vizinhanças disjuntas: P de p e Q de q.

▸ **EXERCÍCIO x18.19.**
Sejam H um espaço Hausdorff, K um subespaço compacto de H e p um ponto fora do K. Logo K e p podem ser separados por abertos assim: existem abertos disjuntos U, P tais que $U \supseteq K$, $P \ni p$. (x18.19 H 0)

▸ **EXERCÍCIO x18.20.**
Seja H um espaço Hausdorff. Todo subespaço compacto de H é fechado. (x18.20 H 0)

O próximo separa conjuntos de pontos fora deles:

D18.46. Definição (regular). Dizemos que X é um espaço *regular*, sse para qualquer fechado F e qualquer ponto $p \notin F$, existem conjuntos abertos e disjuntos G, P com $G \supseteq F$ e $P \ni p$.

D18.47. Definição (normal). Dizemos que X é um espaço *normal*, sse para quaisquer fechados disjuntos F, F', existem abertos disjuntos G, G' com $G \supseteq F$ e $G' \supseteq F'$.

Θ18.48. Lema de Urysohn. *Sejam A, B disjuntos fechados de um espaço normal X. Seja $[\alpha, \beta]$ um intervalo de reais. Logo existe função continua*

$$f : X \to [\alpha, \beta]$$

tal que $f[A] = \{\alpha\}$ e $f[B] = \{\beta\}$.

▸ Esboço. TODO. □

§357. Convergências

§358. Pouco de cats—categorias e espaços topológicos

Problemas

▸ **PROBLEMA Π18.1 (Cantor vs. Reais: 1884).**
Encontramos aqui a segunda demonstração de Cantor sobre a incontabilidade dos reais, [Can84]. Cantor definiu os conceitos de ponto de acumulação, conjunto fechado, conjunto denso em todo lugar, e conjunto perfeito. Demonstre que:

(i) qualquer conjunto perfeito e não vazio é incontável;
(ii) o intervalo $[0,1]$ da reta real é perfeito;

concluindo assim que o $[0,1]$ é incontável. (Π18.1 H 0)

▸ **PROBLEMA Π18.2.**
Por que não podemos usar o mesmo argumento para concluir que o $\{\, q \in \mathbb{Q} \mid a \leq q \leq b \,\}$ também é incontável? (Π18.2 H 0)

Leitura complementar

[Jä95], [Sim68], [Mun00], [Wil12].
[Vic96], [Esc04].
[Joh86].

CAPÍTULO 19

TEORIA DOS TIPOS

Problemas

Leitura complementar

[NG14]. [GLT89]. [NPS90]. [Pie02]. [Uni13].

CAPÍTULO 20

LAMBDAS E COMBINADORES

§359. O λ-calculus não-tipado

§360. Representando matemática fielmente

§361. Programmando

§362. Recursão e fixpoints

§363. Programação funcional revisitada

§364. Lógica de combinadores

D20.1. Definição.

$$\mathsf{I}\,x \triangleright x \qquad \mathsf{B}\,x\,y\,z \triangleright x\,(y\,z) \qquad \mathsf{S}\,x\,y\,z \triangleright x\,z\,(y\,z) \qquad \mathsf{R}\,x\,y\,z \triangleright y\,z\,x$$

$$\mathsf{K}\,x\,y \triangleright x \qquad \mathsf{B}'\,x\,y\,z \triangleright y\,(x\,z) \qquad \mathsf{W}\,x\,y \triangleright x\,y\,y \qquad \mathsf{V}\,x\,y\,z \triangleright z\,x\,y$$

$$\mathsf{M}\,x \triangleright x\,x \qquad \mathsf{C}\,x\,y\,z \triangleright x\,z\,y$$

▸ **EXERCÍCIO x20.1.**
Mostre que o combinador $\mathsf{S}\ \mathsf{K}\ (\mathsf{W}\ (\mathsf{I}\ \mathsf{B}))$ comporta como o I. (x20.1 H 0)

▸ **EXERCÍCIO x20.2.**
Mostre que o combinator $\mathsf{C}\ (\mathsf{W}\ \mathsf{K})\ \mathsf{K}\ \mathsf{W}$ comporta como o I. (x20.2 H 0)

▸ **EXERCÍCIO x20.3.**
Defina o B' dos I, M, B, C. (x20.3 H 0)

▸ **EXERCÍCIO x20.4.**
Defina o R dos I, K, M, B, B', C, S, W. (x20.4 H 0)

▸ **EXERCÍCIO x20.5.**
Defina o V dos I, K, M, B, B', C, S, W, R. (x20.5 H 0)

Leitura complementar

Problemas

▸ **PROBLEMA Π20.1.**
Suponha que já temos definido um λ-term $\underline{\texttt{minus}}$, que comporta corretamente, no sentido que:

$$\underline{\texttt{minus}}\ \underline{n}\ \underline{m} \twoheadrightarrow \begin{cases} \underline{n-m}, & \text{se } n \geq m \\ \underline{0}, & \text{se } n < m. \end{cases}$$

Explique o comportamento do termo

$$\underline{\texttt{f}} := \lambda n\,.\,n\ (\underline{\texttt{minus}}\ \underline{1})\ \underline{0}$$

quando for aplicado para um numeral de Church $\underline{k}$: qual é a função $f : \mathbb{N} \to \mathbb{N}$ que o termo $\underline{\texttt{f}}$ computa? (Π20.1 H 1)

Leitura complementar

Lambda calculus: [NG14], [SU06]. [HS08], [Kri93]. [Bar13].
Lógica de combinadores: [Smu85], [Bim11], [HS08].

CAPÍTULO 21

SEMÂNTICA DENOTACIONAL

Problemas

Leitura complementar

Semântica denotacional de linguagens de programação: [Sto77], [Win93], [Ten76], [Ten91], [Gun92].

Especificamente sobre domínios para programação funcional: [Str06].

E para programação lógica: [Llo87].

CAPÍTULO 22

TEASERS

§365. Lógica linear

§366. Teoria das demonstrações

22.1. Dedução natural.

TODO Escrever

22.2. Cálculo de seqüentes.

TODO Escrever

22.3. Sistemas à la Hilbert.

TODO Escrever

§367. Lógica matemática

§368. Teoria da computabilidade

22.4. Uma questão surpresamente difícil.

TODO Escrever

22.5. Modelos de computação.

TODO Escrever

22.6. Teoria da recursão.

TODO Escrever

22.7. Problemas de decisão.

TODO Escrever

22.8. O problema da parada.

TODO Escrever

§369. Complexidade computacional

22.9. A notação assintótica.

TODO Escrever

22.10. Análise de algorítmos.

TODO Escrever

22.11. Reduções.

TODO Escrever

22.12. Classes de complexidade.

TODO Escrever

Leitura complementar

Teoria das demonstrações: [vP14], [Bim14], [NvP08], [Tak13], [Pra06], [GLT89], [Lau08], [Kle52]. [SU06]. [Gir11].

Lógica linear: [Gir95]. [Gir11].

Computabilidade: [Cut80], [Kle52], [Rog67].

[Koz97], [Koz06].

[Dav58], [DW83], [HU79].

Teoria das funções recursivas: [Kle52: Part III], [Sho01], [Mos16], [Rog67].

[BM77a: Cap. 6–8].

Algoritmos e complexidade: [DPV06], [Jon97]. [GJ79].

Apêndices

APÊNDICE A

DEMONSTRAÇÕES COMPLETAS

Onde tu prometes estudar estas demonstrações apenas depois de ter tentado escrever tuas próprias, baseadas nos esboços que tem no texto.

Capítulo 3

Θ3.68P. Demonstração. Vou demonstrar que para todo p positivo, $p \in P$. Seja p positivo. Separo em casos:
Caso $p \in P$. Imediato.
Caso $p \notin P$. Basta achar uma contradição, eliminando este caso. Seja

$$C \stackrel{\text{def}}{=} \{\, c \in \text{Pos} \mid c \notin P \,\}$$

o conjunto de todos os positivos que "escaparam" do P. Observe que pela sua construção, $C \subseteq \text{Pos}$ e que pela hipótese do caso, $p \in C$. Logo C é habitado e logo (pela PBO) possui mínimo. Logo seja m o menor membro de C. Ou seja: m positivo, $m \notin P$, e para todo x positivo com $x \notin P$, $x \leq m$. Observe que $m \neq 1$, pois $1 \in P$. Logo $m > 1$, já que m é positivo. Logo $m - 1$ é positivo também, e logo $m - 1 \in P$, pela escolha de m como mínimo positivo fora do p. Logo $(m-1)+1 \in P$, pois p é $(+1)$-fechado. Impossível, pois $(m-1)+1 = m$ e $m \notin P$, chegando assim na contradição desejada. ∎

Θ3.101P. Demonstração. Suponha que d, d' são mdc's de a e b. Como d é um mdc, todos os divisores em comum dos a e b o dividem. Mas, como d' é um divisor em comum, então $d' \mid d$. Simetricamente concluimos que $d \mid d'$, e logo d, d' são sócios. ∎

Θ3.114P. Demonstração. Demonstrado no Problema Π3.18 por indução e no Π3.19 pelo princípio da boa ordem. ∎

Λ3.131P. Demonstração. Sejam a, b inteiros e p irredutível tal que $p \mid ab$. Suponha que $p \nmid a$. Logo o $(a, p) = 1$ pode ser escrito como combinação linear de a e p, ou seja, existem $s, t \in \mathbb{Z}$ tais que:

$$1 = as + pt.$$

Multiplicando os dois lados por b, temos:

$$b = asb + ptb.$$

Observe que como $p \mid ab$, segue que $p \mid asb$ (por Lema Λ3.26). Obviamente $p \mid ptb$ também. Logo, $p \mid asb + ptb = b$. ∎

Λ3.133P. Demonstração. Seja $a, b, d \in \mathbb{Z}$, tais que $(d, a) = 1$ e $d \mid ab$. Como $(a, d) = 1$, podemos escrevê-lo como combinação linear dos a e d:

$$1 = sa + td, \qquad \text{para alguns } s, t \in \mathbb{Z}.$$

Multiplicando por b, ganhamos

$$b = sab + tdb,$$

e argumentando como na demonstração do Lemma de Euclides Λ3.131 concluimos que $d \mid b$. ∎

Θ3.136P. Demonstração. Para qualquer conjunto finito de primos $P = \{p_1, \ldots, p_n\}$, observe que o número $p = p_1 \cdots p_n + 1$ não é divisível por nenhum dos p_i's (porque $p_i \mid p$ e $p_i \mid p_1 \cdots p_n$ implicam $p \mid 1$, absurdo). Então, como $p \geq 2$, ou o p é primo e $p \notin P$, ou p é divisível por algum primo $q \notin P$ (por Exercício x3.130). Nos dois casos, existe pelo menos um primo fora do P. ∎

Θ3.159P. Demonstração. Precisamos mostrar as duas direções do ($\Leftrightarrow$):

($\Rightarrow$): Suponha que $a \equiv b \pmod m$, ou seja, $m \mid a - b$. Resolvendo as duas equações das divisões por os restos r_a e r_b, temos:

$$\left.\begin{aligned} r_a &= a - mq_a \\ r_b &= b - mq_b \end{aligned}\right\} \implies \begin{aligned} r_a - r_b &= (a - mq_a) - (b - mq_b) \\ &= (a - b) - (mq_a - mq_b) \\ &= (a - b) - m(q_a - q_b). \end{aligned}$$

Observe que $m \mid a - b$ e $m \mid m(q_a - q_b)$. Então m tem que dividir a diferença deles também:

$$m \mid \underbrace{(a - b) - m(q_a - q_b)}_{r_a - r_b}$$

Usando as duas desigualdades: $0 \leq |r_a - r_b| < m$. Como $|r_a - r_b|$ é um múltiplo de m, concluimos que necessariamente $0 = |r_a - r_b|$, ou seja: $r_a = r_b$.

($\Leftarrow$): Suponha que $r_a = r_b$. Temos:

$$\begin{aligned} a - b &= (mq_a + r_a) - (mq_b + r_b) \\ &= (mq_a - mq_b) - (r_a - r_b) \\ &= (mq_a - mq_b) - 0 \qquad \text{(hipótese)} \\ &= m(q_a - q_b), \end{aligned}$$

e como $q_a - q_b \in \mathbb{Z}$, concluimos que $m \mid a - b$, ou seja: $a \equiv b \pmod m$. ∎

Θ3.162P. Demonstração. (1) Segue imediatamente pois $m \mid a - a = 0$. (2) Pela hipótese temos $m \mid a - b$ e $m \mid b - c$. Então pelo Lema Λ3.26 $m \mid (a - b) + (b - c) = a - c$. (3) Pela hipótese temos $m \mid a - b$; logo (Λ3.26 de novo) $m \mid -(a - b) = b - a$. ∎

Θ3.173P. Demonstração. Como $(c, m) = 1$, existe c^{-1} (módulo m) então:

$$\begin{aligned} ca \equiv cb \pmod m &\implies c^{-1}ca \equiv c^{-1}cb \pmod m \\ &\implies \quad a \equiv \quad b \pmod m. \end{aligned}$$

∎

3.216P. Demonstração. Pelo Teorema fundamental da aritmética Θ3.140 seja

$$n =: p_0^{a_0} p_1^{a_1} \cdots p_k^{a_k}$$

a representação canônica do n. Calculamos:

$$\begin{aligned} \phi(n) &= \phi(p_0^{a_0} p_1^{a_1} \cdots p_k^{a_k}) \\ &= \phi(p_0^{a_0})\phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) && \text{(Teorema Θ3.215)} \\ &= p_0^{a_0}\left(1 - \frac{1}{p_0}\right) p_1^{a_1}\left(1 - \frac{1}{p_1}\right) \cdots p_k^{a_k}\left(1 - \frac{1}{p_k}\right) && \text{(Exercício x3.181)} \\ &= p_0^{a_0} p_1^{a_1} \cdots p_k^{a_k}\left(1 - \frac{1}{p_0}\right)\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\ &= n\left(1 - \frac{1}{p_0}\right)\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

∎

3.218P. Demonstração. Como p é primo, sabemos que $\phi(p) = p - 1$, então temos:

$$\begin{aligned} a^{p-1} &= a^{\phi(m)} && \text{(Propriedade 3.214)} \\ &\equiv 1 \pmod m. && \text{(Teorema Θ3.217)} \end{aligned}$$

∎

Capítulo 4

Λ4.112P. Demonstração. Por indução no tamanho do conjunto A demonstramos que

$$(\forall x \geq 1)(\forall A \text{ conjunto})[\,|A| = x \implies A \text{ possui mínimo}\,].$$

Observe que agora nossa indução virou "indução original".
Base: demonstrar que *se* $|A| = 1$ *então* A *possui mínimo*. Suponha $|A| = 1$. Logo temos que A é um singleton e pronto: seu único membro é seu mínimo. Passo Indutivo. Seja $k \geq 1$ tal que para qualquer conjunto H

(H.I.) $$|H| = k \implies H \text{ possui mínimo.}$$

Preciso demonstrar que para qualquer conjunto A

$$|A| = k + 1 \implies A \text{ possui mínimo.}$$

Seja A conjunto de inteiros tal que $|A| = k+1$. Basta verificar que A possui mínimo. Como $|A| = k+1$, temos:

$$(\exists a \in A)(\exists A' \subseteq A)[\, a \notin A' \;\&\; |A'| = k \;\&\; (\forall x \in A)[\, x = a \text{ ou } x \in A'\,]\,]$$

e logo sejam $m \in A$, $A' \subseteq A$, tais que

$$(1) \qquad \underbrace{m \notin A'}_{(1a)} \;\&\; \underbrace{|A'| = k}_{(1b)} \;\&\; \underbrace{(\forall x \in A)[\, x = m \text{ ou } x \in A'\,]}_{(1c)}.$$

Usamos a (HI) agora com $H := A'$, e já que $|A'| = k$ (pela (1b)) temos que A' possui mínimo. Seja $m' = \min A'$ então. Seja m_* o menor dos m, m'. Afirmo que $\min A = m_*$. Basta verificar, ou seja, mostrar que m_* é menor de qualquer membro de A. Seja $x \in A$ então. Novamente pela escolha dos m, A' temos que $x = m$ ou $x \in A'$. Tem cada subcaso vou demonstrar que $m_* \leq x$. Subcaso $x = m$. Imediato pois pela escolha de $m_* \leq m = x$. Subcaso $x \in A'$. Pela escolha dos m_* e m' respectivamente temos $m_* \leq m' \leq x$. ∎

Capítulo 8

Θ8.133P. Demonstração. Veja **[Apo67:** §10.21 & Teorema 10.22**]**. ∎

Capítulo 9

Θ9.186P. Demonstração. Primeiramente vamos verificar que as duas funções tem o mesmo domínio:

$$\begin{aligned} \operatorname{dom}(h \circ (g \circ f)) &= \operatorname{dom}(g \circ f) && (\text{def. } h \circ (g \circ f)) \\ &= \operatorname{dom} f && (\text{def. } g \circ f) \end{aligned}$$

e do lado direito

$$\operatorname{dom}((h \circ g) \circ f) = \operatorname{dom} f. \qquad (\text{def. } (h \circ g) \circ f)$$

Similarmente elas têm os mesmos codomínios (caso que seguimos a definição D9.26)

$$\operatorname{cod}(h \circ (g \circ f)) = \operatorname{cod} h \qquad (\text{def. } h \circ (g \circ f))$$

e do lado direito

$$\begin{aligned} \operatorname{cod}((h \circ g) \circ f) &= \operatorname{cod}(h \circ g) && (\text{def. } (h \circ g) \circ f) \\ &= \operatorname{cod} h. && (\text{def. } h \circ g) \end{aligned}$$

Agora precisamos mostrar que as duas funções comportam no mesmo jeito para todos os elementos no A. Suponha $a \in A$ então, e calcule:

$$\begin{aligned} (h \circ (g \circ f))(a) &= h((g \circ f)(a)) && (\text{def. } h \circ (g \circ f)) \\ &= h(g(f(a))) && (\text{def. } g \circ f) \end{aligned}$$

e o lado direito:

$$\begin{aligned} ((h \circ g) \circ f)(a) &= (h \circ g)(f(a)) && (\text{def. } (h \circ g) \circ f) \\ &= h(g(f(a))) && (\text{def. } h \circ g) \end{aligned}$$

∎

Θ9.190P. Demonstração. Observe que dado conjunto A, a id_A tem o domínio e codomínio certo. Basta então verificar que ela tem as propriedades (i)–(ii) e que ela é única.
id_A tem a primeira propriedade. Seja $f : A \to B$. Preciso mostrar que $f \circ \mathrm{id}_A = f$. Primeiramente verifico que têm o mesmo domínio e—para satisfazer até os categoristas—o mesmo codomínio:

$$\begin{aligned} \mathrm{dom}(f \circ \mathrm{id}_A) &= \mathrm{dom}(\mathrm{id}_A) = A = \mathrm{dom}\, f; \\ \mathrm{cod}(f \circ \mathrm{id}_A) &= \mathrm{cod}\, f. \end{aligned}$$

Basta ver se tem o mesmo comportamento. Seja $x \in A$ então, e calcule:

$$\begin{aligned} (f \circ \mathrm{id}_A)x &= f(\mathrm{id}_A x) && \text{(def. } f \circ \mathrm{id}_A\text{)} \\ &= f(x). && \text{(def. } \mathrm{id}_A\text{)} \end{aligned}$$

id_A tem a segunda propriedade. Similar.
id_A é única. Seja $\mathrm{id}'_A : A \to A$ função tal que

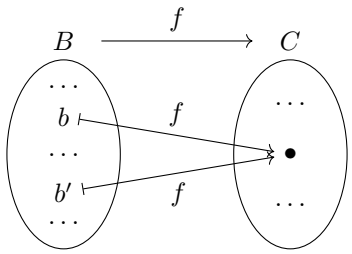
$$\begin{aligned} &\text{para toda } f : A \to B, \quad f \circ \mathrm{id}'_A = f; \\ &\text{para toda } f : B \to A, \quad \mathrm{id}'_A \circ f = f. \end{aligned}$$

Preciso mostrar que $\mathrm{id}_A = \mathrm{id}'_A$. Calculamos:

$$\begin{aligned} \mathrm{id}_A &= \mathrm{id}_A \circ \mathrm{id}'_A && \text{(primeira propriedade da } \mathrm{id}'_A \text{ com } f := \mathrm{id}_A\text{)} \\ &= \mathrm{id}'_A. && \text{(segunda propriedade da } \mathrm{id}_A \text{ com } f := \mathrm{id}'_A\text{)} \end{aligned}$$

∎

Θ9.252P. Demonstração. ($\Rightarrow$): Exercício x9.113:
($\Leftarrow$): Suponha $b, b' \in B$ tais que $f(b) = f(b')$. Basta mostrar que $b = b'$. Temos então o diagrama interno seguinte:



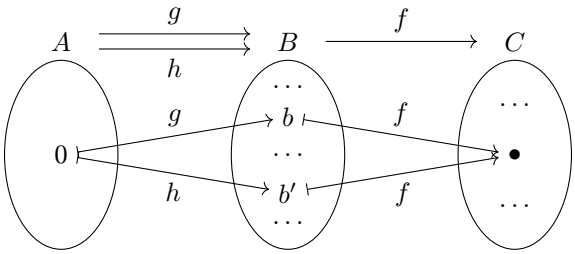
Seja $A = \{0\}$ e defina as g, h no diagrama

$$\{0\} \underset{h}{\overset{g}{\rightrightarrows}} B \xrightarrow{\ f\ } C$$

como as funções constantes definidas pelas

$$g(0) = b \qquad \text{e} \qquad h(0) = b'.$$

Então agora estamos com o diagrama interno assim:



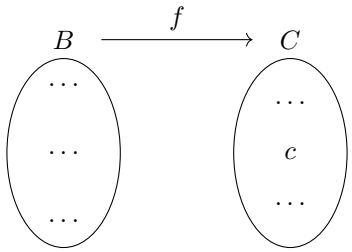
Observe que como

$$(f \circ g)(0) = f(g(0)) = f(b)$$
$$(f \circ h)(0) = f(h(0)) = f(b')$$

e $f(b) = f(b')$, temos $f \circ g = f \circ h$ e agora usamos a hipótese para ganhar $g = h$. Logo as g, h concordam no 0, ou seja, $b = b'$. ∎

Θ9.253P. Demonstração. ($\Rightarrow$): Exercício x9.114.

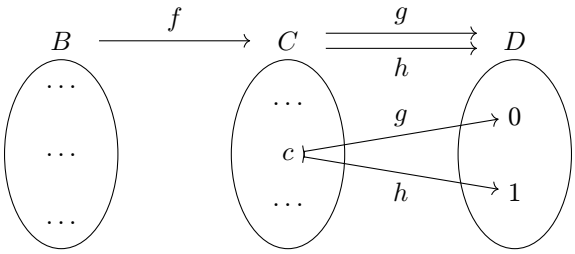
($\Leftarrow$): Suponha $c \in C$. Procuramos $b \in B$ tal que $f(b) = c$. Começamos então com o diagrama interno seguinte:



Seja $D = \{0, 1\}$ e defina as funções $g, h : C \to D$ pelas

$$g(y) = 0 \qquad \text{e} \qquad h(y) = \begin{cases} 1, & \text{se } y = c; \\ 0, & \text{se } y \neq c. \end{cases}$$

Logo $g(c) \neq h(c)$, mas $g(y) = h(y)$ para todo $y \neq c$. Agora estamos assim:



Como $g \neq h$ então, pela hipótese concluimos que $g \circ f \neq h \circ f$, ou seja, as $g \circ f$ e $h \circ f$ discordam em pelo menos um membro de B, e seja b um tal membro:

$$(g \circ f)(b) \neq (h \circ f)(b).$$

Logo

$$g(f(b)) \neq h(f(b)),$$

ou seja, g e h discordam no $f(b)$. Mas g e h discordam apenas no c; ou seja, $f(b) = c$ como desejamos. ∎

Capítulo 10

10.33P. Demonstração. Demonstrarei em detalhe a

$$a\ ((R \diamond S) \diamond T)\ d \implies a\ (R \diamond (S \diamond T))\ d.$$

A ($\Leftarrow$) é similar:

> Suponha $a \in A$ e $d \in D$ tais que $a\ (RS)T\ d$.
>
> Logo seja $c \in C$ tal que $a\ RS\ c$ (1) & $c\ T\ d$ (2).
>
> Logo Seja $b \in B$ tal que $a\ R\ b$ (3) & $b\ S\ c$ (4). (pelo (1))
>
> Logo $b\ ST\ d$ (5). (pelos (4) e (2))
>
> Logo $a\ R(ST)\ d$. (pelos (3) e (5))

∎

Capítulo 11

Λ11.35P. Demonstração. Seja G grupo. Sabemos que G tem pelo menos uma identidade graças à (G2), então o que precisamos mostrar é sua unicidade mesmo. Suponha que $e_1, e_2 \in G$ tais que e_1, e_2 são identidades do G; em outras palavras:

(1) $$\text{para todo } a \in G, \quad e_1 * a \overset{\text{L}}{=} a \overset{\text{R}}{=} a * e_1$$

(2) $$\text{para todo } b \in G, \quad e_2 * b \overset{\text{L}}{=} b \overset{\text{R}}{=} b * e_2.$$

Agora exatamente a mesma demonstração pode ser escrita em dois caminhos meio diferentes:

Caminho 1: Temos

$$\begin{aligned} e_1 &= e_1 * e_2 && \text{(pela (2R), com } b := e_1) \\ &= e_2 && \text{(pela (1L), com } a := e_2) \end{aligned}$$

e demonstramos o que queremos: $e_1 = e_2$, ou seja, em cada grupo existe única identidade.

Caminho 2. Temos

$$\begin{aligned} e_1 * e_2 &= e_1 && \text{(pois } e_2 \text{ é uma R-identidade (2R))} \\ e_1 * e_2 &= e_2 && \text{(pois } e_1 \text{ é uma L-identidade (1L))} \end{aligned}$$

e concluimos o desejado $e_1 = e_2$. ∎

Λ11.39P. Demonstração. Seja $(G\ ;\ *, e)$ grupo, e suponha que existem $a, a_1, a_2 \in G$ tais que a_1, a_2 são inversos de a, ou seja,

(1) $$a_1 * a \overset{\text{L}}{=} e \overset{\text{R}}{=} a * a_1 \qquad (a_1 \text{ é um inverso de } a)$$

(2) $$a_2 * a \overset{\text{L}}{=} e \overset{\text{R}}{=} a * a_2. \qquad (a_2 \text{ é um inverso de } a)$$

Vamos mostrar que $a_1 = a_2$. Temos:

$$\begin{aligned} a_1 * a &= a_2 * a && \text{(pelas (1L), (2L))} \\ a_1 &= a_2 && \text{(pelo Λ11.41 (GCR))} \end{aligned}$$

e *ficamos devendo* demonstrar a (GCR) do Lema Λ11.41. ∎

A11.41P. Demonstração. Sejam $a, x, y \in G$ tais que

$$a * x = a * y. \tag{1}$$

Pela (G3) o a possui inverso no G; daí, seja a_0 *um* inverso de a, ou seja,

$$a_0 * a \overset{\text{L}}{=} e \overset{\text{R}}{=} a * a_0. \tag{2}$$

Agora temos:

$$\begin{aligned}
a_0 * (a * x) &= a_0 * (a * y) && \text{(pela (1))}\\
(a_0 * a) * x &= (a_0 * a) * y && \text{(pela (G1): } * \text{ é associativa)}\\
e * x &= e * y && \text{(pela escolha do } a_0\text{: (2L))}\\
x &= y && \text{(pela definição do } e\text{)}
\end{aligned}$$

Demonstramos assim a (GCL). A (GCR) é completamente simétrica (e vamos precisar a (2R) em vez da (2L)). ∎

A11.56P. Demonstração. Vamos ver duas maneiras de demonstrar isso:
Maneira 1: Basta demonstrar que a satisfaz a propriedade de ser inverso do a^{-1}:

$$aa^{-1} \overset{\text{L}}{=} e \overset{\text{R}}{=} a^{-1}a$$

e ambas são imediatas: a (L) pela (G3R), e a (R) pela (G3L).
Maneira 2: Pelas definições de $\left(a^{-1}\right)^{-1}$ e a^{-1} ganhamos as equações:

$$\begin{aligned}
\left(a^{-1}\right)^{-1} * a^{-1} &= e && \text{(def. } \left(a^{-1}\right)^{-1}\text{)}\\
a * a^{-1} &= e. && \text{(def. } a^{-1}\text{)}
\end{aligned}$$

Logo

$$\left(a^{-1}\right)^{-1} * a^{-1} = a * a^{-1}$$

e cancelando agora pela direita (GCR), chegamos na desejada $\left(a^{-1}\right)^{-1} = a$. ∎

A11.58P. Demonstração. Calculamos

$$\begin{aligned}
\left(b^{-1} * a^{-1}\right) * (a * b) &= \left(\left(b^{-1} * a^{-1}\right) * a\right) * b && \text{(assoc.)}\\
&= \left(b^{-1} * \left(a^{-1} * a\right)\right) * b && \text{(assoc.)}\\
&= \left(b^{-1} * e\right) * b && \text{(def. } a^{-1}\text{)}\\
&= \left(b^{-1}\right) * b && \text{(def. } e\text{)}\\
&= e && \text{(def. } b^{-1}\text{)}
\end{aligned}$$

A $(a * b) * \left(b^{-1} * a^{-1}\right) = e$ é similar. ∎

Λ11.59P. Demonstração. Aplicando $(a^{-1}*)$ nos dois lados da primeira e $(*a^{-1})$ nos dois lados da segunda temos:

$$\begin{aligned} a*x=b &\overset{a^{-1}*}{\Longrightarrow} a^{-1}*(a*x)=a^{-1}*b \\ &\Longrightarrow (a^{-1}*a)*x=a^{-1}*b \\ &\Longrightarrow e*x=a^{-1}*b \\ &\Longrightarrow x=a^{-1}*b \end{aligned} \qquad \begin{aligned} y*a=b &\overset{*a^{-1}}{\Longrightarrow} (x*a)*a^{-1}=b*a^{-1} \\ &\Longrightarrow y*(a*a^{-1})=b*a^{-1} \\ &\Longrightarrow y*e=b*a^{-1} \\ &\Longrightarrow y=b*a^{-1} \end{aligned}$$

∎

Λ11.81P. Demonstração. Existência: existem n potências de a.
Demonstramos isso mostrando que os $a^0,\dots,a^{n-1}$ são distintos dois-a-dois. Sejam $i,j\in\{0,\dots,n-1\}$ com $i\neq j$. *Sem perda de generalidade*, suponha que $i<j$, ou seja:

$$0\leq i<j<n.$$

Para chegar num absurdo, suponha que $a^i=a^j$. Assim temos:

$$\underbrace{aa\cdots a}_{i}=\underbrace{aa\cdots aaa\cdots a}_{j}$$

E como $i<j$, quebramos o lado direito assim:

$$\underbrace{aa\cdots a}_{i}=\underbrace{\overbrace{aa\cdots a}^{i}\overbrace{aa\cdots a}^{j-i}}_{j}$$

Ou seja,

$$a^i=a^ia^{j-i}$$

e logo

$$e=a^{j-i}$$

pelo Corolário 11.62. Achamos então uma potência de a igual à identidade e: $a^{j-i}=e$. Como $0<j-i<n$, isso contradiza a definição de n como a ordem de a: $n=o(a)$. Logo $a^i\neq a^j$, que foi o que queremos demonstrar.
Unicidade: os $a^0,\dots,a^{n-1}$ são as *únicas* potências de a. Ou seja, para todo $M\in\mathbb{Z}$ o a^M é um dos $a^0,\dots,a^{n-1}$.
Tome $M\in\mathbb{Z}$. Aplicando a divisão de Euclides (Lemma da Divisão de Euclides Λ3.82) no M por n, ganhamos $q,r\in\mathbb{Z}$ tais que:

$$M=q\cdot n+r,\qquad 0\leq r<n.$$

Só basta calcular o a^M para verificar que realmente é um dos $a^0,\dots,a^{n-1}$:

$$a^M=a^{q\cdot n+r}=a^{q\cdot n}a^r=(a^n)^qa^r=e^qa^r=ea^r=a^r$$

e como $0\leq r<n$, demonstramos o que queríamos demonstrar. ∎

Λ11.84P. Demonstração. Precisamos demonstrar que para todo $r, s \in \mathbb{Z}$,

$$a^r = a^s \implies r = s.$$

Sem perda de generalidade suponhamos $s \leq r$ e usando a hipótese temos

$$a^s a^{r-s} = a^s$$

e logo $a^{r-s} = e$ (Corolário 11.62). Agora, como $o(a) = \infty$, usando o contrapositivo do Exercício x11.47 obtemos que não existe nenhum inteiro $m \neq 0$ tal que $a^m = e$. Logo $r - s = 0$, ou seja $r = s$. ∎

11.99P. Demonstração. Precisamos verificar as leis (G0)–(G3) para o $(H\ ;\ *)$. Os (1) e (2) garantam as (G0) e (G3) respectivamente, e o fato que G é grupo garanta a (G1) também. Basta verificar a (G2), ou seja, que $e \in H$:

Tome $a \in H$.	$(H \neq \emptyset)$
Logo $a^{-1} \in H$.	(pela (ii))
Logo $a * a^{-1} \in H$.	(pela (i))
Logo $e \in H$.	(def. a^{-1})

∎

11.102P. Demonstração. Graças ao Critérion 11.99, basta mostrar que todos os membros de H têm seu inverso dentro do H. Tome um $a \in H$ e considere a seqüência das suas potências positivas:

$$a, a^2, a^3, \ldots \in H \qquad \text{(graças à hipótese (1))}$$

Como o H é finito vamos ter um elemento repetido, $a^r = a^s$ para alguns distintos positivos $r, s \in \mathbb{N}$. Sem perda de generalidade, suponha $r > s$. Temos

$$\overbrace{a * a * \cdots * a}^{r \text{ vezes}} = \overbrace{a * a * \cdots * a}^{s \text{ vezes}}$$

e como $r > s$, reescrevemos assim:

$$\overbrace{\underbrace{a * a * \cdots * a}_{r-s \text{ vezes}} * \underbrace{a * a * \cdots * a}_{s \text{ vezes}}}^{r \text{ vezes}} = \overbrace{a * a * \cdots * a}^{s \text{ vezes}}.$$

Agora operando nos dois lados pela direita por $(a^s)^{-1}$:

$$\overbrace{a * a * \cdots * a}^{r-s \text{ vezes}} = e$$

Ou seja, $e = a^{r-s}$ e acabamos de demonstrar que $e \in H$. Observe que $r - s > 0$, então temos pelo menos um a na esquerda:

$$\overbrace{a * \underbrace{a * \cdots * a}_{r-s-1 \text{ vezes}}}^{r-s \text{ vezes}} = e$$

e agora *precisamos* considerar dois casos:
Caso $r - s = 1$: Nesse caso então temos $e = a^1 = a$, e logo $a^{-1} = e^{-1} = e = a \in H$.
Caso $r - s > 1$: Nesse caso, temos $e = aa^{r-s-1}$, ou seja, achamos o inverso do a: é o a^{r-s-1}, e ele pertence no H, pois é potência positiva de a (e H é fechado sob a operação).

Em ambos dos casos mostramos que $a^{-1} \in H$ e podemos aplicar o Critérion 11.99 para concluir o desejado $H \leq G$. ∎

Λ11.140P. Demonstração. Vamos demonstrar que $\mathcal{R}_H$ é uma partição do G. A demonstração que $\mathcal{L}_H$ também é, é similar. Precisamos demonstrar:

(P1) $\bigcup \mathcal{R}_H \supseteq G$; ou seja: para todo $x \in G$, existe coclasse H' com $x \in H'$;
(P2) as coclasses no $\mathcal{R}_H$ são disjuntas duas-a-duas;
(P3) nenhuma coclasse é vazia ($\emptyset \notin \mathcal{R}_H$).

(P1) Como H é um grupo, sabemos que $e \in H$, então para qualquer $x \in G$, temos que $x = ex \in Hx$, ou seja todos os elementos de G pertencem àlguma coclasse. (P3) Toda coclasse direita de H, tem a forma Ha para algum $a \in G$, e tem pelo menos um elemento: esse mesmo a (a gente demonstrou isso no Exercício x11.97). Para o (P2) suponha que $Ha \cap Hb \neq \emptyset$ e tome $w \in Ha \cap Hb$. Logo

$$h_a a = w = h_b b \qquad \text{para alguns } h_a, h_b \in H.$$

Para demonstrar que $Ha = Hb$, mostramos que $Ha \subseteq Hb$ e $Hb \subseteq Ha$. Suponha então que $x \in Ha$, logo $x = ha$ para algum $h \in H$. Precisamos mostrar que $x \in Hb$. Calculamos:

$$\begin{aligned} x = ha &= h\big({h_a}^{-1}h_a\big)a \\ &= h{h_a}^{-1}(h_a a) \\ &= h{h_a}^{-1}(h_b b) \\ &= \big(h{h_a}^{-1}h_b\big)b \\ &\in Hb. \end{aligned}$$

A outra direção ($Ha \supseteq Hb$) é similar. ∎

Λ11.150P. Demonstração. Seja $n \in \mathbb{N} = |H|$, e sejam $h_1, \ldots, h_n$ os membros de H:

$$H = \{h_1, h_2, h_3, \ldots, h_n\}.$$

Para qualquer $a \in G$ temos

$$Ha = \{h_1 a, h_2 a, h_3 a, \ldots, h_n a\}.$$

Queremos demonstrar que o Ha também tem n elementos. Basta demonstrar então que os

$$h_1 a, h_2 a, h_3 a, \ldots, h_n a$$

são distintos dois-a-dois, e logo, são n também. Mas isso é imediato:

$$\begin{aligned} h_u a = h_v a &\implies h_u = h_v && \text{((GCR))} \\ &\implies u = v && \text{(pois os } h_i\text{'s são distintos dois-a-dois)} \end{aligned}$$

A demonstração sobre as coclasses esquerdas é similar. ∎

Θ11.155P. Demonstração. ($\Rightarrow$): Precisamos mostrar que HK é fechado sobre a operação e fechado sobre os inversos. Tomamos aleatórios $h_1k_1, h_2k_2 \in HK$ e calculamos:

$$\begin{aligned} (h_1k_1)(h_2k_2) &= h_1(k_1h_2)k_2 && \text{(ass.)} \\ &= h_1(h_3k_3)k_2 \quad \text{para alguns } h_3 \in H \text{ e } k_3 \in K && (k_1h_2 \in KH = HK) \\ &= (h_1h_3)(k_3k_2) && \text{(ass.)} \\ &\in HK \end{aligned}$$

Para os inversos temos:

$$(h_1k_1)^{-1} = {k_1}^{-1}{h_1}^{-1} \in KH = HK.$$

($\Leftarrow$): Mostramos as "$\subseteq$" e "$\supseteq$" separadamente. "$\subseteq$": Tome $x \in HK$, logo $x^{-1} \in HK$ e $x^{-1} = hk$ *para alguns* $h \in H$ e $k \in K$. Como H e K são sub*grupos* de G seus inversos também estão em H e K respectivamente. Mas

$$x = \left(x^{-1}\right)^{-1} = (hk)^{-1}k^{-1}h^{-1} \in KH.$$

"$\supseteq$": Tome $x \in KH$, logo $x = kh$ *para alguns* $k \in K$, $h \in H$. Logo $k^{-1} \in K$ e $h^{-1} \in H$. Como $HK \leq G$, basta apenas demonstrar que $x^{-1} \in HK$ pois isso garantará que $x \in HK$ também. Realmente, $x^{-1} = (kh)^{-1} = h^{-1}k^{-1} \in HK$. ∎

Λ11.182P. Demonstração. Mostramos cada direção da

$$g \in (Na)(Nb) \iff g \in N(ab)$$

separadamente.
($\Rightarrow$). Suponha $g \in (Na)(Nb)$. Logo sejam $a' \in Na$ e $b' \in Nb$ tais que $g = a'b'$. Pelas definições dos Na e Nb, sejam $n_a, n_b \in N$ tais que $a' = n_aa$ e $b' = n_bb$. Logo temos

$$g = (n_aa)(n_bb) = n_a(an_b)b$$

Mas como $an_b \in aN$ e $aN = Na$ (pois $N \trianglelefteq G$), temos que $an_b = n'_ba$ para algum $n'_b \in N$. Logo

$$g = n_a(n'_ba)b = (n_an'_b)(ab) \in N(ab)$$

pois $n_an'_b \in N$.
($\Leftarrow$). Suponha $g \in N(ab)$. Logo seja $n \in N$ tal que $g = n(ab)$. Logo temos

$$g = n(ab) = (na)b \in (Na)(Nb)$$

pois $na \in Na$ e $b \in Nb$. ∎

Θ11.183P. Demonstração. Graças ao Critérion 11.64, basta verificar que G/N com sua operação (Definição D11.180) satisfaz uma definição unilateral de grupo: (G0), (G1), (G2L), (G3L). (G1): Sejam $a, b, c \in N$. Calculamos:

$$\big((Na)(Nb)\big)(Nc) = \big(N(ab)\big)(Nc) = N((ab)c) = N(a(bc)) = (Na)\big(N(bc)\big) = (Na)\big((Nb)(Nc)\big).$$

(G2L): Procuramos um membro de G/N que satisfaz a lei de identidade esquerda. Afirmação: o $N \in G/N$ é uma identidade esquerda do G/N. Para demonstrar essa afirmação precisamos mostrar que para todo $a \in N$, temos $N(Na) = Na$. Realmente, seja $a \in N$. Calculamos:

$$N(Na) = (Ne)(Na) = N(ea) = Na.$$

(G3L): Seja $a \in N$. Afirmação: o $N(a^{-1})$ é um inverso esquerdo de Na. Para demonstrar essa afirmação precisamos verificar que:

$$(N(a^{-1}))(Na) = N.$$

Calculamos:

$$\big(N(a^{-1})\big)(Na) = N(a^{-1}a) = Ne = N$$

e pronto. ∎

Θ11.223P. Demonstração. ($\Rightarrow$): Como $e_A \in \ker\varphi$, basta demonstrar que todos os membros de $\ker\varphi$ são iguais. Sejam $x, y \in \ker\varphi$ então. Logo $\varphi(x) = e_B = \varphi(y)$, e como φ é injetora, concluimos o desejado $x = y$.
($\Leftarrow$).

Sejam $x, y \in A$ tais que $\varphi(x) = \varphi(y)$.	
Logo $\varphi(x)\varphi(y)^{-1} = e_B$.	$((*\varphi(y)^{-1}))$
Logo $\varphi(x)\varphi(y^{-1}) = e_B$.	(φ homo (inv.))
Logo $\varphi(xy^{-1}) = e_B$.	(φ homo (op.))
Logo $xy^{-1} \in \ker\varphi$.	(def. $\ker\varphi$)
Logo $xy^{-1} \in \{e_A\}$.	(hipótese)
Logo $xy^{-1} = e_A$.	($\{e_A\}$ singleton)
Logo $x = y$.	$((*y))$

∎

Capítulo 12

Λ12.24P. Demonstração. Verificamos que $(-a)b$ realmente é o inverso de ab:

$$\begin{aligned} ab + (-a)b &= (a + (-a))b && \text{(pela (RDR))} \\ &= 0b && \text{(def. } (-a)\text{)} \\ &= 0 && \text{(Lema Λ12.22 com } x := b\text{)} \end{aligned}$$

e como a equação $ab + \boxed{?}$ tem resolução única (pois o $(R\ ;+)$ é um grupo) e o $-(ab)$ também a resolve, concluimos que $(-a)b = -(ab)$. A outra igualdade é similar. ∎

Λ12.32P. Demonstração. Tome $a, b \in \operatorname{im}\varphi$. Logo

$$\begin{aligned} a &= \varphi(a') && \text{para algum } a' \in R \\ b &= \varphi(b') && \text{para algum } b' \in R. \end{aligned}$$

Calculamos:

$$\begin{aligned} 1_S &= \varphi(1_R); && (\varphi \text{ homo } (1)) \\ a + b &= \varphi(a') + \varphi(b') && (\text{pela escolha dos } a', b') \\ &= \varphi(a' + b'); && (\varphi \text{ homo } ((+))) \\ -a &= -\varphi(a') && (\text{pela escolha do } a') \\ &= \varphi(-a'); && (\varphi \text{ homo } (-)) \\ ab &= \varphi(a')\varphi(b') && (\text{pela escolha dos } a', b') \\ &= \varphi(a'b'). && (\varphi \text{ homo } (\cdot)) \end{aligned}$$

Ou seja: $1_S, a + b, -a, ab \in \operatorname{im}\varphi$ e podemos usar o Critério 12.28. ∎

Capítulo 13

Λ13.22P. Demonstração. Vamos demonstrar o lemma na maneira "round-robin", demonstrando as implicações (1) ⇒ (2) ⇒ (3) ⇒ (1). As duas primeiras são conseqüências imediatas das definições—nada interessante—mas para a (3) ⇒ (1) precisamos mais cuidado.
(1) ⇒ (2). Caso A finito, para algum $n \in \mathbb{N}$ temos $A =_c \overline{n} \subseteq \mathbb{N}$ e logo $A \leq_c \mathbb{N}$. Caso que A infinito, temos $A =_c \mathbb{N} \subseteq \mathbb{N}$ e logo $A \leq_c \mathbb{N}$.
(2) ⇒ (3). Suponha que $A \neq \emptyset$. Vamos construir uma enumeração do A, ou seja, uma $\pi : \mathbb{N} \twoheadrightarrow A$. Pela hipótese, seja $N_0 \subseteq \mathbb{N}$ tal que $A =_c N_0$. E logo temos uma bijecção $f : N_0 \rightarrowtail A$. Seja $a_0 \in A$ ($A \neq \emptyset$) e defina a função $\pi : \mathbb{N} \to A$ pela

$$\pi(x) = \begin{cases} f(x), & \text{se } x \in N_0 \\ a_0, & \text{se não.} \end{cases}$$

Basta verificar que π é realmente sobrejetora, mas isso é fácil: para cada $a \in A$, temos

$$\pi(f^{-1}(a)) = a.$$

(3) ⇒ (1). Caso A finito, A é contável. Suponha que A infinito, e seja $\pi : \mathbb{N} \twoheadrightarrow A$ uma enumeração de A. Precisamos definir uma bijecção $f : \mathbb{N} \rightarrowtail A$ ou $f : \overline{n} \rightarrowtail A$. Defina a f pela recursão

$$\begin{aligned} & & f(0) &= \pi(0) \\ \text{e para } n > 0 \text{ defina} & & f(n) &= \pi(m_n) \end{aligned}$$

onde m_n é o menor natural m tal que $\pi(m) \notin \{f(0), \ldots, f(n-1)\}$. Observe que tal m_n existe pois a ($\leq$) no $\mathbb{N}$ é uma boa ordem (Problema II4.5). ∎

Capítulo 14

Θ14.40P. Demonstração. Seja $D := \{\, x \in L \mid x \leq Fx \,\}$. Vamos demonstrar que $\bigvee D$ é um fixpoint de F, ou seja $F(\bigvee D) = \bigvee D$. Quebramos a demonstração em duas partes: $\bigvee D \leq F(\bigvee D)$: Basta mostrar que $F(\bigvee D)$ é um upper bound de D. Tome $d \in D$. Logo $d \leq Fd$ (1) (pela definição de D) e também $d \leq \bigvee D$ (2), pois $\bigvee D$ é um upper bound de D. Como F é monótona, da (2) ganhamos $Fd \leq F(\bigvee D)$ (3). Juntando (transitividade) as (1) e (3):

$$d \leq Fd \leq F(\bigvee D)$$

ou seja, $d \leq F(\bigvee D)$ e como d foi arbitrário elemento de D, concluimos que $F(\bigvee D)$ é um upper bound de D. Logo $\bigvee D \leq F(\bigvee D)$. $F(\bigvee D) \leq \bigvee D$: Basta demonstrar que $F(\bigvee D) \in D$, pois $\bigvee D$ é um upper bound de D. Como já demonstramos que $\bigvee D \leq F(\bigvee D)$, ganhamos a $F(\bigvee D) \leq F(F(\bigvee D))$ (pela monotonicidade da F). Ou seja, o $F(\bigvee D)$ satisfaz a definição de D, e logo pertence nele: $F(\bigvee D) \in D$. Como $\bigvee D$ é um upper bound de D, temos $F(\bigvee D) \leq \bigvee D$. ∎

Θ14.48P. Demonstração. Pelo Exercício x14.20, o P possui $\bot$. Consideramos a π-órbita do $\bot$:

$$\bot, \pi(\bot), \pi(\pi(\bot)), \ldots$$

O conjunto dos seus membros é uma cadeia (Exercício x14.21) e logo possui lub pois P é chain-completo. Tome

$$x^* := \bigvee \{\bot, \pi(\bot), \pi^2(\bot), \dots\}$$

então. Confirmamos que: (i) x^* é um fixpoint (Exercício x14.22); e, ainda mais (ii) o strongly least (Exercício x14.23). ∎

Capítulo 16

Θ16.90P. Demonstração. A única coisa que deixamos para completar a demonstração foi verificar os (P1)–(P5), que é feito nos exercícios x16.44–x16.48. ∎

Θ16.92P. Demonstração. A demonstração completa segue do seu esboço junto com os exercícios: x16.53, x16.54, x16.55, x16.56, e x16.57. ∎

APÊNDICE B

DÍCAS

Onde tu prometes consultar as dicas apenas depois de ter tentado resolver a atividade sem elas.

Dícas #1

x1.20H1. Use metavariáveis para abstrair as partes interessantes de cada loop que precisarás (e assim poderás) usar na sua implementação.

x1.21H1. Recursão.

x2.3H1. Presta atenção na definição do $(|)$.

Π2.4H1. Não. Da pra aceitar apenas duas elas como axiomas e derivar as outras duas. Quais? Como?

x3.1H1. Ambas as $(+), (\cdot)$ são comutativas.

x3.5H1. Adicione o $(-c)$ nos dois lados pela direita para demonstrar a primeira.

x3.7H1. Imite a demonstração do Unicidade da $(+)$-identidade Θ3.11.

x3.8H1. Separe em duas partes: existência e unicidade.

x3.15H1. A chave principal na demonstração é nosso axioma mais recente de não zerodivisores, (Z-NZD).

x3.22H1. O contexto deve incluir um conjunto de inteiros A e uma operação binária $\heartsuit : A \times A \to A$.

x3.23H1. Para cada conjunto basta achar um testemunha, ou seja, um parzinho (x, y) de membros dele tal que $x + y$ não pertence a ele.

x3.32H1. Deveriam ser 1 nesta demonstração. Como?

x3.34H1. Use a tricotomía (ZP-Tri).

x3.42H1. Por fight club: suponha que um conjunto tem mínima m_1, m_2 e aplicando a definição de "mínimo" e propriedades de $(\leq)$, conclua que são iguais.

x3.48H1. Use a (ZO-Tri) para separar em casos.

x3.49H1. Use a (ZO-Tri) para separar em casos.

Π3.2H1. Começa com o

$$(\mathbb{Z}\,;0,1,+,-,\cdot,<)$$

estipulando as proposições do Teorema Θ3.43 como axiomas. Defina a , e demonstre suas leis como teoremas.

x3.56H1. É só "shiftar" o Teorema Θ3.63.

x3.59H1. Nenhum inteiro negativo satisfaz $0 < m < 1$. Então para demonstrar que nenhum inteiro fica estritamente entre 0 e 1, basta demonstrar que todos os não-negativos n satisfazem $n = 0$ ou $n \geq 1$

x3.65H1. Cuidado sobre o produtório vazio.

x3.66H1. $\sum_{i=s}^{t} c\tau(i) = c\sum_{i=s}^{t} \tau(i)$.

x3.67H1. $\sum_{i=s}^{t} (\tau(i) + \sigma(i)) = \left(\sum_{i=s}^{t} \tau(i)\right) + \left(\sum_{i=s}^{t} \sigma(i)\right)$.

x3.68H1. Para qualquer w tal que $s \leq w \leq t$, $\sum_{i=s}^{t} \tau(i) = \sum_{i=s}^{w-1} \tau(i) + \sum_{i=w}^{t} \tau(i)$.

x3.69H1. $\sum_{i=s}^{t} \tau(i) = \sum_{i=s+d}^{t+d} \tau(i-d)$.

x3.70H1. $\sum_{i=s}^{t} 1 = \begin{cases} t-s+1, & \text{caso } s \leq t; \\ 0, & \text{caso } s > t. \end{cases}$

x3.71H1. $\prod_{i=s}^{t} c\tau(i) = c^n \prod_{i=s}^{t} \tau(i)$, onde $n = \begin{cases} t-s+1, & \text{caso } s \leq t; \\ 0, & \text{caso } s > t. \end{cases}$

x3.72H1. $\prod_{i=s}^{t} (\tau(i) \cdot \sigma(i)) = \left(\prod_{i=s}^{t} \tau(i)\right) \cdot \left(\prod_{i=s}^{t} \sigma(i)\right)$.

x3.73H1. Para qualquer w tal que $s \leq w \leq t$, $\prod_{i=s}^{t} \tau(i) = \prod_{i=s}^{w-1} \tau(i) \cdot \prod_{i=w}^{t} \tau(i)$.

x3.74H1. $\prod_{i=s}^{t} \tau(i) = \prod_{i=s+d}^{t+d} \tau(i-d)$.

x3.75H1. $\prod_{i=s}^{t} c^{\tau(i)} = c^{\sum_{i=s}^{t} \tau(i)}$.

x3.76H1. Indução.

x3.84H1. Use o que tu acabou de demonstrar sobre o $(x+y)^2$, no Exercício x3.83.

x3.85H1. Aplique a hipótese indutiva.

x3.86H1. Seja $a = a_0$. Assim $a_i = a + i$.

x3.87H1. Ou fatore o $n^2 - 1$ e use o Exercício x3.86, ou considere os casos possíveis dependendo dos restos da divisão de n por 3.

x3.88H1. Use a divisão de Euclides.

x3.93H1. $k = (k-3)+3$.

Π3.8H1. Quantos $i \in \mathbb{Z}_{\geq 0}$ satisfazem $i < 0$?

Π3.10H1. Indução no tamanho do conjunto finito.

x3.95H1. Use o PBO (mas cuidado pois precisas de demonstrar algo antes de usá-lo).

x3.96H1. Use indução, mas cuidado para não esquecer nada.

x3.97H1. Tome um arbitrário $a \in S$ e use o lemma da Divisão de Euclides.

x3.98H1. Existe $n \in \mathbb{Z}_{\geq 0}$ tal que $S = \{\, kn \mid k \in \mathbb{Z} \,\}$.

x3.102H1. Aqui o que devemos demonstrar é que a relação é simétrica; sem isso a gente precisaria especificar quem é sócio de quem.

x3.103H1. Demonstre.

x3.104H1. Demonstre.

x3.109H1. Não é. Mostre um contraexemplo.

x3.110H1. Já demonstramos (Lemma de Bézout Λ3.107) que

$$C = \{\, ax + by \mid x, y \in \mathbb{Z} \,\} = d\mathbb{Z}$$

onde d é um mdc dos a, b.

x3.111H1. Lembre a definição de mdc.

x3.112H1. Tu não pulou o Exercício x3.111, certo?

x3.115H1. $\cdots$

x3.117H1. Separe os casos: ou $b > a/2$ ou $b \leq a/2$.

x3.118H1. Indução.

x3.120H1. Olha na forma final do somatório. O que acontece em cada passo?

x3.121H1. Como nos livramos dos pontos informais "$\cdots$"?

x3.126H1. Tá certo. Demonstre.

x3.131H1. Considere o menor divisor de a. O que pode afirmar sobre ele?

Π3.18H1. Precisa expressar o alvo na forma $(\forall n)[\,\varphi(n)\,]$.

Π3.19H1. Considera as duas partes separamente: qual conjunto é o não vazio em cada parte?

Π3.20H1. $C(p,r) \in \mathbb{Z}$, $r < p$, e $p - r < p$.

Π3.22H1. Olhe para o $n! - 1$.

Π3.23H1. !

Π3.24H1. O que acontece se $a = b = 0$? O que acontece se pelo menos um dos a e b não é o 0?

Π3.25H1. Tente quebrar o 10 usando várias estratégias. O que tu percebes?

Π3.26H1. Use o teorema fundamental da aritmética (Θ3.140).

Π3.27H1. Qual foi tua resposta no Exercício x6.1?

Π3.28H1. Comece achando um p tal que $V(p) > 0$.

x3.138H1. Qual seria o valor de $4 \bmod 0$?

x3.141H1. Use as definições de congruência (D3.155) e de $(|)$ (D3.22) para escrever o x na forma $x = mk + t$.

x3.146H1. Para a $(\Leftarrow)$, considere sua contrapositiva. Para a $(\Rightarrow)$, lembre que todos os x com $1 \leq x \leq p - 1$ são invertíveis.

x3.151H1. Já descobrimos que

$$x \equiv 31 \pmod{60} \iff \begin{array}{l} x \equiv 1 \pmod 5 \\ x \equiv 7 \pmod{12} \end{array}$$

e logo

$$\begin{array}{l} x \equiv 1 \pmod 5 \\ x \equiv 7 \pmod{12} \\ x \equiv 3 \pmod 7 \end{array} \iff \begin{array}{l} x \equiv 31 \pmod{60} \\ x \equiv \ \ 3 \pmod 7. \end{array}$$

Como $(60, 7) = 1$, sabemos que o sistema tem resolução única módulo 420 e ainda mais, sabemos como achar essa resolução (tudo isso graças ao Teorema chinês do resto (binário) Θ3.179).

x3.152H1. Procure um contraexemplo com três inteiros.

x3.154H1. Observe que não podes aplicar o teorema chinês diretamente: $(6, 15) > 1$.

x3.155H1. $6 = 2 \cdot 3$

x3.156H1. Veja o Corolário 3.134.

x3.157H1. $8 = 2^3$, e $2 \mid 10$.

x3.158H1. Os 2 e 5 são divisores de 10.

Π3.29H1. Caso que qualquer um dos a, b, c é multiplo de 3, já éra. Basta então considerar o caso onde nenhum deles é multiplo de 3.

Π3.30H1. Use o teorema binomial Θ3.80.

Π3.31H1. Esquecendo o 2, todos os primos são da forma $4n+1$ ou $4n+3$. Suponha que $p_1, p_2, \ldots, p_k$ ($k \in \mathbb{N}$) são todos os primos da segunda forma.

Π3.32H1.

$$(4n+3)(4n+3) \stackrel{?}{=} 4n'+3 \qquad\qquad (-1)^n \stackrel{?}{=} -1$$

x3.159H1. Sendo a coprimo com p, a é invertível módulo p.

x3.160H1. $a^{p-1} = a^{p-2}a$.

x3.161H1. Tome $a := 108$ e $p := 241$ no Fermatinho.

x3.163H1. Escreva o inteiro como somatório baseado na sua forma decimal.

x3.164H1. Qual a solução do sistema

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 0 \pmod 2? \end{aligned}$$

x3.165H1. Procure y tal que $41^{75} \equiv y \pmod 3$.

x3.180H1. Ache uma maneira de "casar" entre-si todos os $1 \leq i < n$ que são coprimos com o n.

x3.181H1. Use a definição de ϕ e o Exercício x3.179.

x3.182H1. Calcule o valor de cada termo aplicando o Exercício x3.181.

Π3.34H1. Considere módulo 2.

Π3.35H1. Considere módulo m.

Π3.38H1. O que seria o $p^{q-1} + q^{p-1}$ módulo p? E módulo q?

Π3.39H1. Nesse caso *não* temos

$$a^{b-1} + b^{a-1} \equiv 1 \pmod{ab}.$$

x4.5H1. Pensando fora do Nat: como podemos calcular o valor de $2(n+1)$, se sabemos como dobrar qualquer número menor de $n+1$?

x4.6H1. Precisa de novo duas equações:

$$\begin{aligned} n \cdot 0 &= ____ \\ n \cdot Sm &= ____ \end{aligned}$$

x4.12H1. Para a (ii), calcule os q 11, q 12, r 11, e r 12.

x4.13H1. Pega um lado e calcule até chegar no outro; ou se não conseguir chegar no outro lado, trabalhe no outro lado separadamente até chegar no mesmo canto.

x4.14H1. O Princípio 4.17 não tem nada a ver com isso.

x4.15H1. Está no passo indutivo.

x4.16H1. Por indução no k.

x4.17H1. Por indução em qualquer uma das m, n.

x4.18H1. Indução no z.

x4.19H1. Indução no b.

x4.20H1. Indução no c.

x4.21H1. Indução no n.

x4.24H1. Use a hipótese (que é uma disjunçaõ) para separar em casos.

x4.28H1. Uma idéia é usar um legalzão em vez dum legalzinho. Outra é usar um legalzinho mesmo, mas aproveitar o Lema Λ4.51.

Π4.3H1. Depois de definir confira tuas definições seguindo elas para calcular uns valores. Por exemplo, $t\ h\ 2$ e $T\ h\ (5,2)$ devem dar os resultados

$$t\ h\ 2 = (h\ 0)(h\ 1) \qquad\qquad T\ h\ (5,2) = (h\ 5)(h\ 6).$$

Π4.4H1. Qual é o codomínio da h?

Π4.5H1. Reductio ad absurdum.

Π4.6H1. Indução!

x4.35H1. Precisa definir uma $\mathrm{eq} : \mathsf{Nat} \times \mathsf{Nat} \to \mathsf{Bool}$ e demonstrar que, de fato, corresponde à igualdade (=) entre Nats.

x4.42H1. Nos dois branches a expressão retornada é algo aplicado ao $\mathrm{filter}\ p\ xs$.

Π4.11H1. A demonstração compila sim, mas mesmo assim ela não pode ser usada para nos livrar da estipulação da injetividade como princípio para o Nat. Por que não?

Π4.12H1. Não dá. Agora a demonstração não compila por outro motivo.

x4.45H1. Com uma exeção, todos têm como atender a especificação de functor.

x4.50H1.

x4.52H1. Não esqueça os functors que descubriu no Exercício x4.45.

x4.53H1. Recursão!

x4.54H1. Indução!

x4.59H1. subtree : BinTree $\alpha \to$ Path $\to$ Maybe (BinTree α).

x4.60H1. Pode sim. Basta definir uma map que atende a Especificação S4.81 (demonstrar as duas leis de functor).

x4.66H1. Falta só adicionar 3 mais casos na segunda regra, imitando para os outros operadores o caso do (+).

Π4.19H1. Tome um string arbitrário s, e demonstre por indução que *para todo* $n \in \mathbb{N}$, ${}^n s = s^n$.

x5.2H1. Cuidado: aqui a *quantidade* das opções da segunda escolha, depende sim na escolha anterior!

x5.3H1. Começando com a mesma resposta (7!) do Exemplo 5.11, claramente nos hipocontamos—mas quanto?

x5.4H1. Construa cada configuração em passos.

x5.5H1. Se tu achar o problema igual com o Exemplo 5.11, tu hipercontarás... Quanto?

x5.6H1.

(1) Como no Exemplo 5.13, considere o problema onde C, D, e E são uma pessoa só.
(2) Conte o complementar e subtraia do total sem restricção;
(3) Conte as configurações em quais C, D, e E sentam juntos e subtraia as configurações onde, além disso, F e G também sentam juntos.

x5.7H1. Presta atenção na frase "*em cada passo a quantidade das opções disponíveis não depende nas escolhas anteriores*".

x5.8H1. Teorema binomial Θ3.80.

x5.9H1. O $\binom{a}{b}$ está na linha a, na posição b (começando contar com 0).

x5.10H1. Demonstre diretamente usando apenas a definição de fatorial.

x5.11H1. Indução.

x5.12H1. Recursão.

x5.13H1. Use a f do Exercício x5.12.

x5.14H1. Sem recursão!

x5.15H1. Recursão.

x5.16H1. Recursão.

Π5.3H1. Construa cada configuração em passos e use o princípio da multiplicação.

Π5.6H1. Recursão.

Π5.9H1. Recursão.

Π5.11H1. Recursão.

Π5.12H1. Para o (4), seria diferente se a restricção fosse "os `S` não aparecem todos juntos".

Π5.15H1. Inclusão–exclusão.

Π5.16H1. Separe os strings em dois grupos, aqueles que terminam em 0 e aqueles que terminam em 1, e conta os strings de cada grupo usando recursão.

Π5.17H1. Recursão.

x6.52H1. Duas bases.

x6.54H1. Para a ($\Rightarrow$), obtenha $-a \leq |x|$, bote tudo junto e observe que o x só pode ser $|x|$ ou $-|x|$. Para a ($\Leftarrow$), separe em casos sobre o x logo; em cada caso teu alvo segue facilmente por uma das duas partes da hipótese.

x6.76H1. Use as definições!

x6.78H1. Não.

x6.81H1. Daria, mas não faria sentido essa abordagem, pois seria complicada demais. Tanto para os inteiros, quanto para os racionais, existem maneiras bem mais fáceis para definir seus correspondentes conjuntos naturais. Como?

x6.82H1. O que fizemos sobre mínima e máxima tanto estudando inteiros, quanto estudando reais?

x6.83H1. Defina $\mathsf{ExtReal} \stackrel{\text{def}}{=} 1 + \mathsf{Real} + 1$; quais (nomes de) coprojeções tu escolheria?

x6.91H1. Use a hipótese com $\varepsilon := x$, já que $x > 0$ neste caso.

x6.92H1. Resolveu o Exercício x6.58, né?

x6.96H1. $|x - x| = 0$.

x6.98H1. Não! Por quê?

x6.100H1. Precisa escolher qual será o centro c e qual o raio r da bola associada ao (u, v), e verificar que $\mathcal{B}_r(c) = (u, v)$ com tua escolha.

x6.104H1. O problema fica na $\lim_n a_n = \ell$. Qual é?

x6.109H1. $(a_n)_n$ convergente & eventualmente $(a_n)_n \subseteq \mathbb{R}_{\mathbb{Z}} \implies (a_n)_n$ é eventualmente constante.

x6.118H1. Seria errado inferir que $(a_n)_n < (b_n)_n$.

x6.126H1. Aqui dá para conseguir uma subseqüência crescente.

x6.127H1. Aqui dá para conseguir uma subseqüência decrescente.

Π6.1H1.

$$\frac{2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot \cdots}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot \cdots} = \frac{2\cdot 2\cdot 2}{1\cdot 2\cdot 3}\cdot \cdots$$

x6.128H1. Tu vai precisar usar a lei de completude.

x6.133H1. Adicione a hipotese que $A, B > 0$, ou seja, que todos os seus membros são positivos.

x6.134H1. Mostre que $(\vartheta^n)_n$ é decrescente e inf-cotada (por quem mesmo?).

x6.137H1. Para a parte (iii), lembre como demonstramos o Exercício x6.134.

x6.138H1. $1 \in A$. Por quê?

x6.139H1. Uma sup-cota é o 2. Por quê?

Π6.7H1. Reductio ad absurdum.

x8.4H1. Já definimos o $(\subseteq)$, então podemos usá-lo!

x8.5H1. Substitua a fórmula longa com uma equivalente aproveitando uns açúcares sintácticos dos quantificadores $\forall, \exists$.

x8.6H1. "o"

x8.8H1. Use o set builder.

x8.9H1. Em outras palavras, demonstre que:

$$\text{se } A, B \text{ são vazios, então } A = B.$$

x8.10H1. Suponha que A, B são vazios. Queremos mostrar que $A = B$. Então suponha o contrário $(A \neq B)$ pera chegar num absurdo.

x8.11H1. Já demonstrou a existência (Exercício x8.8) e a unicidade (Exercício x8.9 ou x8.10) do vazio?

x8.14H1. Quais noções são envolvidas nessa afirmação? Quais são as definições delas?

x8.18H1. O "$x \in A$" é um termo?

x8.20H1. Primeiramente calcule a extensão do A:

$$A = \{\ldots?\ldots\}.$$

x8.22H1. Precisa descrever (definir) o conjunto

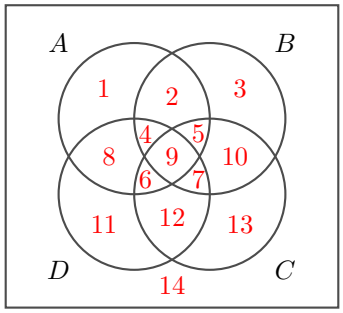
$$\{\, t(x_1,\ldots,x_n) \mid \varphi(x_1,\ldots,x_n) \,\}$$

com uma notação que já temos:

$$\{\, t(x_1,\ldots,x_n) \mid \varphi(x_1,\ldots,x_n) \,\} \stackrel{\text{def}}{=} \ldots?$$

x8.25H1. Não siga tua intuição; siga fielmente a definição!

x8.28H1.



Contamos 14 regiões. Qual o problema?

x8.40H1. Siga a definição e nada mais!

x8.41H1. Siga a definição e nada mais!

x8.45H1. Depende: ache um exemplo e contra exemplo.

x8.47H1. A afirmação é verdadeira. Demonstre!

Π8.4H1. Introduza uma notação para o conjunto

$$\{\, a \mid a \text{ pertence a uma quantidade ímpar dos } A_1, \ldots, A_n \,\}.$$

Já que ele depende de n, algo do tipo $A_{[n]}$ serve bem aqui. Assim, basta demonstrar o seguinte:

$$(\forall n \in \mathbb{N})\big[\, \Delta_{i=1}^{n} A_i = A_{[n]} \,\big].$$

Π8.5H1. O que significa $A_1 \triangle \cdots \triangle A_n$ nesse caso? Por quê?

Π8.6H1. A airmação é verdadeira. Demonstre.

Π8.7H1. Procure uma $\mathscr{C} \subseteq \wp\mathbb{R}$.

Π8.8H1. Esqueça a idéia de usar 4 cíclos.

x8.50H1. Se conseguiu demonstrar, tá errado. Eu imagino que em algum ponto tu "sejou" algum objeto em algum conjunto que não podia! Lembra a Questão Q8.36?

x8.51H1. Uma direção é trivial—por quê?

x8.54H1. Inspire-se a roubar o Nota 8.89.

x8.55H1. Já que definimos triplas em termos de duplas, para definir o interface de triplas vamos precisar usar o interface de duplas, ou seja, as projecções π_0, π_1.

x8.63H1. Quais são os dados que precisamos ter per aplicar a Proposição 8.131?

x8.66H1. Use as definições e/ou a Proposição 8.131.

x8.67H1. Cuidado com os ligadores de variáveis na notação dos operadores grandes limitados.

Π8.9H1. Procure contraexemplos: para cada afirmação, defina duas seqüências $(A_n)_n$ e $(B_n)_n$ que satisfazem a condição do problema, e mesmo assim, não é válida a conclusão proposta.

x8.68H1. Depende. Agora ache um exemplo e um contraexemplo.

x8.71H1. Quatro delas são, as outras não.

x8.73H1. $|A \times B| = ?$

Π8.12H1. Podemos demonstrar que $A_* \subseteq A^*$.

Π8.13H1. Comece rascunhando os dois lados, usando '$\cdots$', etc.

x9.1H1. O tipo de `foo` não é `int`. Se fosse `int` mesmo, o `foo` seria um `int`.

x9.2H1. Já que falei que isso foi bem antes de estudar funções, apague da

$$\frac{f : A \to B \qquad x : A}{f\ (x) : B}\ \text{FunApp}$$

as partes que têm a ver com funções:

$$\frac{f : A \to B \qquad x : A}{f\ (x) : B}\ \text{FunApp}$$

x9.3H1. Cardinalidade.

x9.4H1. O que significa que os domínios de duas funções são diferentes?

x9.5H1. Aplique a cod nos $\sin_1, \sin_2, \sin_3$ do Nota 9.16.

x9.7H1. Quais são o domínio e o codomínio da f?

x9.8H1. Nenhuma é sobrejetora. As f, g são injetoras; a h não. Demonstre tudo isso.

x9.12H1. Lembe-se as condições no 9.11.

x9.13H1. Não. Em vez de melhorar, a situação piorou: agora nem m nem s são funções!

x9.14H1. Lembre o que $f : A \to B$ significa para cada religião.

x9.16H1. Qual é a sobreposição dos casos que aparecem na definição da h e quais os valores da h seguindo cada um deles?

x9.19H1. O que significa ser função?

x9.26H1. Como a função $\lambda x\,.\,f\,x$ comporta?

x9.28H1. Respeite as aridades!

x9.35H1. Queremos definir a

$$uncurry : (A \to (B \to C)) \to ((A \times B) \to C)$$

então sabemos já como começar: basta definir o

$$uncurry(\ldots ?$$

Peraí: qual seria uma opção boa para denotar esse argumento?

x9.40H1. Tu vai precisar definir uma terceira função i, e usar seu black box na tua construção.

x9.44H1. Nota 9.17.

x9.45H1. $A \subseteq B \ \& \ B \subseteq C \implies A \subseteq C$.

x9.46H1. $\emptyset$.

x9.47H1. $\emptyset$.

x9.50H1. Tente achar contraexemplo desenhando diagramas internos.

x9.51H1. Siga essa definição e tente achar alguam função que não vai ser chamada constante.

x9.53H1. Use um diagrama interno para endomapas!

x9.54H1. A implicação é válida. Demonstre!

x9.56H1. O fato que uma composição é definida dá informação sobre um domínio e um codomínio envolvido.

x9.58H1. Defina como composição de funções conhecidas.

x9.60H1. O que exatamente garanta a injectividade da f^{-1}, e o que a sua sobrejectividade?

x9.61H1. Quando a função inversa é definida?

x9.64H1. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

x9.68H1. Pode acontecer que $X \in A$ e também $X \subseteq A$?

x9.70H1. É um igualdade de conjuntos, então mostre cada uma das $(\subseteq)$ e $(\supseteq)$ separadamente.

x9.71H1. Quando f *não* é bijetora, nenhum.

x9.72H1. Precisamos demonstrar que no caso que $f : A \rightarrowtail B$ as duas interpretações do símbolo $f_{-1}[Y]$ *denotam o mesmo objeto.*

x9.75H1. Pense... Como podes matar um alvo que um conjunto S é unitário? Como podes usar um fato que um conjunto S é unitário?

x9.77H1. Nenhuma é válida em geral. Procure contraexemplos.

x9.79H1. Ataque cada direção ($(\subseteq)$ e $(\supseteq)$) da primeira separadamente. Das duas $\overset{?}{=}$, são válidas as inclusões:

$$f[A \cap B] \subseteq f[A] \cap f[B]$$
$$f[A \setminus B] \supseteq f[A] \setminus f[B]$$

Demonstre; e mostre contraexemplos que demonstram que as reversas inclusões não são válidas em geral.

x9.80H1. Já demonstrou metade de cada igualdade no Exercício x9.79 até sem a hipótese que f é injetora. Basta então demonstrar as duas inclusões:

$$f[A \cap B] \supseteq f[A] \cap f[B]$$
$$f[A \setminus B] \subseteq f[A] \setminus f[B].$$

x9.82H1. Aqui uma maneira de definir a f como composição de 4 fatores:

$$f = \mathrm{inverse} \circ \mathit{squareRoot} \circ \mathit{succ} \circ \mathit{square} \circ \mathit{succ}.$$

A definição de cada um deve ser óbvia pelo próprio nome.

Π9.2H1. Fez o Exercício x9.52 né?

Π9.3H1. Lembra se que a definição é apenas aplicável numa *função*. Mas cuidado com os casos especiais que envolvem o $\emptyset$.

Π9.5H1. Para garantir que e é sobrejetora escolher como C o próprio $\mathrm{range}(f)$.

Π9.6H1. Cuidado: sobre o A não podes supor nada mais que $A \neq \emptyset$.

Π9.7H1. Calcule uns valores primeiro. Por exemplo,

$$\pi(2, \langle 2,3,5,7\rangle) = 5 \qquad \pi(0, \langle 2\rangle) = 2 \qquad \pi(3, \langle 2,0,0,1\rangle) = 1$$

Π9.10H1. Justificar um passo de demonstração com a palavrinha "lógica" não vai aumentar a confiança de ninguém sobre a validez de tal passo. De fato, nessa demonstração pelo menos um desses passos é errado.

Π9.11H1. Ambas as implicações são válidas. (Observe que $f(-)$ é a própria f.)

Π9.12H1.

$$f(-)\left\{\begin{array}{c}\text{injetora}\\ \text{sobrejetora}\end{array}\right\} \overset{?}{\iff} \left\{\begin{array}{c}f[-]\\ f_{-1}[-]\end{array}\right\}\left\{\begin{array}{c}\text{injetora}\\ \text{sobrejetora}\end{array}\right\}$$

Π9.13H1. $\bigcap_{n=0}^{\infty} \mathit{succ}^n[\mathbb{N}] = \emptyset$.

Π9.14H1. Dá pra achar um tal exemplo usando uma função $f : \wp\mathbb{N} \to \wp\mathbb{N}$.

x9.87H1. Use uma $f : A \to B$, e as identidades $\mathrm{id}_A, \mathrm{id}_B$.

x9.88H1. A forma do diagrama parece com o diagrama das leis de identidade (Exercício x9.87).

x9.98H1. Olha nas setinhas.

Π9.17H1. Seja $n = |A|$.

x9.99H1. Já calculou como achar a cardinalidade de $(X \to Y)$ para quaisquer finitos X, Y. Então *hackeia!*

x9.101H1. Isso é mais um exercício pra ver se tu consegue definir funções do que em fixpoints.

x9.102H1. Uma "distância" está sendo cada vez menor. Qual?

x9.105H1. Se tu achou valores para todas as expressões, tu errou (pelo menos uma vez). Todos eles são definidos exceto um!

x9.108H1. Por "fight club": suponha que f, f' são resoluções do sistema (FIB); demonstre que $f = f'$.

x9.110H1. Suponha que uma $h : \mathbb{N} \to \mathbb{N}$ satisfaz essa definição, e suponha que seu valor $h(5) = v$ para algum $v \in \mathbb{N}$. O que podes concluir sobre os valores da h para suas outra entradas?

x9.111H1. Por que termina a recursão para toda entrada?

Π9.18H1. Cada função parcial $f : A \rightharpoonup B$ pode ser representada como uma função total $f : A \to B'$ onde B' é um outro conjunto. Qual B' serve?

Π9.20H1. Tem sim.

Π9.21H1. A $(\Leftarrow)$ é muito fácil; para a $(\Rightarrow)$ use indução.

x9.118H1. A f^{-1} foi definida apenas quando f é bijetora.

x9.119H1. Primeiramente observe:

$$\left.\begin{array}{rcl} f \text{ tem retracção} & \implies & f \text{ é injetora} \\ f \text{ tem secção} & \implies & f \text{ é sobrejetora} \end{array}\right\} \implies f \text{ bijetora.}$$

Π9.26H1. Vai precisar de usar um singleton, $\{*\}$, não importa qual é o seu único membro.

Π9.30H1. Botei esse problema para desenferrujar tuas armas de teoria dos números (Capítulo 3).

x10.1H1. Relações *não são...*

x10.4H1. Lembre a Definição D8.68.

x10.8H1. As afirmações:

$$\begin{array}{c} \text{a pessoa } p \text{ leu a palavra } w \text{ num livro} \\ \text{a pessoa } p \text{ leu um livro onde a palavra } w \text{ aparece} \end{array}$$

estão afirmando a mesma coisa?

x10.12H1. $\mathrm{Child} \diamond \mathrm{Parent} \neq \mathrm{Parent} \diamond \mathrm{Child}$. Agora refute!

x10.13H1. Sem pensar, dois candidatos prováveis para considerar seriam a igualdade no A e a relação trivial True satisfeita por todos os pares de elementos de A:

$$\text{ou} \begin{cases} x \; I \; y \iff^{\text{def}} \mathsf{True} \\ x \; I \; y \iff^{\text{def}} x = y \end{cases}$$

x10.14H1. Questão: o que precisa achar para tua definição servir para o caso $n = 0$ também?

x10.15H1. Exercício x10.10.

x10.17H1. $(R \diamond S)^{\partial} = S^{\partial} \diamond R^{\partial}$. Demonstre!

x10.20H1. Contrapositivo.

x10.21H1. Como uma relação assimétrica poderia não ser antissimétrica? (O que significa "não ser antissimétrica"?)

x10.23H1. Cuidado: nas propriedades que acabam ser implicações, as variáveis que aparecem nas suas premissas não denotam obrigatoriamente objetos distintos!

x10.25H1. Seja justo.

x10.26H1. Use diagramas internos.

x10.27H1. Aplique fielmente essa definição na relação do Exemplo 10.49.

x10.34H1. O que podemos concluir se $a \mid b$ e $b \mid a$?

x10.37H1. Não é necessariamente nem reflexiva nem transitiva. Invente um contraexemplo para cada propriedade.

x10.38H1. Ache um contraexemplo que refuta sua transitividade.

x10.40H1. Deixe para responder junto com o Exercício x10.60.

x10.42H1. Primeiramente lembre o mesmo problema mas para a relação:

$$x \sim_{\varepsilon} y \iff^{\text{def}} |x - y| < \varepsilon$$

onde $\varepsilon > 0$; foi resolvido—eu espero—no Exercício x6.98.

x10.46H1. Será que já sabemos a outra "direção" da igualdade?

x10.47H1. Não: nossa definição vai permitir mais colecções ser chamadas "partição" do que deveriam.

Π10.2H1. Supondo que $x \; S \; y$, o que tu consegues concluir?

Π10.3H1. Não. Para achar um contraexemplo desenha as setinhas das relações envolvidas para construir os desejados x, y, z.

Π10.4H1. Indução.

Π10.5H1. Já jogou "pedra–papel–tesoura"?

Π10.6H1. Não.

Π10.8H1. Seja $n \in \mathbb{N}$. Temos:

$$a \to^n b \iff a + n = b.$$

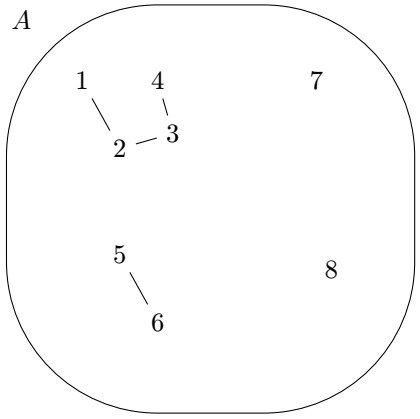
Agora demonstre que isso é válido para todo $a, b, n \in \mathbb{N}$.

Π10.10H1. Primeiramente tente entender (visualizar) essas relações.

Π10.11H1. Ache um contraexemplo para a $\overset{\infty}{=}$. As outras, são.

Π10.12H1. Se um subconjunto $X \subseteq \mathbb{R}$ é infinito, isso não quis dizer que $\mathbb{R} \setminus X$ é finito!

x10.48H1. Considere o conjunto A com a relação de equivalência R como no diagrama interno seguinte:



Lembra-se que como já declaramos a R de ser uma relação de equivalência, não precisamos botar todas as setinhas, apenas as necessárias para "gerar" a R (veja Observação 10.46). Agora, seguindo fielmente sua definição, qual é o conjunto $\mathscr{A}_R$?

x10.49H1. Mande os membros de A se separar: «se juntem todos os relacionados entre si!».

x10.54H1. Entendeu o Exemplo 10.95?

x10.56H1. Uma é a igualdade e outra é a trivial `True`. Qual é qual? Demonstre.

x10.58H1. Defina a relação tal que dois objetos são relacionados sse eles pertencem no mesmo membro da família $\mathscr{A}$.

x10.63H1. Para cada uma delas, precisa definir completamente a $f : A \to B$ (esclarecendo também quais são os A, B).

Π10.18H1. Precisas mostrar que: (1) a $\tilde{f}$ é bem-definida; (2) a $\tilde{f}$ é uma bijecção.

Π10.20H1. A ordem R' não vai ser uma ordem no A, pois não podemos decidir como "resolver conflitos" do tipo $R(a,b)$ e $R(b,a)$. Não podemos arbitrariamente escolher um dos a,b como "menor", botando assim por exemplo $R'(a,b)$ e $\neg R'(b,a)$. Isso não seria justo! Então, em qual conjunto A' faz sentido definir nossa ordem R'?

Π10.21H1. Conte "manualmente" os casos com $|A| = 0, 1, 2, 3$.

Π10.23H1. Sobre a (i): veja o Nota 10.98. Sobre a (ii): a afirmação é falsa; refute!

x11.5H1. Quem é esse e que aparece no (G3)?

x11.9H1. Capítulo 3.

x11.14H1. Não: tem como adicionar dois matrizes invertíveis e resultar numa matriz que não é.

x11.22H1. Sim; mas por quê?

x11.23H1. Não tem como achar um contraexemplo em grupos abelianos.

x11.24H1. O que exatamente é um contraexemplo nesse caso?

x11.29H1. A idéia é descrever cada lado da

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

como um caminho. Pense em duas listas de instruções para ser aplicadas no $\langle a, b\rangle$, tais que: seguindo uma das listas acabamos no $b^{-1} * a^{-1}$, e seguindo a outra no $(a * b)^{-1}$. Para o lado $(a * b)^{-1}$ existe apenas uma maneira razoável de "quebrá-lo" em sub-passos. Para o lado $b^{-1} * a^{-1}$ existem duas equivalentes. Escolha uma, ou desenha as duas no mesmo diagrama.

x11.32H1. Procure contraexemplo!

x11.34H1. Não!

x11.36H1. Só tem uma maneira. Qual? Por quê?

x11.38H1. *Essencialmente* são apenas 2. Se achar mais, verifique que renomeando seus membros umas viram iguais, e só tem dois que realmente não tem como identificá-las, mesmo renomeanos seus membros. Tudo isso vai fazer bem mais sentido daqui umas secções onde vamos estudar o conceito de isomorfia (§258).

x11.40H1. Como o próprio "operador" de exponenciar fica escondido na notação comum a^b, melhor escrever temporariamente as duas definições como:

$$\begin{aligned} a \uparrow_1 0 &= e & a \uparrow_2 0 &= e \\ a \uparrow_1 (n+1) &= a * (a \uparrow_1 n) & a \uparrow_2 (n+1) &= (a \uparrow_2 n) * a. \end{aligned}$$

Agora tem uma notação melhor para demonstrar o que queremos: $\uparrow_1 = \uparrow_2$. O que significa que duas operações (funções) são iguais?

x11.43H1. Nota 11.53 e Conselho 11.54.

x11.44H1. As potências de elementos de grupo foram definidas *recursivamente*.

x11.45H1. Sejam $x, y \in G$. Calcule o $(xy)^2$ em dois jeitos.

x11.47H1. Precisamos mostrar que existe $n \in \mathbb{N}_{>0}$ com $a^n = e$.

x11.49H1. Sejam $a, b, c \in G$. Calcule:

$$\begin{aligned}\Big(\Big(c(ab)^{-1}\Big)^{-1}(cb^{-1})\Big)(b^{-1}b)^{-1} &= \Big(\Big(c(ab)^{-1}\Big)^{-1}(cb^{-1})\Big)(b^{-1}(b^{-1})^{-1}) \\ &= \Big(\Big(c(ab)^{-1}\Big)^{-1}(cb^{-1})\Big)(b^{-1}b) \\ &\vdots \\ &= a\end{aligned}$$

x11.50H1. Basta achar um *modelo* (ou seja, algo que satisfaz as leis) que não satisfaz a proposição que queremos mostrar sua indemonstrabilidade. Qual modelo tu escolheria para cada uma delas?

x11.52H1. $\mathrm{Cls}\,(e) = \{e\}$. Por quê?

x11.53H1. Já achou uma no Exercício x11.52.

x11.54H1. Indução para os inteiros não-negativos. E os negativos?

x11.55H1. Lembre o Exercício x11.54.

Π11.2H1. O que precisamos na demonstração do fato que as leis de cancelamento implicam a existência de inversos únicos?

Π11.4H1. Para diminuir as chances de "roubar" sem querer, use uma notação adaptada às novas leis: chame 1_{R} a identidade-direita grantida pela (G2R) e use a^{R} para o inverso-direito de a, garantido pela (G3R); similarmente use 1_{L} e a^{L} para a identidade-esquerda e os inversos-esquerdos, garantidos pelas (G2L) e (G3L).

Π11.5H1. Como podemos usar o fato que um conjunto é finito?

Π11.6H1. Não. Como podemos demonstrar isso?

Π11.7H1. Separe os casos em $o(a) = n \in \mathbb{N}$ e $o(a) = \infty$.

Π11.8H1. Num grupo abeliano, o que podes afirmar se $a \approx b$? (A próxima dica já tem a resposta, depois disso vai faltar só demonstrá-la.)

x11.60H1. Demonstre primeiro que H é fechado sob inversos, tomando um $h \in H$ e demonstrando que $h^{-1} \in H$. Depois basta demonstrar que H é fechado sob a operação, tomando $a, b \in H$ e demostrando que $ab \in H$.

x11.63H1. São 6. Ache todos.

x11.64H1. (G0).

x11.65H1. Precisa mostrar que $H_1 \cap H_2 \neq \emptyset$ e que é fechado sobre a operação do grupo e sobre inversos.

x11.68H1. É uma relação de equivalência. Demonstre as 3 propriedades!

x11.69H1. Use o Critérion 11.99.

x11.72H1. Calcule o $\langle 4, 6\rangle$ no $(\mathbb{Z}\,;+)$.

x11.73H1. Se G fosse abeliano, daria certo.

x11.75H1. Considere o "produto vazio" igual ao $e \in G$.

x11.78H1. Tem como mostrar $b^{-8} \in A_4$.

x11.82H1. Como já demonstramos que $\bigcap \mathscr{H}$ é um grupo, e como K também é grupo, basta demonstrar $\bigcap \mathscr{H} \subseteq K$.

x11.85H1. Ele tem dois.

Π11.12H1. Tem como construir mesmo esse N.

Π11.15H1. Não! O Q_1 tem "buracos" nele, e o Q_2 não tem! Tem com achar um tal buraco no Q_1.

x11.93H1. Tome $G := (\mathbb{Z}\,;+)$ e $H := (m\mathbb{Z}\,;+)$. E agora? O que cada uma das

$$a \equiv b \pmod{m} \qquad\qquad a \equiv b \pmod{H}$$

tá dizendo nesse caso?

x11.94H1. Sem perda de generalidade, podes supor que $a \in H$ e $b \notin H$. Comece desenhando como fizermos no CASO 1.

x11.95H1. Ache dois exemplos com $a, b \notin H$, tais que num $a \equiv b \pmod{H}$ e no outro $a \not\equiv b \pmod{H}$.

x11.99H1. Podemos concluir que: *se $a \notin H \leq G$ então H e Ha são disjuntos.*

x11.105H1. Se $H \leq G$, pelo teorema de Lagrange temos que $o(H) \mid o(G)$. Quais são os divisores de $o(G)$?

x11.106H1. Se achar um subgrupo $H \leq G$ com $o(H) = o(a)$, acabou (graças ao Lagrange).

x11.107H1. Corolário 11.163.

x11.115H1. Basta demonstrar que qualquer escolha de representante envolvida não afetará o resultado.

x11.118H1. A $(\forall g \in G)\big[\, gNg^{-1} = N \,\big]$. Por quê?

x11.121H1. Maneira 1: imediato pelos: Teorema Θ11.155 e Corolário 11.192.
Maneira 2: Use o "one-test" Critérion 11.103. Observe que SN é indexado pelo conjuto $S \times N$ e logo basta tomar um arbitrário par $\langle s, n\rangle \in S \times N$ para ganhar um arbitrário membro do SN: o sn.

x11.122H1. Temos $S \cap N \leq N \leq G$ como intersecção de subgrupos (veja exercícios x11.65 e x11.61). Para mostrar que $S \cap N \trianglelefteq S$, tente demonstrar que $S \cap N$ é fechado pelos conjugados no S.

Π11.18H1. Para chegar num absurdo, suponha que P é o maior primo. Considere o número $2^P - 1$.

Π11.20H1. Sendo o H infinito, basta demonstrar que o Ha também é?

Π11.22H1. A afirmação é válida; demonstre.

x11.123H1. Ela não é uma isometria. Demonstre!

x11.125H1. São 8.

x11.128H1.

$$\overbrace{\{I, R, R', R'', \Delta_1, \Delta_2, H, V\}}^{\mathcal{D}_4}$$

? ? ?

? ? ? ? ?

?

x11.129H1. Não pode ser o S_4 obviamente, por questão de tamanho!

x11.141H1. Procure uma propriedade grupoteórica que um dos dois tem e o outro não.

x11.142H1. Primeiramente verifique que $\ker\varphi \neq \emptyset$. Agora, graças ao Critérion 11.99, precisas demonstrar: (i) $\ker\varphi$ é $*$-fechado; (ii) $\ker\varphi$ é $^{-1}$-fechado.

x11.143H1. Acabamos de demonstrar que $\ker\varphi \leq \mathcal{A}$ no Exercício x11.142. Basta demonstrar que $\ker\varphi$ é fechado pelos conjugados. Seja $k \in \ker\varphi$ e tome $a \in A$. Precisamos demonstrar que o a-conjugado de k também está no $\ker\varphi$: $aka^{-1} \in \ker\varphi$. Ou seja, basta verificar que realmente $\varphi(aka^{-1}) = e_B$.

x11.144H1. Aplicamos a propriedade que homomorfismos preservam os inversos. Aplique outra propriedade de homomorfismos.

x11.145H1. Precisas mostrar que $\operatorname{im}\varphi$ é fechado sob a operação e sob inversos.

x11.147H1. Basta demonstrar que $! : F \to G \times H$ é um homomorfismo mesmo. Demonstre!

x11.150H1. Que tipo de coisa é o coproduto literalmente?

Π11.26H1. Se F é injetora, então: $x = y \iff F(x) = F(y)$.

Π11.27H1. Enxergue bem todos os seus alvos: (i) $\operatorname{Inn} G \subseteq \operatorname{Aut} G$; (ii) $\operatorname{Inn} G \leq \operatorname{Aut} G$; (iii) $\operatorname{Inn} G \trianglelefteq \operatorname{Aut} G$. O que precisas demonstrar para matar cada um deles?

Π11.28H1. Não é! Ela não é transitiva. Demonstre!

Π11.29H1. Formalização: *Seja G grupo e $N \trianglelefteq G$. Logo existem grupo G' e homomorfismo $\varphi : G \to G'$ tal que N é o kernel de φ.*

x12.2H1. Não! Mas como podemos demonstrar que não tem como demonstrar isso?

x12.3H1. Precisamos demonstrar que $\varphi(\varepsilon_M) = \varepsilon_N$. Como podemos ler essa igualdade em lingua (mais) natural?

x12.9H1. Lembre o Exercício x11.16?

x12.10H1. Lema Λ12.22.

x12.12H1. $p + p = (p + p)^2 = \dots$

x12.13H1. Calcule o $(p + q)^2$.

x12.14H1. Use os Exercício x12.12 e x12.13.

x12.19H1. $a \vee (a \wedge (a \vee a))$.

x13.1H1. Começa com o $\mathbb{N}$ e filtre seus elementos usando suas relações de ordem.

x13.2H1. Cuidado com as operações e os tipos dos seus argumentos.

x13.4H1. $\mathbb{N} <_{\mathrm{c}} \mathbb{Z}$?

x13.5H1. Realmente

$$A \leq_{\mathrm{c}} B \iff (\exists f)[\, f : A \rightarrowtail B \,].$$

Demonstre!

x13.12H1. Nenhuma. Ache contraexemplos.

x13.13H1. Curry!

x13.15H1. $S_n = \{\, (x, y) \mid ____ ? ____ \,\}$.

x13.19H1. As expansões são distintas sim; os números que representão não.

x13.20H1. Os únicos conflitos de expansões envolvem reais com exatamente duas expansões: uma que a partir duma posição só tem 0's, e uma que a partir duma posição só tem 9's.

x13.21H1. Como tu vai demonstrar que o número construido pela método diagonal de Cantor realmente é um elemento de $\mathbb{Q} \cap [0,1]$?

x13.23H1. Tente aproveitar que composição de bijecções é bijecção, quebrando assim cada tarefa em tarefas menores e mais fáceis para resolver, tais que a composição das resoluções delas, resultará na resolução da tua tarefa inicial.

x13.24H1. Esticar um intervalo dum comprimento finito para outro maior é bem facil visualizar. Mas como esticamos um intervalo de comprimento finito para a reta dos reais cujo comprimento é infinito?

x13.25H1. Escolhe uma pessoa $x \in A \cup B$. Independente se ela é homem ou mulher, podemos a perguntar: *«quem te ama?»*. Duas possibilidades existem: ou ela é amada por algum $x_1 \in A \cup B$, ou ninguém ama x. No primeiro caso perguntamos x_1 a mesma pergunta, definindo assim o x_2, se x_1 é uma pessoa amada, etc. Observerve que cada $x \in A \cup B$ defina assim um *caminho amoroso* $x, x_1, x_2, \ldots$. Esse caminho ou é infinito, ou termina num certo membro $x_n \in A \cup B$. Vamos agora separar todas as pessoas do $A \cup B$ em três grupos:

$$\begin{aligned} G_A &= \{\, x \in A \cup B \mid \text{o caminho amoroso de } x \text{ termina num membro de } A \,\} \\ G_B &= \{\, x \in A \cup B \mid \text{o caminho amoroso de } x \text{ termina num membro de } B \,\} \\ G_\infty &= \{\, x \in A \cup B \mid \text{o caminho amoroso de } x \text{ é infinito} \,\} \end{aligned}$$

Tente casar todos os membros de cada um desse grupo entre si!

x13.31H1. Seja A conjunto e defina a $f : A \to \wp A$ pela

$$f(x) = \{x\}\,.$$

Demonstre que é injetora.

x13.32H1. O que significa que dois conjuntos são iguais?

Π13.3H1. (1) Precisamos disso para que f seja bem-definida (por quê?). (2) A f não é bijetora! (Por quê?)

Π13.4H1. Aqui duas maneiras diferentes para o $(a,b) =_{\mathrm{c}} [a,b)$: (i) demonstre $[0,+\infty) =_{\mathrm{c}} (-\infty,+\infty)$; (ii) demonstre $(0,1] =_{\mathrm{c}} (0,1)$.

Π13.5H1. Já sabemos que o $\mathbb{Q}$ é contável; logo o $\mathbb{Q} \cap [0,1] \subseteq \mathbb{Q}$ também é. Seja $(q_n)_n$ uma enumeração dos racionais do $[0,1]$.

Π13.7H1. Cada relação de equivalência corresponde numa partição e vice-versa, então basta definir três partições.

Π13.8H1. Seja $T \subseteq A$ o conjunto de todos os terminantes elementos de A. Basta demonstrar que $T \notin \varphi[A]$, ou seja, que para todo $x \in A$, $A_x \neq T$, demonstrando assim que φ não é bijetora.

Π13.9H1. Considere a diámetro horizontal $\{\, (x,0) \mid -1 < x < 1 \,\}$.

Π13.10H1. Se π fosse algébrico, $i\pi$ também seria.

x14.3H1. Praticamente já resolvido no Lema Λ4.112. Por quê? (O que falta observar ou verificar?)

Π14.3H1. Seja $A_n := \mathbb{N} \setminus \{0, 2, \ldots, 2n-2\}$ o $\mathbb{N}$ sem os primeiros n números pares. Mostre que: *se* $B \subseteq A_n$ *para todo* $n \in \mathbb{N}$*, então* B *não é cofinito.*

Π14.6H1. O $(\wp A\,;\subseteq)$ é um reticulado completo.

x16.2H1. (ZF2) & Teorema Θ16.23.

x16.4H1. No exercício anterior construimos uns conjuntos com cardinalidade até 2. Tente construir conjunto com cardinalidade 3.

x16.5H1. Não são 4.

x16.6H1. Usando o (ZF4), criamos subconjunto de um conjunto dado.

x16.7H1. Começa considerando dados conjuntos a e b. Procure um *conjunto* que contenha todos os membros da classe $a \setminus a$ que tu queres construir como conjunto. Cuidado: nesse caso não temos as duas opções que tivemos na Definição D16.30.

x16.8H1. Dados conjuntos a e b, precisas achar um *conjunto* W que contenha todos os membros de $a \cup b$, para depois filtarar apenas os certos usando como filtro a fórmula

$$\varphi(x) := x \in a \vee x \in b$$

para a operação $- \cup -$; e similarmente para a $- \triangle -$ só que para essa o filtro vai ser a fórmula

$$\varphi(x) := (x \in a \wedge x \notin b) \vee (x \notin a \wedge x \in b).$$

x16.12H1. Não. Por quê?

x16.14H1. Dado $n \in \mathbb{N}$ construa primeiramente um conjunto com cardinalidade maior-ou-igual, e aplique o Separation (ZF4) para ficar com apenas n elementos. Formalmente, use indução!

x16.15H1. (Sobre o operador $\cup$.) Combine os operadores $\bigcup -$ e $\{-,-\}$!

x16.16H1. De jeito nenhum! Por quê?

x16.19H1. Como a direção '$\Longleftarrow$' poderia ser inválida?

x16.22H1. Trabalhe como fizemos para o par ordenado de Kuratowski no Exercício x16.21 e nas proposições 16.50–16.51.

x16.23H1. Calcule os $\langle 0,0\rangle$, $\langle 0,1\rangle$, $\langle 1,0\rangle$, $\langle 1,1\rangle$.

x16.24H1. O $\langle x,y\rangle$ não satisfaz a (TUP1). Mostre um contraexemplo, ou seja, ache objetos x, y, x', y' tais que:

$$\langle x,y\rangle = \langle x',y'\rangle$$

e mesmo assim não temos $x = x'$ e $y = y'$.

x16.25H1. Para demonstrar a (TUP2), dados conjuntos a, b, tome $x \in a$ e $y \in b$ e ache um conjunto w tal que $\langle x, y\rangle \in w$. (Exatamente como a gente fez no Propriedade 16.51.)

x16.33H1. (Resolva primeiro o Problema Π9.18.) Cada função parcial $f : A \rightharpoonup B$ pode ser representada como uma função total $f : A \to B'$ onde B' é um outro conjunto. Qual B' serve?

x16.37H1. Esse $\mathbb{N}$ aí é o que mesmo?

x16.38H1. Apague o $\cdot$ do ; ué.

Π16.2H1. Para o (1), veja o (2); para o (2), veja o (1)!

Π16.4H1. (ii) Absurdo.

Π16.6H1. Indução!

Π16.7H1. O desafio aqui é conseguir escrever a afirmação "o x é um conjunto finito" com uma fórmula.

x16.40H1. *Não é* uma conseqüência imediata do Infinity (ZF7). Por que não?

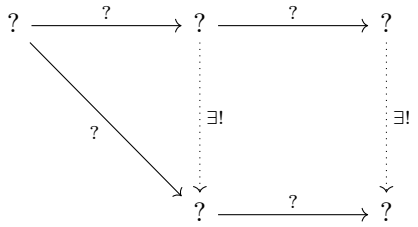
x16.41H1. O artigo.

x16.42H1. Olhe para os subconjuntos de I.

x16.50H1. Pela definição de sobrejetora e de imagem, basta demonstrar que $\varphi[\mathbf{N}_1] = \mathbf{N}_2$.

x16.51H1. O que é uma função em nosso dicionário, e quem garanta que escrevendo assim do nada duas equações sobre um certo objeto F, isso realmente defina uma função?

x16.52H1. Uma forma razoável tem a forma seguinte:



Basta nomear os objetos e as setas.

x16.53H1. Podemos "quebrar" a afirmação nessas partes:

(1) $f : \mathbf{N} \rightharpoonup A$
(2) $\langle 0, a\rangle \in f$
(3) Para qualquer $n \in \mathbf{N}_{\neq 0}$, se f é definida no n, então ela também é definida no predecessor de n, e o valor dela no n é o correto, ou seja, o valor que ganhamos aplicando a h no valor do predecessor de n.

O único que precisamos formalizar agora é o último.

x16.55H1. Verifique que $\operatorname{dom} F \subseteq \mathbf{N}$. Agora basta demonstrar que $\operatorname{dom} F = \mathbf{N}$, usando o princípio da indução.

x16.57H1. Seja $X \subseteq \mathbf{N}$ o conjunto onde F e G "concordam". Mostre que $X = \mathbf{N}$ usando o princípio da indução.

x16.58H1. Indução no $m \in \mathbf{N}_1$.

x16.59H1. Demonstre as duas direções da ($\Leftrightarrow$) separadamente.

Π16.8H1. Para representar a multiplicidade, use uma função com codomínio o $\mathbb{N}_{>0}$.

x16.67H1. Qual operador $\Phi(-)$ tu podes definir para aplicá-lo no a?

x16.69H1. Seja x conjunto. Não podemos aplicar o α16.110 diretamente no x, pois talvez $x = \emptyset$. Uma abordagem seria separar casos. Ao inves disso, aplique o α16.110 no conjunto $\{x\}$.

x16.75H1. Lembre-se que usamos a ordem (anti)lexicográfica nos produtos. Tome A tal que $\emptyset \neq A \subseteq \omega^2 + 1$ e ache se u mínimo. Separe casos dependendo se $A = \{\top\}$ ou não, onde $\top$ o máximo elemento do $\omega^2 + 1$.

Π16.11H1. Tente achar uma class-function Φ tal que aplicada nos elementos dum conjunto A, vai "identificar" todos aqueles que *não* tem a propriedade $\varphi(-)$, mas mesmo assim sendo injetora quando restrita naqueles que satisfazem a.

Π16.12H1. Podemos sim. Dados *objetos* a, b, mostre que existe o conjunto $\{a, b\}$ que consiste em exatamente esses objetos.

Π16.14H1. Obviamente, teu contraexemplo tem que envolver conjuntos mal-fundamentados.

x17.2H1. De Pythagoras. Como? Demonstre!

x17.4H1. Olhe para a demonstração do Teorema Θ6.90.

x17.7H1. A afirmação é falsa. Ache uma vizinhança N_x dum ponto x tal que N_x não é aberto. Dá pra achar nos reais.

x18.7H1. (1) A definição de $A^\flat$ é simétrica nos A e A^c.

x18.10H1. Precisa demonstrar que as leis de categorias são satisfeitas considerando como objetos espaços topológicos e como setas funções contínuas.

Π20.1H1. Cuidado com Curry.

Dícas #2

x1.20H2. Para implementar o `while` por exemplo, considere que o desafío é transformar o programa `while`$(\alpha)\{\kappa\}$. Para o `for`, talvez algo como `for`$(\alpha;\beta;\gamma)\{\kappa\}$ ajudaria.

x2.3H2. Procure um contraexemplo onde a e b tem um fator em comun.

Π2.4H2. Podemos derivar a simetria e a transitividade a partir da reflexividade e da substituição (que aceitamos sim como axiomas). Como?

x3.8H2. Para a existência procure achar o que pode encaixar no lugar do x para satisfazer a igualdade (umas coisas precisam ser canceladas.

x3.22H2. Começa assim:

> «Sejam A conjunto de inteiros e $\heartsuit$ uma operação binária:
>
> $$\heartsuit : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int}.\text{»}.$$

Isso estabelece o contexto desejado para finalmente definir o que precisamos. Continuaria assim:

> «Chamamos o conjunto A de ($\heartsuit$)-fechado sse. . . »

x3.34H2. Sejam a, b inteiros. Aproveitando a tricotomía (ZP-Tri) basta demonstrar as três equivalências:

$$b - a \in \iff a < b \qquad b - a = 0 \iff a = b \qquad -(b - a) \in \iff a > b.$$

x3.42H2. Pelas $m_1 \leq m_2$ e $m_2 \leq m_1$ concluimos que $m_1 = m_2$.

x3.56H2. Supondo que há inteiro estritamente entre dois inteiros consecutivos, forneça um inteiro entre 0 e 1.

x3.59H2. Seja $\varphi(n) \overset{\text{def}}{\iff} n = 0$ ou $n \geq 1$.

x3.85H2.

$$x(x+y)^k y(x+y)^k = x\sum_{r=0}^{k} C(k,r)x^{k-r}y^r + y\sum_{r=0}^{k} C(k,r)x^{k-r}y^r.$$

x3.86H2. Divida o a por n e, olhando para o resto r, ache o certo i tal que $n \mid a_i$.

x3.95H2. Antes de usar o PBO precisas demonstrar que o S possui membros positivos.

x3.111H2. Talvez as propriedades do Λ3.26 são úteis.

x3.115H2. $\cdots$

x3.117H2. Qual seria o resto em cado caso?

x3.118H2. $x > y \implies quot(x, y) \geq 1$.

x3.121H2. Indução.

x3.126H2. Temos p, q primos distintos e logo coprimos e logo o Corolário 3.134 ajuda.

Π3.18H2. "*Para todo $x \in \mathbb{Z}$, o* EUCLID(x, n) *termina com o resultado certo.*"

Π3.19H2. Vai pelo absurdo.

Π3.22H2. Se $n! - 1$ não é primo, toma um dos seus primos divisores, p.

Π3.23H2. $m! + 2$.

Π3.25H2. Qual é o maior termo e como ele muda depois cada passo?

Π3.26H2. Seja p_i o i-ésimo primo ($p_0 = 2$, $p_1 = 3$, $p_2 = 5$, ...). Como podemos escrever o aleatório $n \in \mathbb{N}$?

x3.141H2. Agora divida o k por a.

x3.146H2. Para a ($\Rightarrow$), lembre os $(\cdot)$-inversos vêm em parzinhos; quais deles são casados com eles mesmo? (Ou seja: quais são o seu próprio inverso?)

x3.154H2. Tente substituir a congruência $5x \equiv 2 \pmod 6$ com um sistema equivalente, de *duas* congruências.

x3.157H2. $2 \mid 10 \implies 2^3 \mid 10^3$.

Π3.29H2. O quadrado dum número que não é múltiplo de 3 é congruente ao 1 módulo 3.

Π3.30H2. Use o Problema Π3.20.

Π3.31H2. O que Euclides faria?

x3.163H2. Divide ele por 10.

x3.165H2. $(41, 3) = 1$.

Π3.38H2. China.

Π3.39H2. $p - 1 = \phi(p)$ para qualquer primo p.

x4.5H2. $2(n + 1) = 2n + 2$.

x4.6H2. A primeira equação é fácil completar:

$$n \cdot 0 = 0$$

talvez ajuda pensar numa outra equação mais simples:

$$n \cdot S0 = ____$$

Depois?

x4.13H2. Calculamos:

$$\begin{aligned} (a + m) + y &= (a + m) + 0 \qquad \text{(hipótese do caso)} \\ &= \ldots? \end{aligned}$$

x4.15H2. Está no último cálculo.

x4.16H2. Não seria bom ter uma distributividade?

x4.17H2. Demonstre a base da tua indução com uma sub-indução!

x4.19H2. Base: $(\forall x)(\forall a)\big[\, x^{a+0} = x^a \cdot x^0 \,\big]$.

x4.20H2. Base: $(\forall a)(\forall b)\big[\, a^{b\cdot 0} = (a^b)^0 \,\big]$.

x4.21H2. Base: $S0^0 \stackrel{?}{=} S0$:

Π4.3H2. Mesmo que a função T tem aridade 2, escolhendo bem, tu não precisarás escrever 4 equações, mas apenas 2.

Π4.4H2. $0 \in \mathbb{N}$.

Π4.5H2. Para chegar num absurdo suponha que existe $C \subseteq \mathbb{N}$ não vazio tal que C não possui mínimo. Vamos demonstrar que para todo $n \in \mathbb{N}$, C não possui membros $c \leq n$. Isso é suficiente para garantir que C é vazio.

x4.35H2. Definimos a internalização da $(=)$, eq, assim:

$$\begin{aligned}
&\mathrm{eq} : \mathsf{Nat} \times \mathsf{Nat} \to \mathsf{Bool} \\
&\mathrm{eq}\ (\mathsf{O}, \mathsf{O}) &&= \mathsf{True} \\
&\mathrm{eq}\ (\mathsf{O}, \mathsf{S}\ _) &&= \mathsf{False} \\
&\mathrm{eq}\ (\mathsf{S}\ _, \mathsf{O}) &&= \mathsf{False} \\
&\mathrm{eq}\ (\mathsf{S}\ m, \mathsf{S}\ n) &&= \mathrm{eq}\ (m, n).
\end{aligned}$$

Π4.11H2. A demonstração depende desse mesmo princípio que está demonstrando, e logo acaba sendo uma demonstração trivial (tendo já o princípio), ou incompilável (não o tendo). O desafio é perceber onde que tal princípio foi usado nesta demonstração.

x4.53H2. Cada uma dessas funções é definida por exatamente duas equações, uma para cada construtor de $\mathsf{Tree}alpha$.

x4.54H2. O formato da indução aqui vai ter dois casos: Caso $(\mathsf{Tip}\ t')$; Caso $(\mathsf{Fork}\ \ell\ r)$. No primeiro não há hipótese indutiva; no segundo temos duas: uma sobre ℓ e uma sobre r.

x4.60H2. Defina a

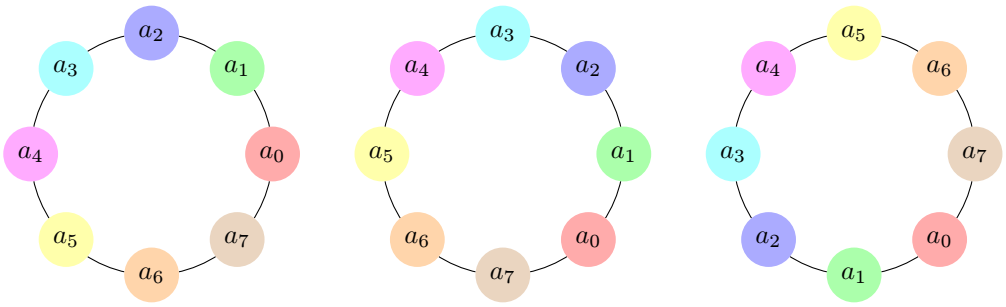
$$\begin{aligned}
&\mathrm{map} : (\alpha \to \beta) \to \mathsf{Tree}\ \alpha \to \mathsf{Tree}\ \beta \\
&\mathrm{map}\ f\ (\mathsf{Tip}\ x) &&= \mathsf{Tip}\ (f\ x) \\
&\mathrm{map}\ f\ (\mathsf{Fork}\ \ell\ r) &&= \mathsf{Fork}\ (\mathrm{map}\ f\ \ell)\ (\mathrm{map}\ f\ r)
\end{aligned}$$

e demonstre por indução as duas leis:

$$\begin{aligned}
\mathrm{map}\ \mathrm{id} &= \mathrm{id} \\
\mathrm{map}\ (f \circ g) &= \mathrm{map}\ f \circ \mathrm{map}\ g.
\end{aligned}$$

Note que, traduzindo essas igualdades, ambas são proposições da forma

$$(\forall t : \mathsf{Tree}\ \alpha)[\ldots].$$



Apenas uma das configurações da pulseira, representada em três desenhos.

Π4.19H2. Uma base não é suficiente: demonstre para $n := 0, 1$.

x5.2H2. Separa os strings possíveis em colecções e conta os strings de cada colecção separadamente, somando no final (princípio de adição) para achar o resultado.

x5.3H2. Considere uma configuração do Exemplo 5.11. Com quantas configurações do problema atual ela corresponde?

x5.4H2. Primeiramente, esqueça os homens (ou as mulheres) e coloca as 4 mulheres (ou os 4 homens) num ciclo. De quantas maneiras pode escolher o resto para entrar no círculo?

x5.5H2. Veja a figura. Pode explicar por que as três representações correspondem na mesma configuração?

x5.8H2. Cada somatório é apenas um caso especial do teorema binomial.

x5.12H2. Separe as seqüências em dois grupos: aquelas que começam com 2, e aquelas que começam com 3.

x5.13H2. Quando $g(n) \neq f(n)$?

x5.14H2. Em cada intersecção tem 3 opções: `L`, `F`, `R`.

x5.15H2. Seja $f(a)$ o número de caminhos diferentes que o motorista pode seguir com a unidades de combustível.

x5.16H2. Seja $f(a, x, y)$ o número de caminhos diferentes que acabam com descolamento total de y unidades para norte e x para leste, para um motorista que tem a unidades de combustível no seu carro.

Π5.3H2. Coloque os não-múltiplos de 3 primeiramente numa ordem, deixando espaços entre-si para os múltiplos de 3.

Π5.6H2. O quadradinho na posição $(1, 1)$ pode ser coberto em apenas duas maneiras: (A) por uma peça ocupando as posições $(1, 1)$–$(1, 2)$; (B) por uma peça ocupando as posições $(1, 1)$–$(2, 1)$.

Π5.9H2. Sejam $a(n)$ e $b(n)$ o número de maneiras que Aleco e Bego podem subir uma escada de n degraus, respectivamente.

Π5.11H2. Seja $a(n)$ o número dos strings ternários de tamanho n tais que não aparece neles o substring 00.

Π5.15H2. Considere as propriedades:

$$\alpha : \text{aparece o } \texttt{AA} \qquad \beta : \text{aparece o } \texttt{BB} \qquad \gamma : \text{aparece o } \texttt{CC} \qquad \delta : \text{aparece o } \texttt{DD}.$$

Π5.16H2. Sejam $a(n)$ e $b(n)$ o número de strings binários de tamánho n que terminam em 0 e em 1 respectivamente.

Π5.17H2. Seja $f(m,n)$ o número de maneiras que Xÿźźÿ pode matar todos os n lemmings, começando com m pontos de mana.

x6.118H2. Mas eventualmente?

Π6.1H2.

$$\frac{2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot \cdots}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot \cdots} = \frac{2\cdot 2\cdot 2}{1\cdot 2\cdot 3}\cdot\frac{2\cdot 2\cdot 2\cdot 2\cdot \cdots}{4\cdot 5\cdot 6\cdot 7\cdot \cdots} = \frac{4}{3}\cdot\frac{2\cdot 2\cdot 2\cdot 2\cdot \cdots}{4\cdot 5\cdot 6\cdot 7\cdot \cdots} \leq \frac{2\cdot 2\cdot 2\cdot 2\cdot \cdots}{4\cdot 4\cdot 4\cdot 4\cdot \cdots}$$

e agora?

x6.128H2. Procure definir um subconjunto de $\mathbb{R}$ que será garantido ter um supremum, e use esse supremum para definir o infimum de A.

x6.134H2. Pelo (MCT), seja ℓ o limite da $(\vartheta^n)_n$.

x6.139H2. Lembre do Exercício x6.41.

Π6.7H2. Para chegar num absurdo, suponha que ambos os

$$S = e + \pi \qquad\qquad P = e\pi$$

são algébricos. Se conseguir achar um polinómio com coeficientes algébricos tal que e, π são raizes dele então acabou!

x8.5H2. Escrevemos a fórmula

$$\exists a(a \in A \wedge \forall x(x \in A \to x = a))$$

como

$$(\exists a \in A)(\forall x \in A)[\, x = a \,].$$

x8.8H2. Basta achar um filtro que garante que nenhum objeto "passa":

$$\{\, x \mid ____ ? ____ \,\}$$

x8.9H2. Suponha que A, B são vazios. Qual é teu alvo agora, e o que ele significa mesmo?

x8.10H2. Qual é teu alvo agora? Achar um absurdo qualquer! Como podemos usar o fato de $A \neq B$? Lembre-se que $A \neq B$ é apenas uma abreviação para $\neg(A = B)$.

x8.22H2.

$$\{\, t(x_1,\ldots,x_n) \mid \varphi(x_1,\ldots,x_n) \,\} \stackrel{\text{def}}{=} \{\, x \mid __?__ \,\}$$

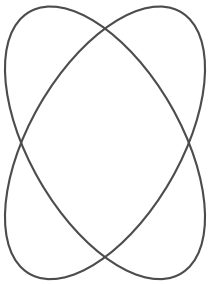
x8.41H2. $\bigcap \mathcal{U} = \emptyset$. Por quê?

x8.47H2. O teu alvo é demonstrar que um conjunto está contido em outro. Como atacamos isso?

Π8.4H2. Indução.

Π8.7H2. Intervalos não triviais (com pelo menos 2 membros) de reais com certeza são infinitos.

Π8.8H2. Começa assim:



x8.51H2. Como usamos os fatos $A \neq \emptyset$ e $B \neq \emptyset$?

x8.55H2. Seja t tripla. Definimos

$$\pi^3_0 t = \ldots?\ldots \qquad \pi^3_1 t = \ldots?\ldots \qquad \pi^3_2 t = \ldots?\ldots$$

Π8.12H2. Use as definições, passo a passo.

Π8.13H2. Vamos primeiramente analisar o $A_* = \bigcup_i \bigcap_{j\geq i} A_j$. É uma união duma seqüência de conjuntos, então faz sentido observar pelo menos os primeiros membros dessa seqüência. Quais são?

x9.3H2. Se por acaso $|(A \to B)| = |B|^{|A|}$, isso seria uma justificativa boa para a notação B^A. (Lembra da $|A \times B| = |A| \cdot |B|$?)

x9.8H2. Para refutar que h é injetora, observe que $12 = 2^2 \cdot 3$ e $18 = 2 \cdot 3^2$.

x9.35H2. Que tipo de coisa é esse argumento? Uma função $A \to (B \to C)$, ou seja, uma função de ordem superior; vou escolher F aqui, para me lembrar desse fato. Voltando então:

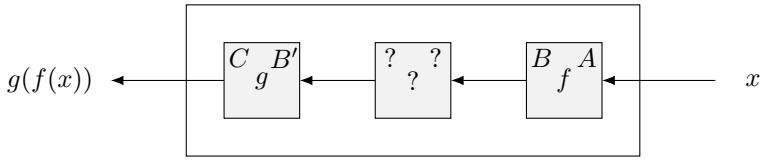
$$\mathit{uncurry}(F) = \ldots?$$

O que eu ganhei e o que eu preciso construir? Ganhei

$$F : A \to (B \to C)$$

e preciso algo do tipo $(A \times B) \to C$. Então já sei como começar. Como?

x9.40H2. O que falta é decidir o que botar nos "?" abaixo, e definir formalmente a função que corresponde nesta caixa:



x9.53H2. Observe que em geral, aparecem certos "redemoinhos" num diagrama interno de endomapa quando ela é idempotente.

x9.58H2. Inclusão.

x9.60H2. Considere:

$$\begin{aligned} \text{totalidade da } f &\implies f^{-1} \text{ sobrejetora} \\ \text{determinabilidade da } f &\implies f^{-1} \text{ injetora.} \end{aligned}$$

x9.61H2. Aplique duas vezes a Definição D9.162 de função inversa para demonstrar que as duas funções são iguais.

x9.64H2. Para demonstrar a $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, tome $x \in C$ e $z \in A$ e mostre a equivalência

$$(g \circ f)^{-1}(x) = z \iff \big(f^{-1} \circ g^{-1}\big)(x) = z.$$

x9.68H2. Vamos adoptar temporariamente a notação $f(X)$. Daí, te pergunto: se $f : \mathbb{N} \to \mathbb{N}$ é o sucessor, tem como calcular os seguinte?:

$$f(5); \qquad f(8); \qquad f(\{1,7\}); \qquad f(2\mathbb{N});$$

onde $2\mathbb{N} \subseteq \mathbb{N}$ é o conjunto dos pares naturais. "Fácil" tu pensou (certo?), e explicou:

$$f(5) \ldots \text{é o valor da } f \text{ no } 5, \text{ definido pois } 5 \in \operatorname{dom} f$$

e similarmente sobre o $f(8)$, mas

$$f(\{1,7\}) \ldots \text{não pode ser o valor da } f \text{ no } \{1,7\}, \text{ pois } \{1,7\} \notin \operatorname{dom} f.$$

Então $f(\{1,7\})$ só pode ser a f-imagem do $\{1,7\}$ que realmente é um subconjunto do $\operatorname{dom} f$; e similarmente sobre o $f(2\mathbb{N})$. E assim tu calculou as respostas:

$$f(5) = 6; \qquad f(8) = 9; \qquad f(\{1,7\}) = \{2,8\}; \qquad f(2\mathbb{N}) = \{1,3,5,\ldots\}.$$

Beleza, mas acontece que o $\mathbb{N}$ é um conjunto homogêneo (8.6). Imagine que o domínio da f tem todos os objetos seguintes como membros:

$$1, \quad 7, \quad \{1,7\}.$$

Agora, se eu perguntar qual é o $f(\{1,7\})$ tu tens um dilemma:

$$f(\{1,7\}) \stackrel{?}{=} \begin{cases} \text{a } f\text{-imagem do } \{1,7\} & \text{(que realmente é um subconjunto do seu domínio)} \\ \ldots \text{ou} \ldots & \\ \text{o valor da } f \text{ no } \{1,7\} & \text{(que realmente é um membro do seu domínio)?} \end{cases}$$

x9.71H2. Se f é bijetora, o símbolo $f_{-1}[Y]$ pode ter duas interpretações diferentes. Quais? E isso é um problema mesmo por quê?

x9.72H2. Temporariamente mude tua notação para ajudar teus olhos distinguir entre as duas interpretações melhor. Use, por exemplo, $f_{-1}[-]$ para denotar a preimagem através da f. Assim teu alvo fica enxergável:

$$(\forall Y \subseteq B)\big[\, f^{-1}[Y] = f_{-1}[Y] \,\big].$$

x9.75H2. Como matar o alvo que um conjunto S é unitário? Basta mostrar duas coisas: (1) S tem pelo menos um membro (ou seja: $S \neq \emptyset$); (2) S tem no máximo um membro (ou seja: para todo $s, s' \in S$, temos $s = s'$). E como usar o fato que um conjunto S é unitário? Para todos os $s, s' \in S$, ganhamos que $s = s'$.

x9.77H2. O enunciado do Teorema Θ9.176 pode te ajudar pensar em contraexemplos.

x9.82H2. Não se preocupe se não conseguir a k neste momento. Daqui a pouco (§214) vai parecer fácil.

Π9.2H2. Basta demonstrar que para todo $n \in \mathbb{N}$

$$(\forall x \in \mathbb{N})[\, succ^n(x) = x + n \,]$$

e como $succ^n$ (oficial) foi definida recursivamente, como tu vai demonstrar isso?

Π9.6H2. A parte do problema sobre a $f : A \rightarrowtail \wp A$ foi resolvida no Exercício x9.10. Falta a parte sobre a $g : \wp \twoheadrightarrow A$.

Π9.10H2. O problema está na $\overset{6}{\Longleftrightarrow}$. Uma da suas direções não é válida.

Π9.13H2. Suponha que tem $w \in \bigcap_{n=0}^{\infty} succ^n[\mathbb{N}] = \emptyset$ e chegue numa contradicção.

Π9.14H2. $\emptyset \in \wp\mathbb{N}$, mas também $\emptyset \in \wp\wp\mathbb{N}$ (pois $\emptyset \subseteq \wp\mathbb{N}$).

x9.99H2. Considere um objeto $\perp$ fora do B.

x9.108H2. Ou seja, basta demonstrar que para todo $n \in \mathbb{N}$, $fn = f'n$.

Π9.18H2. Uma idéia seria adicionar no B um objeto "fresco" para representar a falta de valor; outra idéia seria tomar como B' um subconjunto do $\wp B$. Qual?

Π9.20H2. Esqueceu o Capítulo 3?

Π9.30H2. Observe que a seqüência desses valores começa com 6, assim:

$$6 \rightsquigarrow 9 \rightsquigarrow 12 \rightsquigarrow 15 \rightsquigarrow 18 \rightsquigarrow 21 \rightsquigarrow \cdots$$

Mas, somando +3 num número par, sabemos já que o próximo número será ímpar e logo não pode ser potência de 2, e logo já sabemos que o próximo passo será somar +3 novamente. Então podemos pular os ímpares acima, e reduzir nosso trabalho focando nessa seqüência:

$$6 \rightsquigarrow 12 \rightsquigarrow 18 \rightsquigarrow 24 \rightsquigarrow 30 \rightsquigarrow 36 \rightsquigarrow \cdots$$

De 6 para 12 ela "pulou" a potência (de 2) 8. E de 12 para 18 também pulou o 16. A próxima potência é o 32, que nossa seqüência tambem conseguiu pular ($30 \rightsquigarrow 36$). Teu objectivo é *demonstrar* que ela consegue "pular" *todas* as potências de 2.

x10.14H2. Resposta: precisa achar o elemento neutro da operação $\diamond$. Já fez o Exercício x10.13, né?

x10.15H2. Exercício x10.12

x10.21H2. Procure contraexemplo nos exemplos típicos de relação antissimétrica.

x10.26H2. Tente achar um contraexemplo para o (ii). Qual a dificuldade de achar contraexemplo para o (i) e qual para o (iii)?

x10.27H2. Essa definição pode acabar apagando setas!

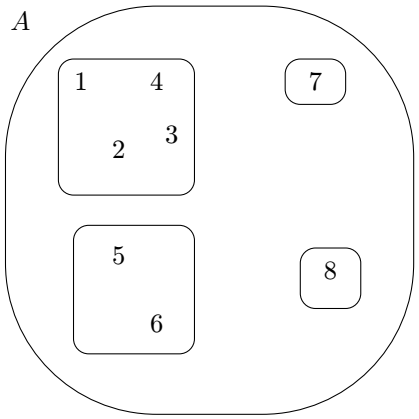
x10.42H2. Reflexividade e simetria das $(\sim_\varepsilon)$ e $(\approx_\varepsilon)$ são imediatas. Sobre a transitividade, um desenho na linha real ajudaria.

x10.47H2. Uma das colecções não-partições do Exercício x8.71 vai acabar sendo partição.

Π10.6H2. A f não é necessariamente injetora.

Π10.12H2. A $\sim$ é a relação de equivalência. Demonstre.

x10.48H2. *Não* é o conjunto dos seguintes subconjuntos de A:



Ache um $C \subseteq A$ tal que $C \in \mathscr{A}_R$ mas *não deveria*.

x10.58H2. Definimos a $\sim_{\mathscr{A}}$ pela

$$x \sim_{\mathscr{A}} y \iff^{\text{def}} (\exists C \in \mathscr{A})[\, x, y \in C\,].$$

Demonstre que $\sim_{\mathscr{A}}$ é uma relação de equivalência.

Π10.18H2. (1) Para mostrar que $\tilde{f}$ é bem-definida, precisa mostrar que a escolha do representante da classe não afeta o valor da função. Ou seja, tome $a, a' \in A$ e mostre que:

$$[a]_= [a'] \implies f(a) = f(a').$$

(2) A bijectividade da $\tilde{f}$ não precisa de dicas!

Π10.21H2. (Os números que tu achou na dica anterior devem ser: 1, 1, 2, e 5, respectivamente.) Chame B_n o número de partições dum conjunto finito com n elementos. Use recursão para definir o B_n.

Π10.23H2. Sobre a (i): Defina a partição de $\mathbb{R}$

$$\mathscr{C} \stackrel{\text{def}}{=} \underbrace{\{\,(n, n+1) \mid n \in \mathbb{Z}\,\}}_{\mathcal{I}} \cup \underbrace{\{\,\{n\} \mid n \in \mathbb{Z}\,\}}_{\mathcal{S}}.$$

Basta demonstrar que $\mathscr{C} = \mathbb{R}/\breve{\sim}$.
Sobre a (ii): mostre com um contraexemplo que $\ddot{\sim}$ não é transitiva.

x11.5H2. Como assim *o* inverso?

x11.22H2. Não precisamos nem saber que G é um grupo nem nada sobre $*$, etc.

x11.23H2. Tem contraexemplo no S_3.

x11.29H2. Podes começar com os conjuntos seguintes:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ \downarrow & & \\ G \times G & & \downarrow \\ \downarrow & & \\ G \times G & \longrightarrow & G \end{array}$$

A coluna esquerda corresponde num caminho do $\langle a, b\rangle$ para o $\langle b^{-1}, a^{-1}\rangle$.

x11.34H2. Procure um contraexemplo. (Claramente, a operação não pode ser comutativa.)

x11.40H2. Precisamos mostrar que:

$$\text{para todo } a \in G \text{ e todo } n \in \mathbb{N}, \quad a \uparrow_1 n = a \uparrow_2 n$$

ou, simbolicamente:

$$(\forall a \in G)(\forall n \in \mathbb{N})[\, a \uparrow_1 n = a \uparrow_2 n\,].$$

Seja $a \in G$. Agora queremos demonstrar:

$$(\forall n \in \mathbb{N})[\, a \uparrow_1 n = a \uparrow_2 n\,].$$

Como demonstrar isso?

x11.43H2. Tem como demonstrar isso numa linha só! Se não enxergar como, seja $a \in G$. O que tu precisas mostrar, é que $\left(a^{-1}\right)^2$ é o inverso do a^2. O que significa «ser o inverso do a^2»?

x11.44H2. Indução.

x11.47H2. Se $m > 0$, tome $n := m$. Se não?

x11.50H2. Para a (GA) basta achar um grupo que não seja abeliano; para a (G3) basta achar um *monóide* (ou seja, algo que satisfaz as (G0)–(G2)) que não é um grupo; para a (G2) basta achar um *semigrupo* (ou seja, algo que satisfaz as (G0)–(G1)) que não é um monóide; para a (G1) basta achar um *magma* (ou seja, algo que satisfaz a (G0)) que não é um semigrupo.

Π11.4H2. Precisas mostrar as (G2)–(G3). Ou seja, verificar que o 1_{R} é uma identidade-esquerda,

$$\text{(G2')} \qquad (\forall a \in G)\Big[\, 1_{\mathrm{R}} a = a \,\Big]$$

e que para todo $a \in G$, seu inverso direito a^{R} é um inverso esquerdo também:

$$\text{(G3')} \qquad (\forall a \in G)\Big[\, a^{\mathrm{R}} * a = 1_{\mathrm{R}} \,\Big].$$

Π11.5H2. O G é finito, logo sejam $G =: \{a_1, \ldots, a_n\}$.

Π11.6H2. Basta achar um contraexemplo: um conjunto estruturado $(G\ ;\ *)$ tal que G é finito e satisfaz as (G0),(G1),(GCL) mas mesmo assim não é um grupo; isso mostraria que não podemos apagar o (GCR). Similarmente para o (GCL).

Π11.7H2. Lembre o Exercício x11.55 e o Exercício x11.52.

Π11.8H2.

$$G \text{ abeliano} \iff (\approx) = (=_G)$$

Demonstre!

x11.65H2. Para mostrar que é fechado sobre a operação do grupo tome $a, b \in H_1 \cap H_2$ e mostre que $ab \in H_1 \cap H_2$. Similarmente, para mostrar que é fechado sobre os inversos, tome $a \in H_1 \cap H_2$ e mostre que $a^{-1} \in H_1 \cap H_2$.

x11.72H2. Ele é um subgrupo?

x11.78H2.

$$\cfrac{\cfrac{\cfrac{\cfrac{b \in A}{b \in A_0}}{b^2 \in A_1}}{b^4 \in A_2}}{b^8 \in A_3}$$

Como justificar cada linha?

Π11.12H2. Sejam $G =: \{a_1, \ldots, a_n\}$ os n membros de G.

Π11.15H2. $(0, 0) \in Q_2 \setminus Q_2$. Por quê?

x11.94H2. Mostre que $b^{-1} \notin H$. (Qual seria o problema se $b^{-1} \in H$?)

x11.95H2. Um exemplo consiste em: um grupo G, um subgrupo $H \leq G$, e dois elementos $a, b \in G \setminus H$ tais que satisfazem (ou não) a congruência $a \equiv b \pmod{H}$.

x11.106H2. Lembra que $\langle a \rangle$ é um subgrupo do G...?

x11.115H2. Basta demonstrar que para quaisquer $a, a', b, b' \in G$ temos:

$$\left.\begin{aligned} aN &= a'N \\ bN &= b'N \end{aligned}\right\} \implies (ab)N = (a'b')N$$

x11.121H2. Se escolheste investigar a segunda maneira da dica anterior:
Tome $s_1, s_2 \in S$ e $n_1, n_2 \in N$; assim o $s_1 n_1$ e $s_2 n_2$ são dois arbitrários membros do SN. Basta demonstrar que $(s_1 n_1)(s_2 n_2)^{-1} \in SN$.

Π11.18H2. Como o $2^P - 1$ não é primo, seja q um fator primo do $2^P - 1$. Então

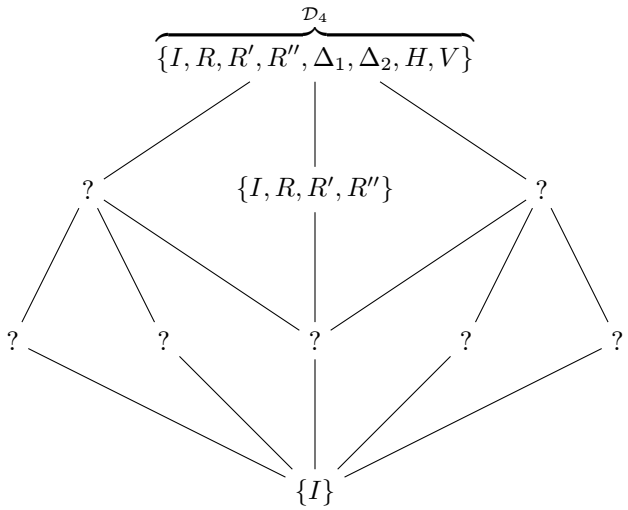
$$2^P - 1 \equiv 0 \pmod{q}.$$

Π11.20H2. Deixe a pergunta da dica anterior para o Capítulo 13. Por enquanto, demonstre uma bijecção entre H e Ha.

Π11.22H2. Mostre que NM é fechado pelos conjugados.

x11.123H2. Precisa achar dois pontos p, q no triângulo tal que a distância $d(p,q) \neq d(T'p, T'q)$.

x11.128H2.



x11.129H2. Mas olhe dentro do S_4: no seus subgrupos!

x11.142H2. Para o (i), tome $x, y \in \ker\varphi$ e mostre que $xy \in \ker\varphi$, ou seja, que $\varphi(xy) = e_B$.

x11.145H2. $\operatorname{im}\varphi$ FECHADO SOB A OPERAÇÃO: Tome $x', y' \in \operatorname{im}\varphi$ e ache um $w \in A$ tal que que $\varphi(w) = x'y'$.
$\operatorname{im}\varphi$ FECHADO SOB INVERSOS: Tome $x' \in \operatorname{im}\varphi$ e ache um $x \in A$ tal que $\varphi(x) = (x')^{-1}$.

x11.150H2. Na Abel, o $G \times H$ serve como objeto tanto de produto, quanto de coproduto! Demonstre!

Π11.28H2. Basta achar contraexemplo: grupo G e subgrupos $A, B \leq G$ tais que $A \trianglelefteq B \trianglelefteq G$ mas $A \not\trianglelefteq G$.

Π11.29H2. O G' é o G/N.

x12.2H2. Procure um contraexemplo: monóides $\mathcal{M}, \mathcal{N}$ e função $\varphi : M \to N$ tais que φ preserva a operação do monóide mas não a identidade.

x12.3H2. Queremos: «o $\varphi(\varepsilon_M)$ é a identidade do $\mathcal{N}$». O que significa «ser a identidade dum monóide»? Ou seja, o que precisamos demonstrar sobre esse objeto, $\varphi(\varepsilon_M)$ para mostrar que realmente ele é a identidade?

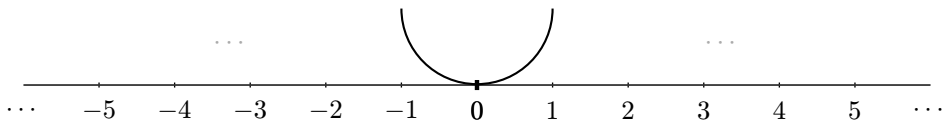
x12.9H2. Graças ao Exercício x11.16, a adição do anel deve ser a $\triangle$.

x12.10H2. Não pode. Exceto se...

x13.13H2. Use lambdas (veja Secção §205).

x13.20H2. Basta determinar uma maneira de trocar os digitais da diagonal que garanta que cada dígito mudou mesmo e que o número criado não termina nem em 0's nem em 9's.

x13.24H2. Uma maneira geometrica para resolver o $(a, b) =_{\mathrm{c}} (-\infty, +\infty)$ é pegar o (a, b), curvá-lo para parecer um semicírculo, e posicioná-lo em cima da reta real como parece na figura seguinte:



E agora?

Π13.4H2. Seguindo a idéia (i) da primeira dica: lembre como demonstramos que $\mathbb{N} =_{\mathrm{c}} \mathbb{Z}$; e seguindo a idéia (ii): faz sentido mandar o 1 para o 1/2; e o 1/2?

Π13.5H2. Agora defina uma seqüência $(\eta_n)_n$ de irracionais no $[0, 1]$ distintos dois a dois. Tente ser específico, mas não importa qual tu vai escolher.

Π13.8H2. Suponha para chegar num absurdo que $T = A_a$ para algum $a \in A$.

Π14.6H2. Considere a função $F : \wp A \to \wp A$ definida pela

$$F(X) = A \setminus (g[B \setminus f[X]]).$$

Mostre que ela é monótona.

x16.2H2. Comece com o $\emptyset$ e aplique iterativamente o operador $\{-\}$.

x16.4H2. Não tem como. Por quê?

x16.5H2. Não é um número finito de axiomas!

x16.6H2. Quais são todas as cardinalidades possíveis para o conjunto em qual usamos o (ZF4)?

x16.8H2. Não tem como!

x16.12H2. Como vimos no Exercício x16.4, usando os (ZF1)+(ZF2)+(ZF3) podemos consturir apenas conjuntos com cardinalidades 0, 1, e 2. Se aplicar o Powerset (ZF5) num conjunto A com cardinalidade finita n, qual será a cardinalidade do $\wp A$?

x16.15H2. (Sobre o operador $\triangle$.) Suponha a, b conjuntos. Temos $a \triangle b \subseteq a \cup b$.

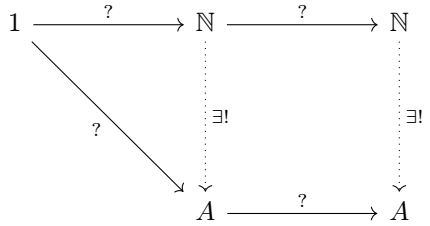
x16.23H2. Separe em casos: $x = y$ ou não.

x16.33H2. Duas idéias razoáveis:
Idéia 1: Dados conjuntos A, B, escolha (como?) um objeto fora do B para representar a "diverjão", ou valor "não-definido". Lembra-se que $\mathbf{r}(B) \notin B$, algo que temos graças ao Teorema Θ16.32. Então tome $B' := B \cup \mathbf{r}(B)$.
Idéia 2: Tome

$$B' := \{\, Y \subseteq B \mid \text{Singleton}(Y) \text{ ou } Y = \emptyset \,\}.$$

x16.50H2. Já sabemos que $\varphi[\mathbf{N}_1] \subseteq \mathbf{N}2$. Para demonstrar a igualdade mesmo, use o princípio da indução.

x16.52H2. Aqui os objetos:



Π16.11H2. Além de tudo isso, os "originais" $a \in A$ tem que ser recuperáveis pelas suas imagens atraves da Φ.

Π16.12H2. Tente achar uma class-function Φ tal que aplicada nos elementos dum conjunto suficientemente grande, vai ter como imagem o desejado $\{a, b\}$.

Π16.14H2. Considere conjuntos x, y, o com a propriedade

$$x = \{o, \{x, y\}\}$$

onde $o \neq y$.

Dícas #3

x3.8H3. Para a unicidade, já que achou um objeto que serve na existência, basta supor que um x satisfaz mesmo a equação $a + x = b$ e concluir que x deve ser igual ao objeto que achou na parte da existência.

x3.59H3. A base é trivial.

x3.85H3. O x sendo distribuido no primeiro somatório aumenta $+1$ no expoente de x, e similarmente o y no segundo aumenta $+1$ no expoente de y.

x3.86H3. Para a unicidade, ache o resto da divisão de n pelo arbitrário a_j.

x3.117H3. Num caso, dá para achar exatamente o resto. No outro, use a restricção que o resto satisfaz.

x3.121H3. Seja $steps(x)$ o número de passos necessários para quebrar o x em 1's.

Π3.18H3. O que significaria $\varphi(0)$? $\varphi(b)$?

Π3.19H3. O que seria um contraxemplo para cada parte? *O que acontece se existem contraexemplos?*

Π3.22H3. Necessariamente $p > n$.

Π3.23H3. $m! + 3\ldots$

Π3.26H3. Olha nos exponentes na forma $n = p_0^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_{k_n}^{a_{k_n}}$.

x3.154H3. Mostre que para qualquer $a \in \mathbb{Z}$,

$$a \equiv 2 \pmod 6\} \iff \begin{cases} a \equiv 0 \pmod 2 \\ a \equiv 2 \pmod 3. \end{cases}$$

Π3.31H3. Tente achar (criar) um número da mesma forma tal que nenhum dos p_i o divide.

x3.165H3. $41^{75} = 41^{74} \cdot 41$.

Π3.39H3. Demonstre que:

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}.$$

x4.6H3. Tu tens acesso na operação '$+$' pois já definimos!

x4.13H3.

$$\begin{aligned} (a+m)+y &= (a+m)+0 && \text{(hipótese do caso)} \\ &= a+m && \text{(pela (+).1)} \end{aligned}$$

Se travou aqui, sem problema: trabalhe no outro lado até chegar em $a+m$:

$$\begin{aligned} a+(m+y) &= \ldots? \\ &\vdots \\ &= a+m \end{aligned}$$

x4.17H3. Teu passo indutivo vai precisar duma sub-indução também! Alternativamente, tu podes demonstrar outras propriedades que ajudaria ter (por exemplo distributividade) e usá-las como lemmas nas tua prova.

x4.19H3. Passo indutivo. Seja $k : \mathsf{Nat}$ tal que

(H.I.) $$(\forall x)(\forall a)\big[\, x^{a+k} = x^a \cdot x^k \,\big].$$

Agora precisas demonstrar que

$$(\forall x)(\forall a)\big[\, x^{a+Sk} = x^a \cdot x^S k \,\big].$$

x4.20H3. Passo indutivo. Seja $k : \mathsf{Nat}$ tal que

(H.I.) $$(\forall a)(\forall b)\big[\, a^{b\cdot k} = (a^b)^k \,\big].$$

Agora precisas demonstrar que

$$(\forall a)(\forall b)\big[\, a^{b\cdot Sk} = (a^b)^{Sk} \,\big].$$

x4.21H3. Passo indutivo. Seja $k : \mathsf{Nat}$ tal que

(H.I.) $$S0^k = S0.$$

Agora precisas demonstrar que

$$S0^{Sk} = S0.$$

Π4.4H3. O que acontece se $h(i) = 0$ para algum $i \in \mathbb{N}$?

Π4.5H3. Agora indução.

Π4.11H3. A demonstração usa a pred, mas como ela foi definida mesmo?

x4.53H3. Por exemplo, a definição da nodes tem essa forma:

$$\begin{aligned} &\mathrm{nodes} : \mathsf{Tree}\ \alpha \to \mathsf{Nat} \\ &\mathrm{nodes}\ (\mathsf{Tip}\ x) \quad = _\,?\,_ \\ &\mathrm{nodes}\ (\mathsf{Fork}\ \ell\ r) = _\,?\,_. \end{aligned}$$

Π4.19H3. Para teu passo indutivo, tu terás um $k \geq 2$ tal que ${}^{k-1}s = s^{k-1}$ (HI1) e ${}^{k-2}s = s^{k-2}$ (HI2). E com essas duas hipoteses indutivas basta demonstrar ${}^{k}s = s^{k}$.

x5.8H3. Toma $x, y := 1$ no teorema para resolver o primeiro.

x5.12H3. Cuidado com a "base" $f(0)$. Quantas seqüências de 2 e 3, somam em 0?

x5.13H3. Considere os casos: (1) n não pode ser escrito nem como $n = 2+2+\cdots+2$, nem como $n = 3+3+\cdots+3$; (2) n pode ser escrito como $n = 2+2+\cdots+2$, e como $n = 3+3+\cdots+3$ também; (3) nenhum dos casos (1)–(2).

x5.15H3. Separa todos os caminhos possíveis em 3 grupos, dependendo na primeira escolha do motorista. Conta o número de caminhos em cada grupo separadamente (recursivamente!), e e use o princípio da adição para contar quantos são todos.

x5.16H3. Separa todos os caminhos possíveis em 4 grupos, dependendo na primeira escolha do motorista. Conta o número de caminhos em cada grupo separadamente (recursivamente!), e e use o princípio da adição para contar quantos são todos.

Π5.3H3. Escolhe 10 dos 21 lugares possíveis para colocar os múltiplos de 3.

Π5.9H3. Grupe as maneiras em colecções (para aplicar o princípio da adição), olhando para o primeiro salto.

Π5.11H3. Defina a $a(n)$ e depois calcule o $a(7)$, calculando em ordem os $a(0), a(1), \ldots, a(7)$.

x6.118H3. Demonstre que eventualmente $(a_n)_n < (b_n)_n$, ou seja, que

$$(\exists N)(\forall n \geq N)[\, a_n < b_n \,].$$

x6.134H3. Calcule o ℓ para chegar no $\ell = \vartheta\ell$, e obtenha $\ell = 0$ a partir disso.

x8.9H3. Teu alvo é mostrar que $A = B$. Para fazer isso é necessário lembrar a definição de $(=)$ nos conjuntos (D8.18).

x8.47H3. Como usarás a hipótese $\mathscr{A} \cap \mathscr{B} \neq \emptyset$?

Π8.13H3. Os primeiros membros são:

$$\bigcap_{j\geq 0} A_j, \quad \bigcap_{j\geq 1} A_j, \quad \bigcap_{j\geq 2} A_j, \quad \ldots$$

Faça a mesma coisa sobre o $A^* = \bigcap_i \bigcup_{j\geq i} A_j$.

x9.35H3. Sendo uma função, vou já escrever:

$$\mathit{uncurry}(F) = \lambda \ldots ? \ldots .$$

e preciso escolher como denotar a sua entrada. E aqui tenho duas abordagens razoáveis: ou escolher alguma variável como $w, t, \vec{w}, \vec{t}$, etc., onde ela terá o tipo $A \times B$; ou usar a λ-notação de aridades maiores escrevendo $\langle a, b\rangle$ para a arbitrária entrada dessa função. Vamos escolher segunda opção (se quiser, pode escolher a primeira). Continue!

x9.53H3. Separe as funções idempotentes dependendo na quantidade de "redemoinhos" que aparecem nos seus diagramas.

x9.64H3. Calcule cada lado separadamente:

$$\begin{aligned}
(g \circ f)^{-1}(x) = z &\iff (g \circ f)(z) = x && \text{(def. } (g \circ f)^{-1}\text{)} \\
&\iff \ldots \\
\big(f^{-1} \circ g^{-1}\big)(x) = z &\iff f^{-1}\big(g^{-1}(x)\big) = z && \text{(def. } f^{-1} \circ g^{-1}\text{)} \\
&\iff \ldots
\end{aligned}$$

Π9.2H3. Indução!

Π9.6H3. É para a parte do problema sobre a $g : \wp A \twoheadrightarrow A$ que precisas o $A \neq \emptyset$.

x9.108H3. Indução!

Π9.18H3. A primeira idéia não precisa de mais dicas. Sobre a segunda:

$$B' := \{\, X \subseteq B \mid |X| \leq 1 \,\}.$$

Π9.20H3. Use um dos $\mathbb{Z}_n$'s.

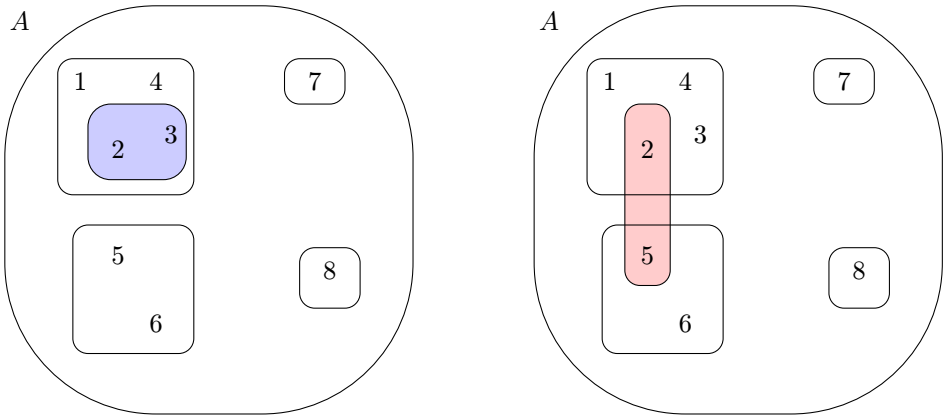
Π9.30H3. Módulo 6.

x10.15H3. Temos Parent $=$Child$^\partial$ (e logo Child $=$Parent$^\partial$ também).

x10.42H3. Como contraexemplo, tome os reais 0, $\varepsilon/2$, e ε e observe que $0 \sim_\varepsilon \varepsilon/2$ e $\varepsilon/2 \sim_\varepsilon \varepsilon$ mas mesmo assim não temos $0 \sim_\varepsilon \varepsilon$.

Π10.12H3. A $\approx$ não é transitiva. Refute!

x10.48H3. A definição do aluno garanta que todos os elementos numa classe realmente relacionam entre si através da R; mas não garanta que cada classe C é feita por *todos* os elementos de A que relacionam com os membros da C mesmo. Por exemplo, ela *corretamente exclue* conjuntos como $\{2, 5\}$; mas ela *incorretamente inclue* conjuntos como o $\{2, 3\}$.



Π10.21H3. Já temos umas bases desde a dica anterior:

$$B_0 = 1$$
$$B_1 = 1$$
$$B_2 = 2$$
$$B_3 = 5$$

Para a equação recursiva,

$$B_{n+1} = \ldots$$

lembra-se que podes considerar conhecidos *todos* os números B_k para $k \leq n$.

x11.23H3. Procuramos a, x, y num grupo tais que

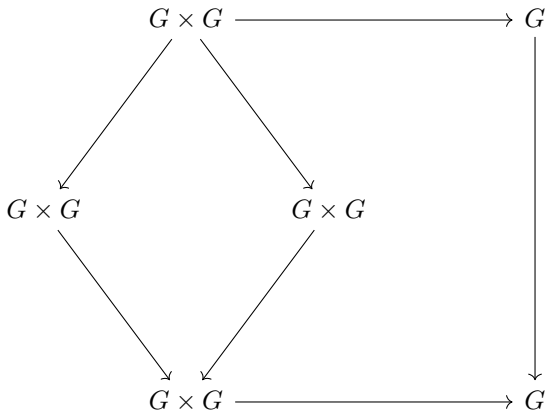
$$ax = ya \implies x = y,$$

ou seja, tais que $ax = ya$ e $x \neq y$. Mas, o que podemos concluir se $ax = ya$?

$$ax = ya \implies x = a^{-1}ya.$$

Então nossos a, x, y tem que ser tais que $x = a^{-1}ya$ e mesmo assim $x \neq y$. Pensando nesses membros como processos e na operação como "seguindo" (exatamente a intuição da composição de funções), para conseguir um contraexemplo, precisamos achar a e y tais que: fazendo o a, depois o y, e depois desfazendo o a, não vai ter o mesmo efeito com o processo de fazer apenas o y.

x11.29H3. Substitui a coluna esquerda por dois caminhos formando o rombo na esquerda (ele comuta):



Agora só basta botar nomes nas setas.

x11.34H3. Dá pra construir contraexemplo com apenas 2 membros.

x11.40H3. As definições envolvidas são recursivas.

x11.43H3. $\left(a^{-1}\right)^2 * a^2 \stackrel{?}{=} e \stackrel{?}{=} a^2 * \left(a^{-1}\right)^2$.

Π11.4H3. Para demonstrar a (G2') tome um $a \in G$ e comece com:

$$\begin{aligned} 1_{\mathrm{R}} \cdot a &= (1_{\mathrm{R}} \cdot a) \cdot 1_{\mathrm{R}} \\ &= 1_{\mathrm{R}} \cdot (a \cdot 1_{\mathrm{R}}) \\ &= 1_{\mathrm{R}} \cdot (a \cdot (\,? \cdot ?^{\mathrm{R}}\,)) \qquad \text{(qual membro de } G \text{ serve aqui?)} \\ &\vdots \\ &= a \end{aligned}$$

Para a (G3'), o lemma seguinte pode ajudar:

$$(\forall g \in G)\Big[\, gg = g \implies g = 1_{\mathrm{R}} \,\Big].$$

Use isso para demonstrar que um inverso direito é esquerdo também.

Π11.5H3. Seja $g \in G = \{a_1, \ldots, a_n\}$. Considere o $Ga \stackrel{\text{def}}{=} \{\, ga \mid a \in G \,\} = \{ga_1, \ldots, ga_n\}$. E agora?

Π11.12H3. Dado $a \in G$ sabemos que $a^{o(a)} = e$.

Π11.15H3. Para "passar pelo $(0,0)$", uma corda obrigatoriamente tem que ser uma diámetro.

x11.94H3. Se $b{-}1 \in H$ seu inverso também deveria estar no H, pois H é um grupo.

x11.95H3. Procure teus exemplos no grupo dos inteiros com adição $(\mathbb{Z}\,;+)$.

x11.106H3. ... e que sua ordem é $o(\langle a \rangle) = o(a)$?

x11.115H3. Temos que $N \trianglelefteq G$ e logo $a'N = Na'$ e $b'N = Nb'$.

Π11.18H3. Temos

$$2^P \equiv 1 \pmod{q}.$$

O que podemos concluir sobre a ordem de 2 no grupo... Em qual grupo mesmo?

Π11.20H3. A restricção (Definição D9.161) no H do a-ator direito (Definição D11.148).

x11.129H3. Renomeia teus A, B, C, D para $1, 2, 3, 4$. Agora veja cada uma das simetrias do $\mathcal{D}_4$, para onde ela leva cada número, e escreva sua permutação correspondente do S_4. Basta demonstrar que esse conjunto realmente é um subgrupo de S_4.

x11.142H3. Para o (ii), tome $x \in \ker\varphi$ e mostre que $x^{-1} \in \ker\varphi$, ou seja, que $\varphi(x^{-1}) = e_B$.

Π11.28H3. Procure teu contraexemplo no $G := S_4$ e seus subgrupos (considere o $A := \langle (1\ 2)(3\ 4) \rangle$. Alternativamente, procure no $\mathcal{D}_4$ e seus subgrupos; talvez olhando para o diagrama Hasse do $\mathcal{D}_4$ ajuda.

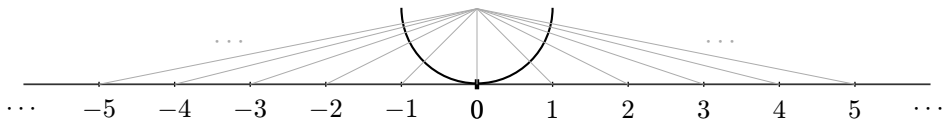
x12.3H3. Precisamos demonstrar que:

$$(\forall n \in N)[\, n \cdot_N \varphi(\varepsilon_M) = n = \varphi(\varepsilon_M) n \,].$$

Como começaria essa demonstração?

x12.9H3. $(\wp X\,; \triangle, \cap)$.

x13.24H3. Agora estabelecemos uma correspondência (bijecção) entre os pontos da reta e os pontos do nosso semicírculo juntando cada ponto $x \in \mathbb{R}$ com um segmento reto até o centro do semicírculo e mapeando o x para o ponto que o segmento intersecta o semicírculo:



Π13.4H3. Seguindo a idéia (i): $\mathbb{R} = \bigcup_n [n, n+1)$. Seguindo a idéia (ii): defina uma função $f : (0,1] =_c (0,1)$ por casos:

$$f(x) = \begin{cases} __?__ & \text{se } ____?____ \\ __?__ & \text{caso contrário} \end{cases}$$

tal que

$$\begin{aligned} 1 &\overset{f}{\longmapsto} 1/2 \\ 1/2 &\overset{f}{\longmapsto} __?__ \\ &\vdots \\ __?__ &\overset{f}{\longmapsto} __?__ \end{aligned}$$

Π13.5H3. Cantor usou a seqüência de irracionais $(\eta_n)_n$ definida pela $\eta_n = \sqrt{2}/2^{n+1}$. Outra escolha seria a $\frac{1}{n+\sqrt{2}}$. (Verifique que todos os membros de ambas as seqüências são irracionais.)

Π13.8H3. $T = \emptyset$?

Π14.6H3. Pelo teorema Knaster–Tarski Θ14.40 a F tem um fixpoint $C \subseteq A$, e

$$C = F(C) \iff C = A \setminus (g[B \setminus f[C]]) \iff A \setminus C = g[B \setminus f[C]].$$

x16.50H3. Precisas demonstrar duas coisas então: (1) $\mathsf{O}_2 \in \varphi[\mathbf{N}_1]$; (2) para todo $n \in \mathbf{N}_2$, se $n \in \varphi[\mathbf{N}_1]$ então $\mathsf{S}_2 n \in \varphi[\mathbf{N}_1]$.

Π16.14H3. Calcule o

$$\langle \{x, y\}, o \rangle$$

e ache que ele é igual com um par ordenado diferente. (Tem que demonstrar que é difernete mesmo!)

Dícas #4

x3.59H4. Para o passo indutivo, tomando um $k \in \mathbb{N}$ tal que $\varphi(k)$, separa tua prova em dois casos, dependendo da razão que o $\varphi(k)$ seja verdade.

x3.85H4.

$$x \sum_{r=0}^{k} C(k,r) x^{k-r} y^r + y \sum_{r=0}^{k} C(k,r) x^{k-r} y^r = \sum_{r=0}^{k} C(k,r) x^{(k-r)+1} y^r + \sum_{r=0}^{k} C(k,r) x^{k-r} y^{r+1}.$$

Π3.18H4. Ser forte é coisa boa.

Π3.19H4. Sobre sua terminação: Considere o menor m tal que o EUCLID(x, m) não termina para algum $x \in \mathbb{Z}$.

Π3.23H4. $m! + m$.

Π3.26H4. Teste tua codificação nas seqüências $\langle 1, 3\rangle$ e $\langle 1, 3, 0\rangle$. Como essas seqüências são diferentes, suas codificações devem ser diferentes também. E a seqüência vazia $\langle\rangle \in S$?

x3.154H4. Não todos os sistemas de congruências têm soluções. (Acontéce quando temos restricções contraditórias.) Nesse exercício um dos dois sistemas não tem solução.

Π3.31H4. $N = 4p_1p_2 \cdots p_k - 1$.

x3.165H4. Fermat.

x4.6H4. Provavelmente até agora tens:

$$\begin{aligned} n \cdot 0 &= 0 \\ n \cdot S0 &= n \\ n \cdot SS0 &= n + n \\ n \cdot SSS0 &= (n + n) + n \\ &\vdots \end{aligned}$$

Observe que o "valor" (lado direito) de cada nova linha é o valor da linha anterior "$+n$". Mas temos um nome para o lado direito da linha anterior: *seu lado esquerdo!* Isso deve ser suficiente para achar como escrever a segunda linha da definição:

$$\begin{aligned} n \cdot 0 &= ____ \\ n \cdot Sm &= ____ \end{aligned}$$

Π4.5H4. Base: C não possui membros $c \leq 0$. Imediato, pois o único natural $n \leq 0$ é o próprio 0 que é o menor membro do $\mathbb{N}$. Sabemos então que $0 \notin C$ pois caso contrário o C teria um mínimo.

x5.8H4. Toma $x := 1$ e $y := -1$ para resolver o segundo.

x5.12H4. Para calcular o valor de $f(17)$, *não* use a definição recursiva "top-down", mas "bottom-up": calcule os valores em seqüência linear $f(0), f(1), f(2), \ldots$ até o valor desejado.

x5.13H4. $g(n) = \begin{cases} \cdots \\ \cdots \\ \cdots \end{cases}$

x6.134H4. Em geral, $\lim_n an = \lim_n a_{n+1}$, onde entendemos esta igualdade como: ou ambas as seqüências convergem no mesmo limite, ou ambas as seqüências divergem.

x8.47H4. Use as definições de $\bigcap$ e $\bigcup$.

Π8.13H4. Cada um desses membros também é uma intersecção ou união duma seqüência. Escrava cada uma delas como uma expressão que envolve '$\cdots$'.

x9.35H4. Estamos aqui então:

$$\mathit{uncurry}(F) = \lambda\langle a, b\rangle \ldots .?$$

e o que precisamos construir aqui? Sendo a "saída" duma função com tipo $(A \times B) \to C$, eu preciso construir uma coisa do tipo C. Mas o que mais eu tenho agora? Meus dados tem aumentado:

$$F : A \to (B \to C)$$
$$\langle a, b\rangle : (A \times B)$$

e logo

$$a : A$$
$$b : B$$
$$?? : C$$

Como posso usá-los para construir algo do tipo C? Eu não tenho um "fornecedor" de C's imediato, mas percebo que tenho um... fornecedor de fornecedores de C's! (Minha F.) E para ela funcionar preciso oferecer A'zinho, e pronto, ela vai fornecer um fornecedor de C's. Felizmente temos um $a : A$. Então temos:

$$F(a) :??$$

Π9.6H4. Seja $a_0 \in A$. Defina a $g : \wp A \to A$ pela

$$g(X) = \begin{cases} \ldots?\ldots, & \ldots?\ldots \\ \ldots?\ldots, & \text{caso contrário.} \end{cases}$$

Novamente: cuidado para não supor nada mais que $A \neq \emptyset$ sobre o A. Por exemplo: não sabemos se A tem *mais* que um elemento (sabemos apenas que tem *pelo menos* um); não sabemos se os membros dele são ordenados; etc. Se a gente soubesse que os membros de A são *bem ordenados* a gente poderia definir o primeiro caso acima pela

$$g(X) = \begin{cases} \min X, & \text{se } X \neq \emptyset \\ \ldots?\ldots, & \text{caso contrário.} \end{cases}$$

mas sem a informação que o A é bem ordenado a g não seria bem-definida. Por enquanto: um conjunto é chamado *bem ordenado* sse todo $\emptyset \subsetneq X \subseteq A$ possui elemento mínimo. No Secção §329 estudamos conjuntos bem ordenados e suas propriedades.

x9.108H4. Vai precisar de duas bases.

Π9.30H4. Como parecem *todas* as potências de 2 "dentro do módulo 6"?

x10.42H4. Como podes usar a não-transitividade da $(\sim_\varepsilon)$ para deduzir a não-transitividade da $(\approx_\varepsilon)$?

Π10.21H4. Sejam $a_0, \ldots, a_n$ os $n+1$ elementos de A e considere uma partição arbitrária $\mathscr{A}$ dele. Sendo partição, existe exatamente um conjunto-classe A_0 no $\mathscr{A}$ tal que $a_0 \in A_0$. Influenciados pela notação de classes de equivalência, denotamos o A_0 por $[a_0]$. Tirando esse conjunto da partição $\mathscr{A}$ chegamos no

$$\mathscr{A} \setminus \{[a_0]\}$$

que é (certo?) uma partição do conjunto

$$\bigcup(\mathscr{A} \setminus \{[a_0]\}).$$

Seja k o número de elementos desse conjunto. Quais são os possíveis valores desse k?

x11.34H4. Considere como operação binária a *outl*.

x11.40H4. Ou seja: indução.

Π11.4H4. Para a (G2'), qual produto podes botar no lugar do (?) da dica anterior? Sabendo que (G2R) é válida, faz sentido substituí-lo com um termo $\left(xx^{\mathrm{R}}\right)$ para algum $x \in G$, mas qual seria esse x? *Não precisamos adivinhar ainda!* Continue assim com um x não-especificado por enquanto, e logo tu vai chegar numa expressão que vai te ajudar escolher teu x para continuar, pois tu vai querer que esse x "anula" a coisa que aparecerá na sua esquerda.

Para a (G3'), teu objectivo é demonstrar que dado qualquer $a \in G$, $a^{\mathrm{R}}a = 1_{\mathrm{R}}$; e o Lemma te oferece um critério para decidir que algo é o 1_{R}. Use!

Π11.15H4. Por enquanto só podemos responder "não" por causa desse buraco. Tem outros buracos? Paciência até o Capítulo 13, onde revisitamos essa pergunta nos seus problemas.

x11.94H4. Suponha que $ab^{-1} \in H$ para chegar num absurdo, mostrando assim que necessariamente, $a \not\equiv b \pmod{H}$. Cuidado:

$$xy \in H \implies x \in H \;\&\; y \in H.$$

x11.95H4. Tome $G := (\mathbb{Z}\,;+)$, $H := 2\mathbb{Z}$, $a := 1$, $b := 3$ e observe que $1 \equiv 3 \pmod{2\mathbb{Z}}$.

Π11.20H4. Já sabemos que é injetora (Lema Λ11.149). Basta demonstrar que é sobre o Ha.

x12.3H4. «Seja $n \in N$.» Depois dessa frase, queremos demonstrar que

$$n \cdot_N \varphi(\varepsilon_M) = n = \varphi(\varepsilon_M)n.$$

Π13.5H4. Defina a $f : [0,1] \to [0,1] \setminus \mathbb{Q}$ mandando cada $x \in [0,1]$ nele mesmo, exceto os membros das $\{q_n\}_n$ e $\{\eta_n\}_n$. Fazer o que com eles?

Π14.6H4. Defina a desejada $h : A \rightarrowtail B$ por casos:

$$h(x) = \begin{cases} \dots, & \text{se } x \in C \\ \dots, & \text{se } x \in A \setminus C. \end{cases}$$

Dícas #5

x3.85H5. Separe o primeiro termo do primeiro somatório e o último termo do segundo.

Π3.19H5. Sobre sua corretude: Considere o menor m tal que o EUCLID(x, m) termina com resultado errado par algum $x \in \mathbb{Z}$. Mas mostre primeiro a terminação.

Π3.31H5. N não pode ter apenas divisores da forma $4n+1$. Por quê?

x4.6H5. Na segunda equação, no seu lado direito, tu tens acesso no valor $n \cdot m$, pois é "mais simples" do que o $n \cdot Sm$. Isso é o poder da recursão: podes considerar o problema que tu tá tentando resolver (definir a multplicação), como resolvido para as "entradas mais simples".

Π4.5H5. Passo Indutivo. Seja k tal que C não possui membros $c \leq k$. Basta demonstrar que C não possui membros $c \leq k+1$.

Π8.13H5. Temos:

$$A_* = \bigcup \left\{ \begin{array}{r} A_0 \cap A_1 \cap A_2 \cap A_3 \cap A_4 \cap \cdots \\ A_1 \cap A_2 \cap A_3 \cap A_4 \cap \cdots \\ A_2 \cap A_3 \cap A_4 \cap \cdots \\ \ddots \end{array} \right\} \qquad A^* = \bigcap \left\{ \begin{array}{r} A_0 \cup A_1 \cup A_2 \cup A_3 \cup A_4 \cup \cdots \\ A_1 \cup A_2 \cup A_3 \cup A_4 \cup \cdots \\ A_2 \cup A_3 \cup A_4 \cup \cdots \\ \ddots \end{array} \right\}$$

E agora precisamos *entender* as proposições

$$x \in A_* \qquad\qquad x \in A^*$$

para enxergar se uma implica a outra, etc.

x9.35H5. Temos

$$\begin{aligned} F &: A \to (B \to C) \\ \langle a, b \rangle &: (A \times B) \\ a &: A \\ b &: B \\ F(a) &: B \to C \end{aligned}$$

e logo

$$F(a)(b) : ??$$

Termine!

Π9.6H5. Seja $a_0 \in A$. Defina a $g : \wp A \to A$ pela

$$g(X) = \begin{cases} x, & \text{se } X \text{ é o singleton } \{x\} \\ a_0, & \text{caso contrário.} \end{cases}$$

Falta demonstrar que ela é sobrejetora e que não é injetora.

Π9.30H5. A seqüência de todas as potências de 2 é:

$$1, 2, 4, 8, 16, 32, 64, \ldots$$

que, módulo 6 fica:

$$1, 2, 4, 2, 4, 2, 4, 2, \ldots \pmod 6.$$

Isso é fácil de demonstrar: então demonstre.

x10.42H5. Para todo $\alpha \in \mathbb{R}_{\geq 0}$ temos:

$$\cdots \iff \sqrt{\alpha} \in (0,1) \iff \alpha \in (0,1) \iff \alpha^2 \in (0,1) \iff \cdots$$

Π10.21H5. Vamos melhorar nossa notação para nos ajudar raciocinar. O conjunto

$$\bigcup(\mathscr{A} \setminus \{[a_0]\}).$$

da dica anterior, depende de quê? Como a gente fixou uma enumeração dos elementos do A, ele depende apenas na partição $\mathscr{A}$. Introduzimos então a notação

$$R_{\mathscr{A}} := \bigcup(\mathscr{A} \setminus \{[a_0]\}).$$

E denotamos o k da dica anterior com $k_{\mathscr{A}} := |R_{\mathscr{A}}|$. O $k_{\mathscr{A}}$ da dica anterior pode ter qualquer um dos valores $k_{\mathscr{A}} = 0, \ldots, n$. E agora?

x11.40H5. Base: demonstrar que $a \uparrow_1 0 = a \uparrow_2 0$:

x11.94H5. Mostre que $a^{-1} \in H$.

x11.95H5. Não é possível achar o outro exemplo com o mesmo subgrupo $2\mathbb{Z}$, mas pode sim no $3\mathbb{Z}$.

x12.3H5. Já demonstramos no Exercício x12.2 que não tem como ganhar a preservação da identidade como conseqüência da preservação da operação tendo uma função $\varphi : M \to N$ qualquer. Então com certeza precisamos usar nossa hipótese nova aqui, que a φ é sobrejetora.

Dícas #6

x3.85H6.

$$\sum_{r=0}^{k} C(k,r)x^{(k-r)+1}y^r + \sum_{r=0}^{k} C(k,r)x^{k-r}y^{r+1}$$
$$= x^{k+1} + \sum_{r=1}^{k} C(k,r)x^{(k-r)+1}y^r + \sum_{r=0}^{k-1} C(k,r)x^{k-r}y^{r+1} + y^{k+1}.$$

Π3.31H6. . . . porque multiplicando numeros da forma $4n+1$ seu produto continua da mesma forma.

Π8.13H6. O que podemos concluir sobre a *quantidade* dos A_n's que x pertence, sabendo a primeira? O que sabendo a segunda?

Π9.30H6. Observe que somando $+6$ num número não o muda "módulo 6". (Lembre que $6 \equiv 0 \pmod 6$.)

Π10.21H6. Agora separe todas as partições $\mathscr{A}$ de A em grupos dependendo no valor de $k_{\mathscr{A}}$, ache o tamanho de cada grupo separadamente, e use o princípio da adição para achar a resposta final.

x11.40H6. Seja $k \in \mathbb{N}$ tal que $a \uparrow_1 k = a \uparrow_2 k$ (hipótese indutiva). Queremos mostrar que

$$a \uparrow_1 (k+1) = a \uparrow_2 (k+1).$$

x12.3H6. Seja $n \in N$. Como φ é sobrejetora, tome $m \in M$ tal que $\varphi(m) = n$.

Dícas #7

x3.85H7. Mexa com os índices utilizados nos dois somatórios para conseguir que ambos começam e terminam no mesmo r.

Π8.13H7. Em ambos os casos podemos concluir que x pertence a uma quantidade infinita de A_i's, então isso não é suficiente para nosso objectivo. A segunda proposição realmente é *equivalente* a essa afirmação, ou seja:

$$x \in A^* \iff x \text{ pertence a uma quantidade infinita de } A_n\text{'s.}$$

Mas a primeira afirma algo *mais forte*, ou seja, realmente

$$x \in A_* \implies x \in A^*.$$

Mas para enxergar isso precisamos entender qual é toda a informação que a proposição '$x \in A^*$' contem:

$$x \in A_* \iff \ldots ? \ldots$$

Π9.30H7. Ou seja: começando com qualquer número m que módulo 6 é um dos $0, 3, 5$ sabemos que $d(m)$ *diverge*, ou seja, o $d(m)$ não é definido. E se m é 1 módulo 6? A única potência de 2 que é 1 módulo 6 é o próprio 1, e logo qualquer outro inteiro que é 1 módulo 6 não pode ser uma potência de 2.

Π10.21H7. Todas as partições do A são separadas assim em:

- as partições $\mathscr{A}$ de A tais que $k_{\mathscr{A}} = 0$;
- as partições $\mathscr{A}$ de A tais que $k_{\mathscr{A}} = 1$;
- $\vdots$
- as partições $\mathscr{A}$ de A tais que $k_{\mathscr{A}} = n$.

Seja N_i o número das partições $\mathscr{A}$ de A tais que $k_{\mathscr{A}} = i$. Graças ao princípio da adição, procura-se o somatório $\sum_{i=0}^{n} N_i$. Ache o valor do arbitrário N_i.

x11.40H7. Seguindo as dicas anteriores, provavelmente tu chegou aqui:

$$\begin{aligned} a \uparrow_1 (k+1) &= a * (a \uparrow_1 k) && \text{(def. } \uparrow_1\text{)} \\ &= a * (a \uparrow_2 k) && \text{(HI)} \end{aligned}$$

...e agora? *Se* $*$ fosse comutativa (ou seja, se o grupo fosse abeliano), a gente *poderia* continuar assim:

$$\begin{aligned} &= (a \uparrow_2 k) * a && \text{(comutatividade (GA))} \\ &= a \uparrow_2 (k+1). && \text{(def. } \uparrow_2\text{)} \end{aligned}$$

Só que não! Sobre o G sabemos apenas que é um grupo, então não podemos contar na comutatividade da sua operação $*$. (Inclusive, se a $*$ fosse comutativa o resultado seria trivial e nem precisaria indução.) Voltando no passo que tivemos colado

$$\begin{aligned} a \uparrow_1 (k+1) &= a * (a \uparrow_1 k) && \text{(def. } \uparrow_1\text{)} \\ &= a * (a \uparrow_2 k) && \text{(HI)} \end{aligned}$$

percebemos que precisamos "abrir mais" a expressão $(a \uparrow_2 k)$, aplicando a definição de $\uparrow_2$, mas não podemos, pois não sabemos se $k = 0$ ou não. Neste momento então percebemos que saber a veracidade dessa equação apenas para o valor $n = k$ não é suficiente. Tu vai precisar o $n = k - 1$ também.

Ou seja, tu vai precisar *duas* bases ($n = 0, 1$), e supor que tem um $k \geq 2$ tal que ambos os $k-1$ e $k-2$ satisfazem a $a \uparrow_1 n = a \uparrow_2 n$. Ou seja, tu ganharás as *duas* hipoteses indutivas:

(HI1) $$a \uparrow_1 (k-1) = a \uparrow_2 (k-1)$$
(HI2) $$a \uparrow_1 (k-2) = a \uparrow_2 (k-2)$$

e só bastará demonstrar que $a \uparrow_1 k = a \uparrow_2 k$.

Dícas #8

П8.13H8. Se $x \in A_*$, a quantos dos A_n's pode ser que o x *não* pertence? E se $x \in A^*$?

П10.21H8. De quantas maneiras pode acontecer que o

$$R_{\mathscr{A}} = \bigcup (\mathscr{A} \setminus \{[a_0]\})$$

tem i elementos?

Dícas #9

П10.21H9. Sabemos que o a_0 não pode ser um deles, então precisamos escolher i elementos dos n seguintes: $a_1, \ldots, a_n$. Ou seja, de $C(n, i)$ maneiras. Cada escolha A_i corresponde numa colecção de partições:

$$\Big\{ [a_0] \,,\ \underbrace{\quad\ldots\quad}_{\text{partição do } A_i} \Big\}$$

Dícas #10

Π10.21H10. Sabemos a quantidade de partições de qualquer conjunto de tamanho i com $i \leq n$: são B_i.

APÊNDICE C

RESOLUÇÕES

Onde tu prometes estudar as resoluções apenas depois de ter consultado todas as dicas disponíveis no appêndice anterior.

Capítulo 1

x1.1S.

$$\begin{aligned} A &\implies B: \quad A \text{ somente se } B \\ A &\impliedby B: \quad A \text{ se } B \end{aligned}$$

x1.2S.

$$\begin{aligned} A &\implies B: \quad A \text{ é suficiente para } B \\ A &\impliedby B: \quad A \text{ é necessário para } B. \end{aligned}$$

x1.3S.

(1) $(x+y)^2 = x^2 + 2xy + y^2$.
(2) $x(a-(b+c)) = xa - x(b+c) = xa - xb - xc$.
(3) Concluimos que $(A \subseteq B) \iff (B \subseteq A)$.
(4) Suponha que n é lindo. Vamos demonstrar que $n+1$ é feio.

x1.4S. Essa definição não aceita objetos que deveria aceitar. Por exemplo, o 2 não é um número par segundo essa definição, pois, lembrando:

$$6 \text{ é par} \iff \text{para todo inteiro } k,\ 6 = 2k.$$

Para *refutar* a afirmação que 6 é par então, basta achar um inteiro k tal que $6 \neq 2k$. Tome $k := 1$ e observe que $6 \neq 2 \cdot 1$ e pronto, o 6 acabou sendo um número não par! Para consertar a definição basta trocar o "para todo" por "para algum"!

x1.6S. Temos:

- '$\Longleftrightarrow$' para os pares: (3), (4), (11);
- '$\Longleftrightarrow$' para os pares: (5), (7), (9), (10), (8);
- '$\equiv$' para o par (12);
- '$=$' para os pares: (1), (2), (6).

Aqui considerei que elevar um número ao 2 *significa* multiplicar o número por ele mesmo. Caso que considerou exponenciação como operação primitiva e não definida em termos da multiplicação, seria correto mudar as (11) e (12) de intensional para extensional. Similarmente considerei que *ser professor de alguém* envolve mais coisas do que simplesmente ensinar algo para alguém.

x1.7S.

$$\begin{aligned}(x+y)^2 = x^2 + 2xy &: \text{proposição}\\ \text{a mãe de } p &: \text{objeto}\\ 2^n + 1 &: \text{objeto}\\ p \text{ é irmão de } q &: \text{proposição}\\ \text{a capital do país } p &: \text{objeto}\\ a \text{ mora em Atenas} &: \text{proposição}\end{aligned}$$

x1.8S. (1) proposição; (2) proposição; (3) objeto; (4) objeto; (5) proposição.

x1.9S. (1) existe número inteiro tal que seu dobro mais um é igual ao 13; (2) existem dois números inteiros tais que sua soma quadrada é igual à soma do quadrado do primeiro e do dobro do produto do primeiro com o segundo; (3) aquela função que dada um número retorna a soma desse número com o 1; (4) o conjunto de todos livros em quais aparece palavra com tantas letras quantas as letras do título do próprio livro.

(Se enunciou a (1) com a simples «13 é ímpar» tá tudo OK; vamos voltar a discutir questões de paridade (par, ímpar, etc.) no Capítulo 2.)

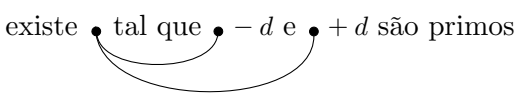
x1.10S.

(1) existem pessoas que se amam mutalmente;
(2) existe pessoa que ama e é amada pela pessoa q;
(3) $x + y = z$;
(4) existe número tal que sua soma com x é igual ao z;
(5) existem números tais que somando y num deles resulta no outro;
(6) para qualquer número, existe número tal que a soma com o primeiro é igual ao z;
(7) para quaisquer dois números, existe número cuja soma com o primeiro é igual ao segundo.

x1.11S. A proposição (3) escrita com variáveis

(3) existe n tal que $n - d$ e $n + d$ são primos

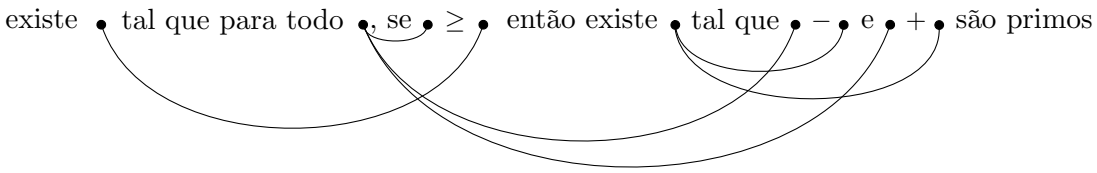
e agora com ligações:



A proposição (5) escrita com variáveis:

(5) existe N tal que para todo n, se $n \geq N$ então existe d tal que $n - d$ e $n + d$ são primos

e agora com ligações:



x1.13S. (i) sim, pois m não aparece livre no escopo e assim não vai acontecer capturamento de variável não-desejado; (ii) não, pois d aparece livre no escopo e assim seria capturado e logo nem seria mais uma afirmação sobre d; (iii) não, pois não seria mais uma afirmação sobre o d, mas sobre o x.

x1.14S. (i) não, pois teriamos sombreamento do antigo 'N' e precisamos referi-lo; (ii) sim—mesmo que fica esquisito!—pois o sombreamento acontece num escopo onde não precisamos referir mais o antigo 'N'; (iii) não, pois teriamos sombreamento do antigo 'N' e precisamos referi-lo; (iv) não, pois teriamos sombreamento do antigo 'n' que tá sendo referido depois; (v) não: mesmo problema com o (iv); (vi) sim: mesma situação com o (ii).

x1.15S. As pessoas que não tem nenhuma irmã, e também as pessoas que tem mais que uma!

x1.16S. Começamos assim:

> Definição. Sejam a, b duas linhas. Dizemos que a, b são parallelas sse a, b não se tocam.

Não podemos parar com essa definição pois no lado direito usamos uma frase que não significa nada (por enquanto): não definimos o que significa que duas linhas "se tocam". Basta então definir isso:

> Definição. Sejam a, b duas linhas. Dizemos que a, b se tocam sse não existe ponto p tal que p pertence à linha a e p pertence à linha b.

Pronto, agora nada ficou "solto", acabou sendo reduzido para as noções primitivas de ponto, linha, e o predicado primitivo de "ponto pertence a linha".

x1.17S. Temos:

(i) $a + b + c \not\equiv a + (b + c)$
(ii) $a + b + c \equiv (a + b) + c$
(iii) $a + b + c = a + (b + c)$
(iv) $a + b + c = (a + b) + c$
(v) $2 \cdot 0 + 3 = 0 + 3$
(vi) $2 \cdot 0 + 3 \not\equiv 0 + 3$

(vii) $(2 \cdot 0) + 3 + 0 = 1 + 1 + 1$
(viii) $2 \cdot 0 + 3 \not\equiv 1 + 1 + 1$
(ix) $2 \cdot 0 + 3 \not\equiv 2 \cdot (0 + 3)$
(x) $2 \cdot 0 + 3 \neq 2 \cdot (0 + 3)$
(xi) $2 \cdot 0 + 3 \equiv (2 \cdot 0) + 3$
(xii) $1 + 2 \not\equiv 2 + 1$

x1.19S. Não tem como!

Capítulo 2

x2.2S. A segunda ocorrência da palavra «porque» não faz sentido nenhum: o que segue depois não é uma justificação da tese $8 \nmid 12$, mas sim apenas uma repetição da mesma afirmação. Essencialmenteo que tá escrito nessa frase é:

o 8 não divide o 12 porque o 8 não divide o 12.

Substituindo por um «ou seja», a frase faz sentido, e serve apenas como um *comentário*, lembrando para o leitor a definição:

$8 \nmid 12$, *ou seja*, nenhum inteiro u satisfaz $12 = 8u$.

Procure mais sobre isso no Nota 2.31.

x2.3S. O erro fica na aplicação da definição de $a \mid b$: ao invés de $(\exists k \in \mathbb{Z})[\, b = ak \,]$, a demonstração usou $(\exists k \in \mathbb{Z})[\, a = bk \,]$.

Para ver que a proposição realmente é falsa, considere o contraexemplo seguinte:

$$a = 6, \qquad b = 15, \qquad m = 30.$$

Realmente temos $6 \mid 30$ e $15 \mid 30$, mas $6 \cdot 15 = 90 \nmid 30$.

x2.4S. A (ii) é falsa: um contraexemplo seria o $a = 2$, $b = c = 1$. Realmente, temos

$$2 \mid 1 + 1 = 2 \;\;\&\;\; 2 \mid 1 - 1 = 0, \qquad \text{mas} \qquad 2 \nmid 1.$$

A (iii) é verdadeira:

$$\left.\begin{array}{rl} a \mid b + c \implies & a \mid 2b + 2c \\ & a \mid \;\; b + 2c \end{array}\right\} \implies a \mid \underbrace{(2b + 2c) - (b + 2c)}_{b}.$$

x2.5S. A frase

«Se $__ A __$, (então) $__ B __$.»

é uma afirmação: que a proposição A implica a proposição B. Ou seja, não está afirmando que a proposição A é verdadeira (nem que é falsa), e também nada sobre a veracidade da B. Por outro lado, a frase

$$\text{«Como } __A__\text{, (logo) } __B__\text{.»}$$

é uma *argumentação*. Seu escritor já usa como fato conhecido que A é verdadeira, e além disso, ele tá afirmando que B também é verdadeira por causa disso. Em outras palavras, o escritor está *inferindo* a B a partir das afirmações A e $A \implies B$ que ele deixa como implícito que o leitor aceita ambas.

Capítulo 3

x3.5S. Vou começar com a primeira. Sejam a, b, c inteiros. Suponha $a + c = b + c$. Logo $(a + c) + (-c) = (b + c) + (-c)$ (pelo Exercício x3.3). Logo $a + (c + (-c)) = b + (c + (-c))$ pela $(+)$-associatividade nos dois lados. Logo $a + 0 = b + 0$ pela (ZA-InvR) nos dois lados. Logo $a = b$ pela (ZA-IdR) nos dois lados. A segunda é similar, algo que podemos afirmar graças ao Exercício x3.1! Alternativamente, podemos demonstrar a segunda aplicando a comutatividade da adição nos dois lados da hipótese, virando assim um corolário simples da primeira.

x3.15S. Primeiramente demonstrarei a (Z-MCanL). Sejam c, a, b inteiros tais que $c \neq 0$ (1) e $ca = cb$ (2). Vou demonstrar que $a = b$. Pela (2), $ca - cb = 0$. Logo $c(a - b) = 0$. Logo $c = 0$ ou $a - b = 0$. Separamos em casos, e o primeiro é impossível pelo (1). Caso $a - b = 0$. Logo $a = b$.
Segundamente a (Z-MCanR). Ela é similar, e também segue como corolário da (Z-MCanL) aplicando a comutatividade da multiplicação na sua hipótese.

x3.22S. Sejam A conjunto de inteiros e $\heartsuit$ uma operação binária:

$$\heartsuit : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int}.$$

Chamamos o conjunto A de $(\heartsuit)$-fechado sse

$$(\forall a, b \in A)[\, a \heartsuit b \in A \,].$$

x3.23S. Aqui três testemunhas, um para cada conjunto respectivamente:

$$1 + 1 = 2 \qquad (-5) + 5 = 0 \qquad 17 + 4 = 21$$

x3.25S. Seja f uma operação n-ária nos inteiros. Dizemos que A é f-fechado sse para quaisquer $a_1, \ldots, a_n \in A$, temos $f(a_1, \ldots, a_n) \in A$.

x3.27S. Seja $a \in m\mathbb{Z}$ e logo seja u tal que $a = mu$. Calculamos:

$$\begin{aligned} -a &= -(mu) && \text{(pela escolha de } u\text{)} \\ &= m(-u) && \text{(pelo Exercício x3.11)} \\ &\in m\mathbb{Z}. \end{aligned}$$

x3.32S. Deveriamos perceber a oportunidade de demonstrar um lemmazinho que nos permite diretamente ir de $-(a+c)$ para $(-a)+(-c)$.

x3.34S. Sejam a, b inteiros. Aproveitamos a tricotomía (ZP-Tri) e para conseguir a (ZO-Tri) basta demonstrar as três equivalências:

$$b-a \in \iff a<b \qquad b-a=0 \iff a=b \qquad -(b-a) \in \iff a>b.$$

A primeira é imediata (temos até $\iff$, pois se trata da própria definição de $a<b$). A terceira segue diretamente pelo Exercício x3.13 ($-(b-a)=a-b$). Para a segunda demonstramos cada direção separadamente: ($\Rightarrow$): Temos $b+(-a)=0$ pela hipótese desta direção e também $a+(-a)=0$ pela (ZA-InvR). Logo $a=b$ pela Unicidade de resoluções Λ3.14 para a equação $_+(-a)=0$. ($\Leftarrow$): Precisamos demonstrar $b-a=0$, só que $a=b$ e logo basta demontrar $a-a=0$, que é imediato pela (ZA-InvR).

x3.42S. Sejam m_1, m_2 mínima dum conjunto A, ou seja, temos $m_1, m_2 \in A$, e também

$$(\forall a \in A)[\, m_1 \leq a \,] \qquad (\forall a \in A)[\, m_2 \leq a \,]$$

Usando a primeira com $a := m_2$ e a segunda com $a := m_1$ temos:

$$m_1 \leq m_2 \;\;\&\;\; m_2 \leq m_1.$$

Portanto, $m_1 = m_2$ (pela antissimetria da ($\leq$)).

x3.56S. Seja u inteiro. Suponha que já inteiros entre u e $u+1$, e logo seja k tal que $u<k<u+1$. Logo $0<k-u<1$, contradizendo o Teorema Θ3.63.

x3.65S. Definimos recursivamente:

$$\prod_{i=s}^{t} \tau(i) \stackrel{\text{def}}{=} \begin{cases} 1, & \text{caso } s>t; \\ \prod_{i=s}^{t-1} \tau(i)\cdot\tau(t), & \text{caso } s\leq t. \end{cases}$$

x3.76S. Por indução. Primeiramente demonstramos a BASE:

$$2\sum_{i=1}^{0} i \stackrel{?}{=} 0(0+1).$$

Calculamos:

$$2\sum_{i=1}^{0} i = 2\cdot 0 = 0 = 0(0+1).$$

PASSO INDUTIVO. Seja $k \geq 0$ tal que

(H.I.) $$2\sum_{i=1}^{k} i = k(k+1).$$

Calculamos:

$$\begin{aligned}
2\sum_{i=1}^{k+1} i &= 2\left(\left(\sum_{i=1}^{k} i\right) + (k+1)\right) \\
&= 2\left(\sum_{i=1}^{k} i\right) + 2(k+1) \\
&= k(k+1) + 2(k+1) && \text{(pela H.I.)} \\
&= (k+2)(k+1) \\
&= (k+1)(k+2).
\end{aligned}$$

x3.85S. Calculamos:

$$\begin{aligned}
&(x+y)^{k+1} \\
&\quad= (x+y)(x+y)^k \\
&\quad= x(x+y)^k + y(x+y)^k \\
&\quad= x\left(\sum_{r=0}^{k} C(k,r)x^{k-r}y^r\right) + y\left(\sum_{r=0}^{k} C(k,r)x^{k-r}y^r\right) \\
&\quad= \left(\sum_{r=0}^{k} C(k,r)x^{(k-r)+1}y^r\right) + \left(\sum_{r=0}^{k} C(k,r)x^{k-r}y^{r+1}\right) \\
&\quad= x^{k+1} + \left(\sum_{r=1}^{k} C(k,r)x^{(k-r)+1}y^r\right) + \left(\sum_{r=0}^{k-1} C(k,r)x^{k-r}y^{r+1}\right) + y^{k+1} \\
&\quad= x^{k+1} + \left(\sum_{r=1}^{k} C(k,r)x^{(k-r)+1}y^r\right) + \left(\sum_{r=1}^{k} C(k,r-1)x^{k-(r-1)}y^{(r-1)+1}\right) + y^{k+1} \\
&\quad= x^{k+1} + \left(\sum_{r=1}^{k} C(k,r)x^{k-(r-1)}y^r\right) + \left(\sum_{r=1}^{k} C(k,r-1)x^{k-(r-1)}y^r\right) + y^{k+1} \\
&\quad= x^{k+1} + \left(\sum_{r=1}^{k} (C(k,r) + C(k,r-1))x^{k-(r-1)}y^r\right) + y^{k+1} \\
&\quad= x^{k+1} + \left(\sum_{r=1}^{k} C(k+1,r)x^{k-(r-1)}y^r\right) + y^{k+1} \\
&\quad= C(k+1,0)x^{k+1} + \left(\sum_{r=1}^{k} C(k+1,r)x^{k-(r-1)}y^r\right) + C(k+1,k+1)y^{k+1} \\
&\quad= C(k+1,0)x^{(k+1)-0}y^0 + \left(\sum_{r=1}^{k} C(k+1,r)x^{(k+1)-r}y^r\right) + C(k+1,k+1)x^{(k+1)-(k+1)}y^{k+1} \\
&\quad= \sum_{r=0}^{k+1} C(k+1,r)x^{(k+1)-r}y^r.
\end{aligned}$$

x3.93S. Seja $k \geq 8+3 = 11$ tal que $k-1$, $k-2$, e $k-3$ podem ser escritos como somatórios de 3's

e 5's (H.I.). Temos

$$\begin{aligned} k &= (k-3)+3 \\ &= (3x+5y)+3 \quad \text{para alguns } x,y \in \mathbb{N} \qquad \text{(pela H.I.)} \\ &= 3(x+1)+5y. \end{aligned}$$

Como precisamos a veracidade da proposição para o valor $k-3$, devemos mostrar as 3 bases, para os inteiros 8, 9, e 10:

$$\begin{aligned} 8 &= 3+5 &&= 3\cdot 1+5\cdot 1 \\ 9 &= 3+3+3 &&= 3\cdot 3+5\cdot 0 \\ 10 &= 5+5 &&= 3\cdot 0+5\cdot 2. \end{aligned}$$

x3.94S. «Seja $k \geq 0$ tal que $\varphi(k-1)$ (H.I.1) e $\varphi(k)$ (H.I.2). Vou demonstrar que $\varphi(k+1)$.» Nessa maneira, preciso tomar cuidado com inteiros menores de $k-1$.

x3.95S. Vou demonstrar que S tem membros positivos. Seja $x \in S$ tal que $x \neq 0$ ($S \neq \emptyset$ e $S \neq \{0\}$). Caso $x > 0$, já encontramos um membro positivo do S. Caso $x < 0$, basta mostrar que $-x \in S$, pois $-x > 0$. Como S é $(-)$-fechado, temos $x - x \in S$; ou seja, $0 \in S$. Usando novamente que S é $-$-fechado, temos $0 - x \in S$, ou seja $-x \in S$. Pelo PBO, *seja d o menor membro positivo do S*.

x3.96S. Primeiramente vou demonstrar por indução que para todo $n \in \mathbb{N}$, $nd \in S$. A base é imediata: $0d = 0 \in S$. Seja $k \in \mathbb{N}$ tal que $kd \in S$ (HI). Calculamos:

$$(k+1)d = kd + d \in S$$

pois $d \in S$ e $kd \in S$ (pela HI) e S é $(+)$-fechado (pelo Exercício x3.29) Seja $x < 0$, e observe que $(-x)d \in S$ (pois $-x > 0$) e logo $0 - (-x)d \in S$, ou seja, $xd \in S$.

x3.105S. Duas coisas:

EXISTÊNCIA: *para todos inteiros a, b, existe inteiro d que satisfaz as relações acima.*
UNICIDADE: *se g, g', são inteiros que satisfazem essas relações, então $g = g'$.*

x3.106S. O «os a, b são ... (entre si)» presuponha que tal propriedade é simétrica nos seus argumentos a, b, e logo precisamos demonstrar a comutatividade: $(a, b) = (b, a)$, que faz parte do Exercício x3.108.

x3.109S. Toma 3 e 4. Temos $(4, 3) = 1$, mas:

$$\begin{aligned} 1 &= (-2)\cdot 4 + 3\cdot 3 \\ 1 &= \quad 4 \ \cdot 4 - 5\cdot 3. \end{aligned}$$

x3.110S. Pelo Lemma de Bézout Λ3.107 temos que

$$C = \{\, ax + by \mid x, y \in \mathbb{Z} \,\} = d\mathbb{Z}$$

onde d é um mdc dos a, b. Pela hipótese (ii), $c \in C = d\mathbb{Z}$, e logo $d \mid c$. Pela hipótese (i), c sendo um divisor comum dos a, b, divide o mdc deles: $c \mid d$. Portanto c é um mdc dos a, b.

x3.111S. Basta mostrar que os conjuntos dos divisores comuns dos a, b e dos $a, a+b$ são iguais.
$\mathit{comdivs}(a,b) \subseteq \mathit{comdivs}(a, a+b)$. Seja c divisor comum dos a, b. Preciso mostrar que $c \mid a$ (que é imediato pela escolha de c), e que $c \mid a+b$, que segue pela Lema Λ3.26.
$\mathit{comdivs}(a,b) \supseteq \mathit{comdivs}(a, a+b)$. Seja c divisor comum dos $a, a+b$. Preciso mostrar que $c \mid a$ (que é imediato pela escolha de c), e que $c \mid b$, que segue pela Lema Λ3.26 pois $b = 1 \cdot (a+b) + (-1) \cdot a$.

x3.112S. Vamos demonstrar o pedido por indução. A base

$$(F_0, F_1) = (0, 1) = 1.$$

Seja $k \in \mathbb{N}$ tal que $(F_k, F_{k+1}) = 1$ (HI). Precisamos mostrar que $(F_{k+1}, F_{k+2}) = 1$. Calculando,

$$\begin{aligned}
(F_{k+1}, F_{k+2}) &= (F_{k+1}, F_{k+1} + F_k) && \text{(pela definição da } F_n\text{)} \\
&= (F_{k+1}, F_k) && \text{(pelo Exercício x3.111, com } a := F_{k+1},\ b := F_k\text{)} \\
&= (F_k, F_{k+1}) && \text{(pelo Exercício x3.108)} \\
&= 1. && \text{(pela hipótese indutiva)}
\end{aligned}$$

x3.113S. (i) Para o $(108, 174) = (174, 108)$ calculamos:

$$\begin{array}{rll}
174 = 108 \cdot 1 + 66, & 0 \le 66 < 108 & (174, 108) = (108, 66) \\
108 = \ 66 \cdot 1 + 42, & 0 \le 42 < \ 66 & = (66, 42) \\
\ 66 = \ 42 \cdot 1 + 24, & 0 \le 24 < \ 42 & = (42, 24) \\
\ 42 = \ 24 \cdot 1 + 18, & 0 \le 18 < \ 24 & = (24, 18) \\
\ 24 = \ 18 \cdot 1 + 6, & 0 \le \ 6 < \ 18 & = (18, 6) \\
18 = \boxed{6} \cdot 3 + 0 & & = (6, 0) = \boxed{6}.
\end{array}$$

(ii) Calculamos:

$$\begin{array}{rll}
2016 = 305 \cdot 6 + 186, & 0 \le 186 < 305 & (2016, 305) = (305, 186) \\
305 = 186 \cdot 1 + 119, & 0 \le 119 < 186 & = (186, 119) \\
186 = 119 \cdot 1 + 67, & 0 \le \ 67 < 119 & = (119, 67) \\
119 = \ 67 \cdot 1 + 52, & 0 \le \ 52 < \ 67 & = (67, 52) \\
\ 67 = \ 52 \cdot 1 + 15, & 0 \le \ 15 < \ 52 & = (52, 15) \\
\ 52 = \ 15 \cdot 3 + 7, & 0 \le \ \ 7 < \ 15 & = (15, 7) \\
\ 15 = \ \ 7 \cdot 2 + 1, & 0 \le \ \ 1 < \ \ 7 & = (7, 1) \\
\ 7 = \boxed{1} \cdot 7 + 0 & & = (1, 0) = \boxed{1}.
\end{array}$$

x3.114S. A definição do mdc (a, b) não foi «o $(\le)$-maior divisor comum dos a e b». Lembre-se a Definição D3.98. Veja também o Problema Π3.24.

x3.115S. São os "$\cdots$" mesmo! Para formalizá-los em definições usamos recursão; pra formalizá-los em demonstrações usamos indução.

x3.117S. Caso $b > a/2$: Então $r = a - b < a/2$. Caso $b < a/2$: Então $r < b < a/2$.

x3.118S. Por indução. Base. Sejam inteiros $a > b > 0$ tais que Euclid(a, b) precisa 1 passo para terminar: Precisamos inferir que $a \geq F_3 = 2$ e $b \geq F_2 = 1$, imediato pois $a > b > 0$. Passo indutivo. Seja $k \geq 1$ tal que para quaisquer inteiros $u > v > 0$, se Euclid(u, v) precisa k passos (divisões) para terminar, emtão $u \geq F_{k+2}$ e $v \geq F_{k+1}$:

(HI) $\quad (\forall u > v > 0)[\,\text{Euclid}(u, v)$ termina em k passos $\implies u \geq F_{k+2}$ & $v \geq F_{k+1}\,]$.

Sejam inteiros $a > b > 0$ tais que Euclid(a, b) termina em $k + 1$ passos. Executamos o primeiro desses passos, obtendo os q_0, r_0:

$$a \;=\; b\,q_0 + r_0, \qquad\qquad 0 \leq r_0 < b$$

Agora em k passos o algoritmo terminará, mas neste ponto o algoritmo manda executar o Euclid(b, r_0). Ou seja o Euclid(b, r_0) precisa k passos, e $b > r_0 > 0$, e logo pela HI com $u := b$ e $v := r_0$ inferimos:

(HI*) $\qquad\qquad b \geq F_{k+2} \qquad r_0 \geq F_{k+1}.$

Calculamos:

$$\begin{aligned} a &= bq_0 + r_0 \\ &\geq F_{k+2}q_0 + F_{k+1} && \text{(HI*)} \\ &\geq F_{k+2}\,1 + F_{k+1} && (q_0 \geq 1 \text{ pois } a > b) \\ &= F_{k+2} + F_{k+1} \\ &= F_{k+3}. && \text{(def. } F_{k+3}) \end{aligned}$$

x3.120S. Todas as estratégias são iguais: em cada passo, um (+) é adicionado, e todas terminam no mesmo somatório com n '1's e $n-1$ '+'s. Então começando com qualquer número n, depois de $n-1$ passos chegamos na sua forma $n = 1 + 1 + \cdots + 1$.

x3.122S. Esquecendo a ordem que os fatores parecem, são iguais: cada construção precisa os mesmos blocos atômicos (o 2, o 3, e o 7), e cada um deles foi usado o mesmo número de vezes: $2016 = 2^5 3^2 7$.

x3.123S. Calculamos:

$$\begin{array}{llll} 15 = 3 \cdot 5 & 17 = 17 & 100 = 2^2 \cdot 5^2 & 2015 = 5 \cdot 13 \cdot 31 \\ 16 = 2^4 & 81 = 3^4 & 280 = 2^3 \cdot 5 \cdot 7 & 2017 = 2017. \end{array}$$

x3.126S. Como $p \mid pq$ e $pq \mid n^2$, logo $p \mid n^2$. Ou seja $p \mid n$ (1) pelo Lemma de Euclides Λ3.131. Similarmente $q \mid n$ (2). Mas p, q são primos distintos, logo coprimos, e ambos dividem o n ((1) e (2)) logo $pq \mid n$ (pelo Corolário 3.134).

x3.127S. Nenhum dos dois é nem primo nem composto: a definição começa declarando p como um natural tal que $p \geq 2$. Logo, não é aplicável nem para o 0 nem para o 1.

Π3.18S. Seja

$$\varphi(n) \iff^{\text{def}} (\forall x \in \mathbb{Z})[\,\textsc{Euclid}(x,n) \text{ termina com } (x,n)\,]$$

Vamos demonstrar que $(\forall n \in \mathbb{N})[\,\varphi(n)\,]$ por indução forte. Seja $k \in \mathbb{N}$ tal que $\varphi(i)$ para todo $i < k$ (hipótese indutiva). Precisamos demonstrar o $\varphi(k)$, ou seja, que *para todo* $x \in \mathbb{Z}$, $\textsc{Euclid}(x,k)$ *termina e* $\textsc{Euclid}(x,k) = (x,k)$. Seja $x \in \mathbb{Z}$, e aplica o $\textsc{Euclid}(x,k)$ para um passo. Se $k = 0$, a computação termina imediatamente com o resultado x, que é correto (3.108). Se $k > 0$, o algoritmo manda reduzir sua computação para a computação do $\textsc{Euclid}(k,r)$, onde $r = x \bmod k < k$. Seguindo o Lema Λ3.113 $(x,k) = (k,r)$, então falta verificar que o $\textsc{Euclid}(k,r)$ termina mesmo com (k,r), que segue pela hipótese indutiva porque $r < k$ e logo $\varphi(r)$ é válido.

Π3.19S. Demonstramos cada parte separamente:

Terminação. Para chegar num absurdo, suponha que existem contraexemplos: *inteiros* $c \geq 0$, *tais que o* $\textsc{Euclid}(a,c)$ *não termina para algum* $x \in \mathbb{Z}$. Seja m o menor deles (PBO):

$$m = \min\{\, c \in \mathbb{N} \mid (\exists x \in \mathbb{Z})[\,\textsc{Euclid}(x,c) \text{ não termina}\,]\,\}.$$

Logo, para algum certo $a \in \mathbb{Z}$, temos que $\textsc{Euclid}(a,m)$ não termina. Com certeza $m \neq 0$, porque nesse caso o algoritmo termina imediatamente. Logo $m > 0$ e aplicando o $\textsc{Euclid}(a,m)$ para apenas um passo a sua computação é reduzida no computação do $\textsc{Euclid}(m,r)$, onde $r = a \bmod m < m$, *e agora precisamos mostrar que o* $\textsc{Euclid}(m,r)$ *termina para chegar num absurdo.* Pela escolha do m como *mínimo* dos contraexemplos, o r não pode ser contraexemplo também. Em outras palavras, o $\textsc{Euclid}(x,r)$ realmente termina para qualquer x, então para $x = m$ também, que foi o que queríamos demonstrar.

Corretude. Para chegar num absurdo, suponha que existem contraexemplos: *inteiros* $c \geq 0$, *tais que o* $\textsc{Euclid}(x,c)$ *acha resultado errado para algum* $x \in \mathbb{Z}$. Seja m o menor desses contraexemplos (PBO):

$$m = \min\{\, c \in \mathbb{N} \mid (\exists x \in \mathbb{Z})[\,\textsc{Euclid}(x,c) \neq (x,c)\,]\,\}.$$

Logo, para algum certo $a \in \mathbb{Z}$, temos $\textsc{Euclid}(a,m) \neq (a,m)$. Esse m não pode ser 0, porque nesse caso o algoritmo retorna sua primeira entrada a; resultado correto por causa do Propriedade 3.108. Então $m > 0$. Aplicamos para um passo o $\textsc{Euclid}(a,m)$. Como $m \neq 0$, o algoritmo manda realizar o segundo passo: retornar o que $\textsc{Euclid}(m,r)$, onde $r = a \bmod m < m$. (E sabemos que o $\textsc{Euclid}(m,r)$ vai retornar algo, porque já demonstramos a terminação do algoritmo para todas as suas possíveis entradas!) Para concluir, observe:

$$\begin{aligned} \textsc{Euclid}(m,r) &= \textsc{Euclid}(a,m) && \text{(pelas instruções do algoritmo)} \\ &\neq (a,m) && \text{(escolha dos } m \text{ e } a\text{)} \\ &= (m,r)\,. && \text{(pelo Lema Λ3.113)} \end{aligned}$$

Então $\textsc{Euclid}(m,r) \neq (m,r)$ e achamos um contraexemplo (o r) menor que o mínimo (o m)—absurdo!

Π3.24S. Se $a = b = 0$, o símbolo (a,b) não é definido, porque todo $n \in \mathbb{N}$ é um divisor em comum, mas como o $\mathbb{N}$ não tem um elemento máximo, não existe o maior deles.

Precisamos restringir a definição para ser aplicável apenas nos casos onde pelo menos um dos a e b não é o 0 (escrevemos isso curtamente: $ab \neq 0$). Assim, quando a nova definição é aplicável, ela realmente defina o mesmo número, fato que segue pelas propriedades:

$$\begin{aligned} (x,0) = 0 &\implies x = 0 \\ x \mid y \;\;\&\;\; y \neq 0 &\implies |x| \leq |y| \,. \end{aligned}$$

Π3.25S. Agora a estratégia ótima seria quebrar cada termo "no meio". Assim, para o 10 temos:

$$\begin{aligned} 10 &= 5 + 5 \\ &= (2+3) + (2+3) \\ &= [(1+1) + (1+2)] + [(1+1) + (1+2)] \\ &= 1+1+1+1+1+1+1+1+1+1 \end{aligned}$$

em apenas 4 pássos. Depois de cada passo, se o maior termo fosse o m, agora é o $\lceil \frac{m}{2} \rceil$. Precisamos tantos passos quantas vezes que podemos dividir o n por 2 até chegar na unidade 1: precisamos $\lceil \log_2(n) \rceil$ passos.

Π3.26S. Seja

$$p_0 < p_1 < p_2 < p_3 < \cdots$$

a seqüência infinita dos primos. (Assim, $p_0 = 2$, $p_1 = 3$, $p_2 = 5$, etc.) Seja

$$\langle s_0, s_1, \ldots, s_{n-1} \rangle \in S$$

uma seqüência de naturais de tamanho n. Vamos codificá-la com o inteiro

$$c_s = \prod_{i=0}^{n-1} p_i^{s_i+1} = p_0^{s_0+1} p_1^{s_1+1} p_2^{s_2+1} \cdots p_{n-1}^{s_{n-1}+1}.$$

(Note que a seqüência vazia ($n = 0$) correponde no número $1 \in \mathbb{N}_{>0}$.)

Conversamente, dado um número $c \in \mathbb{N}_{>0}$ que codifica uma seqüência, como podemos "decodificar" a seqüência que corresponda com ele? Graças o teorema fundamental da aritmética (Θ3.140), temos

$$c = p_0^{a_0} p_1^{a_1} \cdots p_{m-1}^{a_{m-1}}.$$

Se existe exponente $a_j = 0$, o c não codifica nenhuma seqüência. Caso contrário, todos os exponentes são positivos, e o c codifica a seqüência

$$\langle a_0 - 1, a_1 - 1, \ldots, a_m - 1 \rangle \in S.$$

x3.138S. Pelo Lemma da Divisão de Euclides Λ3.82, precisamos $b \neq 0$ para definir a divisão de a por b.

x3.139S. Vamo lá:

(1) $69 \pmod 5 = 4$ não significa nada.

(2) $12 = 3 \pmod 8$ não significa nada.[114]
(3) $12 \equiv 20 \pmod 4$ significa $4 \mid 12 - 20 = -8$, que é válido.
(4) $8 \pmod 3 \equiv 12$ não significa nada.
(5) $108 \equiv 208 \pmod{(43 \bmod 30)}$ significa que $43 \bmod 30 \mid 108 - 208$, e para decidir se é válida ou não, calculamos $43 \bmod 30 = 13$, e $108 - 208 = -100$ e substituimos: $13 \mid -100$, que é falso.
(6) $(\forall x \in \mathbb{Z})[\, x \bmod 4 = 2 \to x \equiv 0 \pmod 2\,]$ denota a afirmação que para todo $x \in \mathbb{Z}$, se $x \bmod 4 = 2$ então $x \equiv 0 \pmod 2$, que é válido: seja $x \in \mathbb{Z}$ tal que $x \bmod 4 = 2$. Logo $x = 4k + 2 = 2(2k + 1)$ para algum $k \in \mathbb{Z}$, ou seja, $2 \mid x = x - 0$.
(7) $5^{192 \bmod 3}$ é o número 5 elevado ao resto da divisão de 192 por 3. Como $3 \mid 192$ (por quê? $1 + 9 + 2 = 12$; $1 + 2 = 3$; veja o Critérion 3.187), temos $192 \bmod 3 = 0$, então o valor da expressão é o número $5^0 = 1$.
(8) $13 \pmod 8 \equiv 23 \pmod{18}$ não significa nada.

x3.141S. Pela definição de congruência (D3.155) e de $(|)$ (D3.22) temos que:

$$x = mk + t, \quad \text{para algum } k \text{ inteiro.}$$

Dividindo o k por a, temos $k = aq + i$, onde $q, i \in \mathbb{Z}$ e $0 \leq i < a$. Substituindo:

$$\begin{aligned} x &= m(aq + i) + t \\ &= maq + (mi + t). \end{aligned}$$

Logo, chegamos nas a congruências

$$x \equiv mi + t \pmod{ma}, \quad \text{para } i = 0, \ldots, a - 1,$$

e x tem que satisfazer (exatamente) uma delas.

x3.144S. Para o símbolo a^{-1} ser bem-definido, precisamos mostrar que, caso que existe um inverso, ele é único, que nos realmente mostramos no Teorema Θ3.168.

x3.145S. Pela hipótese $m \mid ca - cb = c(a - b)$. Mas $(m, c) = 1$, então (pelo Lema Λ3.133) $m \mid a - b$, ou seja, $a \equiv b \pmod m$.

x3.149S. Somamos o $-b_1$ aos dois lados.

x3.150S. É da forma $ax \equiv b \pmod m$ com a invertível (pois $(a, m) = 1$), ou seja, sabemos como resolver desde a Secção §72.

x3.152S. Os 2, 4, 5 são coprimos entre si (têm mdc 1) mas mesmo assim não são coprimos dois-a-dois: $(2, 4) = 2$.

[114] Se o '$=$' fosse '$\equiv$', então significaria que $8 \mid 12 - 3 = 9$ (que é falso).

x3.155S. Observe que por causa do Corolário 3.134, temos:

$$6 \mid c \iff 2 \mid c \ \&\ 3 \mid c.$$

Logo, aplicamos os critéria de divisibilidade por 2 e por 3.

x3.156S. Como $(4,2) = 4 \neq 1$, não podemos aplicar o Corolário 3.134. Um contraexemplo: $2 \mid 12$ e $4 \mid 12$, mas $2 \cdot 4 = 8 \nmid 12$.

Π3.30S. Temos

$$\begin{aligned}
(x+y)^p &= \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i && \text{(por Teorema binomial Θ3.80)} \\
&= \binom{p}{0} x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^{p-i} y^i + \binom{p}{p} y^p && (p \geq 2) \\
&= x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^{p-i} y^i + y^p \\
&= x^p + \sum_{i=1}^{p-1} p c_i x^{p-i} y^i + y^p, \quad \text{para algum } c_i \in \mathbb{Z} && \text{(por Problema Π3.20)} \\
&= x^p + p \sum_{i=1}^{p-1} c_i x^{p-i} y^i + y^p \\
&\equiv x^p + y^p \pmod{p}.
\end{aligned}$$

Π3.31S. Considere $k \in \mathbb{N}$ arbitrário. Basta encontrar um primo da forma $4n+3$ que é maior que o k-ésimo primo. Seja $N = 4p_1 p_2 \cdots p_k - 1$, que é um numero da forma $4n+3$ que não é divisível por nenhum dos $p_1, \cdots, p_k$. Agora observe que N não pode ter apenas divisores da forma $4n+1$, pois se fosse o caso ele seria da mesma forma. Logo pelo menos um dos primos que o dividem é da forma $4n+3$ e maior que o p_k (pelo (1)) e logo achamos o primo que estavamos procurando.

x3.159S. Pelo Fermatinho (Θ3.192), temos

$$a^p \equiv_p a = a1$$

e como p é primo, logo $p > 0$ e logo $a^p = aa^{p-1}$. Substituindo obtemos

$$aa^{p-1} \equiv_p a1.$$

Como a é coprimo com p, logo a é cancelável, e logo

$$a^{p-1} \equiv_p 1.$$

x3.160S. Dado um a coprimo com p, já que $a^{p-1} \equiv_p 1$, logo $a^{p-2}a = a^{p-1} \equiv_p 1$, e logo a^{p-2} é um inverso de a módulo p.

x3.161S. Pelo Fermatinho (Θ3.192), $108^{240} \equiv_{241} 1$, ou seja, $108^{239}108 \equiv_{241} 1$. Segue que 108^{239} é um inverso de 108 módulo 241.

x3.163S. Para o número n escrito em base decimal como $\delta_k\delta_{k-1}\cdots\delta_1\delta_0$, temos:

$$\begin{aligned} n &= d_0 + 10d_1 + 100d_2 + \cdots 10^{k-1}d_{k-1} + 10^k d_k \\ &= \underbrace{d_0}_{\text{resto}} + 10\underbrace{(d_1 + 10d_2 + \cdots 10^{k-2}d_{k-1} + 10^{k-1}d_k)}_{\text{quociente}}, \end{aligned}$$

onde d_i é o correspondente valor do dígito δ_i. (Evitamos aqui confundir o "dígito" com seu valor usando notação diferente para cada um, para enfatizar a diferença entre os dois conceitos.)

x3.164S. Podemos ou aplicar o teorema chinês (Teorema chinês do resto Θ3.182) no sistema de congruências

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 0 \pmod 2, \end{aligned}$$

ou, como $5 \mid 10$, usar diretamente o Exercício x3.141, para concluir que $x = 10k + 5i + 1$, onde $i = 0, 1$.

x3.165S. Como $(41, 3) = 1$, pelo teorema de Fermat (Fermatinho (Θ3.192)) temos

$$41^2 \equiv 1 \pmod 3,$$

e agora dividindo o 75 por 2, temos $75 = 2 \cdot 37 + 1$, então:

$$\begin{aligned} 41^2 \equiv 1 \pmod 3 &\implies (41^2)^{37} \equiv 1 \pmod 3 \\ &\implies 41^{74} \equiv 1 \pmod 3 \\ &\implies 41^{74}41 \equiv 41 \pmod 3 \\ &\implies 41^{75} \equiv 41 \pmod 3 \\ &\implies 41^{75} \equiv 2 \pmod 3. \end{aligned}$$

Outro jeito para escrever exatamente a mesma idéia, mas trabalhando "de fora pra dentro", seria o seguinte:

$$\begin{aligned} 41^{75} &= 41^{2\cdot 37+1} \\ &= 41^{2\cdot 37}41 \\ &= (41^2)^{37}41 \\ &\equiv 1^{37}41 \pmod 3 \\ &\equiv 41 \pmod 3 \\ &\equiv 2 \pmod 3. \end{aligned}$$

x3.181S. Seguindo a definição de ϕ, vamos contar todos os números no $\{1, 2, \ldots, p^i\}$ que são coprimos com p^i. Quantos não são? Observe que como p é primo, os únicos que não são coprimos com ele, são os múltiplos de p. Pelo Exercício x3.179 temos a resposta.

Capítulo 4

x4.4S. Um caminho para calcular a primeira é o seguinte:

$$\begin{aligned}
SSS0 + \underline{(SS0 + S0)} &= SSS0 + S\underline{(SS0 + 0)} && \text{(por } (+).2\text{)}\\
&= \underline{SSS0 + SSS0} && \text{(por } (+).1\text{)}\\
&= S\underline{(SSS0 + SS0)} && \text{(por } (+).2\text{)}\\
&= SS\underline{(SSS0 + S0)} && \text{(por } (+).2\text{)}\\
&= SSS\underline{(SSS0 + 0)} && \text{(por } (+).2\text{)}\\
&= SSSSSS0 && \text{(por } (+).1\text{)}
\end{aligned}$$

e um caminho para calcular a segunda é o:

$$\begin{aligned}
\underline{(SSS0 + SS0) + S0} &= S(\underline{(SSS0 + SS0)} + 0) && \text{(por } (+).2\text{)}\\
&= S(S\underline{(SSS0 + S0)} + 0) && \text{(por } (+).2\text{)}\\
&= S\underline{(SS(SSS0 + 0) + 0)} && \text{(por } (+).2\text{)}\\
&= SSS\underline{(SSS0 + 0)} && \text{(por } (+).1\text{)}\\
&= SSSSSS0 && \text{(por } (+).1\text{)}
\end{aligned}$$

x4.5S. Definimos:

$$\begin{aligned}
&\mathit{double} : \mathsf{Nat} \to \mathsf{Nat}\\
&\mathit{double}\ \mathsf{O} \quad\ = \mathsf{O}\\
&\mathit{double}\ (\mathsf{S}\ n) = \mathsf{S}\ (\mathsf{S}\ (\mathit{double}\ n)).
\end{aligned}$$

Calculamos:

$$\begin{aligned}
\mathit{double}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O}))) &= \mathsf{S}\ (\mathsf{S}\ (\mathit{double}\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O})))) && (\text{por } \mathit{double}.2)\\
&= \mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathit{double}\ (\mathsf{S}\ \mathsf{O}))))) && (\text{por } \mathit{double}.2)\\
&= \mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathit{double}\ \mathsf{O}))))) && (\text{por } \mathit{double}.2)\\
&= \mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O})))). && (\text{por } \mathit{double}.1)
\end{aligned}$$

x4.6S.

(m1) $n \cdot 0 = 0$

(m2) $n \cdot Sm = (n \cdot m) + n$

x4.9S. Definimos:

$$\begin{aligned}
n \mathbin{\hat{}} 0 &= S0\\
n \mathbin{\hat{}} Sm &= (n \mathbin{\hat{}} m) \cdot n.
\end{aligned}$$

ou, se preferir usar a notação padrão para exponenciação e multiplicação:

$$\begin{aligned} n^0 &= S0 \\ n^{Sm} &= n^m \cdot n. \end{aligned}$$

Também pode ser definida assim:

$$\begin{aligned} n^0 &= S0 \\ n^{Sm} &= n \cdot n^m. \end{aligned}$$

Depois vamos comparar essas duas definições.

x4.12S. (i) Uma maneira bem mais curta para defini-las:

$$\begin{array}{ll} q : \mathsf{Nat} \to \mathsf{Nat} & \\ q\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ \mathsf{O}))) = \mathsf{S}\ (q\ n) & \\ q\ _ \qquad\qquad\quad = \mathsf{O} & \end{array} \qquad \begin{array}{ll} r : \mathsf{Nat} \to \mathsf{Nat} & \\ r\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ n)))) = r\ n & \\ r\ n \qquad\qquad\quad = n & \end{array}$$

(ii) A q calcula o quociente da divisão da sua entrada por 3, e a r o resto.

x4.13S. Calculamos:

$$\begin{aligned} (a+m)+y &= (a+m)+0 && \text{(hipótese do caso)} \\ &= a+m && \text{(pela (+).1)} \\ a+(m+y) &= a+(m+0) && \text{(hipótese do caso)} \\ &= a+m && \text{(pela (+).1)} \end{aligned}$$

x4.15S. O erro está na primeira equação do último cálculo:

$$Sk+m = S(k+m). \qquad ((+).2)$$

A (+).2 não nos permite concluir isso; só o seguinte:

$$k+Sm = S(k+m).$$

Se soubessimos que $Sk+m = k+Sm$ seria fácil terminar essa demonstração corretamente. Essa propriedade parece razoável para afirmar:

$$(\forall x)(\forall y)[\,Sx+y = x+Sy\,].$$

Bora demonstrar então!

x4.16S. Por indução no k.
Base: $\forall n \forall m\big((n\cdot m)\cdot 0 = n\cdot(m\cdot 0)\big)$. Sejam n, m naturais. Calculamos:

$$\begin{aligned} (n\cdot m)\cdot 0 &= 0 && ((\cdot).1) \\ n\cdot(m\cdot 0) &= n\cdot 0 && ((\cdot).1) \\ &= 0. && ((\cdot).1) \end{aligned}$$

Passo indutivo. Seja w natural tal que

$$\text{(H.I.)} \qquad \forall n \forall m \big((n \cdot m) \cdot w = n \cdot (m \cdot w) \big).$$

Ou seja: "w na direita associa com todos". Queremos demonstrar que seu sucessor Sw faz a mesma coisa:

$$\forall n \forall m \big((n \cdot m) \cdot Sw = n \cdot (m \cdot Sw) \big).$$

Sejam n, m naturais. Calculamos:

$$\begin{aligned}
(n \cdot m) \cdot Sw &= ((n \cdot m) \cdot w) + (n \cdot m) && ((\cdot).2) \\
n \cdot (m \cdot Sw) &= n \cdot ((m \cdot w) + m) && ((\cdot).2) \\
&= (n \cdot (m \cdot w)) + (n \cdot m) && ((*)) \\
&= ((n \cdot m) \cdot w) + (n \cdot m). && ((\text{H.I.}))
\end{aligned}$$

Onde devemos para o (*) demonstrar como lemma a distributividade (esquerda) da $(\cdot)$ sobre a $(+)$ (feito no Exercício x4.18).

x4.17S. Por indução no m.
Base: $(\forall n)[\, n \cdot 0 = 0 \cdot n \,]$. Vamos demonstrar por indução! Sub-base: $0 \cdot 0 = 0 \cdot 0$. Trivial!
Sub-passo indutivo. Seja $k : \mathsf{Nat}$ tal que

$$\text{(S.H.I.1)} \qquad k \cdot 0 = 0 \cdot k.$$

Ou seja, *k é um número que comuta com o 0*. Vamos demonstrar que $Sk \cdot 0 = 0 \cdot Sk$. Calculamos:

$$\begin{aligned}
Sk \cdot 0 &= 0 && ((\cdot).1) \\
0 \cdot Sk &= 0 \cdot k + 0 && ((\cdot).2) \\
&= 0 \cdot k && ((+).1) \\
&= k \cdot 0 && ((\text{S.H.I.1})) \\
&= 0. && ((\cdot).1)
\end{aligned}$$

Isso demonstra nossa base. Passo indutivo. Seja $w \in \mathbb{N}$ tal que

$$\text{(H.I.)} \qquad \forall n (n \cdot w = w \cdot n).$$

Ou seja, *w é um número que comuta com todos*. Queremos demonstrar que seu sucessor Sw faz a mesma coisa:

$$\forall n (n \cdot Sw = Sw \cdot n).$$

Vamos demonstrar por mais uma indução! Sub-base: $0 \cdot Sw = Sw \cdot 0$. Calculamos:

$$\begin{aligned}
0 \cdot Sw &= 0 \cdot w + 0 && ((\cdot).2) \\
&= 0 \cdot w && ((+).1) \\
&= w \cdot 0 && (\text{Base (0 comuta com todos) ou (H.I.) (w comuta com todos)}) \\
&= 0 && ((\cdot).1) \\
&= Sw \cdot 0. && ((\cdot).1)
\end{aligned}$$

Sub-passo indutivo. Seja $p \in \mathbb{N}$ tal que ele comuta com o Sw:

$$\text{(S.H.I.2)} \qquad p \cdot Sw = Sw \cdot p.$$

Vamos demonstrar que Sp também comuta com o Sw:

$$Sp \cdot Sw = Sw \cdot Sp.$$

Calculamos:

$$\begin{aligned}
Sp \cdot Sw &= Sp \cdot w + Sp && ((\cdot).2)\\
&= w \cdot Sp + Sp && ((\text{H.I.}):\ w \text{ comuta com todos})\\
&= (w \cdot p + w) + Sp && ((\cdot).2)\\
&= w \cdot p + (w + Sp) && (\text{associatividade da } (+))\\
&= w \cdot p + S(w + p) && ((+).2)\\
&= w \cdot p + S(p + w) && (\text{comutatividade da } (+))\\
&= w \cdot p + (p + Sw) && ((+).2)\\
Sw \cdot Sp &= Sw \cdot p + Sw && ((\cdot).2)\\
&= p \cdot Sw + Sw && ((\text{S.H.I.2}):\ p \text{ comuta com o } Sw)\\
&= (p \cdot w + p) + Sw && ((\cdot).2)\\
&= p \cdot w + (p + Sw) && (\text{associatividade da } (+))\\
&= w \cdot p + (p + Sw). && ((\text{H.I.}):\ w \text{ comuta com todos})
\end{aligned}$$

x4.18S. Demonstramos a afirmação por indução no z.
Base: $(\forall x)(\forall y)[\, x \cdot (y + 0) = (x \cdot y) + (x \cdot 0)\,]$. Sejam $x, y : \mathsf{Nat}$. Queremos demonstrar que

$$x \cdot (y + 0) = (x \cdot y) + (x \cdot 0).$$

Calculamos:

$$\begin{aligned}
x \cdot (y + 0) &= x \cdot y && ((+).1)\\
&= x \cdot y + 0 && ((+).1)\\
&= x \cdot y + x \cdot 0. && ((\cdot).1)
\end{aligned}$$

Passo indutivo. Seja $k : \mathsf{Nat}$ tal que

(H.I.) $$(\forall x)(\forall y)[\, x \cdot (y + k) = (x \cdot y) + (x \cdot k)\,].$$

Vamos demonstrar que

$$(\forall x)(\forall y)[\, x \cdot (y + Sk) = (x \cdot y) + (x \cdot Sk)\,].$$

Sejam $x, y : \mathsf{Nat}$. Calculamos

$$\begin{aligned}
x \cdot (y + Sk) &= x \cdot S(y + k) && ((+).1)\\
&= (x \cdot (y + k)) + x && ((\cdot).2)\\
&= (x \cdot y + x \cdot k) + x && ((\text{H.I.}) \text{ com } x := x,\ y := y)\\
&= x \cdot y + (x \cdot k + x) && (\text{associatividade de } (+))\\
&= x \cdot y + x \cdot Sk. && ((\cdot).2)
\end{aligned}$$

x4.19S. Por indução no b.

Base: $(\forall x)(\forall a)\big[\, x^{a+0} = x^a \cdot x^0 \,\big]$. Sejam $x, a : \mathsf{Nat}$. Calculamos:

$$\begin{aligned} x^{a+0} &= x^a && ((+).1) \\ &= x^a \cdot S0 && (S0 \text{ identidade } (\Theta 4.46)) \\ &= x^a \cdot x^0. && ((\hat{}).1) \end{aligned}$$

Passo indutivo. Seja $k : \mathsf{Nat}$ tal que

(H.I.) $$(\forall x)(\forall a)\big[\, x^{a+k} = x^a \cdot x^k \,\big].$$

Basta demonstrar que

$$(\forall x)(\forall a)\big[\, x^{a+Sk} = x^a \cdot x^{Sk} \,\big].$$

Sejam $x, a \in \mathbb{N}$. Queremos demonstrar $x^{a+Sk} = x^a \cdot x^{Sk}$. Calculamos:

$$\begin{aligned} x^{a+Sk} &= x^{S(a+k)} && ((+).2) \\ &= x^{a+k} \cdot x && ((\hat{}).2) \\ &= (x^a \cdot x^k) \cdot x && ((\text{H.I.})) \\ &= x^a \cdot (x^k \cdot x) && (\text{assoc. da } (\cdot) \text{ (x4.16)}) \\ &= x^a \cdot x^{Sk}. && ((\hat{}).2) \end{aligned}$$

x4.20S. Por indução no c.
Base: $(\forall a)(\forall b)\big[\, a^{b\cdot 0} = (a^b)^0 \,\big]$. Sejam $a, b : \mathsf{Nat}$. Calculamos:

$$\begin{aligned} a^{b\cdot 0} &= a^0 && ((\cdot).1) \\ &= S0 && ((\hat{}).1) \\ (a^b)^0 &= S0. && ((\hat{}).1) \end{aligned}$$

Passo indutivo. Seja $k : \mathsf{Nat}$ tal que

(H.I.) $$(\forall a)(\forall b)\big[\, a^{b\cdot k} = (a^b)^k \,\big].$$

Queremos demonstrar que

$$(\forall a)(\forall b)\big[\, a^{b\cdot Sk} = (a^b)^{Sk} \,\big].$$

Sejam $a, b : \mathsf{Nat}$. Basta mostrar que $a^{b\cdot Sk} = (a^b)^{Sk}$. Calculamos:

$$\begin{aligned} (a^b)^{Sk} &= (a^b)^k \cdot (a^b) && ((\hat{}).2,\ n := a^b,\ m := k) \\ &= a^{b\cdot k} \cdot a^b && ((\text{H.I.}),\ a := a,\ b := b) \\ &= a^{(b\cdot k)+b} && (\text{x4.19},\ x := a,\ a := b \cdot k,\ b := b) \\ &= a^{b\cdot Sk}. && ((\cdot).2,\ n := b,\ m := k) \end{aligned}$$

x4.21S. Por indução no n.
Base: $S0^0 \stackrel{?}{=} S0$. Imediato pela definição de $S0^0$.
Passo indutivo. Seja $k : \mathsf{Nat}$ tal que

(H.I.) $$S0^k = S0.$$

Basta demonstrar que

$$S0^{Sk} = S0.$$

Calculamos:

$$\begin{aligned}
(S0)^{Sk} &= S0 \cdot S0^k && ((\hat{}).2,\ n := S0,\ m := k)\\
&= S0^k && (S0 \text{ é identidade da } (\cdot) \text{ (Teorema } \Theta 4.46))\\
&= S0. && ((\text{H.I.}))
\end{aligned}$$

x4.24S. ($\Leftarrow$): Suponha $n \leq m$ ou $n = Sm$. Vamos demonstrar que $n \leq Sm$. Separamos em casos. Caso $n \leq m$. Logo seja u tal que $n + u = m$. Logo $S(n + u) = Sm$. E pela $(+).1$ temos $n + Su = Sm$, e logo $n \leq Sm$. Caso $n = Sm$. Nesse caso imediatamente $n + 0 = Sm$ (pois $n + 0 = n$ pela $(+).2$) e logo $n \leq Sm$.

Π4.3S. Definimos

$$\begin{aligned}
t &: \mathbb{N} \to \mathbb{N} & \qquad T &: \mathbb{N}^2 \to \mathbb{R}\\
t(0) &= 1 & \qquad T(m, 0) &= 1\\
t(n+1) &= h(n) \cdot t(n) & \qquad T(m, k+1) &= h(m+k) \cdot T(m, k).
\end{aligned}$$

Tendo definido primeiro a T, podemos definir a t simplesmente assim:

$$t\ h\ n = T\ h\ (0, n).$$

Π4.4S. Se $h(i) = 0$ para algum $i \in \mathbb{N}$, o $t(j) = 0$ para todo $j > i$. Assim, a expressão $t(m + n)/t(m)$ não é definida para qualquer $m > i$. Observe que a solução seria certa se tivéssemos alguma garantia que h não mapeia ninguém ao 0.

Π4.5S. Usamos reductio ad absurdum. Para chegar num absurdo suponha que existe $C \subseteq \mathbb{N}$ não vazio tal que C não possui mínimo. Vamos demonstrar que para todo $n \in \mathbb{N}$, C não possui membros $c \leq n$. Isso é suficiente para garantir que C é vazio. Base: C não possui membros $c \leq 0$. Imediato, pois o único natural $n \leq 0$ é o próprio 0 que é o menor membro do $\mathbb{N}$. Sabemos então que $0 \notin C$ pois caso contrário o C teria um mínimo. Passo Indutivo. Seja k tal que C não possui membros $c \leq k$. Basta demonstrar que C não possui membros $c \leq k + 1$. Suponha então que C possui $c_0 \leq k + 1$. Logo $c_0 < k + 1$ ou $c_0 = k + 1$. O caso $c_0 < k + 1$ é eliminado pela (HI). No outro caso temos $k + 1 \in C$.

x4.42S.

$$\begin{aligned}
&\text{filter} : (\alpha \to \mathsf{Bool}) \to (\mathsf{List}\ \alpha) \to (\mathsf{List}\ \alpha)\\
&\text{filter}\ p\ [\,] \quad\ = [\,]\\
&\text{filter}\ p\ (x :: xs) = (\textbf{if}\ p\ x\ \textbf{then}\ (x ::)\ \textbf{else}\ \text{id})\ (\text{filter}\ p\ xs)
\end{aligned}$$

Π4.11S. A demonstração usa a pred, mas para sua definição *funcionar* já precisamos da injetividade de S; sem ela, a pred, recebendo seu argumento n, não teria como aproveitar o

pattern-matching para obter acesso *àquele* n' tal que $n = \mathsf{S}\ n'$, para conseguir retorná-lo. Se tivesse outro (distinto) n'' tal que $n = \mathsf{S}\ n''$, qual dos n', n'' a pred retornaria?

O que acontece se tentar resolver isso escolhendo um específico deles para retornar (por exemplo, o menor)? Note que a pred viraria, de fato, função. E agora: com esse ajuste, a demonstração compila e pode ser usada para conseguir o princípio como teorema?

Π4.12S. A nova versão de pred não é mais um $(\circ)$-L-inverso. Considere tais $n' \neq n''$ com $\mathsf{S}\ n' = n = \mathsf{S}\ n''$, e com n' o menor tal Nat (e logo o retornado pela pred recebendo n). Assim temos

$$\mathrm{pred}\ (\mathsf{S}\ n'') = \mathrm{pred}\ n = n' \neq n''$$

e logo pred não é uma inversa esquerda da S.

x4.52S.

$$\begin{aligned}
\mathsf{List}\ (\mathsf{List}\ (\mathsf{Bool} \to \mathsf{Nat})) &= (\mathsf{List} \circ \mathsf{List} \circ (\mathsf{Bool} \to))\ \mathsf{Nat} \\
\mathsf{List}\ (\mathsf{Either}\ \mathsf{Nat}\ (\mathsf{Maybe}\ (\mathsf{List}\ \mathsf{Bool}))) &= (\mathsf{List} \circ (\mathsf{Either}\ \mathsf{Nat}) \circ \mathsf{Maybe} \circ \mathsf{List})\ \mathsf{Bool} \\
\mathsf{Nat} \times \mathsf{List}\ (\mathsf{Maybe}\ \mathsf{Nat}) &= ((\mathsf{Nat} \times) \circ \mathsf{List} \circ \mathsf{Maybe})\ \mathsf{Nat} \\
\mathsf{Either}\ \mathsf{Weekday}\ (\mathsf{Nat} \times \mathsf{Bool}) &= (\mathsf{Either}\ \mathsf{Weekday} \circ (\times\ \mathsf{Bool}))\ \mathsf{Nat}.
\end{aligned}$$

x4.53S. Definimos a nodes que conta os nós duma árvore

$$\begin{aligned}
&\mathrm{nodes} : \mathsf{Tree}\ \alpha \to \mathsf{Nat} \\
&\mathrm{nodes}\ (\mathsf{Tip}\ _) \quad = 0 \\
&\mathrm{nodes}\ (\mathsf{Fork}\ \ell\ r) = 1 + (\mathrm{nodes}\ \ell) + (\mathrm{nodes}\ r);
\end{aligned}$$

a leaves que conta as folhas

$$\begin{aligned}
&\mathrm{leaves} : \mathsf{Tree}\ \alpha \to \mathsf{Nat} \\
&\mathrm{leaves}\ (\mathsf{Tip}\ _) \quad = 1 \\
&\mathrm{leaves}\ (\mathsf{Fork}\ \ell\ r) = (\mathrm{leaves}\ \ell) + (\mathrm{leaves}\ r).
\end{aligned}$$

e a depth que conta a altura, ou a profundidade (ou os "andares")

$$\begin{aligned}
&\mathrm{depth} : \mathsf{Tree}\ \alpha \to \mathsf{Nat} \\
&\mathrm{depth}\ (\mathsf{Tip}\ _) \quad = 0 \\
&\mathrm{depth}\ (\mathsf{Fork}\ \ell\ r) = 1 + (\mathrm{max}\ (\mathrm{depth}\ \ell)\ (\mathrm{depth}\ r)).
\end{aligned}$$

x4.58S. Definimos a search pelas

$$\begin{aligned}
&\mathrm{search} : \alpha \to \mathsf{Tree}\ \alpha \to \mathsf{List}\ (\mathsf{Path}) \\
&\mathrm{search}\ w\ (\mathsf{Tip}\ x) \quad = \mathbf{if}\ w = x\ \mathbf{then}\ [[\,]]\ \mathbf{else}\ [\,] \\
&\mathrm{search}\ w\ (\mathsf{Fork}\ l\ r) = \mathbf{let}\ (\mathrm{lpaths}, \mathrm{rpaths}) = (\mathrm{search}\ w\ l, \mathrm{search}\ w\ r) \\
&\qquad\qquad\qquad\qquad \mathbf{in}\ \mathrm{map}\ (\mathsf{L}::)\ \mathrm{lpaths} +\!\!+ \mathrm{map}\ (\mathsf{R}::)\ \mathrm{rpaths}
\end{aligned}$$

e a fetch assim:

$$\begin{aligned}
&\mathrm{fetch} : \mathsf{Path} \to \mathsf{Tree}\ \alpha \to \mathsf{Maybe}\ \alpha \\
&\mathrm{fetch}\ (\mathsf{L} :: ds)\ (\mathsf{Fork}\ l\ _) &&= \mathrm{fetch}\ ds\ \ell \\
&\mathrm{fetch}\ (\mathsf{R} :: ds)\ (\mathsf{Fork}\ _\ r) &&= \mathrm{fetch}\ ds\ r \\
&\mathrm{fetch}\ []\ \ (\mathsf{Tip}\ x) &&= \mathsf{Just}\ x \\
&\mathrm{fetch}\ _\ \ _ &&= \mathsf{Nothing}
\end{aligned}$$

x4.65S. Uma solução é a seguinte:

$$\begin{aligned}
\langle ArEx \rangle &\overset{(2)}{\rightsquigarrow} (\langle ArEx \rangle + \langle ArEx \rangle) \\
&\overset{(1)}{\rightsquigarrow} (\langle ArEx \rangle + 3) \\
&\overset{(2)}{\rightsquigarrow} ((\langle ArEx \rangle + \langle ArEx \rangle) + 3) \\
&\overset{(2)}{\rightsquigarrow} ((\langle ArEx \rangle + (\langle ArEx \rangle + \langle ArEx \rangle)) + 3) \\
&\overset{(1)}{\rightsquigarrow} ((1 + (\langle ArEx \rangle + \langle ArEx \rangle)) + 3) \\
&\overset{(1)}{\rightsquigarrow} ((1 + (2 + \langle ArEx \rangle)) + 3) \\
&\overset{(1)}{\rightsquigarrow} ((1 + (2 + 2)) + 3)
\end{aligned}$$

x4.66S. Temos:

$$\begin{aligned}
&(1) && \langle ArEx \rangle &&::=\ 0 \mid 1 \mid 2 \mid 3 \mid \cdots \\
&(2) && \langle ArEx \rangle &&::=\ (\langle ArEx \rangle + \langle ArEx \rangle) \\
& && &&\quad \mid\ (\langle ArEx \rangle - \langle ArEx \rangle) \\
& && &&\quad \mid\ (\langle ArEx \rangle \cdot \langle ArEx \rangle) \\
& && &&\quad \mid\ (\langle ArEx \rangle \div \langle ArEx \rangle)
\end{aligned}$$

x4.67S. Capítulo 4.

x4.68S. Não, isso nos levaria dum resultado apenas para os subconjuntos finítos de A. O princípio da boa ordem aplica para qualquer subconjunto habitado de $\mathbb{N}$, até para os infinitos.

Π4.19S. Seja s string. Vamos demonstrar por indução (com duas bases) que *para todo* $n \in \mathbb{N}$, ${}^n s = s^n$. Primeiramente verificamos que para $n := 0$ e $n := 1$, realmente temos ${}^n s = s^n$.

Base ($n := 0$). Calculamos:

$${}^0 s \overset{\text{L1}}{=} \varepsilon \overset{\text{R1}}{=} s^0.$$

Base ($n := 1$). Calculamos:

$$\begin{aligned}
{}^1 s &= {}^0 s +\!\!+ s && \text{(def. } {}^1 s\text{)} \\
&= \varepsilon +\!\!+ s && \text{(def. } {}^0 s\text{)} \\
&= s && \text{(E)}
\end{aligned}
\qquad
\begin{aligned}
s^1 &= s +\!\!+ s^0 && \text{(def. } s^1\text{)} \\
&= s +\!\!+ \varepsilon && \text{(def. } s^0\text{)} \\
&= s. && \text{(E)}
\end{aligned}$$

Logo ${}^{1}s = s^1$.

Passo indutivo. Seja $k \geq 2$ tal que ${}^{k-1}s = s^{k-1}$ (HI1) e ${}^{k-2}s = s^{k-2}$ (HI2). Vou demonstrar que ${}^{k}s = s^k$. Calculamos:

$$\begin{aligned}
{}^{k}s &= {}^{k-1}s +\!\!+ s && \text{(L1)}\\
&= s^{k-1} +\!\!+ s && \text{(HI1)}\\
&= (s +\!\!+ s^{k-2}) +\!\!+ s && \text{(R2)}\\
&= (s +\!\!+ {}^{k-2}s) +\!\!+ s && \text{(HI2)}\\
&= s +\!\!+ ({}^{k-2}s +\!\!+ s) && \text{(Assoc.)}\\
&= s +\!\!+ {}^{k-1}s && \text{(L2)}\\
&= s +\!\!+ s^{k-1} && \text{(HI1)}\\
&= s^k. && \text{(R2)}
\end{aligned}$$

Capítulo 5

x5.6S. (1) Como no Exemplo 5.13, traduzimos o problema para um onde C, D, e E, são uma pessoa—vamos chamá-la de CDE—e as 6 pessoas A, B, CDE, F, G, H querem jantar numa mesa de bar com 6 banquinhos. Cada solução desse problema corresponde em tantas configurações quantas as 3 pessoas C, D, E podem sentar numa ordem, ou seja $P_{\mathsf{tot}}(3)$ configurações. A resposta final:

$$P_{\mathsf{tot}}(6) \cdot P_{\mathsf{tot}}(3) = 6!\,3! = 6!\,6$$

(2) Contamos o complementar: todas as maneiras onde F e G sentam juntos $(7! \cdot 2)$, e o tiramos de todas as maneiras sem restricção $(8!)$:

$$P_{\mathsf{tot}}(8) - P_{\mathsf{tot}}(7) \cdot P_{\mathsf{tot}}(2) = 8! - 7! \cdot 2! = 7!(8-2) = 7!\,6$$

(3) Já achamos quantas maneiras tem onde C, D, e E sentam juntos: $6!\,6$. Disso, precisamos subtrair as configurações onde F e G também sentam juntos: para satisfazer as duas restricções, consideramos as 5 "pessoas" A, B, CDE, FG, H, quais podem sentar numa mesa de bar de tamanho 5 de

$$P_{\mathsf{tot}}(5)\, P_{\mathsf{tot}}(3)\, P_{\mathsf{tot}}(2) = 5!\,3!\,2! = 5!\,6\,2 = 6!\,2$$

maneiras. A resposta final então é

$$6!\,6 - 6!\,2 = 6!(6-2) = 6!\,4.$$

x5.7S. O imporante é que em cada passo, qual das nossas disponíveis opções será escolhida, não vai afeitar a quantidade das nossas opções no passo seguinte. Isso é realmente válido nesse caso. Se escolher colocar as letras em outra ordem, por exemplo a `S`, `E`, `I`, `P`, `O`, `M`, teriamos quantidades diferentes para cada passo sim, *mas*: cada uma das nossas escolhas, não afeitaria a quantidade das escolhas próximas. Com essa ordem, chegamos no mesmo

resultado (com um cálculo que de longe aparece diferente):

$$\underbrace{C(12,4)}_{\texttt{4S}}\underbrace{C(8,1)}_{\texttt{E}}\underbrace{C(7,3)}_{\texttt{3I}}\underbrace{C(4,1)}_{\texttt{P}}\underbrace{C(3,1)}_{\texttt{O}}\underbrace{C(2,2)}_{\texttt{2M}} = \frac{12!}{8!\,4!}\frac{8!}{7!\,1!}\frac{7!}{4!\,3!}\frac{4!}{3!\,1!}\frac{3!}{2!\,1!}\frac{2!}{0!\,2!}$$
$$= \frac{12!}{4!\,1!\,3!\,1!\,1!\,2!}$$
$$= \frac{12!}{4!\,3!\,2!}.$$

x5.9S. Temos as equações:

$$\left.\begin{aligned}\binom{0}{0} &= 1\\ \binom{0}{r} &= 0\\ \binom{n}{r} &= \binom{n-1}{r} + \binom{n-1}{r-1}\end{aligned}\right\} \quad \text{equivalentemente} \quad \left\{\begin{aligned}\binom{0}{0} &= 1\\ \binom{0}{r+1} &= 0\\ \binom{n+1}{r+1} &= \binom{n}{r+1} + \binom{n}{r}.\end{aligned}\right.$$

x5.10S. Sejam $r, n \in \mathbb{N}$ com $0 < r < n$. Calculamos:

$$C(n,r) = C(n-1,r) + C(n-1,r-1)$$
$$\iff \quad \frac{n!}{(n-r)!\,r!} = \frac{(n-1)!}{(n-1-r)!\,r!} + \frac{(n-1)!}{(n-1-(r-1))!\,(r-1)!}$$
$$\iff \quad n! = \frac{(n-1)!\,(n-r)!\,r!}{(n-r-1)!\,r!} + \frac{(n-1)!\,(n-r)!\,r!}{(n-r)!\,(r-1)!}$$
$$\iff \quad n! = \frac{(n-1)!\,(n-r)!\,\cancel{r!}}{(n-r-1)!\,\cancel{r!}} + \frac{(n-1)!\,\cancel{(n-r)!}\,r!}{\cancel{(n-r)!}\,(r-1)!}$$
$$\iff \quad n! = \frac{(n-1)!\,(n-r)\cancel{!}}{(n-r-1)!} + \frac{(n-1)!\,r\cancel{!}}{(r-1)!}$$
$$\iff \quad n! = (n-1)!\,(n-r) + (n-1)!\,r$$
$$\iff \quad n! = (n-1)!\,((n-r)+r)$$
$$\iff \quad n! = (n-1)!\,n$$
$$\iff \quad n! = n!$$

x5.14S. Em cada das a intersecções que ele encontra ele tem 3 opções. Logo, ele pode seguir 3^a caminhos diferentes dirigindo até seu combustível acabar.

Π5.3S. Primeiramente vamos esquecer os múltiplos de 3. O resto dos (20) números pode ser permutado de 20! maneiras. Para qualquer dessa maneira, temos $C(21,10)$ opções para escolher em quais 10 das $20+1$ possíveis posições vamos colocar os múltiplos de 3, e

para cada escolha, correspondem 10! diferentes permutações dos múltiplos de 3 nessas 10 posições. Finalmente,

$$\underbrace{20!}_{\text{(ordenar os não-múltiplos)}} \cdot \underbrace{C(21,10)}_{\text{(escolher as posições dos múltiplos)}} \cdot \underbrace{10!}_{\text{(escolher a ordem dos múltiplos)}}$$

das 30! permutações têm a propriedade desejada.

Π5.6S. Seja $f(n)$ a quantidade de maneiras que podemos cobrir um tabuleiro de tamanho $2 \times n$. Começamos observando que para um tabuleiro 2×0 temos exatamente uma maneira de cobrir todos os quadradinhos: fazendo nada. Vamos pular outros casos específicos e voltar caso que precisar. O quadradinho na posição $(1,1)$ pode ser coberto em apenas duas maneiras: (A) por uma peça ocupando as posições $(1,1)$–$(2,1)$; (B) por uma peça ocupando as posições $(1,1)$–$(1,2)$. No caso (A), para cobrir o resto que é um tabuleiro de $2 \times (n-1)$, temos $f(n-1)$ maneiras. No caso (B), observe que tendo a peça cobrindo os $(1,1)$–$(1,2)$, o quadradinho $(2,1)$ só pode ser coberto por uma peça no $(2,1)$–$(2,2)$. Agora basta cobrir o resto que é um tabuleiro de $2 \times (n-2)$, e logo temos $f(n-2)$ maneiras de fazer isso. Agora percebemos que precisamos mais uma base (por causa do $n-2$). Obviamente para cobrir um tabuleiro de tamanho 2×1 temos exatamente uma maneira. Temos então:

$$\begin{aligned} f(0) &= 1 \\ f(1) &= 1 \\ f(n) &= \underbrace{f(n-1)}_{\text{(A)}} + \underbrace{f(n-2)}_{\text{(B)}}. \end{aligned}$$

Π5.8S. (1) Apenas uma escolha é a certa, então a probabilidade de ganhar é:

$$\frac{1}{C(60,6)} = \frac{6!\,54!}{60!} = \frac{6!}{55 \cdot 56 \cdot 57 \cdot 58 \cdot 59 \cdot 60} = \frac{1}{11 \cdot 14 \cdot 19 \cdot 29 \cdot 59 \cdot 10} = \frac{1}{50063860}.$$

(2) Para ganhar, com certeza acertamos nos 6 números da megasena, então temos que contar todas as maneiras de escolher os 3 outros números dos 9 que escolhemos:

$$\frac{C(60-6,9-6)}{C(60,9)} = \frac{C(54,3)}{C(60,9)} = \frac{54!\,51!\,9!}{51!\,3!\,60!} = \frac{4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9}{55 \cdot 56 \cdot 57 \cdot 58 \cdot 59 \cdot 60} = \frac{3}{1787995}.$$

(3) Generalizando a solução do (2), a probabilidade é

$$\begin{aligned} \frac{C(N-w,m-w)}{C(N,m)} &= \frac{(N-w)!\,(N-m)!\,m!}{((N-w)-(m-w))!\,(m-w)!\,N!} \\ &= \frac{(N-w)!\,(N-m)!\,m!}{((N-\cancel{w}-m+\cancel{w}))!\,(m-w)!\,N!} \\ &= \frac{(N-w)!\,(\cancel{N-m})!\,m!}{(\cancel{N-m})!\,(m-w)!\,N!} \\ &= \frac{(N-w)!\,m!}{(m-w)!\,N!} \\ &= \prod_{i=0}^{w-1} \frac{m-i}{N-i}. \end{aligned}$$

Π5.9S. Sejam $a(n)$ e $b(n)$ o número de maneiras que Aleco e Bego podem subir uma escada de n degraus, respectivamente. Cada maneira do Aleco pode começar com 2 jeitos diferentes: salto de 1 degrau, ou salto de 2 degraus. Cada maneira do Bego pode começar com 3 jeitos diferentes: salto de 1, de 2, ou de 3 degraus. Observe que, por exemplo, se Bego começar com um pulo de 2 degraus, falta subir uma escada de $n-2$ degraus. Pelo princípio da adição então, temos as equações recursivas:

$$a(n) = a(n-1) + a(n-2) \qquad b(n) = b(n-1) + b(n-2) + b(n-3)$$

válidas para $n \geq 2$ e $n \geq 3$ respectivamente. Devemos definir os casos básicos de cada função recursiva: $n = 0, 1$ para a $a(n)$, e $n = 0, 1, 2$ para a $b(n)$:

		$b(0) = 1$	(fica)
$a(0) = 1$	(fica)	$b(1) = 1$	(pula 1)
$a(1) = 1$	(pula 1)	$b(2) = 2$	(pula $1+1$; ou pula 2)
$a(n) = a(n-1) + a(n-2)$		$b(n) = b(n-1) + b(n-2) + b(n-3)$	

Calculamos os 11 primeiros valores:

$$\begin{array}{rccccccccccccc} & \overbrace{1}^{a(0)}, & 1, & 2, & 3, & 5, & 8, & 13, & 21, & 34, & 55, & 89, & \overbrace{144}^{a(11)}, & \ldots \\ b: & \underbrace{1}_{b(0)}, & 1, & 2, & 4, & 7, & 13, & 24, & 44, & 81, & 149, & 274, & \underbrace{504}_{b(11)}, & \ldots \end{array}$$

Agora temos tudo que precisamos para responder facilmente às questões do problema.

(1) Precisamos apenas os valores $a(11)$ e $b(11)$: (1a) De $a(11) = 144$ maneiras. (1b) De $b(11) = 504$ maneiras.

(2) Usamos "$n \to m$" para «pula diretamente do degrau n para o degrau m» e "$n \rightsquigarrow m$" para «vai do degrau n para o degrau m pulando num jeito». (2a) Para conseguir subir, Aleco necessariamente precisa chegar no degrau 5, saltar até o degrau 7, e depois continuar até o degrau 11. Formamos cada maneira então em passos, e usando o princípio da multiplicação achamos que Aleco tem

$$\underbrace{a(5)}_{0\rightsquigarrow 5} \cdot \underbrace{1}_{5\to 7} \cdot \underbrace{a(4)}_{7\rightsquigarrow 11} = 8 \cdot 1 \cdot 5 = 40$$

maneiras de subir a escada toda. (2b) Para o Bego a situação não é tão simples, porque ele pode evitar a cobra de vários jeitos. Vamos agrupá-los assim:

(i) aqueles onde ele pulou a cobra com salto de tamanho 2;
(ii) aqueles onde ele pulou a cobra com salto de tamanho 3 desde o degrau 5;
(iii) aqueles onde ele pulou a cobra com salto de tamanho 3 desde o degrau 4.

Contamos as maneiras em cada grupo como na questão anterior, e no final as somamos (princípio da adição) para achar a resposta final: Bego tem

$$\overbrace{\underbrace{b(5)}_{0\rightsquigarrow 5} \cdot \underbrace{1}_{5\to 7} \cdot \underbrace{b(4)}_{7\rightsquigarrow 11}}^{\text{grupo (i)}} + \overbrace{\underbrace{b(5)}_{0\rightsquigarrow 5} \cdot \underbrace{1}_{5\to 8} \cdot \underbrace{b(3)}_{8\rightsquigarrow 11}}^{\text{grupo (ii)}} + \overbrace{\underbrace{b(4)}_{0\rightsquigarrow 4} \cdot \underbrace{1}_{4\to 7} \cdot \underbrace{b(4)}_{7\rightsquigarrow 11}}^{\text{grupo (iii)}} = 13 \cdot 7 + 13 \cdot 4 + 7 \cdot 7 = 192$$

maneiras de subir a escada toda.

(3) Pela definição, a probabilidade que Cátia morra é a fracção

$$\frac{\text{todas as maneiras em quais Bego pisou no degrau 6}}{\text{todas as maneiras possíveis}},$$

ou seja,

$$\frac{504-192}{504} = \frac{312}{504} = \frac{156}{252} = \frac{78}{126} = \frac{39}{63} = \frac{13}{21}.$$

Π5.10S. (1): $2^{14}-1$: para cada músico e cada instrumento, temos 2 opções: "sim" ou "não". Tiramos 1 porque hipercontamos (a "banda vazia").
(2): Cada músico que toca i instrumentos tem $i+1$ opções (a extra $+1$ corresponde no "não participar na banda"): podemos formar $4\cdot 2\cdot 3\cdot 2\cdot 5\cdot 4-1$ bandas, onde de novo tiramos 1 para excluir a "banda vazia".
(3): Cada músico que toca i instrumentos tem 2^i-1 opções (tirando a opção de "não tocar nada"). Então podemos formar $7\cdot 1\cdot 3\cdot 1\cdot 15\cdot 7$ bandas.

Π5.11S. Seja $a(n)$ o número dos strings ternários de tamanho n tais que não aparece neles o substring 00. Queremos achar o $a(7)$.

Observe que:

$$\begin{aligned}
a(0) &= 1 && \text{(o string vazio: "")}\\
a(1) &= 3 && \text{(os strings: "0", "1", e "2")}\\
a(n) &= \underbrace{a(n-1)}_{1\ldots} + \underbrace{a(n-1)}_{2\ldots} + \underbrace{a(n-2)}_{01\ldots} + \underbrace{a(n-2)}_{02\ldots}\\
&= 2a(n-1) + 2a(n-2)\\
&= 2(a(n-1)+a(n-2))
\end{aligned}$$

Então calculamos os primeiros 8 termos da seqüência:

$$1,\quad 3,\quad 8,\quad 22,\quad 60,\quad 164,\quad 448,\quad \underbrace{1224}_{a(7)}.$$

Π5.12S. (1): Como somos obrigados começar a palavra com `P`, precisamos apenas contar as permutações das letras da palavra `ESSIMISSIMO`, que sabemos que são

$$\frac{11!}{4!\,3!\,2!}.$$

(2): Podemos considerar que temos apenas um I: $\dfrac{10!}{4!\,2!}$

(3): Contamos em quantas palavras eles aparecem juntos, e usando princípio da adição, os subtraimos das permutações sem restricção.

$$\underbrace{\frac{12!}{4!\,3!\,2!}}_{\text{todas}} - \underbrace{\frac{11!}{4!\,3!}}_{\texttt{M}\text{ juntos}}$$

(4): Construimos cada dessas palavras em passos. Primeiramente escolhemos uma das permutações da palavra sem os `M`'s:

* * * * * * * *

(temos $\dfrac{8!}{3!\,2!}$ opções).

No próximo passo escolemos em qual das 9 posições possíves colocamos os M:

$$_*_*_*_*_*_*_*_*_$$

Pelo princípio da multiplicação então, temos $\dfrac{8!}{3!\,2!}\cdot C(9,4)$ palavras que satisfazem essa restricção.

П5.13S. (1) Como a ordem das consoantes e das vogais é predeterminada e as vogais devem aparecer juntas, a única escolha que precisamos fazer é onde colocar as vogais, e temos 21 possíveis posições. Então existem 21 tais strings.

(2)

$$\underbrace{C(20,6)}_{\text{consoantes}},\ \underbrace{C(12,6)}_{\text{suas posições}}\ .$$

(3) Separamos todos os strings que queremos contar em quatro grupos e contamos cada um separadamente:

$$\overbrace{\underbrace{C(20,3)}_{\text{as c.}}}^{\text{3 c., 0 v.}}+\overbrace{\underbrace{C(20,2)}_{\text{as c.}}\underbrace{C(6,1)}_{\text{a v.}}\underbrace{C(3,2)}_{\text{pos. c.}}}^{\text{2 c., 1 v.}}+\overbrace{\underbrace{C(20,1)}_{\text{a c.}}\underbrace{C(6,2)}_{\text{as v.}}\underbrace{C(3,1)}_{\text{pos. c.}}}^{\text{1 c., 2 v.}}+\overbrace{\underbrace{C(6,3)}_{\text{as v.}}}^{\text{0 c., 3 v.}}.$$

Podemos descrever o resultado numa forma mais uniforme e mais fácil para generalizar:

$$\sum_{i=0}^{3}\underbrace{C(20,3-i)}_{\text{as } 3-i \text{ c.}}\underbrace{C(6,i)}_{\text{as } i \text{ v.}}\underbrace{C(3,i)}_{\text{pos. v.}}=\sum_{\substack{c+v=3\\ c,v\in\mathbb{N}}}\underbrace{C(20,c)}_{\text{as c.}}\underbrace{C(6,v)}_{\text{as v.}}\underbrace{C(3,v)}_{\text{pos. v.}}$$

(4) Seguindo a última forma do (3), temos

$$\sum_{i=0}^{\ell}\underbrace{C(20,\ell-i)}_{\text{as } \ell-i \text{ c.}}\underbrace{C(6,i)}_{\text{as } i \text{ v.}}\underbrace{C(\ell,i)}_{\text{pos. v.}}$$

maneiras. O somatório pode ser escrito também assim:

$$\sum\left\{\underbrace{C(20,c)}_{\text{as c.}}\underbrace{C(6,v)}_{\text{as v.}}\underbrace{C(\ell,v)}_{\text{pos. v.}}\ \middle|\ c+v=\ell,\ 0\le c\le 20,\ 0\le v\le 6,\ c,v\in\mathbb{N}\right\}.$$

Note que como o conjunto acima é finito, a adição é comutativa e associativa; logo, nosso somatório é bem-definido.

П5.14S.

(i) Permutações com repetições: 38^8.
(ii) Combinações com repetições: $C(38+8-1,8)=C(45,8)$.

Π5.15S. Seja N o número de permutações totais das létras e defina as 4 propriedades

$$\alpha : \text{aparece o } \texttt{AA} \qquad \beta : \text{aparece o } \texttt{BB} \qquad \gamma : \text{aparece o } \texttt{CC} \qquad \delta : \text{aparece o } \texttt{DD}.$$

Procuramos o número dos strings de tamanho 8 que não tenham nenhuma dessas 4 propriedades. Assim que calcular os $N(\alpha), \dots, N(\alpha, \beta, \gamma, \delta)$ o princípio da inclusão–exclusão, vai nos dar o número que procuramos.

Observamos que

$$\begin{aligned} N(\alpha) = N(\beta) = N(\gamma) = N(\delta) \\ N(\alpha, \beta) = N(\alpha, \gamma) = \cdots = N(\gamma, \delta) \\ N(\alpha, \beta, \gamma) = \cdots = N(\beta, \gamma, \delta). \end{aligned}$$

Calculamos os

$$\begin{aligned} N &= \frac{8!}{2!\,2!\,2!\,2!} = 2520 \\ N(\alpha) &= \frac{7!}{2!\,2!\,2!} = \frac{7!}{8} = 7 \cdot 6 \cdot 5 \cdot 3 = 630 \\ N(\alpha, \beta) &= \frac{6!}{2!\,2!} = \frac{6!}{4} = 180 \\ N(\alpha, \beta, \gamma) &= \frac{5!}{2!} = \frac{5!}{2} = 60 \\ N(\alpha, \beta, \gamma, \delta) &= 4! = 24. \end{aligned}$$

Para responder, temos

$$\begin{aligned} N - C(4,1)N(\alpha) + C(4,2)N(\alpha, \beta) - C(4,3)N(\alpha, \beta, \gamma) + N(\alpha, \beta, \gamma, \delta) \\ = 2520 - 4 \cdot 630 + 6 \cdot 180 - 4 \cdot 60 + 24 = 864 \end{aligned}$$

tais permutações.

Capítulo 6

x6.2S. Demonstrado no Unicidade da (+)-identidade Θ3.11, pois tal demonstração precisou apenas axiomas que temos aqui também.

x6.3S. Demonstrado no Unicidade dos inversos aditivos Θ3.13, pois tal demonstração precisou apenas axiomas que temos aqui também.

x6.4S. Utilizamos a mesma demonstração do Exercício x3.8, já que ela não precisou nenhum axioma que não temos aqui.

x6.5S. Veja o Teorema Θ3.15: não precisou nenhum axioma que não temos.

x6.7S. Feito no Exercício x3.5.

x6.10S. Seja a real. Calculamos:

$$\begin{aligned} a + a(-1) &= a1 + a(-1) && (\text{`/RM-Id,tag'}) \\ &= a(1 + (-1)) && (\text{`/R-Dist,tag'}) \\ &= a0 && (\text{`/RA-Inv,tag'}) \\ &= 0. && (\text{`/R-Ann,tag'}) \end{aligned}$$

Como $a + (-a) = 0$ (pela (RA-Inv)), logo $-a = a(-1)$ pela (R-ResR).

x6.13S. Demonstrado no Unicidade da $(\cdot)$-identidade Θ3.12, pois tal demonstração precisou apenas axiomas que temos aqui também.

x6.14S. Seja $x \neq 0$ e sejam x', x'' $(\cdot)$-inversos de x. Preciso demonstrar que $x' = x''$. Calculamos:

$$\begin{aligned} x' &= x'1 && (1 \text{ é uma } (\cdot)\text{-identidade-R}) \\ &= x'(xx'') && (x'' \text{ é um } (\cdot)\text{-inverso-R de } x) \\ &= (x'x)x'' && ((\cdot)\text{-assoc.}) \\ &= 1x'' && (x' \text{ é um } (\cdot)\text{-inverso-L de } x) \\ &= x''. && (1 \text{ é uma } (\cdot)\text{-identidade-R}) \end{aligned}$$

x6.50S. Seja $n \in \mathbb{N}$. Pelo Teorema binomial Θ3.80 temos

$$\begin{aligned} (1+x)^n &= \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} x^i \\ &= \binom{n}{0} 1^n x^0 + \binom{n}{1} 1^{n-1} x^1 + \overbrace{\sum_{i=2}^{n} \binom{n}{i} 1^{n-i} x^i}^{(\geq 0)} \\ &\geq \binom{n}{0} 1^n x^0 + \binom{n}{1} 1^{n-1} x^1 \\ &= 1 + nx. \end{aligned}$$

x6.54S. ($\Rightarrow$): Como $|x| \leq a$, logo $-a \leq -|x|$. Temos então $-a \leq -|x| \leq x \leq |x| \leq a$.
($\Leftarrow$): Separamos em casos: $x \geq 0$: Temos $|x| = x \leq t$. $x < 0$: Observe que como $-a \leq x$, logo $-x \leq -(-a) = a$. Logo $|x| = -x \leq a$.

x6.65S. Tudo que precisamos dos inteiros para demonstrar o Problema Π3.10 temos aqui nos reais também.

x6.72S. Vou mostrar que $(t_n)_n \leq 1$. Seu primeiro termo é o $0 < 1 \leq 1$. Seja k natural. Temos:

$$\begin{aligned}
t_{k+1} &= t_k + \frac{1}{2}(\vartheta - t_k^2) \\
&= \frac{1}{2}(\vartheta + 2t_k - t_k^2) \\
&= \frac{1}{2}(\vartheta - (t_k^2 - 2t_k)) \\
&= \frac{1}{2}(\vartheta - (t_k^2 - 2t_k + 1 - 1)) \\
&= \frac{1}{2}(\vartheta - (t_k^2 - 2t_k + 1) + 1) \\
&= \frac{1}{2}((\vartheta + 1) - (t_k^2 - 2t_k + 1)) \\
&= \frac{1}{2}((\vartheta + 1) - (t_k - 1)^2) \\
&\leq \frac{1}{2}(\vartheta + 1) \\
&\leq 1.
\end{aligned}$$

x6.73S. Basta mostrar por indução que para todo n, temos $t_{n+1} - t_n \geq 0$. A base é trivial. Seja $k \geq 1$ tal que $t_k - t_{k-1} \geq 0$. Calculamos:

$$\begin{aligned}
t_{k+1} - t_k &= (t_k + \frac{1}{2}(\vartheta - t_k^2)) - (t_{k-1} + \frac{1}{2}(\vartheta - t_{k-1}^2)) \\
&= (t_k - t_{k-1}) + \frac{1}{2}\big((\vartheta - t_k^2) - (\vartheta - t_{k-1}^2)\big) \\
&= (t_k - t_{k-1}) - \frac{1}{2}\big(t_k^2 - t_{k-1}^2\big) \\
&= (t_k - t_{k-1}) - \frac{1}{2}(t_k + t_{k-1})(t_k - t_{k-1}) \\
&= \underbrace{(t_k - t_{k-1})}_{\geq 0}\underbrace{\left(1 - \frac{1}{2}(t_k + t_{k-1})\right)}_{\geq 0} \\
&\geq 0
\end{aligned}$$

onde no último passo usamos a (HI) e que a $(t_n)_n \leq 1$ (e logo $t_i + t_j \leq 2$ para quaisquer i, j).

x6.76S. Temos

$$\begin{aligned}
x \in \bigcup\nolimits_n F_n &\iff (\exists n \in \mathbb{N})[\, x \in F_n \,] \iff x \in (-1, 1) \\
x \in \bigcap\nolimits_n G_n &\iff (\forall n \in \mathbb{N})[\, x \in G_n \,] \iff x \in [-1, 1].
\end{aligned}$$

Ou seja: $\bigcup_n F_n = (-1, 1)$ e $\bigcap_n G_n = [-1, 1]$.

x6.77S. (i) $[0, 1]$; (ii) $[0, 1]$; (iii) $\emptyset$.

x6.78S. Não. Considere como contraxemplo as seqüências

$$(n)_n = 0, 1, 2, \ldots \qquad\qquad (n+1)_n = 1, 2, 3, \ldots$$

e veja que temos $(n)_n \leq (n+1)_n$ mas $\{n\}_n \not\leq \{n+1\}_n$.

x6.81S. Daria, mas não faria sentido essa abordagem, pois seria complicada demais. Poderíamos simplesmente definir esses conjuntos assim:

$$\mathbb{ZN} \stackrel{\text{def}}{=} \{0\} \cup \qquad\qquad \mathbb{Q}_{\mathbb{N}} \stackrel{\text{def}}{=} \left\{ \frac{x}{1} \;\middle|\; x \in \mathbb{ZN} \right\}.$$

x6.82S. Devemos demonstrar a unicidade dos infima e dos suprema.

x6.91S. Basta eliminar o caso $x > 0$: Mas neste caso, usamos o próprio x na hipótese obtendo $0 \leq x < x$, que é uma contradição.

x6.93S. Basta eliminar o caso $a > b$. Neste caso, $a - b > 0$. Logo $a < b + (a - b) = a$, contradição.

x6.97S. Precisamos demonstrar

$$d(x, y) < \varepsilon \iff d(y, x) < \varepsilon$$

que segue imediatamente pela simetria da distância d ((D-Sym)).

x6.99S. A 1/3-bola do 7 é o intervalo $(7 - 1/3, 7 + 1/3)$ e a 2-bola do 0 o $(-2, 2)$.

x6.100S. O intervalo (u, v) de reais é a bola com centro $c = (u + v)/2$ e raio o $r = (v - u)/2$:

$$\begin{aligned} x \in \mathcal{B}_r(c) &\iff d(x, c) < r \\ &\iff |x - c| < r \\ &\iff c - r < x < c + r \\ &\iff x \in (c - r, c + r) \\ &\iff x \in \left(\tfrac{1}{2}(u + v) - \tfrac{1}{2}(v - u), \tfrac{1}{2}(u + v) + \tfrac{1}{2}(v - u)\right) \\ &\iff x \in (u, v). \end{aligned}$$

x6.101S. A bola vazia e o intervalo vazio são representados pelos parzinhos dos conjuntos

$$\{\, (c, r) \;|\; r \leq 0 \,\} \qquad\qquad \{\, (v, u) \;|\; u \leq v \,\}$$

respectivamente.

x6.103S. Considere a distância discreta e o conjunto $\mathbb{R}$. Ele não é cotado; mas $\mathbb{R}$ está contido na bola $\mathcal{B}_2(0)$; de fato: $\mathcal{B}_2(0) = \mathbb{R}$.

x6.104S. Devemos demonstrar pelo menos a unicidade dos limites para usar a notação que envolve o símbolo ' $=$ '. Pois, se uma seqüência tendesse a dois reais distintos

$$(a_n)_n \to \ell \neq \ell' \leftarrow (a_n)_n$$

então escrevendo isso com as notações alternativas

$$\lim_n a_n = \ell \qquad\qquad \lim_n a_n = \ell'$$

inferíamos (confundindo tal notação com igualdade) $\ell = \ell'$ contradizendo nossa hipótese.

x6.106S. Seja $(a_n)_n$ constante. Logo seja c tal que $(\forall n)[\, a_n = c\,]$. Basta demonstrar que $(a_n)_n \to c$. Seja $\varepsilon > 0$. Basta demonstrar: $(\forall n \geq 0)[\, a_n (c, <) \varepsilon\,]$. Seja $m \geq 0$. Calculamos

$$\begin{aligned} d(a_m, c) &= d(c, c) && \text{(escolha de } c\text{)} \\ &= 0 && \text{((D-EqZero))} \\ &< \varepsilon. \end{aligned}$$

x6.107S. Seja $(a_n)_n$ eventualmente constante. Logo seja M tal que $(\exists c)(\forall n \geq M)[\, a_n = c\,]$. Logo seja c tal que $(\forall n \geq M)[\, a_n = c\,]$. Vou demonstrar que $(a_n)_n \to c$. Seja $\varepsilon > 0$. Basta demonstrar: $(\forall n \geq M)[\, d(a_n, c) < \varepsilon\,]$. Seja $m \geq M$. Temos $d(a_m, c) = d(c, c) = 0 < \varepsilon$.

x6.112S. Seja $(a_n)_n$ tal que $(a_n)_n \to \ell$. Logo, usando $\varepsilon := 1$ seja N tal que a partir do a_N todos os a_n's são 1-perto de ℓ. Observe que o conjunto $\{a_0, \ldots, a_N\}$ é finito e habitado, e logo (Exercício x6.65) possui mínimo m e máximo M:

$$m \leq a_0, \ldots, a_N \leq M.$$

Agora, observe que a seqüência é cotada por baixo pelo $\min\{m, \ell - 1\}$ e cotada por cima pelo $\max\{M, \ell + 1\}$.

x6.114S. Caso $c = 0$: já demonstrado, pois acaba sendo reduzido à convergência $(0)_n \to 0$ (Exercício x6.106).
Caso $c \neq 0$: Seja $\varepsilon > 0$. Como $(a_n)_n \to a$, logo seja N tal que

$$(\forall n \geq N)[\, d(a_n, a) < \varepsilon / |c|\,].$$

Asserção: $(\forall n \geq N)[\, d(ca_n, ca) < \varepsilon\,]$. Seja $n \geq N$. Logo $d(a_n, a) < \varepsilon / |c|$ (pela escolha de N). Calculamos:

$$\begin{aligned} d(ca_n, ca) &= |ca_n + ca| \\ &= |c(a_n - a)| \\ &= |c|\, |a_n - a| \\ &= |c|\, d(a_n, a) \\ &= |c|\, \frac{\varepsilon}{|c|} \\ &< \varepsilon. \end{aligned}$$

x6.115S. Seja $\varepsilon > 0$. Pelas escolhas de a, b, sejam N_a e N_b tais que

$$(\forall n \geq N_a)[\, d(a_n, a) < \varepsilon/2\,] \qquad \& \qquad (\forall n \geq N_b)[\, d(b_n, b) < \varepsilon/2\,].$$

Seja $N \geq \{N_a, N_b\}$. Preciso demonstrar que $(\forall n \geq N)[\, d(a_n + b_n, a + b) < \varepsilon\,]$. Seja $n \geq N$. Logo $n \geq N_a$ e $n \geq N_b$ (pela escolha de N). Logo $d(a_n, a) < \varepsilon/2$ e $d(b_n, b) < \varepsilon/2$ (pelas escolhas de N_a e N_b). Calculamos:

$$\begin{aligned} d(a_n + b_n, a + b) &= |(a_n + b_n) - (a + b)| \\ &= |(a_n - a) + (b_n - b)| \\ &\leq |a_n - a| + |b_n - b| \\ &= d(a_n, a) + d(b_n, b) \\ &< \varepsilon/2 + \varepsilon/2 \\ &= \varepsilon. \end{aligned}$$

x6.116S. Vou demonstrar $(a_n b_n)_n \to ab$. Seja $\varepsilon > 0$. Como $(a_n)_n$ é cotada, seja $M_a > 0$ uma cota dela. Pelas escolhas de a, b, sejam N_a e N_b tais que

$$(\forall n \geq N_a)\left[\, d(a_n, a) < \frac{\varepsilon}{2|b| + 1}\,\right] \qquad \& \qquad (\forall n \geq N_b)\left[\, d(b_n, b) < \frac{\varepsilon}{2M_a}\,\right].$$

Seja $N = \max(N_a, N_b)$. Calculamos:

$$\begin{aligned} d(a_n b_n, ab) &= |(a_n b_n) - (ab)| \\ &= |(a_n b_n) - a_n b + a_n b - (ab)| \\ &= |a_n(b_n - b) + (a_n - a)b| \\ &\leq |a_n(b_n - b)| + |(a_n - a)b| \\ &\leq |a_n|\,|b_n - b| + |a_n - a|\,|b| \\ &\leq M_a\,|b_n - b| + |a_n - a|\,|b| \\ &< M_a \frac{\varepsilon}{2M_a} + \frac{\varepsilon}{2\,|b| + 1}\,|b| \\ &< \varepsilon/2 + \varepsilon/2 \\ &= \varepsilon. \end{aligned}$$

x6.122S. Suponha $(a_n)_n$ autoconvergente. Logo seja N tal que a partir de N, todos os a_n's ficam 1-perto entre si. Ou seja: $(\forall i, j \geq N)[\, d(a_i, a_j) < 1\,]$. Vou achar uma cota M_1 para os $\{a_n\}_{n<N}$ e uma cota M_2 para os $\{a_n\}_{n \geq N}$. Assim a seqüência inteira é cotada pelo $\max\{M_1, M_2\}$. Seja $M_1 = \max\{|a_n|\}_{n<N}$, definido pois $\{|a_n|\}_{n<N}$ é um conjunto habitado e finito. Bastra mostrar que para qualquer $n \geq N$, $a_n \leq |a_N| + 1$. Temos

$$|a_n| - |a_N| \leq |a_n - a_N| = d(a_n, a_N) < 1.$$

Logo $|a_n| < |a_N| + 1$.

x6.134S. Primeiramente vou mostrar que $(\vartheta^n)_n$ é inf-cotada e decrescente, assim garantido que é convergente; depois vou garantir que tal limite só pode ser o 0.

Vou mostrar por indução que $(\vartheta^n)_n \geq 0$. Temos $\vartheta^0 = 1 \geq 0$, estabelecendo a base da indução. Seja k natural tal que $\vartheta^k \geq 0$. Temos:

$$\vartheta^{k+1} = \vartheta^k \vartheta \geq 0$$

como produto de não-negativos.

Vou mostrar que $(\vartheta^n)_n$ é decrescente. Seja k natural. Calculamos:

$$\vartheta^{k+1} = \vartheta^k \vartheta < \vartheta^k.$$

Pelo (MCT), seja $\ell = \lim_n \vartheta^n$. Basta mostrar $\ell = 0$. Usando o Exercício x6.114, calculamos:

$$\ell = \lim_n \vartheta^n = \lim_n \vartheta^{n+1} = \lim_n \vartheta^n \vartheta = \vartheta \lim_n \vartheta^n = \vartheta \ell.$$

Logo $\ell = 0$, pois caso $\ell \neq 0$ poderiamos aplicar o cancelamento multiplicativo para obter $\vartheta = 1$, contradizendo nossa hipótese sobre ϑ.

x6.138S. (i) A é habitado, pois $1^2 < 2$, ou seja, $1 \in A$.

x6.139S. Vou mostrar que 2 é uma sup-cota de A. Seja $a \in A$, ou seja, $a^2 < 2$, e logo $a^2 < 4$, ou seja, $a^2 < 2^2$. Logo $a < 2$ pois $(_^2)$ reflete a $(<)$ no $\mathbb{R}_{\geq 0}$.

x6.140S. Aqui a idéia é diminuir o h um tiquinho tão pequeno que ele continuaria sendo uma sup-cota do A. Ou seja: procuramos um h_- tal que

$$A \leq h_- < h.$$

Como $h^2 > 2$, logo seja $\vartheta > 0$ tal que

$$h^2 - \vartheta > 2.$$

Basta achar $\varepsilon > 0$ pequeno o suficiente para que $h - \varepsilon$ serve ser nosso desejado h_-:

$$(\underbrace{h - \varepsilon}_{h_-})^2 > h^2 - \vartheta > 2.$$

Seja $\varepsilon = \dfrac{\vartheta}{2h}$. Calculamos:

$$\begin{aligned}
(h-\varepsilon)^2 &= h^2 - 2h\varepsilon + \varepsilon^2 \\
&> h^2 - 2h\varepsilon \\
&= h^2 - 2h\frac{\vartheta}{2h} && \text{(pela escolha de } \varepsilon\text{)} \\
&= h^2 - \vartheta \\
&> 2. && \text{(pela escolha de } \vartheta\text{)}
\end{aligned}$$

Π6.7S. Demonstramos usando reductio ad absurdum. Suponha então que ambos são algébricos e vamos chamá-los assim:

$$S = e + \pi \qquad\qquad P = e\pi.$$

Agora considere o polinômio

$$f(x) = x^2 - Sx + P$$

e observe que e, π são raizes dele:

$$\begin{aligned}
f(e) &= e^2 - (e+\pi)e + e\pi = 0 \\
f(\pi) &= \pi^2 - (e+\pi)\pi + e\pi = 0.
\end{aligned}$$

Chegamos assim na contradição que e, π são algébricos, pois os coeficientes do f são.

Capítulo 8

x8.1S. O que é significa «colecção (numa totalidade)»? Cuidado: para responder nessa pergunta tu não podes usar a palavra «conjunto», pois assim teria uma definição circular. Em outras palavras, definimos a palavra «conjunto» em termos da palavra «colecção», que no final das contas, é algo sinónimo na nossa metalinguagem. Não dá.

x8.2S. Suponha $A = B$. Vamos mostrar que $A \subseteq B$. Seja $x \in A$. Mas como $A = B$, logo $x \in B$ também; que foi o que queremos demonstrar.

x8.3S. ($\Rightarrow$): Imediata pelo Exercício x8.2 (pois a igualdade é simétrica).

($\Leftarrow$). Suponha $A \subseteq B$ e $B \subseteq A$. Vamos mostrar que $A = B$. Seja x um objeto arbitrário. Calculamos:

$$\begin{aligned} x \in A &\implies x \in B \qquad (\text{def. } A \subseteq B) \\ x \in B &\implies x \in A \qquad (\text{def. } B \subseteq A) \end{aligned}$$

Ou seja,

$$x \in A \iff x \in B$$

que foi o que queremos demonstrar.

x8.4S. $A \subsetneq B \overset{\text{def}}{\iff} A \subseteq B \wedge A \neq B$. (Lembre-se que $A \neq B \overset{\text{abbr}}{\equiv} \neg(A = B)$.)

x8.6S. Como não demonstramos a unicidade do vazio não podemos usar o artigo definido "o", e conseqüentemente, não podemos usar um símbolo para o denotar. Seria mal-definido.

x8.7S. Infinitos! Pois, para cada objeto x já temos um singleton $\{x\}$. E agora o singleton dele $\{\{x\}\}$, e dele, e dele, ...

x8.8S. O conjunto $\{\, x \mid x \neq x \,\}$ é um conjunto vazio.

x8.9S. Suponha que A, B são vazios. Preciso mostrar $A = B$, ou seja, que $\forall x(x \in A \leftrightarrow x \in B)$. Seja x um objeto arbitrário. Pela definição de vazio, as duas afirmações $x \in A$ e $x \in B$ são falsas, e logo a equivalência $(x \in A \leftrightarrow x \in B)$ verdadeira, que foi o que queremos demonstrar.

x8.10S. Suponha que A, B são vazios. Queremos demonstrar que $A = B$. Para chegar num absurdo, suponha que $A \neq B$. Logo, pela definição da igualdade, temos que existe x tal que: $x \in A$ mas $x \notin B$; ou $x \in B$ mas $x \notin A$. As duas alternativas chegam num absurdo: a primeira pois A é vazio e logo $x \notin A$, e similarmente a segunda pois B é vazio e logo $x \notin B$.

x8.12S. Temos:

$\emptyset \subseteq \emptyset$	(sim)	$\emptyset \in \emptyset$	(não)
$\emptyset \subseteq A$	(sim)	$\emptyset \in A$	(depende)
$A \subseteq \emptyset$	(depende)	$A \in \emptyset$	(não)
$A \subseteq A$	(sim)	$A \in A$	(depende).

x8.15S. A fórmula que queremos demonstrar é uma tautologia lógica!

x8.16S. Não; nenhuma das duas proposições implica a outra. Da $A \subseteq A$ não podemos substituir o A com nenhum conjunto para chegar na $\emptyset \subseteq A$. Nem como o $\emptyset$, pois ele teria sido substituito selectivamente em apenas na sua primeira instância, algo que obviamente não podemos fazer. (Similarmente $x = x$ para todos os números x mas não podemos concluir disso que $0 = x$ para todos os x.) Da $\emptyset \subseteq A$ não podemos chegar na $A \subseteq A$, pois precisamos substituir a constante $\emptyset$ pela variável A. (Similarmente $0 + x = x$ para todos os números x, mas não podemos concluir que $x + x = x$.)

x8.18S. Pois o "$x \in A$" não é um termo, mas uma proposição (afirmação).

x8.19S.

$$D_{12} \stackrel{\text{def}}{=} \{\, n \in \mathbb{Z} \mid n \mid 12 \,\} \qquad D_m \stackrel{\text{def}}{=} \{\, n \in \mathbb{Z} \mid n \mid m \,\}$$
$$M_{12} \stackrel{\text{def}}{=} \{\, 12n \mid n \in \mathbb{Z} \,\} \qquad M_m \stackrel{\text{def}}{=} \{\, mn \mid n \in \mathbb{Z} \,\}$$
$$P_{12} \stackrel{\text{def}}{=} \{\, 12^n \mid n \in \mathbb{N} \,\} \qquad P_m \stackrel{\text{def}}{=} \{\, m^n \mid n \in \mathbb{N} \,\}$$

Onde aparece a variável 'm', ela está livre, e onde aparece a variável 'n', ela está ligada.

x8.20S. Calculando a extensão de A achamos:

$$A = \{f(u,u), f(u,v), f(v,u), f(v,v)\}\,.$$

Então o A tem *no máximo* 4 elementos—mas pode acontecer que tem menos (veja Exercício x8.21).

x8.21S. Calculamos:

$$\begin{aligned} B &= \{\, n^2 + m^2 \mid n, m \in \{1,3\} \,\} \\ &= \{1^2 + 1^2, 1^2 + 3^2, 3^2 + 1^2, 3^2 + 3^2\} \\ &= \{2, 10, 10, 18\} \\ &= \{2, 10, 18\}\,. \end{aligned}$$

x8.22S.

$$\{\, t(x_1, \ldots, x_n) \mid \varphi(x_1, \ldots, x_n) \,\} \stackrel{\text{def}}{=} \{\, x \mid \exists x_1 \cdots \exists x_n (x = t(x_1, \ldots, x_n) \wedge \varphi(x_1, \ldots, x_n)) \,\}\,.$$

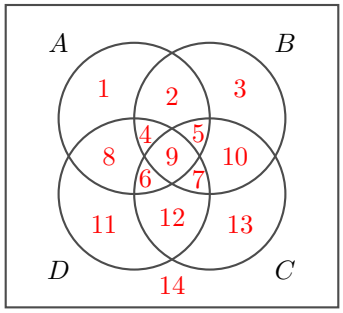
x8.24S. Sejam A, B conjuntos. Qualquer uma das definições seguintes serve:

$$A \cap B \stackrel{\text{def}}{=} \{\, x \mid x \in A \;\&\; x \in B \,\}$$
$$A \cap B \stackrel{\text{def}}{=} \{\, x \in A \mid x \in B \,\}$$
$$A \cap B \stackrel{\text{def}}{=} \{\, x \in B \mid x \in A \,\}$$

x8.25S.

(1) $\{0,1,2,3,4\} \setminus \{4,1\} = \{0,2,3\}$
(2) $\{0,1,2,3,4\} \setminus \{7,6,5,4,3\} = \{0,1,2\}$
(3) $\{0,1,2\} \setminus \mathbb{N} = \emptyset$
(4) $\mathbb{N} \setminus \{0,1,2\} = \{3,4,5,6,\dots\} = \{\, n \in \mathbb{N} \mid n \geq 3 \,\}$
(5) $\{\{0,1\},\{1,2\},\{0,2\}\} \setminus \{0,1\} = \{\{0,1\},\{1,2\},\{0,2\}\}$
(6) $\{\{0,1\},\{1,2\},\{0,2\}\} \setminus \{0,1,2\} = \{\{0,1\},\{1,2\},\{0,2\}\}$
(7) $\{\{0,1\},\{1,2\},\{0,2\}\} \setminus \{\{1,2\}\} = \{\{0,1\},\{0,2\}\}$
(8) $\{\{0,1\},\{1,2\}\} \setminus \{\{1\}\} = \{\{0,1\},\{1,2\}\}$
(9) $\{7,\emptyset\} \setminus \emptyset = \{7,\emptyset\}$
(10) $\{7,\emptyset\} \setminus \{\emptyset\} = \{7\}$
(11) $\mathbb{R} \setminus 0 = \mathbb{R}$
(12) $\mathbb{R} \setminus \{0\} = (-\infty, 0) \cup (0, +\infty)$
(13) $\{1,\{1\},\{\{1\}\},\{\{\{1\}\}\}\} \setminus 1 = \{1,\{1\},\{\{1\}\},\{\{\{1\}\}\}\}$
(14) $\{1,\{1\},\{\{1\}\},\{\{\{1\}\}\}\} \setminus \{\{\{1\}\}\} = \{1,\{1\},\{\{\{1\}\}\}\}$

x8.28S. Temos 4 conjuntos; e como cada objeto pode ou pertencer ou não pertencer a cada um deles, temos no total $2^4 = 16$ distintas configurações. Mas no diagrama do aluno aparecem apenas 14:



Logo tem duas configurações então que não são representadas por nenhuma parte do diagrama. São essas:

$$x \in A \;\&\; x \notin B \;\&\; x \in C \;\&\; x \notin D$$
$$x \notin A \;\&\; x \in B \;\&\; x \notin C \;\&\; x \in D.$$

x8.29S. Vou demonstrar a afirmação.

Suponha que $A \subseteq B$ e $A \subseteq C$. Tome um $a \in A$. Precisamos mostrar que $a \in B \cap C$. Como $a \in A$ e $A \subseteq B$, temos $a \in B$; e como $a \in A$ e $A \subseteq C$, temos $a \in C$. Logo $a \in B \cap C$, pela definição de $B \cap C$.

x8.30S. Vou refutar a afirmação com um contraexemplo. Tome

$$\begin{aligned} A &:= \{2\} \\ B &:= \{1,2\} \\ C &:= \{2,3\}\,. \end{aligned}$$

Realmente $A \subsetneq B$ e $A \subsetneq C$, mas mesmo assim $A = B \cap C$.

x8.33S. Exatamente quando A, B são disjuntos. Em símbolos,

$$|A \cup B| = |A| + |B| \iff A \cap B = \emptyset.$$

x8.34S. Já resolvemos isso na Secção §124! Concluimos que:

$$|\wp A| = 2^{|A|}.$$

x8.36S. Calculamos pela definição de $\wp$:

$$\begin{aligned} \wp\emptyset &= \{\emptyset\} \\ \wp\wp\emptyset &= \{\emptyset, \{\emptyset\}\} \\ \wp\wp\emptyset &= \{\emptyset, \{\emptyset\}\,, \{\{\emptyset\}\}\,, \{\emptyset, \{\emptyset\}\}\} \end{aligned}$$

x8.37S. Qualquer uma das duas definições serve:

$$\begin{aligned} \wp_1 A &\stackrel{\text{def}}{=} \{\, \{a\} \mid a \in A \,\} \\ \wp_1 A &\stackrel{\text{def}}{=} \{\, X \subseteq A \mid \text{Singleton}(X) \,\}\,. \end{aligned}$$

x8.38S. Sejam A, B conjuntos. Botamos

$$A \cup B \stackrel{\text{def}}{=} \bigcup \{A, B\} \qquad\qquad A \cap B \stackrel{\text{def}}{=} \bigcap \{A, B\}\,.$$

x8.40S. Por enquanto a resposta correta é $\bigcap \emptyset = \mathcal{U}$. Mas "stay tuned" pois isso vai mudar no Capítulo 16. Em geral $\mathcal{U}$ não é o que queremos, então vamo tomar cuidado para verificar que uma família de conjuntos não é vazia antes de considerar sua intersecção!

x8.43S. Seja $c \in C$. Para mostrar que $c \in \bigcap \mathscr{A}$, seja $A \in \mathscr{A}$ e agora basta mostrar que $c \in A$. Mas pela definição de $\mathscr{A}$ sabemos que $A \supseteq C$. Logo $c \in A$.

x8.44S. Seja $A \in \mathscr{A}$. Para demonstrar que $\bigcap \mathscr{A} \subseteq A$, tome $x \in \bigcap \mathscr{A}$ (1). Agora basta mostrar que $x \in A$. Pela (1), x pertence a todos os membros da $\mathscr{A}$, e logo $x \in A$ também.

x8.45S. Exemplo. Tome

$$\begin{aligned} A &= \{1,2\} \\ \mathscr{A} &= \{\{1\},\{1,2\}\} \subseteq \wp A. \end{aligned}$$

Observe que realmente $\bigcup \mathscr{A} = A$ e que $A \in \mathscr{A}$.
Contraexemplo. Tome

$$\begin{aligned} A &= \{1,2\} \\ \mathscr{A} &= \{\{1\},\{2\}\} \subseteq \wp A. \end{aligned}$$

Observe que realmente $\bigcup \mathscr{A} = A$ mas mesmo assim $A \notin \mathscr{A}$.

x8.46S. Tome

$$\begin{aligned} A &:= \{\{1,2,3\},\{3,4,5\}\} && (0<1<2<5) \\ B &:= \{\{1,2,3,4\},\{2,3,4,5\}\} && (0<2<3<5). \end{aligned}$$

x8.47S. Vamos demonstrar a afirmação. Suponha $x \in \bigcap \mathscr{A}$ (1). Para mostrar que $x \in \bigcup \mathscr{B}$, basta achar um membro da $\mathscr{B}$ em que o x pertence. Seja $W \in \mathscr{A} \cap \mathscr{B}$ (sabemos que $\mathscr{A} \cap \mathscr{B} \neq \emptyset$). Logo $W \in \mathscr{A}$ (2) e $W \in \mathscr{B}$ (def. $\cap$). Pelas (1),(2) temos $x \in W$, e como $W \in \mathscr{B}$, temos o desejado $x \in \bigcup \mathscr{B}$.

(Obs.: demonstramos assim um W tal que $\bigcap \mathscr{A} \subseteq W \subseteq \bigcup \mathscr{B}$.)

Π8.1S. Vou demonstrar que $\mathscr{A}$ tem exatamente um membro ($\mathscr{A}$ é um singleton).

$\mathscr{A}$ tem pelo menos um membro. Se $\mathscr{A}$ fosse vazio não teriamos $\bigcup \mathscr{A} = \bigcap \mathscr{A}$, pois o primeiro é o vazio e o segundo o universo.

$\mathscr{A}$ tem no máximo um membro. Sejam $A, B \in \mathscr{A}$. Vou mostrar que $A = B$.
($\subseteq$): Para qualquer x temos:

$$\begin{aligned} x \in A &\implies x \in \bigcup \mathscr{A} && (A \in \mathscr{A} \text{ e def. } \textstyle\bigcup \mathscr{A}) \\ &\implies x \in \bigcap \mathscr{A} && (\textstyle\bigcup \mathscr{A} = \bigcap \mathscr{A}) \\ &\implies x \in B && (B \in \mathscr{A} \text{ e def. } \textstyle\bigcap \mathscr{A}) \end{aligned}$$

A ($\supseteq$) é similar:
Alternativa usando reductio ad absurdum. Para chegar numa contradição suponha que $A \neq B$. Logo seja $t \in A \triangle B$, ou seja t pertence a um dos A, B mas não ao outro. Logo $t \in \bigcup \mathscr{A}$ e $t \notin \bigcap \mathscr{A}$, absurdo.

Π8.4S. Dado qualquer natural n, denotamos por

$$A_{[n]} \stackrel{\text{def}}{=} \{\, a \mid a \text{ pertence a uma quantidade ímpar dos } A_1, \ldots, A_n \,\}.$$

Demonstramos por indução que para todo inteiro $n \geq 2$,

$$A_1 \triangle A_2 \triangle \cdots \triangle A_n = A_{[n]}$$

Base ($n := 2$): $x \in A_1 \triangle A_2 \iff x$ pertence a uma quantidade ímpar dos A_1, A_2 (óbvio).

Passo indutivo: Seja $k \in \mathbb{N}$ tal que

$$\text{(H.I.)} \qquad A_1 \triangle \cdots \triangle A_k = A_{[k]}.$$

Precisamos mostrar que:

$$A_1 \triangle \cdots \triangle A_{k+1} = A_{[k+1]}$$

($\subseteq$): Suponha que $x \in A_1 \triangle A_2 \triangle \cdots \triangle A_{k+1}$, ou seja, $x \in (A_1 \triangle A_2 \triangle \cdots \triangle A_k) \triangle A_{k+1}$. Pela definição de $\triangle$, temos dois casos:

Caso 1: $x \in A_1 \triangle A_2 \triangle \cdots \triangle A_k$ & $x \notin A_{k+1}$.
Pela H.I., x pertence a uma quantidade ímpar dos $A_1, \ldots, A_k$, e não ao A_{k+1}, então a uma quantidade ímpar dos $A_1, \ldots, A_{k+1}$.

Caso 2: $x \notin A_1 \triangle A_2 \triangle \cdots \triangle A_k$ & $x \in A_{k+1}$.
Pela H.I., x pertence a uma quantidade par dos $A_1, \ldots, A_k$ e também ao A_{k+1}, então a uma quantidade ímpar dos $A_1, \ldots, A_{k+1}$.

($\supseteq$): Suponha que x pertence a uma quantidade ímpar dos $A_1, \ldots, A_{k+1}$. Separamos em dois casos:

Caso 1: $x \in A_{k+1}$.
Logo x pertence a uma quantidade par dos $A_1, \ldots, A_k$ e logo $x \notin A_1 \triangle \cdots \triangle A_k$ (pela H.I.). Ou seja, $x \in (A_1 \triangle A_2 \triangle \cdots \triangle A_k) \triangle A_{k+1}$.

Caso 2: $x \notin A_{k+1}$.
Nesse caso x pertence a uma quantidade ímpar dos $A_1, \ldots, A_k$, ou seja $x \in A_{[k]}$, e pela H.I. temos que $x \in A_1 \triangle \cdots \triangle A_k$. De novo, $x \in (A_1 \triangle A_2 \triangle \cdots \triangle A_k) \triangle A_{k+1}$.

Π8.5S. Precisamos verificar que a expressão $A_1 \triangle \cdots \triangle A_n$ faz sentido no caso que $n = 0$, ou seja, definir razoavelmente a diferença simétrica de uma seqüência vazia de conjuntos. Formalmente verificamos que $\emptyset \triangle C = C = C \triangle \emptyset$ para qualquer conjunto C: $\emptyset$ é o elemento neutro da operação $\triangle$, e logo o valor próprio da expressão acima.

Na prova, a base muda para $n = 0$, onde devemos apenas demonstrar que nenhum a pertence numa quantidade ímpar dos (zero) A_i's, que é óbvio.

Π8.6S. Vou demonstrar que $\mathscr{C} \cup \{T\}$ é uma chain.

Sejam $A, B \in \mathscr{C} \cup \{T\}$. Preciso mostrar que $A \subseteq B$ ou $B \subseteq A$. Vou separar em casos dependendo de se os A, B pertencem à $\mathscr{C}$ ou ao $\{T\}$.
Caso ambos pertencem à $\mathscr{C}$. Como $\mathscr{C}$ é chain, temos imediatamente $A \subseteq B$ ou $B \subseteq A$.
Caso exatamente um pertence à $\mathscr{C}$. Chame C aquele que pertence à $\mathscr{C}$. O outro pertence ao $\{T\}$ e logo é o próprio $T = \bigcup \mathscr{C}$. Vou mostrar que $C \subseteq T$. Seja $c \in C$. Preciso mostrar que c pertence em algum dos membros do $\mathscr{C}$, que acontece pois $C \in \mathscr{C}$.
Caso nenhum pertence à $\mathscr{C}$. Ou seja, ambos pertencem ao $\{T\}$; ou seja $A = B = T$; e logo $A \subseteq B$ e pronto.

Π8.7S. Defino a $\mathscr{C}$ pela

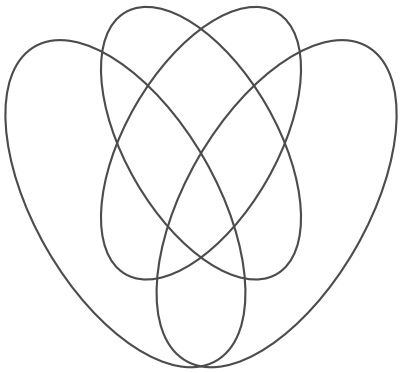
$$\mathscr{C} \stackrel{\text{def}}{=} \{\, (-a, a) \mid a \in \mathbb{R}_{>0} \,\}$$

onde $(-a, a)$ denota o intervalo aberto de reais $\{\, x \in \mathbb{R} \mid -a < x < a \,\}$ (veja D6.28). Realmente temos

$$\bigcup \mathscr{C} = \mathbb{R} \notin \mathscr{C}; \qquad \bigcap \mathscr{C} = \emptyset \notin \mathscr{C}.$$

Demonstração que $\emptyset, \mathbb{R} \notin \mathscr{C}$. Seja $C \in \mathscr{C}$, e logo seja $a_C \in \mathbb{R}$ tal que $C = (-a_C, a_C)$. Como $a_C + 1 \notin C$ e $a_C + 1 \in \mathbb{R}$, temos $C \neq \mathbb{R}$. Como $0 \in C$, temos $C \neq \emptyset$. Demonstrei então que o arbitrário membro da $\mathscr{C}$ não pode ser nem o $\emptyset$ nem o $\mathbb{R}$ e logo nenhum dos dois pertence à $\mathscr{C}$.

Π8.8S. Uma maneira de dezenhá-lo seria assim:



Se tu achou outra e realmente tem todas as 16 configurações possíveis, tá tranqüilo!

x8.48S. Temos $|A \times B| = |A| \cdot |B|$. Isso *é* o princípio da multiplicação (5.3).

x8.49S. Vamos demonstrar a

$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

Mostramos as duas inclusões separadamente:
($\subseteq$): Seja $w \in A \times (B \cup C)$. Logo $w = \langle a, d\rangle$ para algum $a \in A$ e algum $d \in B \cup C$ (def. $\times$). Logo $d \in B$ ou $d \in C$ (def. $\cup$). Caso $d \in B$, temos $w = \langle a, d\rangle \in A \times B$ (def. $\times$). Caso $d \in C$, temos $w = \langle a, d\rangle \in A \times C$ (def. $\times$). Nos dois casos concluimos que $w \in (A \times B) \cup (A \times C)$ pela definição de $\cup$.
($\supseteq$): Seja $w \in (A \times B) \cup (A \times C)$. Logo $w \in (A \times B)$ ou $w \in (A \times C)$ (def. $\cup$). Caso $w \in (A \times B)$, temos $w = \langle a, b\rangle$ para algum $a \in A$ e algum $b \in B$ (def.$\times$). Logo $b \in B \cup C$ (pois $b \in B$) (def. $\cup$). Logo pela definição de $\times$ temos o desejado $w = \langle a, b\rangle \in A \times (B \cup C)$. O caso $w \in (A \times C)$ é similar.
A igualdade

$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

é demonstrada similarmente.

x8.50S. Como contraexemplo tome $A := \emptyset$ e $B := \mathbb{N}$ (qualquer $B \neq \emptyset$ serve). Observe que $A \neq B$, mas mesmo assim

$$A \times B = B \times A$$

pois

$$\emptyset \times \mathbb{N} = \emptyset = \mathbb{N} \times \emptyset.$$

x8.53S. Calculamos:

$$\{\{\emptyset\}\} \times \wp\emptyset = \{\{\emptyset\}\} \times \{\emptyset\} = \{(\{\emptyset\}, \emptyset)\}$$
$$\{\{\emptyset\}\} \mathbin{\triangle} \bigcup \emptyset = \{\{\emptyset\}\} \mathbin{\triangle} \emptyset = \{\{\emptyset\}\}$$

x8.54S. As projecções e o construtor $\langle -, -, - \rangle$ devem satisfazer:

$$\pi^3_0 \langle x, y, z \rangle = x \qquad \pi^3_1 \langle x, y, z \rangle = y \qquad \pi^3_2 \langle x, y, z \rangle = z;$$
$$t = \langle \pi^3_0 t, \pi^3_1 t, \pi^3_2 t \rangle .$$

x8.55S. Seja t tripla. Definimos

$$\pi^3_0 t = \pi_0 t \qquad \pi^3_1 t = \pi_0(\pi_1 t) \qquad \pi^3_2 t = \pi_1(\pi_1 t).$$

x8.56S. Calculamos

$$\begin{aligned} \langle x, y, z \rangle = \langle x', y', z' \rangle &\overset{\text{sug}}{\iff} \langle x, y, z \rangle = \langle x', \langle y', z' \rangle \rangle \\ &\iff x = x' \ \&\ \langle y, z \rangle = \langle y', z' \rangle && \text{(def. de } (=) \text{ para 2-tuplas)} \\ &\iff x = x' \ \&\ y = y' \ \&\ z = z'. && \text{(def. de } (=) \text{ para 2-tuplas)} \end{aligned}$$

que é exatamente o que desejamos mostrar!

x8.57S. Suponha $x \in \bigcup_{n=0}^{\infty} A_n$ (1). Preciso mostrar que $x \in \bigcup_{n=0}^{\infty} B_n$, ou seja, mostrar que x pertence a pelo menos um dos B_n's. (Ou seja, procuro um $k \in \mathbb{N}$ tal que $x \in B_k$.) Seja $m \in \mathbb{N}$ tal que $x \in A_m$ (tal m existe pela (1)). Agora pela hipótese (com $n := m$) $A_m \subseteq B_{m+1}$, e logo $x \in B_{m+1}$, algo que mostra que $x \in \bigcup_{n=0}^{\infty} B_n$, pois $m + 1 \in \mathbb{N}$.

x8.58S. Suponha $x \in \bigcap_{n=0}^{\infty} A_n$. Preciso mostrar que $x \in \bigcap_{n=0}^{\infty} B_n$, ou seja, demonstrar que $x \in B_k$ para todo $k \in \mathbb{N}$. Seja $k \in \mathbb{N}$. Como $x \in \bigcap_{n=0}^{\infty} A_n$, temos $x \in A_{2k}$. Mas $A_{2k} \subseteq B_k$, logo $x \in B_k$.

x8.59S. Suponha $x \in \bigcap_{n=0}^{\infty} A_n$. (1) Preciso mostrar que $x \in \bigcup_{n=28}^{\infty} B_n$, ou seja, achar um inteiro $m \geq 28$ tal que $x \in B_m$. Pela (1) temos $x \in A_{17}$; e como 17 é primo, $A_{17} \subseteq B_{34}$ (pela hipótese). Logo $x \in B_{34}$. Então realmente $x \in \bigcup_{n=28}^{\infty} B_n$.

x8.60S. Seja A_n uma seqüência de conjuntos. Defina

$$\bigcup_{n=0}^{\infty} \overset{\text{def}}{=} \bigcup \{ A_n \mid n \in \mathbb{N} \} \qquad \bigcap_{n=0}^{\infty} \overset{\text{def}}{=} \bigcap \{ A_n \mid n \in \mathbb{N} \}.$$

x8.63S. Dados conjuntos A, B, C, precisamos mostrar que:

$$C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B).$$

Seja $\{A_n\}_n$ a seqüência $A, B, B, B, \cdots$, (ou seja, a seqüência definida pelas: $A_0 = A$; e $A_i = B$ para $i > 0$). Pela Proposição 8.131 temos então:

$$C \setminus \underbrace{\bigcup_{n=0}^{\infty} A_n}_{A \cup B} = \underbrace{\bigcap_{n=0}^{\infty} (C \setminus A_n)}_{(C \setminus A) \cap (C \setminus B)}.$$

x8.64S. Calculamos

$$\begin{aligned}
x \in C \setminus \textstyle\bigcup_{n=0}^{\infty} A_n &\iff x \in C \wedge \neg\left(x \in \textstyle\bigcup_{n=0}^{\infty} A_n\right) && \text{(def. } \setminus\text{)} \\
&\iff x \in C \wedge \neg(\exists n \in \mathbb{N})[x \in A_n] && \text{(def. } \textstyle\bigcup_{n=0}^{\infty}\text{)} \\
&\iff x \in C \wedge (\forall n \in \mathbb{N})[x \notin A_n] && \text{(De Morgan)} \\
&\iff (\forall n \in \mathbb{N})[x \in C \wedge x \notin A_n] && (n \text{ não livre em } x \in C) \\
&\iff (\forall n \in \mathbb{N})[x \in C \setminus A_n] && \text{(def. } \setminus\text{)} \\
&\iff x \in \textstyle\bigcap_{n=0}^{\infty}(C \setminus A_n). && \text{(def. } \textstyle\bigcap_{n=0}^{\infty}\text{)}
\end{aligned}$$

(Observe a semelhança entre essa demonstração e a demonstração da Proposição 8.63, até nas justificativas de cada passo!) A demonstração da outra igualdade é de graça pois é sua dual: é só trocar os $\bigcup$ com os $\bigcap$, e os $\exists$ com os $\forall$!

x8.65S. A afirmação é verdadeira.
($\subseteq$): Suponha $x \in A \cup \bigcap_{n=0}^{\infty} B_n$. Logo $x \in A$ ou $x \in \bigcap_{n=0}^{\infty} B_n$. Caso $x \in A$. Temos que para todo $n \in \mathbb{N}$, $x \in A \cup B_n$ (pois $x \in A$), e logo $x \in \bigcap_{n=0}^{\infty}(A \cup B_n)$. Caso $x \in \bigcap_{n=0}^{\infty} B_n$. Seja $n \in \mathbb{N}$. Preciso mostrar que $x \in A \cup B_n$, que é verdadeiro pois $x \in B_n$ pela hipótese do caso.
($\supseteq$): Suponha $x \in \bigcap_{n=0}^{\infty}(A \cup B_n)$. Logo $x \in A \cup B_n$ para todo $n \in \mathbb{N}$. Caso $x \in A$, o resultado é imediato. Caso $x \notin A$. Seja $m \in \mathbb{N}$. Vou mostrar que $x \in B_m$. Sabemos pela hipótese que $x \in A \cup B_m$, e como $x \notin A$, logo $x \in B_m$. Como o m foi arbitrário, concluimos que para todo $m \in \mathbb{N}$, $x \in B_m$, que foi exatamente o que precisamos demonstrar.

x8.66S. Temos

$$\begin{aligned}
a \in \textstyle\bigcup_n A_n &\iff (\exists n \in \mathbb{N})[\, a \in A_n \,] \iff a \in \mathbb{N} \\
b \in \textstyle\bigcap_n B_n &\iff (\forall n \in \mathbb{N})[\, b \in B_n \,] \iff \mathsf{False}.
\end{aligned}$$

Ou seja: $\bigcup_n A_n = \mathbb{N}$ e $\bigcap_n B_n = \emptyset$. Equivalentemente ganhamos a segunda imediatamente pela primeira e a Proposição 8.131.

x8.67S. Resposta: sim!

($\subseteq$): Seja $x \in \bigcap_{n=0}^{\infty} \bigcap_{m=n}^{\infty} A_m$. Pela hipótese, para todo $n \in \mathbb{N}$, $x \in \bigcap_{m=n}^{\infty} A_m$ (def. $\bigcap_{n=0}^{\infty}$). Logo (com $n := 0$) temos o desejado $x \in \bigcap_{m=0}^{\infty} A_m$.
($\supseteq$): Seja $x \in \bigcap_{n=0}^{\infty} A_n$, ou seja, x pertence a todos os A_n's. Preciso mostrar que

$$x \in \bigcap_{n=0}^{\infty} \bigcap_{m=n}^{\infty} A_m.$$

Seja $w \in \mathbb{N}$ então, e agora basta mostrar que

$$x \in \bigcap_{m=w}^{\infty} A_m.$$

Seja $m \geq w$ então. Preciso mostrar que $x \in A_m$; que segue imediatamentea pela hipótese (tomando $n := m$).

Π8.9S. Vamos construir um contraexemplo para cada afirmação.

Considere as seqüências de conjuntos seguintes: para todo $n \in \mathbb{N}$ define

$$A_n =: (-n, n) \qquad \begin{aligned} B_0 &:= \emptyset \\ B_{n+1} &:= [-n, n]. \end{aligned}$$

Observe que, realmente, para todo $n \in \mathbb{N}$ temos $A_n \subsetneq B_{n+1}$:

$$A_n = (-n, n) \subsetneq [-n, n] = B_{n+1}.$$

Mesmo assim,

$$\bigcup_{n=0}^{\infty} A_n = \mathbb{R} = \bigcup_{n=0}^{\infty} B_n.$$

Para refutar a segunda afirmação, considere as seqüências de conjuntos seguintes: para todo $n \in \mathbb{N}$ defina

$$A_n =: \{\, k \in \mathbb{N} \mid k > n \,\} \qquad B_n =: \{\, k \in \mathbb{N} \mid k \geq n \,\}$$

Observe que, realmente, para todo $n \in \mathbb{N}$ temos $A_n \subsetneq B_n$. Mesmo assim,

$$\bigcap_{n=0}^{\infty} A_n = \emptyset = \bigcap_{n=0}^{\infty} B_n.$$

Π8.10S. Definição da D_n por recursão:

$$\begin{aligned} D_0 &= \emptyset \\ D_{n+1} &= D_n \cup A_n. \end{aligned}$$

Demonstração da afirmação por indução no n:

Base: $D_0 \subseteq \bigcup_{m=0}^{\infty} A_m$. Imediato pois $D_0 = \emptyset$.

Passo indutivo. Seja $w \in \mathbb{N}$ tal que

(H.I.) $$D_w \subseteq \bigcup_{m=0}^{\infty} A_m.$$

Preciso demonstrar que

$$D_{w+1} \subseteq \bigcup_{m=0}^{\infty} A_m.$$

Seja $d \in D_{w+1}$. Basta mostrar que

$$d \in \bigcup_{m=0}^{\infty} A_m,$$

ou seja, que d pertence àlgum dos A_m's. Pela definição de $D_{w+1} = D_w \cup A_w$, temos que $d \in D_w$ ou $d \in A_w$. Separo em casos:
Caso $d \in D_w$. Imediatamente pela (H.I.)

$$d \in D_w \subseteq \bigcup_{m=0}^{\infty} A_m.$$

Caso $d \in A_w$. Imediato.
O que muda trocando de uniões para intersecções: (1) a intersecção vazia tem de ser o $\mathcal{U}$ em vez do $\emptyset$, pois $\mathcal{U}$ é a identidade da $\cap$ binária; (2) o ($\subseteq$) da afirmação tem de mudar pra ($\supseteq$); (3) a base da indução também é imediata pois $\mathcal{U}$ é superconjunto de qualquer conjunto; (4) o passo indutivo muda numa maneira mais interessante: nosso alvo é mostrar que um arbitrario membro a que pertence a intersecção infinita dos A_i's pertence ao D_{w+1} tambem, dado que qualquer membro dela pertence ao D_w; e temos então ambas as coisas que precisamos (o $a \in D_w$ pela (H.I.) e o $a \in A_w$ pois a pertence a todos os A_i's).

x8.68S. Depende! Primeiramente um exemplo onde a afirmação é válida:

$$I = J = \{1\} \qquad\qquad A_1 = \{5\}$$

...e um onde a afirmação é falsa:

$$\begin{aligned} I &= \{1\} \\ J &= \{2\} \end{aligned} \qquad\qquad A_1 = A_2 = \{5\}$$

Realmente, verificamos calculando no primeiro exemplo:

$$\bigcup_{k \in I \cap J} A_k = A_1 \qquad\qquad \bigcup_{k \in I} A_k \cap \bigcup_{k \in J} A_k = A_1 \cap A_1 = A_1$$

...e no segundo:

$$\bigcup_{k \in I \cap J} A_k = \bigcup_{k \in \emptyset} A_k = \emptyset \qquad\qquad \bigcup_{k \in I} A_k \cap \bigcup_{k \in J} A_k = A_1 \cap A_2 = \{5\}$$

x8.70S. Tome

$$\mathscr{A} := \{\{0,1\}, \{1,2\}, \{7\}\}.$$

x8.71S. As $\mathscr{A}_1, \mathscr{A}_3, \mathscr{A}_4, \mathscr{A}_8$ são. As outras não:

- a $\mathscr{A}_2$ não é: $\emptyset$ é seu membro;
- a $\mathscr{A}_5$ não é: o 2 que pertence a dois membros dela;
- a $\mathscr{A}_6$ não é: $4 \in A$ mas não pertence a nenhum membro dela;
- a $\mathscr{A}_7$ não é: $7 \notin A$ mas $7 \in \bigcup \mathscr{A}_7$.

x8.72S. Traduzimos:

$$\begin{aligned}
p \text{ e } q \text{ são irmãos} &: p \neq q \ \ \& \ \ \exists r(\{p,q\} \subseteq C_r) \\
C_p \neq \emptyset &: p \text{ tem pelo menos um filho} \\
p \text{ é filho único} &: (\exists r \in A_p)[\, C_r = \{p\}\,] \\
p \text{ e } q \text{ são parentes} &: A_p \cap A_q \neq \emptyset \\
p \text{ e } q \text{ são primos de primeiro grau} &: \exists r, r'(p \in C_r \ \ \& \ \ q \in C_{r'} \ \ \& \ \ r \text{ e } r' \text{ são irmãos}) \\
r \text{ é filho dos } p \text{ e } q &: r \in C_p \cap C_q \\
C_p \cap C_q \neq \emptyset &: p \text{ e } q \text{ têm pelo menos um filho juntos} \\
A_p \subseteq A_q &: p \text{ é um anscestor ou irmão de } q \\
\emptyset \subsetneq C_p \subsetneq C_q &: q \text{ tem filho(s) com } p \text{ mas com outra pessoa também} \\
(\exists p \in \mathcal{P})[\, p \in C_p\,] &: \text{existe pessoa que é seu próprio filho.}
\end{aligned}$$

(Tuas traduções podem variar, especialmente se tuas definições dessas palavras são diferentes que aquelas que eu usei aqui.)

Π8.12S. Vamos demonstrar que $A_* \subseteq A^*$.

Seja então $x \in A_* = \bigcup_{i=0}^{\infty} \bigcap_{j=i}^{\infty} A_j$. Logo seja $i_0 \in \mathbb{N}$ tal que $x \in \bigcap_{j=i_0}^{\infty} A_j$. Sabemos então que

$$(*) \qquad (\forall j \geq i_0)[\, x \in A_j\,].$$

Queremos demonstrar que $x \in A^* = \bigcap_{i=0}^{\infty} \bigcup_{j=i}^{\infty} A_j$. Seja então $n_0 \in \mathbb{N}$. Agora basta demonstrar que

$$x \in \bigcup_{j=n_0}^{\infty} A_j.$$

Em outras palavras, procuramos um $k \in \mathbb{N}$ que satisfaz: $k \geq n_0$ e $x \in A_k$. Tome $k := \max\{i_0, n_0\}$ e observe que esse k satisfaz ambas as condições. Pela escolha de k a primeira condição é satisfeita imediatamente. Sobre a segunda, como $k \geq i_0$, pela (*) temos que $x \in A_k$, que foi o que queremos demonstrar.

Π8.13S. A idéia é entender o que cada uma das proposições

$$x \in A_* \qquad\qquad x \in A^*$$

quis dizer, para enxergar se uma implica a outra, etc. Como já demonstramos "mecanicamente" no Problema Π8.12 que $A_* \subseteq A^*$, queremos então chegar na conclusão que

$$x \in A_* \implies x \in A^*$$

num caminho diferente: do coração.

Vamos primeiramente analisar o $A_* = \bigcup_i \bigcap_{j \geq i} A_j$. É uma união duma seqüência de conjuntos, então faz sentido observar pelo menos os primeiros membros dessa seqüência:

$$\bigcap_{j \geq 0} A_j, \quad \bigcap_{j \geq 1} A_j, \quad \bigcap_{j \geq 2} A_j, \quad \dots$$

Cada um desses membros também é uma intersecção duma seqüência. Vamos escrever numa maneira que deixa os primeiros termos vizíveis:

$$\begin{aligned}
\bigcap_{j \geq 0} A_j &= A_0 \cap A_1 \cap A_2 \cap \cdots \\
\bigcap_{j \geq 1} A_j &= A_1 \cap A_2 \cap A_3 \cap \cdots \\
\bigcap_{j \geq 2} A_j &= A_2 \cap A_3 \cap A_4 \cap \cdots \\
&\vdots
\end{aligned}$$

Trabalhando dualmente no A^*, chegamos nas:

$$x \in \bigcup \left\{ \begin{array}{r} A_0 \cap A_1 \cap A_2 \cap A_3 \cap A_4 \cap \cdots \\ A_1 \cap A_2 \cap A_3 \cap A_4 \cap \cdots \\ A_2 \cap A_3 \cap A_4 \cap \cdots \\ \ddots \end{array} \right\} \qquad x \in \bigcap \left\{ \begin{array}{r} A_0 \cup A_1 \cup A_2 \cup A_3 \cup A_4 \cup \cdots \\ A_1 \cup A_2 \cup A_3 \cup A_4 \cup \cdots \\ A_2 \cup A_3 \cup A_4 \cup \cdots \\ \ddots \end{array} \right\}$$

Sabendo a primeira concluimos que x pertence a *pelo menos uma* das linhas da esquerda, vamos dizer a u-ésima, ou seja

$$x \in A_u \cap A_{u+1} \cap A_{u+2} \cap \cdots$$

Logo sabemos que

$$x \text{ pertence a todos os } A_u, A_{u+1}, A_{u+2}, \dots.$$

Em outras palavras: *a partir dum ponto, x pertence a todos os membros da seqüência original*. Demonstramos então que

$$x \in A_* \implies \text{a partir dum ponto, } x \text{ pertence a todos os } A_n\text{'s.}$$

Vamos demonstrar o converso agora. Suponha que a partir dum $u \in \mathbb{N}$, sabemos que x pertence a todos os $A_u, A_{u+1}, A_{u+2}, \dots$, ou seja,

$$x \in A_u \cap A_{u+1} \cap A_{u+2} \cap \cdots$$

ou seja, achamos uma linha onde x pertence e logo $x \in A_*$.

Agora a segunda proposição ($x \in A^*$) concluimos que x pertence a *todas* as linhas da direita, ou seja:

$$\begin{aligned}
x &\in A_0 \cup A_1 \cup A_2 \cup A_3 \cup A_4 \cup \cdots \\
x &\in \quad A_1 \cup A_2 \cup A_3 \cup A_4 \cup \cdots \\
x &\in \quad\quad A_2 \cup A_3 \cup A_4 \cup \cdots \\
&\vdots
\end{aligned}$$

Observe que a j-ésima linha afirma que *mesmo depois de andar j passos na seqüência, ainda terá A_n's com x neles.* Sabendo então que cada uma dessas linhas é verdade, podemos concluir que x pertence a uma infinidade dos A_n's, e vice versa:

$$x \in A^* \iff x \text{ pertence a uma infinidade dos } A_n\text{'s.}$$

Vamos demonstrar isso.

($\Rightarrow$): Temos como hipótese todas as

$$\begin{aligned} x &\in A_0 \cup A_1 \cup A_2 \cup A_3 \cup A_4 \cup \cdots \\ x &\in \quad A_1 \cup A_2 \cup A_3 \cup A_4 \cup \cdots \\ x &\in \quad\quad A_2 \cup A_3 \cup A_4 \cup \cdots \\ &\vdots \end{aligned}$$

e queremos mostrar que x pertence a uma infinidade dos A_n's. Basta mostrar que para qualquer "desafio" $v \in \mathbb{N}$, x pertence àlgum dos $A_v, A_{v+1}, A_{v+2}, \ldots$. Seja $v \in \mathbb{N}$ então. Olha na v-ésima linha e é exatamente o que queremos.

($\Leftarrow$): Agora sabendo que x pertence a uma quantidade infinita de A_n's precisamos mostrar que

$$\text{para todo } v \in \mathbb{N}, \quad x \in A_v \cup A_{v+1} \cup A_{v+2} \cup \cdots$$

Seja $v \in \mathbb{N}$ então. Para chegar num absurdo, suponha que

$$x \notin A_v \cup A_{v+1} \cup A_{v+2} \cup \cdots$$

ou seja, x não pertence a nenhum dos $A_v, A_{v+1}, A_{v+2}, \ldots$. Mas isso quis dizer que x pertence no máximo em v dos A_n's, contradizendo nossa hipótese que x pertence numa infinidade deles.

Concluimos então que

$$x \in A^* \iff x \text{ pertence a uma infinidade dos } A_n\text{'s.}$$

Como comparam essas afirmações?

- $x \in A_*$: a partir dum ponto, x pertence a todos os A_n's;
- $x \in A^*$: x pertence a uma infinidade dos A_n's.

Deve ser óbvio que

$$x \in A_* \implies x \in A^*.$$

E como já entendemos o que cada proposição quis dizer mesmo, podemos facilmente demonstrar que o converso não é sempre válido. Para um contraexemplo onde

$$x \in A_* \not\Leftarrow x \in A^*$$

considere a seqüência

$$\begin{aligned} A_0 &= \{0\} \\ A_1 &= \{0, 1\} \\ A_2 &= \{0\} \\ A_3 &= \{0, 1\} \\ A_4 &= \{0\} \\ A_5 &= \{0, 1\} \\ &\vdots \end{aligned}$$

Observe que os $0, 1$ são aqueles que pertencem a uma infinidade dos A_n's. Mas apenas o 0 pertence a todos os A_n's a partir dum certo ponto.

Π8.14S. Sem a restricção uma tal seqüência seria a

$$\emptyset, \quad \{1\}, \quad \emptyset, \quad \{1\}, \quad \emptyset, \quad \{1\}, \quad \dots$$

Assim temos $A_* = \emptyset$ e $A^* = \{1\}$.

Para satisfazer a restricção, considere a seqüência:

$$A_n = \begin{cases} \{\, k \leq n \mid k \text{ é primo} \,\}, & \text{se } n \text{ par;} \\ \{\, k \leq n \mid k \text{ é ímpar} \,\}, & \text{caso contrário.} \end{cases}$$

Seus primeiros termos:

$$\begin{aligned} A_0 &= \emptyset & A_1 &= \{1\} \\ A_2 &= \{2\} & A_3 &= \{1,3\} \\ A_4 &= \{2,3\} & A_5 &= \{1,3,5\} \\ A_6 &= \{2,3,5\} & A_7 &= \{1,3,5,7\} \\ A_8 &= \{2,3,5,7\} & A_9 &= \{1,3,5,7,9\} \\ &\vdots & &\vdots \end{aligned}$$

Nesse caso,

$$\begin{aligned} A_* &= \{3,5,7,11,13,17,\dots\} &&= \{\, n \in \mathbb{N} \mid n \text{ é um primo ímpar} \,\} \\ A^* &= \{1,2,3,5,7,9,11,13,\dots\} &&= \{\, n \in \mathbb{N} \mid n = 2 \text{ ou } n \text{ ímpar} \,\}. \end{aligned}$$

Capítulo 9

x9.1S. O tipo de `x` é `int`. O tipo de `foo` é: "função de `int` para `int`". Programadores de *C* muitas vezes erram nessa terminologia, dizendo que o tipo de `foo` é `int`. Se fosse `int` mesmo, o `foo` seria um `int`. O que eles querem dizer é que o *return type* de `foo` é `int`, e isso tá certo. Mas a pergunta foi identificar o *tipo* de `foo`.

x9.2S. Esquecendo as partes que têm a ver com funções chegamos na regra

$$\frac{A \to B \qquad A}{B} \text{ ModusPonens?!}$$

que é... a modus ponens (Nota 2.19) mesmo? A regra de como usar implicação?! Sim. Continue lendo o texto agora.

x9.3S. Temos $|A|$ coisas para definir até determinar uma função de A para B. Para cada uma delas (para cada $a \in A$) temos $|B|$ opções para mandá-lo (nossas escolhas não afetam a quantidade de opções que teremos nas próximas). Logo pelo princípio da multiplicação

$$|(A \to B)| = |A|^{|B|}.$$

x9.4S. Se $f : A \to B$ e $g : C \to D$ são funções com $A \neq C$, pela definição de igualdade de conjuntos, existe $x \in A \triangle C$. Para esse x, as funções vão comportar diferentemente. Se $x \in A$ (e logo $x \notin C$), a f vai aceitar o x e vamos observar sua saída $f(x)$, mas a g não vai aceitar o x, e assim não vamos ver nenhuma saída; Similarmente, se $x \in C$ (e logo $x \notin A$).

x9.5S. Aplicando essa definição de cod nas $\sin_1, \sin_2, \sin_3$ do Nota 9.16, temos que

$$\operatorname{cod}(\sin_1) = \operatorname{cod}(\sin_2) = \operatorname{cod}(\sin_3)$$

mesmo que claramente não foi essa a nossa intenção.

x9.6S. É fácil responder sobre as $\sin_4$ e $\sin_7$, pois realmente são apenas restricções da função $\sin : \mathbb{R} \to \mathbb{R}$ (veja Definição D9.161). Mas a situação com as $\sin_5$ e $\sin_6$ é bem mais complicada que isso! Sobre a $\sin_5$, supondo que sabemos que $\pi \notin \mathbb{Q}$, concluimos que o seu tipo está errado, pois $\sin(\pi) = 0 \notin \mathbb{R} \setminus \mathbb{Q}$. Note que para responder nisso precisamos saber a irracionalidade de π, algo que não é trivial! Mesmo sabendo disso, não é fácil responder sobre a $\sin_6$. Seu tipo é realmente errado, pois

$$\text{para todo } x \in \mathbb{Q}_{\neq 0},\ \sin(x) \notin \mathbb{Q}$$

mas a demonstração desse resultado é fora do escopo desse texto. (Veja **[Niv05:** Cor. 2.7**]** para mais detalhes.) Ou seja, podemos considerar a sin com tipo

$$\sin_8 : \mathbb{Q}_{\neq 0} \to \mathbb{R} \setminus \mathbb{Q}.$$

x9.7S. (1) Não, f não é injetora. Tome uma letra do alfabeto $a \in \Sigma$ e observe que

$$f(a, 0) = aa = f(aa, 1).$$

Como $(a, 0) \neq (aa, 1)$, a f não é injetora.
(2) Sim, f é sobrejetora. Tome um aleatório string $w \in S$, e seja w' o string reverso de w. Temos

$$f(w', 1) = (w')' = w.$$

x9.10S. (i) Sim. Sejam $a, a' \in A$ tais que $f(a) = f(a')$, ou seja, $\{a\} = \{a'\}$. Logo $a = a'$.
(ii) Não, pois nenhum membro do A é mapeado para o $\emptyset$, que é um membro do $\wp A$. Seja $a \in A$. Logo $f(a) = \{a\} \neq \emptyset \in \wp A$.

x9.12S. A função m é bem definida, ou seja, é uma função mesmo: *cada pessoa* tem (totalidade) exatamente uma (determinabilidade) mãe e logo ambas as condições de funcionalidade (9.11) são satisfeitas. Por outro lado, a s não satisfaz nenhuma das condições: tem pessoas sem filhos, e logo a totalidade já era; e também tem pessoas com mais que um filho, e logo nem determinabilidade temos.

x9.13S. Não. O $s(p)$ é a única pessoa y tal que y é filho de p e sim, sabemos que tal y existe e que é único mas... talvez essa pessoa y não possui exatamente um filho, ou seja, talvez

$y \notin \mathcal{P}'$. De fato, a situação piorou, pois agora nem a m é função, pelo mesmo motivo: uma pessoa p mesmo tendo exatamente um filho, a mesma coisa não é garantida para a mãe de p, e logo o $m(p)$ talvez não pertence ao $\mathcal{P}'$.

x9.14S. Não: tanto para Conjuntistas quanto para Categoristas a saida $f(x)$ duma função $f : A \to B$ deve pertence ao B.

x9.15S. Temos

$$f_1(5) = 2 \neq 5 = f_2(5),$$

logo $f_1 \neq f_2$.

x9.16S. A h realmente é bem-definida, mas isso não é imediatamente óbvio, pois os dois primeiros casos na sua definição não são distintos, e os valores que cada um escolhe para a h são aparentemente diferentes. Para demonstrar que a h é uma função bem-definida precisamos ver quais são os membros do seu codomínio que satisfazem mais que um caso (aqui os dois primeiros casos, pois o terceiro é o "caso contrário") e verificar que o valor da h para esses membros são os mesmos, independente do caso escolhido. O único número natural que é primo e par e o 2. Seguindo o primeiro caso temos

$$h(2) = 2 + 2 = 4,$$

e seguindo o segundo caso temos

$$h(2) = 2^2 = 4.$$

Logo, a h realmente é uma função bem-definida.

x9.17S. A f não é bem-definida: perdemos a unicidade; pois, por exemplo, como $1^2 = 1 = (-1)^2$, o $f(1)$ fica sem valor unicamente determinado.

A g não é bem-definida: perdemos a totalidade; pois para o $2 \in \mathbb{N}$ por exemplo, não existe nenhum $y \in \mathbb{N}$ com $y^2 = 2$.

A h realmente é bem-definida, conhecida como "floor".

A u não é bem-definida: perdemos a unicidade; por exemplo o $u(1, 5)$ fica sem valor determinado, pois 2 é primo e $2 \mid 6$ mas 3 também é primo e $3 \mid 6$.

A v também não é bem-definida: perdemos a totalidade; por exemplo o $v(0, 1)$ fica sem valor nenhum, pois nenhum primo divide o $0 + 1 = 1$.

x9.18S. Temos:

$f : \{0, 1, 2, 3\} \to \mathbb{N}$	$r : \emptyset \to \mathbb{N}$
$g : \{0\} \to \mathbb{N}$	s : não é (range não contido no codomínio)
$h : \{0, 1, 3, 8\} \to \mathbb{N}$	t : não é (quebrou determinabilidade)
$k : \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\} \to \mathbb{N}$	$w : \{0, \langle 1, 2\rangle, \langle 12, 12\rangle, \langle 0, 1, 0, 0\rangle\} \to \mathbb{N}$

x9.19S. $A = \emptyset$, pois, caso contrário, pegando um $a \in A$, chegamos na contradição $f(a) \in \emptyset$. Quantas funções f têm esse tipo? Vamos resolver isso logo: veja Definição D9.71 e Exercício x9.21.

x9.21S. Para o conjuntista: «a» mesmo! Pois, tome f, g funções vazias. Logo $f : \emptyset \to A$ e $g : \emptyset \to B$ para alguns conjuntos A, B. Vacuamente temos que para todo $x \in \emptyset$, $f(x) = g(x)$. Para o categorista: para cada conjunto A, temos exatamente uma função vazia com codomínio A.

x9.22S. Calculamos:

$$\begin{aligned}
(2 + \bullet)(40) &= 2 + 40 = 42 \\
(\bullet + 2\bullet)(2, 4) &= 2 + 2^4 = 18 \\
(- \cdot 2^-)(3, 0) &= 3 \cdot 2^0 = 3 \\
(\{1, 2, 3\} \cup -)(\{2, 8\}) &= \{1, 2, 3\} \cup \{2, 8\} = \{1, 2, 3, 8\}
\end{aligned}$$

x9.23S. Calculamos:

$$\begin{aligned}
\underline{(\lambda x \,.\, x)\ 5} &\rhd_\lambda 5 \\
\underline{(\lambda y \,.\, 42)\ 5} &\rhd_\lambda 42 \\
\underline{(\lambda z \,.\, x)\ 5} &\rhd_\lambda x \\
\underline{(\lambda x \,.\, x + 1)\ 41} &\rhd_\lambda 41 + 1 \\
&= 42 \\
\underline{(\lambda x \,.\, 2 + (\lambda y \,.\, 3y)\ 5)\ 3} &\rhd_\lambda 2 + \underline{(\lambda y \,.\, 3y)\ 5} \\
&\rhd_\lambda 2 + 3 \cdot 5 \\
&= 17 \\
\underline{(\lambda x \,.\, 2 + (\lambda y \,.\, 3y)(x^2))\ 3} &\rhd_\lambda 2 + \underline{(\lambda y \,.\, 3y)\ (3^2)} \\
&\rhd_\lambda 2 + 3 \cdot 3^2 \\
&= 29 \\
(\lambda x \,.\, 2 + \underline{(\lambda y \,.\, xy)\ 4})\ 3 &\rhd_\lambda \underline{(\lambda x \,.\, 2 + x \cdot 4)\ 3} \\
&\rhd_\lambda 2 + 3 \cdot 4 \\
&= 14 \\
\lambda x \,.\, (\lambda x \,.\, x + 1)\ 1 \cdot \underline{(\lambda y \,.\, xy)\ 4} &\rhd_\lambda \lambda x \,.\, \underline{(\lambda x \,.\, x + 1)\ 1} \cdot x \cdot 4 \\
&\rhd_\lambda \lambda x \,.\, (1 + 1) \cdot x \cdot 4) \\
&= \lambda x \,.\, 8x.
\end{aligned}$$

Se o último cálculo parece insatisfatório, é apenas por causa de um preconceito teu que favorece os objetos de tipo "número" contra os objetos de tipo "função". Mais sobre isso no Nota 9.112.

x9.26S. f.

x9.27S. $A = \{\, x \mid x \in A \,\}$.

x9.28S. Temos

$$\begin{array}{l} f_1(2) \\ f_2(1,2,5) \\ f_3(1,5,a) \\ f_4(1,5,2a) \\ f_5(\cos(1+5\sqrt[3]{2})^{2a},5) \\ f_6(a) \\ f_7(2,5). \end{array}$$

x9.29S. Temos

$$\begin{array}{lll} F_1 = \cos(1+5\sqrt[3]{2})^{2a} + \bullet(5) & : & (\mathbb{R}\to\mathbb{R})\to\mathbb{R} \\ F_2 = \bullet(1+5\sqrt[3]{2})^{2a} + \sin(5) & : & (\mathbb{R}\to\mathbb{R})\to\mathbb{R} \\ F_3 = \bullet(1+5\sqrt[3]{2})^{2a} + \bullet(5) & : & ((\mathbb{R}\to\mathbb{R})\times(\mathbb{R}\to\mathbb{R}))\to\mathbb{R} \\ F_4 = \cos(\bullet(1,5\sqrt[3]{2})^{2a} + \sin(5) & : & (\mathbb{R}^2\to\mathbb{R})\to\mathbb{R} \\ F_5 = \cos(\bullet(1,5\sqrt[3]{2})^{2a} + \bullet(\bullet) & : & \big((\mathbb{R}^2\to\mathbb{R})\times(\mathbb{R}\to\mathbb{R})\times\mathbb{R}\big)\to\mathbb{R} \\ F_6 = \lambda r,t,u\,.\cos(1+r(u,\sqrt[3]{2}))^{r(t,a)} + \sin(u) & : & \big((\mathbb{R}^2\to\mathbb{R})\times\mathbb{R}\times\mathbb{R}\big)\to\mathbb{R} \end{array}$$

x9.30S. Seguindo a definição da $F(25)$ ela é a função que recebendo um valor (agora tá recebendo o 3), retorna a soma de 25 e esse valor: $25+3=28$.

x9.33S. Temos

$$\begin{array}{rcl} f\restriction - & : & \wp A \to \bigcup_{X\in\wp A}(X\to B) \\ (-\restriction X)\restriction(A\to B) & : & ((A\to B)\to(X\to B)) \end{array}$$

x9.34S. Dados a $F:\mathbb{Z}\to(\mathbb{Z}\to\mathbb{Z})$, é só definir a $f:\mathbb{Z}^2\to\mathbb{Z}$ pela $f(x,y)=F(x)(y)$. Note que a expressão "$F(x)(y)$" quis dizer "$\big(F(x)\big)(y)$" mesmo.

x9.35S. Queremos definir a

$$\mathit{uncurry} : (A\to(B\to C))\to((A\times B)\to C)$$

e *seguindo as dicas* chegamos em:

$$\mathit{uncurry}(F) = \lambda\langle a,b\rangle\,.\,\big(F(a)\big)(b).$$

x9.36S.

$$\dfrac{\dfrac{f:A\to(B\to C) \qquad \dfrac{t:A\times B}{\mathit{outlt}:A}}{f(\mathit{outlt}):B\to C} \qquad \dfrac{t:A\times B}{\mathit{outrt}:B}}{f(\mathit{outlt})(\mathit{outrt}):C}$$

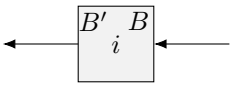
Π9.1S. (1) Apenas o conjunto vazio: a única função que existe de $\emptyset$ para A, é a função vazia. Se $S \neq \emptyset$ tome $s \in S$ e considere o conjunto $A = \{0, 1\}$. Já temos duas funções diferentes $f, g : S \to A$: basta apenas diferenciar elas no s. Tome por exemplo $f = \lambda x \,.\, 0$ e $g = \lambda x \,.\, 1$. Como $f(s) = 0 \neq 1 = g(s)$, temos $f \neq g$. (2) Todos os singletons. Se $T = \emptyset$, tome $A \neq \emptyset$ e observe que não existe nenhuma função $f : A \to T$. E se $|T| > 1$, tome $u, v \in T$ com $u \neq v$ e considere o $A = \{0\}$. Já temos duas funções $f, g : A\,\{T\}$: a $f = \lambda x \,.\, u$ e a $g = \lambda x \,.\, v$. Elas são realmente distintas, pois $f(0) = u \neq v = g(0)$, e logo $f \neq g$.

x9.39S. Nem é definida a $f \circ g$ no caso geral! Para ser definida, é necessário e suficiente ter $A = C$.

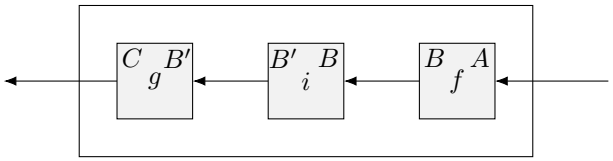
x9.40S. Definimos a função $i : B \to B'$ pela regra

$$i(x) = x, \quad \text{para todo } x \in B.$$

Seu black box então, parece assim:

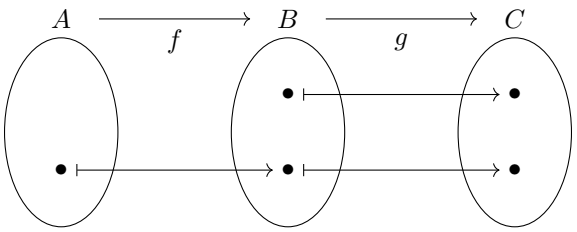


e é exatamente o "missing link" para construir nosso black box:



Construimos e usamos então a $g \circ i \circ f : A \to C$ em vez da "gambiarrada" e proibida $g \circ f$. Essa função i é chamada a *inclusão do A no B* que definimos na Definição D9.144.

x9.43S. Não. Aqui um contraexemplo:



x9.44S. Sim: até para o Conjuntista cada conjunto tem sua própria identidade. Para conjuntos distintos $A \neq B$ temos

$$\mathrm{dom}(\mathrm{id}_A) = A \neq B = \mathrm{dom}(\mathrm{id}_B)$$

e logo as identidades são distintas também: $\mathrm{id}_A \neq \mathrm{id}_B$. Lembre que o domínio é observável pelo Conjuntista: Nota 9.17. O mesmo argumento não passaria sobre as funções vazias, pois para diferenciá-las precisamos olhar para os seus codomínios, e isso é algo inobservável pelo Conjuntista.

x9.46S. Não. Por exemplo a função vazia $f : \emptyset \to \emptyset$ é invariável mas não constante. Mas realmente temos que

$$f \text{ invariável} \iff f \text{ constante}:$$

Suponha $f : A \to B$ constante, e logo seja $b \in B$ tal que $f = \mathrm{k}_b$. Sejam $x, y \in A$ e calculamos:

$$f(x) = \mathrm{k}_b(x) = b = \mathrm{k}_b(y) = f(y)$$

e logo f é invariável.

x9.47S. Pode sim. Isso aconrece exatamente quando $A = \emptyset$ e B possui pelo menos dois membros distintos $b \neq b'$. Nesse caso temos

$$\mathrm{k}_b^A = \mathrm{k}_{b'}^A .$$

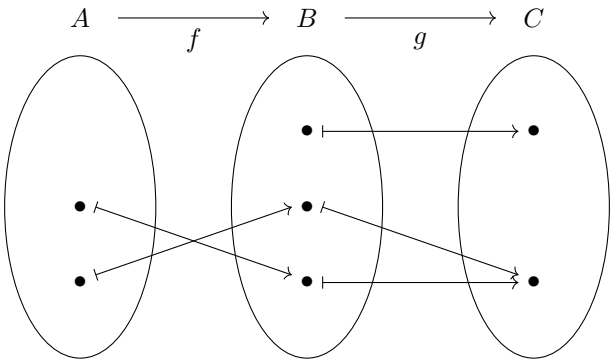
x9.48S. ($\Rightarrow$): Seja $a \in A$ ($A \neq \emptyset$). Vamos mostrar que tomando $b := f(a)$ a proposição na direita é satisfeita. Observe que o $f(a) \in B$ e satisfaz

$$(\forall x \in A)[\, f(x) = f(a)\,]$$

pela definição de constante.
($\Leftarrow$): Seja $b_0 \in B$ tal que para todo $x \in A$, $f(x) = b_0$. Agora para todo $x, y \in A$ temos $f(x) = b_0 = f(y)$ pela hipótese, ou seja, f é constante.

x9.49S. Sim, a ($\Leftarrow$). Observe *bem* que na demonstração dessa direção não precisamos $A \neq \emptyset$. E pelo Exercício x9.46 já sabemos que a ($\Rightarrow$) não é válida em geral.

x9.50S. Falso. Um contraexemplo é o seguinte:



x9.51S. A definição tem o problema que vai aceitar toda função como constante, pois o que ela exige é satisfeito por toda função. *Substituindo* o $\exists$ por $\exists!$ nada muda nesse sentido, pois toda função satisfaz essa afirmação mais forte (determinabilidade de função, 9.11).

O problema é que os quantificadores estão na ordem errada! Simplesmente *trocando a ordem deles*, chegamos numa definição equivalente à do Exercício x9.46:

$$f : A \to B \text{ constante} \overset{\text{def}}{\iff} (\exists b \in B)(\forall a \in A)[\, f(a) = b\,].$$

x9.52S. Temos $succ^3 = \lambda x \,.\, x + 3 \;:\; \mathbb{N} \to \mathbb{N}$.

x9.53S. Vamos tentar definir uma f idempotente e contar as escolhas que temos. Observe que assim que mandamos um $x \mapsto y$, o $f(y)$ "não tem mais escolha": precisa ser $f(y) = y$, pois f deve ser idempotente. Ou seja, y vai ser um *ponto fixo* (ou *fixpoint*) da f (mais sobre isso na §220). A f então deve ter pelo menos 1 fixpoint, e no máximo $|A| = 3$. Separamos então por casos, contamos as maneiras em cada caso e usamos o Princípio da adição (5.2) para contar quantidade total das maneiras. Defina então

$$F_i \stackrel{\text{def}}{=} \{\, f : A \to A \;\mid\; f \text{ tem exatamente } i \text{ fixpoints} \,\}.$$

Queremos achar o $|F_1| + |F_2| + |F_3|$. Calculamos separadamente.:
Quantas funções no F_1? Temos 3 funções, uma para cada escolha de fixpoint, pois assim que determinamos o único fixpoint, todos os outros membros devem ser mapeados nele.
Quantas funções no F_2? Temos $C(3,2) = 3$ maneiras de escolher 2 dos membros de A para ser os fixpoints da f. Para cada uma dessas escolhas, temos 2 opções para o não-fixpoint (escolher em qual dos dois fixpoints vamos mandá-lo). Pelo Princípio da multiplicação (5.3) então temos $3 \cdot 2 = 6$ funções no F_2.
Quantas funções no F_3? Apenas uma: a identidade.

Finalmente podemos responder: existem $3 + 6 + 1 = 10$ funções idempotentes num conjunto de cardinalidade 3.

x9.54S. Vamos demonstrar a implicação. Suponha que $f : A \to A$ é constante. Caso $A = \emptyset$ a f é a função vazia e a $f \circ f$ também. Caso $A \neq \emptyset$, usamos a definição alternativa da Exercício x9.48. Seja $c \in A$ tal que para todo $x \in A$, $f(x) = c$ (1). Queremos mostrar que $f \circ f = f$, ou seja, que para todo $a \in A$,

$$(f \circ f)(a) = f(a)$$

(definição de igualdade de funções D9.28). Calculamos no lado esquerdo:

$$\begin{aligned} (f \circ f)(a) &= f(f(a)) && \text{(def. } (\circ)) \\ &= f(c) && \text{(pelo (1), com } x := a) \\ &= c && \text{(pelo (1), com } x := c) \end{aligned}$$

e no lado direito:

$$f(a) = c. \qquad \text{(pelo (1), com } x := a)$$

Logo, $f \circ f = f$ como desejamos.

Alternativamente, podemos nos livrar dum passo no calculo do lado esquerdo assim:

$$\begin{aligned} (f \circ f)(a) &= f(f(a)) && \text{(def. } (\circ)) \\ &= c. && \text{(pelo (1), com } x := f(a)) \end{aligned}$$

x9.56S. Temos $\chi_A : X \to \{0,1\}$. Como a composição $\chi_A \circ \chi_A$ é definida, concluimos que $\text{cod}(\chi_A) = \text{dom}(\chi_A)$. Ou seja, $X = \{0,1\}$.

O A sendo um subconjunto de $\{0,1\}$ so tem 4 possibilidades:

$$A=\emptyset; \qquad A=\{0\}; \qquad A=\{1\}; \qquad A=\{0,1\}=X.$$

Calculamos em todos os casos:

$$\begin{aligned}
A=\emptyset &\implies \begin{cases}(\chi_A\circ\chi_A)(0)=\chi_A(\chi_A(0))=0\\(\chi_A\circ\chi_A)(1)=\chi_A(\chi_A(1))=0\end{cases}\\
A=\{0\} &\implies \begin{cases}(\chi_A\circ\chi_A)(0)=\chi_A(\chi_A(0))=\chi_A(1)=0\\(\chi_A\circ\chi_A)(1)=\chi_A(\chi_A(1))=\chi_A(0)=1\end{cases}\\
A=\{1\} &\implies \begin{cases}(\chi_A\circ\chi_A)(0)=\chi_A(\chi_A(0))=\chi_A(0)=0\\(\chi_A\circ\chi_A)(1)=\chi_A(\chi_A(1))=\chi_A(1)=1\end{cases}\\
A=X &\implies \begin{cases}(\chi_A\circ\chi_A)(0)=\chi_A(\chi_A(0))=1\\(\chi_A\circ\chi_A)(1)=\chi_A(\chi_A(1))=1\,.\end{cases}
\end{aligned}$$

Sobre a $\chi_A\circ\chi_A$ então concluimos que se A é um dos singletons $\{0\}$ ou $\{1\}$ então ela é a identidade. Caso contrário, ela é uma constante: se $A=\emptyset$, a constante 0; se $A=X$, a constante 1.

x9.57S. $f\restriction X : X\to B$.

x9.58S. $f\restriction X = \imath_{X\hookrightarrow A}\circ f$.

x9.59S. Pelo menos um tal $x\in A$ existe, pois a f é sobrejetora. E como f é injetora, existe no máximo um. Demonstramos assim a unicidade, algo que nos permite *definir a função* no jeito que definimos na Definição D9.162.

x9.61S. Pelo Exercício x9.60 temos que f^{-1} é bijetora, então sua inversa $\left(f^{-1}\right)^{-1}$ é definida sim (e pelo Exercício x9.60 de novo ela é bijetora também). As f e $\left(f^{-1}\right)^{-1}$ têm domínios e codomínios iguais. Basta verificar que concordam em todo o seu domínio. Seja $x\in\operatorname{dom} f$ então. Calculamos

$$\begin{aligned}
\left(f^{-1}\right)^{-1}(x)=f(x) &\iff f^{-1}(f(x))=x && (\text{def. } (f^{-1})^{-1})\\
&\iff f(x)=f(x) && (\text{def. } f^{-1})
\end{aligned}$$

e a última igualdade é trivialmente válida, e logo $\left(f^{-1}\right)^{-1}=f$.

x9.62S. Seja $a\in A$ e $b\in B$. Calculamos:

$$\begin{aligned}
f^{-1}(f(a)) &= \text{aquele } x\in A \text{ que } f(x)=f(a)\\
&= a. && (f \text{ inj.})
\end{aligned}$$

Agora tomando $y\in B$ calculamos a outra numa maneira diferente:

$$\begin{aligned}
f(f^{-1}(b))=y &\iff f^{-1}(b)=f^{-1}(y)\\
&\iff b=y && (f^{-1} \text{ inj. (x9.60)})\\
&\iff \mathrm{id}_B(b)=y.
\end{aligned}$$

x9.63S. Temos $\mathrm{id}_A, {\mathrm{id}_A}^{-1} : A \rightarrowtail A$ então basta verificar que comportam igualmente.
Jeito 1. Seja $a \in A$ então e calculamos:

$$\begin{aligned} {\mathrm{id}_A}^{-1} a &= \text{aquele } v \in A \text{ que } \mathrm{id}_A v = a && (\text{def. } {\mathrm{id}_A}^{-1}) \\ &= a && (\text{def. } \mathrm{id}_A) \\ &= \mathrm{id}_A a. && (\text{def. } \mathrm{id}_A) \end{aligned}$$

Jeito 2. Sejam $a, a' \in A$. Calculamos:

$$\begin{aligned} {\mathrm{id}_A}^{-1} a = v &\iff a = \mathrm{id}_A v && (\text{def. } {\mathrm{id}_A}^{-1}) \\ &\iff a = v && (\text{def. } \mathrm{id}_A) \\ &\iff \mathrm{id}_A a = v. && (\text{def. } \mathrm{id}_A) \end{aligned}$$

x9.64S. Vamos demonstrar que

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Tome $x \in C$ e $z \in A$. Basta demonstrar que

$$(g \circ f)^{-1}(x) = z \iff \big(f^{-1} \circ g^{-1}\big)(x) = z.$$

pois isso quis dizer que as duas funções concordam em todo o seu domínio. Calculamos:

$$\begin{aligned} (g \circ f)^{-1}(x) = z &\iff x = (g \circ f)(z) && (\text{def. } (g \circ f)^{-1}) \\ &\iff x = g(f(z)) && (\text{def. } g \circ f) \\ &\iff g^{-1}(x) = f(z) && (\text{def. } g^{-1}) \\ &\iff f^{-1}\big(g^{-1}(x)\big) = z && (\text{def. } f^{-1}) \\ &\iff \big(f^{-1} \circ g^{-1}\big)(x) = z. && (\text{def. } f^{-1} \circ g^{-1}) \end{aligned}$$

x9.65S. Sejam $b \in B$, $a \in A$. Caso que f' satisfaz a (L) calculamos:

$$\begin{aligned} f^{-1} b = a &\iff b = fa && (\text{def. } f^{-1}) \\ &\iff f'b = f'(fa) && (f' \text{ inj.}) \\ &\iff f'b = (f'f)\, a && (\text{def. } (f'f)) \\ &\iff f'b = a. && ((\text{L}) \text{ da } f' \ (\text{com } w := a)) \end{aligned}$$

E caso que f' satisfaz a (R):

$$\begin{aligned} f'b = a &\iff f(f'b) = fa && (f \text{ inj.}) \\ &\iff (ff')\, b = fa && (\text{def. } (ff')) \\ &\iff b = fa && ((\text{R}) \text{ da } f' \ (\text{com } w := b)) \\ &\iff f^{-1} b = a. && (\text{def. } f^{-1}) \end{aligned}$$

x9.66S.

$$\begin{aligned} f[-] &: \wp A \to \wp B \\ f_{-1}[-] &: \wp B \to \wp A. \end{aligned}$$

x9.67S. As duas afirmações seguem diretamente pelas definições:

$$f[\emptyset] = \{\, f(a) \mid a \in \emptyset \,\} = \emptyset$$
$$f_{-1}[\emptyset] = \{\, x \in X \mid f(x) \in \emptyset \,\} = \emptyset.$$

x9.68S. Sejam $A = \{1, 7, \{1, 7\}\}$, e $X = \{1, 7\}$. Observe que $X \in A$ e $X \subseteq A$. Seja $f : A \to \{3\}$ a função constante definida pela $f(x) = 3$. Assim a notação $f(X)$ fica ambígua: a f-imagem de $X \subseteq A$ é o $\{3\}$, mas o valor da f no X é o 3. E $3 \neq \{3\}$!

x9.69S. Não! O símbolo $f^{-1}(y)$ nem é definido no caso geral: o definimos *apenas para funções bijetoras*.

x9.70S. Caso $f_{-1}[Y] = \emptyset$, necessariamente $Y = \emptyset$ também (pois f é sobrejetora) e logo

$$\{\, f^{-1}(y) \mid y \in Y \,\} = \emptyset$$

também. Caso contrário, mostramos as duas direções separadamente:

($\subseteq$): Seja $x \in f_{-1}[Y]$ e logo seja $y_x \in Y$ tal que $f(x) = y_x$ (pela def. $f_{-1}[Y]$). Logo $x = f^{-1}(y_x)$ pela definição da função inversa (D9.162), ou seja $x \in \{\, f^{-1}(y) \mid y \in Y \,\}$.

($\supseteq$): É só seguir os passos da ($\subseteq$) em reverso.

x9.71S. Se f é bijetora, o símbolo $f_{-1}[Y]$ pode ter duas interpretações diferentes:

$$f_{-1}[Y] \stackrel{?}{=} \begin{cases} (f)_{-1}[Y] & \text{a preimagem de } Y \text{ através da função } f \\ \ldots \text{ou} \ldots & \\ (f^{-1})[Y] & \text{a imagem de } Y \text{ através da função } f^{-1} \end{cases}$$

onde usamos cores e parenteses para enfatizar o "parsing" diferente de cada interpretação. Observe que a segunda alternativa não é possível quando f não é bijetora, pois a função f^{-1} nem é definida nesse caso!

x9.72S. Seja $f : A \rightarrowtail B$. Introduzimos temporariamente a notação

$$f_{-1}[Y] \stackrel{\text{def}}{=} \text{a } f\text{-preimagem de } Y.$$

Com essa notação precisamos demonstrar que

$$\text{para todo } Y \subseteq B, \quad f^{-1}[Y] = f_{-1}[Y]$$

Seja $Y \subseteq B$.

($\subseteq$). Seja $x \in f^{-1}[Y]$ (1). Para mostrar que $x \in f_{-1}[Y]$ basta verificar que $f(x) \in Y$ (1). Seja $y_x \in Y$ tal que $f^{-1}y_x = x$ (pela (1)). Logo $y_x = f(x)$ pela definição de f^{-1} e logo pertence ao Y pela (2).

($\supseteq$). Seja $x \in f_{-1}[Y]$ (1). Como $fx \in Y$ (pelo (1)) e $fx \xmapsto{f^{-1}} x$ (pela definição da f^{-1}), logo $x \in f^{-1}[Y]$.

x9.73S. Verdade:

$$f[\{x\}] = \{\, f(z) \mid z \in \{x\} \,\} = \{f(x)\}\,.$$

x9.75S. ($\Rightarrow$): Suponha que f bijetora, e seja $b \in B$. Vou demonstrar que $f_{-1}[\{b\}]$ é unitário. Vamos chamá-lo de A_b. Como f é sobrejetora, logo seja $a_b \in A$ tal que $f(a_b) = b$. Logo $a_b \in A_b$ pela definição da preimagem, e logo $A_b \neq \emptyset$ (pois tem pelo menos um membro). Basta mostrar que tem no máximo um membro. Sejam $a, a' \in A_b$ então e vamos mostrar que $a = a'$. Pela escolha dos a, a', temos $f(a) = f(a') = b$; e agora pela injectividade da f temos o desejado $a = a'$.

($\Leftarrow$). Suponha que para todo $b \in B$, o $f_{-1}[\{b\}]$ é unitário. Preciso mostrar que f é injetora e sobrejetora.

f INJETORA: Suponha que temos $x, y \in A$ tais que $f(x) = f(y)$ e chame esse valor comum de b. Basta demonstrar que $x = y$. Pela hipótese, o $f_{-1}[\{b\}]$ é unitário, e pela escolha dos x, y sabemos que x, y pertencem a ele. Logo $x = y$.

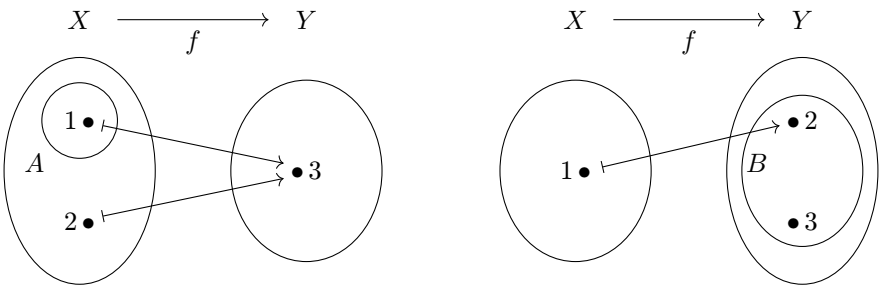
f SOBREJETORA: Seja $b \in B$. Procuramos $a \in A$ tal que $f(a) = b$. Pela hipótese, o conjunto $f_{-1}[\{b\}]$ é unitário (e logo não vazio). Tome a o (único) membro desse conjunto e observe que pela definição de preimagem temos que $f(a) = b$.

x9.76S. Vamos demonstrar as duas afirmações.

DEMONSTRAÇÃO DE $A \subseteq f_{-1}[f[A]]$. Suponha $a \in A$. Logo $f(a) \in f[A]$ pela definição da função-imagem, e logo $a \in f_{-1}[f[A]]$ pela definição da função-preimagem.

DEMONSTRAÇÃO DE $B \supseteq f[f_{-1}[B]]$. Suponha $y_0 \in f[f_{-1}[B]]$. Logo tome $x_0 \in f_{-1}[B]$ tal que $y_0 = f(x_0)$ (1). Pela definição da função-preimagem $f(x_0) \in B$, e agora pela (1) temos $y_0 \in B$.

x9.77S. Mostramos dois contraexemplos, um para cada afirmação.



No primeiro contraexemplo temos: $A = \{1\}$; $f[A] = \{3\}$; e $f_{-1}[\{3\}] = \{1, 2\}$. Logo

$$A = \{1\} \neq \{1, 2\} = f_{-1}[f[A]].$$

No segundo contraexemplo temos: $B = \{2, 3\}$; $f_{-1}[B] = \{1\}$; e $f[\{1\}] = \{2\}$. Logo

$$B = \{2, 3\} \neq \{2\} = f[f_{-1}[B]].$$

x9.78S. Temos duas implicações para demonstrar.

IDA DA (I). Suponha que f é injetora, e seja $A \subseteq X$. Já temos a

$$A \subseteq f_{-1}[f[A]]$$

pelo Exercício x9.76, então basta mostrar

$$f_{-1}[f[A]] \subseteq A.$$

Tome então $x_0 \in f_{-1}[f[A]]$. Logo $f(x_0) \in f[A]$. Logo $f(a) = f(x_0)$ para algum $a \in A$ (pela definição da função-imagem). Mas f é injetora, então $a = x_0$ e logo $x_0 \in A$.

Ida da (ii). Suponha que f é sobrejetora, e seja $Y \subseteq B$. Já temos a

$$f[f_{-1}[B]] \subseteq B$$

pelo Exercício x9.76, então basta mostrar

$$B \subseteq f[f_{-1}[B]]$$

Tome então $b \in B$. Agora seja $x_b \in X$ tal que $f(x_b) = b$ (pois f é sobrejetora). Então $x_b \in f_{-1}[B]$. Logo $f(x_b) \in f[f_{-1}[B]]$. Logo $b \in f[f_{-1}[B]]$.

x9.79S. Vamos primeiramente demonstrar a $f[A \cup B] = f[A] \cup f[B]$. ($\subseteq$): Tome $y \in f[A \cup B]$. Logo seja $x \in A \cup B$ tal que $f(x) = y$. Caso $x \in A$, temos $f(x) \in f[A]$ e logo $f(x)$ pertence na união $f[A] \cup f[B]$. Caso $x \in B$, concluímos similarmente que $f(x) \in f[B] \subseteq f[A] \cup f[B]$. ($\supseteq$): Tome $y \in f[A] \cup f[B]$. Caso $y \in f[A]$, seja $a \in A$ tal que $f(a) = y$. Mas $a \in A \cup B$, logo $y \in f[A \cup B]$. O caso $y \in f[B]$ é similar.

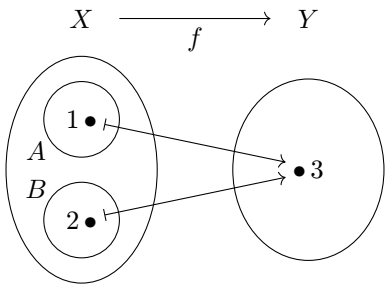
Vamos demonstrar a $f[A \cap B] \subseteq f[A] \cap f[B]$ agora. Tome $y \in f[A \cap B]$ e seja $d \in A \cap B$ tal que $f(d) = y$. Mas $d \in A$ e $d \in B$, ou seja $y \in f[A]$ e $y \in f[B]$, e logo $y \in f[A] \cap f[B]$.

Vamos demonstrar a $f[A \setminus B] \supseteq f[A] \setminus f[B]$ agora. Tome $y \in f[A] \setminus f[B]$ então, ou seja $y \in f[A]$ e $y \notin f[B]$. Traduzindo:

$$(\exists a \in A)[\, f(a) = y \,] \qquad \& \qquad (\forall b \in B)[\, f(b) \neq y \,].$$

Usando a primeira afirmação abaixo tome $a \in A$ tal que $f(a) = y$, e observe que graças à segunda, $a \notin B$. Logo $a \in A \setminus B$, e chegamos no desejado $y \in f[A \setminus B]$.

Finalmente, usamos apenas um contraexemplo para refutar simultaneamente as duas inclusões que são inválidas no caso geral:

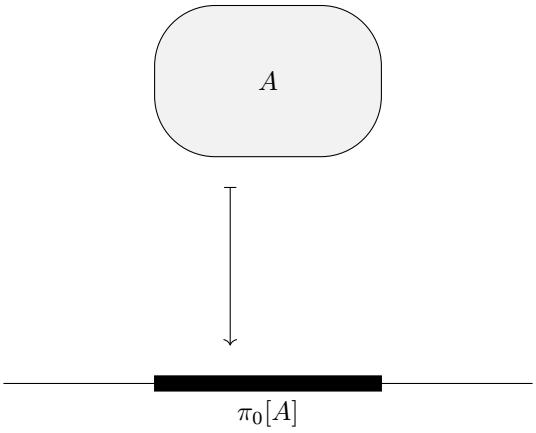


Calculamos para verificar:

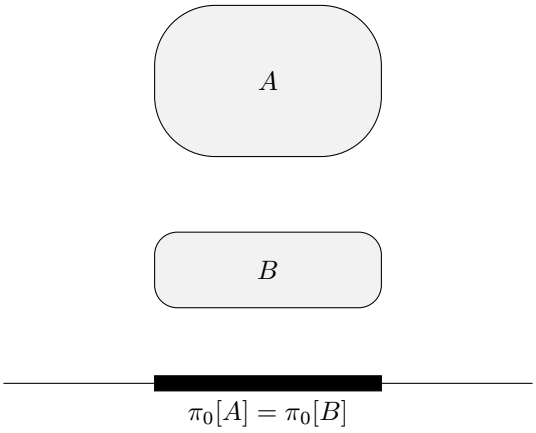
$$f[A \cap B] = f[\emptyset] = \emptyset \qquad f[A \setminus B] = f[A] = \{3\}$$
$$f[A] \cap f[B] = \{3\} \cap \{3\} = \{3\} \qquad f[A] \setminus f[B] = \{3\} \setminus \{3\} = \emptyset.$$

Um contraexemplo mais pictorial seria considerar uma função f que mapeia pontos do plano $\mathbb{R}^2$ para pontos da reta $\mathbb{R}$, mandando cada entrada $\langle x, y \rangle$ para sua "sombra" x. Já

conhecemos essa função: é a primeira projecção: $f = \pi_0$. Observe que a $\pi_0[-]$ manda cada subconjunto de $\mathbb{R}^2$ para sua "sombra":



Para achar o contraexemplo agora, basta só escolher dois subconjuntos de $\mathbb{R}^2$ como esses:



Verifique que isso é um contraexemplo que refuta as duas igualdades que queremos refutar.

x9.80S. Já demonstramos metade de cada igualdade no Exercício x9.79 para qualquer função, então para nossa injetora f também. Basta então demonstrar as duas inclusões:

$$f[A \cap B] \supseteq f[A] \cap f[B]$$
$$f[A \setminus B] \subseteq f[A] \setminus f[B].$$

DEMONSTRAÇÃO DE $f[A \cap B] \supseteq f[A] \cap f[B]$: Suponha $y \in f[A] \cap f[B]$. Logo $y \in f[A]$ e $y \in f[B]$. Tome então $a \in A$ tal que $f(a) = y$ e $b \in B$ tal que $f(b) = y$. Juntando as duas igualdades temos $f(a) = f(b)$. Mas f é injetora, e logo $a = b$. Ou seja, $a \in A \cap B$, e chegamos no desejado $y \in f[A \cap B]$.
DEMONSTRAÇÃO DE $f[A \setminus B] \subseteq f[A] \setminus f[B]$: Suponha $y \in f[A \setminus B]$. Tome então $a_0 \in A \setminus B$ tal que $f(a_0) = y$. Logo $a_0 \in A$ e $a_0 \notin B$. Já sabemos então que $y \in f[A]$. Agora usamos a injectividade da f para demonstrar que $y \notin f[B]$. Se y fosse um membro de $f[B]$, existiria $b \in B$ com $f(b) = y$. Mas já temos o único (f injetora) membro do domínio X que f mapeia no y, o a_0, e sabemos que $a_0 \notin B$! Logo $y \notin f[B]$ e chegamos no $y \in f[A] \setminus f[B]$.

x9.82S. Temos:

$$\begin{aligned} f &= \text{inverse} \circ \mathit{squareRoot} \circ \mathit{succ} \circ \text{square} \circ \mathit{succ} \\ g &= \mathit{succ} \circ \text{square} \circ \mathit{outl} \\ h &= \mathit{succ} \circ \text{double} \circ + \\ k &= \mathit{succ} \circ \text{double} \circ + \circ \mathit{doubleHeight}. \end{aligned}$$

A definição de cada função-fator que aparece na direita deve ser óbvia pelo próprio nome, exceto talvez da *doubleHeight*. (Tá vendo como é bom escolher nomes bons?) Definimos a $\mathit{doubleHeight} : \mathbb{N}^2 \to \mathbb{N}$ pela $\mathit{doubleHeight}(x, y) = (x, 2y)$. Observe também que a *succ* da primeira linha é diferente da *succ* das outras, por causa do seu tipo. Mesma coisa sobre a square. Teria sido melhor usar $\mathit{succ}_{\mathbb{Q}}$ para diferenciá-la mas escolhi deixar pra lá essa decoração e todo o resto da informação de tipos dos componentes intermediários contando que tu consegues inferir cada domínio e cada codomínio envolvido. Espero que tu achou a resolução de k meio "meh", por causa dessa bizarra (muito *ad hoc*) função *doubleHeight* que talvez até "forcei a barra" para nomeá-la. Se preocupe não: como avisei na dica, daqui a pouco (§214) vamos ver como resolver isso numa maneira bem legal mesmo. Por enquanto, podemos melhorar a resolução assim:

$$k = h \circ \mathit{doubleHeight}$$

que com certeza é mais elegante, já que

$$k = \underbrace{(\mathit{succ} \circ \text{double} \circ +)}_{h} \circ \mathit{doubleHeight}.$$

x9.83S. Temos as funções

$$\mathbb{N} \xrightarrow{\Delta} \mathbb{N} \times \mathbb{N} \xrightarrow{\cdot} \mathbb{N} \xrightarrow{\Delta} \mathbb{N} \times \mathbb{N} \xrightarrow{+} \mathbb{N}.$$

Assim defino

$$f = (+ \circ \Delta_{\mathbb{N}} \circ \cdot \circ \Delta_{\mathbb{N}}) : \mathbb{N} \to \mathbb{N}$$

e tomando um $x \in \mathbb{N}$ confirmo:

$$\begin{aligned} f(x) &= (+ \circ \Delta \circ \cdot \circ \Delta)(x) && \text{(def. } f\text{)} \\ &= +(\Delta(\cdot(\Delta(x)))) && \text{(def. } \circ\text{)} \\ &= +(\Delta(\cdot(x, x))) && \text{(def. } \Delta\text{)} \\ &= +(\Delta(x^2)) \\ &= +(x^2, x^2) && \text{(def. } \Delta\text{)} \\ &= x^2 + x^2 \\ &= 2x^2. \end{aligned}$$

x9.84S. A configuração na esquerda implica as equações na direita:

(F-Inv) $$A \overset{f}{\rightarrowtail\!\!\!\!\twoheadrightarrow} B \implies \begin{cases} f^{-1} \circ f = \mathrm{id}_A \\ f \circ f^{-1} = \mathrm{id}_B \end{cases}$$

Π9.2S. Seja $n \in \mathbb{N}$. A $succ^n : \mathbb{N} \to \mathbb{N}$ é a função definida pela

$$succ^n(x) = x + n.$$

Basta demonstrar que para todo $n \in \mathbb{N}$

$$(\forall x \in \mathbb{N})[\, succ^n(x) = x + n \,]$$

algo que vou demonstrar por indução no n.
Base. Seja $x \in \mathbb{N}$. Calculamos:

$$\begin{aligned} succ^0(x) &= \mathrm{id}_{\mathbb{N}}(x) && \text{(pela def. da } succ^0\text{)} \\ &= x && \text{(pela def. da } 1_A\text{)} \\ &= x + 0. && \text{(pelo ensino fundamental)} \end{aligned}$$

Passo indutivo. Suponha $k \in \mathbb{N}$ tal que

$$(\text{H.I.}) \qquad (\forall x \in \mathbb{N})\big[\, succ^k(x) = x + k \,\big].$$

Basta demonstrar que

$$(\forall y \in \mathbb{N})\big[\, succ^{k+1}(y) = y + (k+1) \,\big].$$

Seja $y \in \mathbb{N}$ então. Calculamos:

$$\begin{aligned} succ^{k+1}(y) &= \big(succ \circ succ^k\big)(y) && \text{(pela def. de } succ^{k+1}\text{)} \\ &= succ\big(succ^k(y)\big) && \text{(pela def. de } succ \circ succ^k\text{)} \\ &= succ(y + k) && \text{(pela HI com } x := y\text{)} \\ &= (y + k) + 1 && \text{(pela def. de } succ\text{)} \\ &= y + (k + 1). && \text{(pelo ensino fundamental)} \end{aligned}$$

Π9.3S. *Quase* nada! Parece ser redundante, pois a definição é aplicável numa *função* e graças à determinabilidade sabemos que se existe, tem que ser único—mas! Vamos tentar demonstrar para achar algo interessante.

Suponha que temos $b, b' \in B$ que satisfazem a condição, ou seja, temos:

$$\begin{aligned} &\text{para todo } x \in A, f(x) = b \\ &\text{para todo } x \in A, f(x) = b' \end{aligned}$$

Logo tomando um $x \in A$, temos

$$b = f(x) = b',$$

ou seja, unicidade mesmo desse b, dado qualquer $x \in A$. Mas isso é, supondo que $A \neq \emptyset$. O que acontece se $A = \emptyset$ e $B \neq \emptyset$? Botando esse "único" na definição, uma função

$$\emptyset \xrightarrow{\ f\ } B$$

vai ser constante com valor b sse B é um singleton e b é seu único membro. Sem o "único", ela vai ser constante sse $B \neq \emptyset$. Veja também o exercício

Π9.4S. (1) f NÃO É INJETORA pois

$$f(1) = 2 = f(1, 0).$$

(2) f É SOBREJETORA. Seja $y \in \mathbb{N}_{>0}$. Pelo teorema fundamental de aritmética Θ3.140 y pode ser escrito como produtório de primos

$$y = q_0^{y_i}$$

(3) ACONTECE que ganha injectividade (veja o Problema Π3.26 e sua resolução) e perde sobrejectividade: nenhuma entrada é mapeada para o 3, pois o único ímpar que realmente está no range f é o 1 ($f() = 1$ pela definição do produtório vazio); todos os outros pontos do domínio da f são múltiplos de 2 pela sua definição. Observe que tem números pares que faltam também, por exemplo o

$$10 = 2^1 \cdot 3^0 \cdot 5^1.$$

Π9.5S. Sejam

$$\begin{aligned} C &= \text{range}(f) \\ e &= \lambda x \,.\, fx : A \to C \\ m &= \imath : C \hookrightarrow B \end{aligned}$$

Basta demonstrar que $f = m \circ e$. Seja $x \in A$. Calculamos:

$$\begin{aligned} (m \circ e)x &= m(ex) && \text{(def. } m \circ e\text{)} \\ &= m(fx) && \text{(def. } e\text{)} \\ &= fx. && \text{(def. } m\text{)} \end{aligned}$$

Π9.6S. A parte do problema sobre a $f : A \rightarrowtail \wp A$ foi resolvida no Exercício x9.10, onde definimos a $f : A \to \wp A$ pela $f(x) = \{x\}$ e demonstramos as (i)–(ii).

Fixe $a_0 \in A$ ($A \neq \emptyset$) e defina a $g : \wp A \to A$ pela

$$g(X) = \begin{cases} x, & \text{se } X \text{ é o singleton } \{x\} \\ a_0, & \text{caso contrário.} \end{cases}$$

(iii) A g É SOBREJETORA. Seja $y \in A$. Observe que $g(\{y\}) = y$. Como $\{y\} \in \wp A$, temos que g é sobrejetora.

(iv) A g NÃO É INJETORA. Observe que $\emptyset, \{a_0\} \in \wp A$ e que $\emptyset \neq \{a_0\}$, mas mesmo assim $g(\emptyset) = a_0 = g(\{a_0\})$. Logo, g não é injetora.

PARA RESPONDER NA PERGUNTA NÃO RETÓRICA precisamos *demonstrar* que não existe nenhuma função $A \rightarrowtail \wp A$ e nenhuma função $\wp A \rightarrowtail A$. Na verdade basta apenas demonstrar apenas uma das duas afirmações, pois quando temos uma função bijetora de A para $\wp A$ também temos "de graça" uma bijetora de $\wp A$ para A: sua inversa. Mas como conseguimos então *demonstrar* que não existe bijecção entre o A e o $\wp A$? Isso eu vou te deixar pensar. Mas te aviso: é algo *muito difícil de pensar*. (Seria fácil se tivermos que A é finito, mas pode ser que não é.) Mas dê uma chance nele! E não se preocupe: no Capítulo 13 estudamos umas idéias de Cantor; foi ele que se perguntou sobre isso, e foi ele que deu a resposta mesmo (teorema de Cantor Θ13.51, §285). As conseqüências do seu teorema são... Brutais! Paciência.

Π9.7S. Injectividade. A injectividade da π depende no n:
Caso $n > 1$, não é: pois tomando $a \in A$,

$$\pi(0, \langle a, \ldots, a\rangle) = a = \pi(1, \langle a, \ldots, a\rangle).$$

Caso $n = 1$, é: tomando $w, w' \in I \times A^n$ com $w \neq w'$, temos que $w = \langle 0, \langle a\rangle\rangle$ e $w' = \langle 0, \langle a'\rangle\rangle$ para alguns $a, a' \in A$. Agora como $w \neq w'$ concluimos que $a \neq a'$ e logo $\pi(0, w) \neq \pi(0, w')$, ou seja, π é injetora nesse caso.
Sobrejectividade. A π é sobrejetora sim: pois para qualquer $a \in A$, $\pi(0, \langle a, \ldots, a\rangle) = a$.

Π9.8S. Já demonstrou as idas no x9.78. Vamos demonstrar as voltas.
Volta da (1). Suponha a hipótese:

$$\text{para todo } A \subseteq X,\ A = f_{-1}[f[A]].$$

Para mostrar que f é injetora, suponha que $x, x' \in X$ tais que $f(x) = f(x')$. Basta verificar que $x = x'$. Considere o conjunto $A = \{x\}$. Observe que $A \subseteq X$, e logo pela hipótese temos

$$A = f_{-1}[f[A]]. \tag{A}$$

Temos $f(x) \in f[A]$ pela definição da função-imagem. Como $f(x') = f(x)$ temos também $f(x') \in f[A]$. Logo

$$x, x' \in f_{-1}[f[A]] \overset{\text{A}}{=} A = \{x\}\,.$$

Como $x, x' \in \{x\}$, logo $x = x'$.
Volta da (2). Suponha a hipótese:

$$\text{para todo } B \subseteq Y,\ B = f[f_{-1}[B]].$$

Tome $y_0 \in Y$. Para mostrar que f é sobrejetora basta mostrar que $f_{-1}[\{y_0\}] \neq \emptyset$. Considere o

$$B = \{y_0\} \subseteq Y$$

e logo pela hipótese temos

$$B = f[f_{-1}[B]]. \tag{B}$$

Ou seja, $f_{-1}[B] \neq \emptyset$ (caso contrário teriamos

$$B \overset{\text{B}}{=} f[f_{-1}[B]] = f[\emptyset] = \emptyset$$

que é absurdo pois $B = \{y_0\}$). Isso mostra que f é sobrejetora.

Π9.9S. (1): Demonstramos cada direção separadamente. ($\subseteq$): Seja $b \in f\big[\bigcup_{i\in\mathcal{I}} A_i\big]$. Seja $a \in \bigcup_{i\in\mathcal{I}} A_i$ tal que $f(a) = b$ (1) (pela definição de função-imagem). Agora tome $i \in \mathcal{I}$ tal que $a \in A_i$ (2). Agora pelas (1),(2) temos que $b \in f[A_i]$. Ou seja, $b \in \bigcup_{i\in\mathcal{I}} f[A_i]$. ($\supseteq$): Seja $b \in \bigcup_{i\in\mathcal{I}} f[A_i]$. Seja $i \in \mathcal{I}$ tal que $b \in f[A_i]$. Tome $a \in A_i$ tal que $f(a) = b$ (1). Como $a \in A_i$, logo $a \in \bigcup_{i\in\mathcal{I}} A_i$ e agora pela (1) ganhamos $b \in f\big[\bigcup_{i\in\mathcal{I}} A_i\big]$.
(2): Demonstramos primeiramente a ($\subseteq$) que é válida para toda f, e mostramos que se f é injetora, a ($\supseteq$) também é válida. ($\subseteq$): Seja $b \in f\big[\bigcap_{i\in\mathcal{I}} A_i\big]$. Logo tome $a \in \bigcap_{i\in\mathcal{I}} A_i$ (1)

tal que $f(a) = b$ [(2)]. Agora, como a pertence a todos os A_i's e $f(a) = b$, então para cada $i \in \mathcal{I}$, $b \in f[A_i]$. Ou seja, b pertence a todos os $f[A_i]$'s. Chegamos então no desejado $b \in \bigcap_{i\in\mathcal{I}} f[A_i]$.

($\supseteq$): Para essa direção vamos supor que f é injetora. Tome $b \in \bigcap_{i\in\mathcal{I}} f[A_i]$, ou seja b pertence a todos os $f[A_i]$'s. Ou seja, para cada um dos A_i's, existe $a_i \in A_i$ tal que $f(a_i) = b$. Mas a f é injetora, então todos esses a_i's são iguais; seja a então esse membro comum dos A_i's. Temos então que: $a \in \bigcap_{i\in\mathcal{I}} A_i$ e $f(a) = b$. Ou seja, $b \in f\big[\bigcap_{i\in\mathcal{I}} A_i\big]$.

(3): Calculamos:

$$\begin{aligned}
a \in f_{-1}\Big[\bigcup_{j\in\mathcal{J}} B_j\Big] &\iff f(a) \in \bigcup_{j\in\mathcal{J}} B_j && (\text{def. } f_{-1}\Big[\bigcup_{j\in\mathcal{J}} B_j\Big]) \\
&\iff (\exists j \in \mathcal{J})[\, f(a) \in B_j \,] && (\text{def. } \bigcup_{j\in\mathcal{J}} B_j) \\
&\iff (\exists j \in \mathcal{J})[\, a \in f_{-1}[B_j] \,] && (\text{def. } f_{-1}[B_j]) \\
&\iff a \in \bigcup_{j\in\mathcal{J}} f_{-1}[B_j]. && (\text{def. } \bigcup_{j\in\mathcal{J}} f_{-1}[B_j])
\end{aligned}$$

Ou seja, $f_{-1}\Big[\bigcup_{j\in\mathcal{J}} B_j\Big] = \bigcup_{j\in\mathcal{J}} f_{-1}[B_j]$.

(4): ($\subseteq$): Seja $a \in f_{-1}\big[\bigcap_{i\in\mathcal{J}}^{\infty} B_j\big]$. Logo $f(a) \in \bigcap_{i\in\mathcal{J}}^{\infty} B_j$, ou seja, para todo $i \in \mathcal{J}$, $f(a) \in B_j$. Logo $a \in f_{-1}[B_j]$ para todo $i \in \mathcal{J}$, ou seja, $a \in \bigcap_{i\in\mathcal{J}}^{\infty} f_{-1}[B_j]$. ($\supseteq$). Similar: é só seguir os passos da ($\subseteq$) em reverso.

Π9.10S. Um primeiro problema é esse "lógica" que aparece várias vezes como suposta justificativa de passos. Já que todos os passos que fazemos numa demonstração supostamente são logicamente válidos, não faz sentido pensar que decorando um tal passo com a palavrinha "lógica" pode convencer alguém sobre algo.

O problema aqui é com a direção ($\Leftarrow$) da $\overset{6}{\iff}$:

$$\cdots \iff \exists a \forall n (a \in A_n \wedge f(a) = b) \overset{6}{\iff} \forall n \exists a (a \in A_n \wedge f(a) = b) \qquad (\text{lógica})$$

Saber que *existe a tal que para todo n algo* $P(a, n)$ *acontece* é uma afirmação bem mais forte do que saber que *para todo n existe algum a tal que* $P(a, n)$ *acontece*. Na primeira temos pelo menos um a que serve para todo n, mas na segunda pode ser que para cada n, o a "que serve" é diferente. Para enfatizar essa dependência podemos escrever: *para todo n existe algum* a_n *tal que* $P(a_n, n)$. É por isso que a ida é válida mas a vólta, em geral, não é. Compare com o Exercício x9.51.

Π9.11S. Ambas as direcções são válidas.

($\Rightarrow$): Suponha f sobrejetora e sejam Y, Y' no $\mathrm{dom}(f_{-1}[-])$ tais que $Y \neq Y'$. (Temos então $Y, Y' \subseteq B$.) Basta demonstrar que $f_{-1}[Y] \neq f_{-1}[Y']$. Como $Y \neq Y'$, sem perda de generalidade, seja $d \in Y \setminus Y'$. Como f é sobrejetora, seja $a_d \in A$ tal que $f(a_d) = d$. Observe que $f(a_d) \in Y$ e que $f(a_d) \notin Y'$. Logo $a_d \in f_{-1}[Y]$ e $a_d \notin f_{-1}[Y']$, pela definição da $f_{-1}[-]$. Logo $f_{-1}[Y] \neq f_{-1}[Y]'$.

($\Leftarrow$): Vou demonstrar a contrapositiva da afirmação. Suponha então que f não é sobrejetora. Vou demonstrar que $f_{-1}[-]$ não é injetora. Basta então achar dois membros distintos no seu domínio mapeados no mesmo objeto. Como f não é sobrejetora, seja $t \in B$ tal que $t \notin \mathrm{range}(f)$, ou seja, tal que para todo $a \in A$, $f(a) \neq t$. Agora considere os: $\emptyset$ e $\{t\}$. Ambos são subconjuntos de B, e eles são distintos, mas mesmo assim

$$f_{-1}[\emptyset] = \emptyset = f_{-1}[\{t\}].$$

Ou seja, a $f_{-1}[-]$ não é injetora.

Π9.13S. Eu vou demonstrar que

$$\bigcap_{n=0}^{\infty} succ^n[\mathbb{N}] = \emptyset.$$

Para chegar num absurdo, suponha que $w \in \bigcap_{n=0}^{\infty} succ^n[\mathbb{N}]$. Logo, para todo $n \in \mathbb{N}$, $w \in succ^n[\mathbb{N}]$. Logo, para todo $n \in \mathbb{N}$, existe $m \in \mathbb{N}$ tal que $succ^n(m) = w$. Mas $succ^n(m) = n+m$ (Problema Π9.2). Ou seja:

$$\text{para todo } n \in \mathbb{N}, \text{ existe } m \in \mathbb{N} \text{ tal que } n + m = w.$$

Ou seja, lembrando da Definição D4.50,

$$(*) \qquad \text{para todo } n \in \mathbb{N},\ n \leq w.$$

Ou seja, w é o máximo do $\mathbb{N}$; absurdo pois $\mathbb{N}$ não tem máximo!
ALTERNATIVAMENTE, bote $n := w + 1$ na (*) para chegar no absurdo $w + 1 \leq w$.

Π9.14S. Considere uma função $f : \wp\mathbb{N} \to \wp\mathbb{N}$. Sobre a f-imagem do $\emptyset$, não tenho opção: sei que vai ser o $\emptyset$ (Exercício x9.67). Mas sobre o *f-valor* do $\emptyset$ eu tenho opção sim—minha função, minhas regras! Defino a f para ser a constante que sempre retorna o $\{1, 2\}$ então. Logo temos:

$$f(\emptyset) = \{1, 2\} \neq \emptyset = f[\emptyset].$$

Ou seja, a notação que usa as parenteses, tá buggada mesmo que os conjuntos que trabalhamos são homogêneos.

TEASER. Talvez o problema seria resolvido se cada objeto chegasse junto com um rótulo, dizendo *que tipo de coisa* ele é. Assim talvez teriamos como diferenciar entre os dois(!?) $\emptyset$'s (algo que no nosso contexto não faz sentido nenhum pois violaria a unicidade do conjunto vazio x8.9). Um $\emptyset$ diria:

> «Eu sou um conjunto de naturais com nenhum membro.»

E o outro $\emptyset$ diria:

> «Eu sou um conjunto de conjuntos de naturais com nenhum membro.»

Vamos voltar nisso bem, bem, bem depois, no Capítulo 19: teoria dos tipos. Por enquanto, esqueça.

x9.85S. Para o primeiro exemplo, escolhe $A = \{0\}$ e $B = \{0, 1\}$. Agora sejam $f : A \to B$ e $g : B \to A$ definidas pelas

$$f(0) = 0 \qquad\qquad g(x) = 0$$

Ambas as $g \circ f$ e $f \circ g$ são definidas mas são diferentes pois nem domínios iguais elas têm:

$$\operatorname{dom}(g \circ f) = \operatorname{dom} g = B \neq A = \operatorname{dom} f = \operatorname{dom}(f \circ g).$$

Para o segundo exemplo, tome $A = B = \{0, 1\}$ e defina as funções *flip*, *zero*, *one* : $A \to A$ pelas:

$$\begin{array}{lll} \mathit{flip}(0) = 1 & \mathit{zero}(0) = 0 & \mathit{one}(0) = 1 \\ \mathit{flip}(1) = 0 & \mathit{zero}(1) = 0 & \mathit{one}(1) = 1. \end{array}$$

Calculando temos $\mathit{flip} \circ \mathit{zero} = \mathit{one}$ mas $\mathit{zero} \circ \mathit{flip} = \mathit{zero}$. De fato, quaisquer duas dessas três funções servem como um exemplo nesse caso!

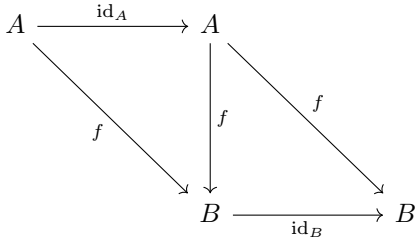
x9.86S. (1) Válida: a composição é definida, e se $a \in A$ então:

$$\begin{aligned} (f \circ \mathrm{id}_A)(a) &= f(\mathrm{id}_A(a)) && (\text{def. } f \circ \mathrm{id}_A) \\ &= f(a). && (\text{def. } \mathrm{id}_A) \end{aligned}$$

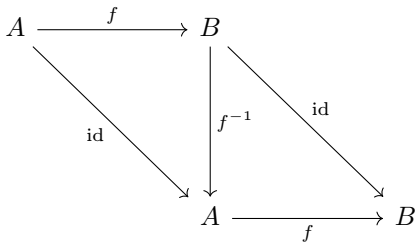
(2) e (3): as composições não são definidas
(4) Similar com (1): a composição é definida e se $a \in A$ então:

$$\begin{aligned} (\mathrm{id}_B \circ f)(a) &= \mathrm{id}_B(f(a)) && (\text{def. } \mathrm{id}_B \circ f) \\ &= f(a). && (\text{def. } \mathrm{id}_B) \end{aligned}$$

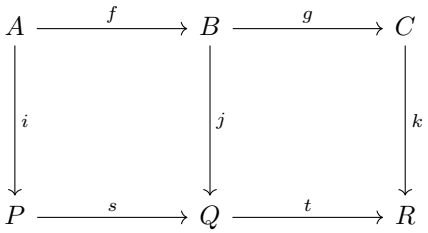
x9.87S. Assim:



x9.88S. Assim:



x9.89S. Temos que os quadrados do



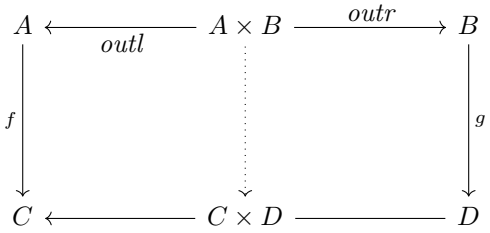
comutam. Precisamos demonstrar que o rectângulo também comuta, ou seja, que

$$k \circ g \circ f = t \circ s \circ i.$$

Calculamos:

$$\begin{aligned} k \circ g \circ f &= (k \circ g) \circ f && \text{(assoc. da } \circ) \\ &= (t \circ j) \circ f && \text{(comut. do quad. direito)} \\ &= t \circ (j \circ f) && \text{(assoc. da } \circ) \\ &= t \circ (s \circ i) && \text{(comut. do quad. esquerdo)} \\ &= t \circ s \circ i. && \text{(assoc. da } \circ) \end{aligned}$$

x9.90S. Bote nomes e direcções onde faltam e demonstre que o diagrama comuta:



x9.92S. Sim. A gente não necessitou nenhuma propriedade especial sobre nossas funções f, g na definição.

x9.94S. Usando λ, a função que procuramos é a seguinte:

$$A \xrightarrow{\lambda x \,.\, \langle x,x\rangle} A \times A.$$

Essa função é a $\langle \mathrm{id}_A, \mathrm{id}_A \rangle$.

Π9.16S. Chame as f e g *compatíveis* sse:

$$\text{para todo } x \in \operatorname{dom} f \cap \operatorname{dom} g,\ f(x) = g(x).$$

Agora dadas compatíveis $f : A \to C$ e $g : B \to D$, definimos a $f \cup g : A \cup B \to C \cup D$ pela

$$(f \cup g)(x) = \begin{cases} f(x), & \text{se } x \in A \\ g(x), & \text{se } x \in B. \end{cases}$$

Equivalentemente, podemos definir a $f \cup g$ definindo seu gráfico:

$$\operatorname{graph}(f \cup g) \stackrel{\text{def}}{=} \operatorname{graph} f \cup \operatorname{graph} g.$$

Observe que nas duas maneiras precisamos a condição de compatibilidade para a $f \cup g$ ser bem-definida.
Resolução alternativa: Usamos a mesma definição mas exigimos que os A, C são disjuntos. A primeira resolução consegue definir a $f \cup g$ em mais casos que essa mas, por outro lado, essa seria aceitável também e é mais simples e "arrumada".

x9.96S. Em vez de cores, tagamos cada membro de A com um 0 e cada membro de B com um 1:

$$A' := \{0\} \times A = \{\, (0,a) \mid a \in A \,\} B' := \{1\} \times B = \{\, (1,b) \mid b \in B \,\}.$$

x9.98S. Podemos obter um diagrama a partir do outro simplesmente trocando a direcção de cada uma das suas setas.

x9.101S. Seja $f : \mathbb{N} \to \mathbb{N}$ definida pela

$$f(n) = \begin{cases} n, & \text{se } n \in D; \\ n+1, & \text{caso contrário.} \end{cases}$$

onde $D := \{0, \ldots, d\}$.

x9.102S. Com cada chamada com entrada x, o número $b - x$ é cada vez menor, onde

$$b = \min \{\, 2^n \mid x \leq 2^n,\ n \in \mathbb{N} \,\}.$$

x9.105S. Calculamos:

$$\begin{aligned}
k(6) = k(7) = k(8) = k(4) = k(2) = k(1) &= 1 \\
k(9) = k(10) = k(11) = k(12) = \cdots = k(16) = k(8) &\eqqcolon 1 \\
d(5) = d(8) = d(4) = d(2) = d(1) &= 1 \\
d(11) = d(14) = d(17) = d(20) = d(23) = d(26) = d(29) = d(32) = d(16) &\eqqcolon 1 \\
d(6) = d(9) = d(12) = d(15) = d(18) = d(21) = d(24) = d(27) = d(30) = d(33) = d(36) &= \cdots
\end{aligned}$$

onde parece que o último cálculo *nunca terminará*. Deixo você se preocupar com a veracidade dessa afirmação no Problema II9.30.

x9.106S. Ela é a função constante do $\mathbb{N}$ com valor 1.

x9.108S. Sejam f, f' resoluções do sistema (FIB). Vou demonstrar por indução que:

$$(\forall n \in \mathbb{N})[\, fn = f'n \,].$$

Vou demonstrar duas bases, ganhando assim 2 hipoteses indutivas.
Base 0: Calculamos:

$$\begin{aligned}
f(0) &= 1 \qquad (f \text{ resolução de (FIB)}) \\
f'(0) &= 1 \qquad (f' \text{ resolução de (FIB)})
\end{aligned}$$

Base 1: Mesma coisa: $f(1) = 1 = f'(1)$.
Passo indutivo. Seja $k \in \mathbb{N}$ tal que f, f' concordam nos pontos $k-1$ e $k-2$:

$$\text{(H.I.1)} \qquad f(k-1) = f'(k-1) \qquad\qquad f(k-2) = f'(k-2). \qquad \text{(H.I.2)}$$

Preciso demonstrar que elas concordam no ponto k também:

$$\begin{aligned} f(k) &= f(k-1) + f(k-2) && (f \text{ resolução de (FIB)}) \\ &= f'(k-1) + f'(k-2) && ((\text{H.I.1}) \text{ e } (\text{H.I.2})) \\ &= f'(k). && (f' \text{ resolução de (FIB)}) \end{aligned}$$

Pronto.

x9.109S. Sobre a f: toda função $f : \mathbb{N} \to \mathbb{N}$ satisfaz essa equação, então não podemos usá-la como definição!

Sobre a g: nenhuma função $g : \mathbb{N} \to \mathbb{N}$ satisfaz essa equação, então não podemos usá-la como definição!

Sobre a h: mais que uma função $h : \mathbb{N} \to \mathbb{N}$ satisfaz essa equação, então não podemos usá-la como definição!

x9.110S. Todas as funções constantes.

x9.111S. Não sabemos se ela satisfaz a totalidade de função, ou seja, se ela é realmente definida em todo o seu domínio. Ate agora, ninguém sabe dizer! Essa é exatamente a conjectura de Collatz (Conjectura ?3.143).

Π9.19S. Podemos representar a $f : A \rightsquigarrow B$ pela função $\bar{f} : A \to \wp B \setminus \{\emptyset\}$ definida pela

$$\bar{f}(x) = \left\{ y \in B \mid x \xmapsto{f} y \right\}.$$

Sejam $f : A \rightsquigarrow B$ e $g : B \rightsquigarrow C$ funções não-determinísticas. Logo temos $\bar{f} : A \to \wp B \setminus \{\emptyset\}$ e $\bar{g} : B \to \wp C \setminus \{\emptyset\}$. Definimos sua composição $g \cdot f : A \rightsquigarrow C$ pela

$$(\overline{g \cdot f})(x) = \bigcup \bar{g}[\bar{f}(x)].$$

O que mais seria legal definir e mostrar para nossa implementação? Bem, seria bom definir pelo menos a identidade não-determinística $id_A : A \rightsquigarrow A$, e investigar se as leis que demonstramos sobre o caso de funções que conectam composição e identidades estão válidas para nossas funções não-determinísticas também.

Π9.20S. A $\mathrm{square} : \mathbb{Z}_6 \to \mathbb{Z}_6$, por exemplo, tem quatro fixpoints: $0, 1, 3, 4$.

Π9.21S. ($\Rightarrow$): Suponha x é um fixpoint da f. Vamos demonstrar o que precisamos por indução no n. Base: Calculamos:

$$\begin{aligned} f^0(x) &= 1_A(x) && (\text{pela def. da } f^0) \\ &= x && (\text{pela def. da } 1_A) \end{aligned}$$

e logo x é um fixpoint da f^0. Passo indutivo: Suponha $k \in \mathbb{N}$ tal que x é um fixpoint da f^k (H.I.). Calculamos:

$$\begin{aligned} f^{k+1}(x) &= (f \circ f^k)(x) && (\text{pela def. de } f^{k+1}) \\ &= f\big(f^k(x)\big) && (\text{pela def. de } f \circ f^k) \\ &= f(x) && (\text{pois } x \text{ é um fixpoint da } f^k \text{ (H.I.)}) \\ &= x && (\text{pois } x \text{ é um fixpoint da } f) \end{aligned}$$

e logo x é um fixpoint da f^{k+1}.
($\Leftarrow$): Usando nossa hipótese com $n := 1$, temos que x é um fixpoint da f^1. Mas f^1 é a própria f (pois $f^1 = f \circ f^0 = f \circ 1_A = f$) e logo x é um fixpoint da f.

Π9.23S. Sempre temos $f[F] = F$ e $f_{-1}[F] \supseteq F$. Se f é injetora, ganhamos a $f_{-1}[F] \subseteq F$ também.
DEMONSTRAÇÃO DE $f[F] \subseteq F$. Seja $y \in f[F]$. Logo tome $p \in F$ tal que $f(p) = y$ (1) (pela definição da função-imagem). Logo p é um fixpoint da f, ou seja, $f(p) = p$ (2). Juntando as (1) e (2), ganhamos $p = y$, ou seja y é um fixpoint da f, e logo $y \in F$.
DEMONSTRAÇÃO DE $f[F] \supseteq F$. Seja $p \in F$. Logo $f(p) \in f[F]$ (pela definição da função-imagem). Mas p é um fixpoint da f (pois $p \in F$), ou seja $f(p) = p$. Logo $p \in f[F]$.
DEMONSTRAÇÃO DE $f_{-1}[F] \supseteq F$. Seja $p \in F$, ou seja p é um fixpoint da f. Logo $f(p) = p \in F$, e logo $p \in f_{-1}[F]$.
CONTRAEXEMPLO PARA $f_{-1}[F] \subseteq F$. Tome $A = \{0, 1\}$ e defina f pela $f(x) = 0$. Nesse caso temos $F = \{0\}$, mas $f_{-1}[F] = \{0, 1\}$.
DEMONSTRAÇÃO DA $f_{-1}[F] \subseteq F$ QUANDO f INJETORA. Seja $a \in f_{-1}[F]$. Logo $f(a)$ é um fixpoint da f. Ou seja, $f(f(a)) = f(a)$ Agora, como f é injetora, temos $f(a) = a$, ou seja, a é um fixpoint também e logo $a \in F$.

x9.112S. INCANCELÁVEL PELA ESQUERDA. Tome por exemplo as

$$\mathbb{R} \underset{\cos}{\overset{\sin}{\rightrightarrows}} \mathbb{R} \xrightarrow{\mathrm{k}_0} \mathbb{R}$$

que obviamente comuta; ou seja $\mathrm{k}_0 \sin = \mathrm{k}_0 \cos (= \mathrm{k}_0)$ mas mesmo assim $\sin \neq \cos$.
INCANCELÁVEL PELA DIREITA. Tome por exemplo as

$$\mathbb{R} \xrightarrow{\mathrm{k}_0} \mathbb{R} \underset{\mathrm{id}}{\overset{\sin}{\rightrightarrows}} \mathbb{R}$$

que obviamente comuta; ou seja $\sin \mathrm{k}_0 = \mathrm{id}\, \mathrm{k}_0 (= \mathrm{k}_0)$ mas mesmo assim $\sin \neq \mathrm{id}$.

x9.113S. Suponha então que $f \circ g = f \circ h$. Vamos mostrar que $g = h$. Seja $x \in A$. Pela hipótese,

$$(f \circ g)(x) = (f \circ h)(x)$$

logo $f(g(x)) = f(h(x))$ e como f injetora, chegamos no desejado $g(x) = h(x)$.

x9.114S. Suponha que $g \circ f = h \circ f$. Vamos mostrar que $g = h$. Seja $c \in C$. Logo existe $b \in B$ tal que $f(b) = c$. Como

$$(g \circ f)(b) = (h \circ f)(b)$$

temos $g(f(b)) = h(f(b))$; e, pela escolha de b, $g(c) = h(c)$. Logo $g = h$.

x9.115S. A FUNÇÃO f É MÔNICA SSE em todo diagrama comutativo da forma

$$A \underset{h}{\overset{g}{\rightrightarrows}} B \xrightarrow{f} C$$

temos $g = h$.

A FUNÇÃO f É ÉPICA SSE em todo diagrama comutativo da forma

$$B \xrightarrow{\quad f \quad} C \underset{h}{\overset{g}{\rightrightarrows}} D$$

temos $g = h$.

x9.116S. Suponha que $f : A \to B$ e que $r : B \to A$ é uma retracção da f. Tome $x, x' \in A$ tais que $f(x) = f(x')$. Logo $r(f(x)) = r(f(x'))$. Logo $(r \circ f)(x) = (r \circ f)(x')$. Como r é retracção, temos $\mathrm{id}_A(x) = \mathrm{id}_A(x')$, ou seja, $x = x'$ e f é injetora.

x9.117S. Suponha que $f : A \to B$ e que $s : B \to A$ é uma secção da f. Tome $b \in B$. Logo $s(b) \in A$, e como s secção, temos $f(s(b)) = b$, ou seja a f é sobrejetora pois mapeia $s(b) \overset{f}{\longmapsto} b$.

x9.119S. Como f tem retracção, ela é injetora; e como ela tem secção, ela é sobrejetora; logo f é bijetora e a f^{-1} é definida. Aplicamos então o Exercício x9.65 com $f' := r$ e com $f' := s$ e ganhamos:

$$r = f^{-1} = s.$$

x9.123S. Pois a definição de função bijectiva (como injectiva e surjectiva) usou a natureza dos objetos e das setas e não apenas suas propriedades categóricas. (Dependeu dos *pontos* dos domínio e do codomínio.)

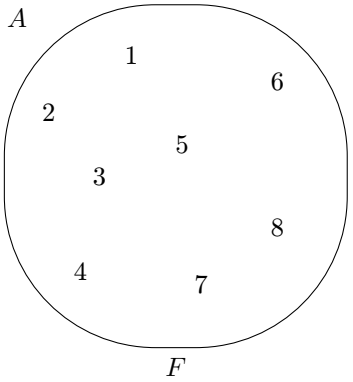
Capítulo 10

x10.1S. Relações *não são* conjuntos!

x10.2S. Digamos que $R = S$ sse para todo $x \in A \cup C$, e todo $y \in B \cup D$, temos $x \mathrel{R} y \iff x \mathrel{S} y$.

x10.4S. Infelizmente não podemos ainda responder nessa pergunta: sua resposta é um dos assuntos principais do Capítulo 13. Paciência! Se tu respondeste "sim, pois todos são conjuntos infinitos", fizeste bem, pois é uma resposta aceitável *neste momento*. Só que... não é uma resposta correta! Aliás, seguindo a Definição D8.68 é uma resposta correta sim, porém vamos ter que redefinir o conceito de cardinalidade logo.

x10.5S. O diagrama da F parece assim:



E o diagrama da T parece uma bagunça.

x10.6S. Para nenhuma! Exatamente como um conjunto não tem noção de *quantas vezes* um certo objeto pertence nele, uma relação também não tem noção de *quantas vezes* um certo objeto relaciona com um certo outro.

x10.7S. $x \left(R^{\partial}\right)^{\partial} y \iff y \, R^{\partial} \, x \iff x \, R \, y$.

x10.8S. Não. Pode ser que a pessoa leu uma palavra w num livro b mas nunca chegou a ler um livro inteiro que contem a w. Nesse caso temos apenas

$$p \, (\text{Read} \diamond \text{Contains}) \, w \implies p \, R \, y$$

pois se p leu um livro que tem a palavra w com certeza p leu w num livro.

x10.9S. Temos:

$$x \left(\text{Author} \diamond \text{Read}^{\partial}\right) y \iff x \text{ escreveu um livro que } y \text{ leu}$$
$$x \left(\text{Read} \diamond \text{Author}^{\partial}\right) y \iff x \text{ leu um livro que } y \text{ escreveu.}$$

Não são iguais: uma é a oposta da outra.

x10.10S. Temos:

$$x \, (\text{Parent} \diamond \text{Parent}) \, y \overset{\text{def}}{\iff} x \text{ é um avô ou uma avó de } y$$
$$x \, (\text{Child} \diamond \text{Child}) \, y \overset{\text{def}}{\iff} x \text{ é um neto ou uma neta de } y$$
$$x \, (\text{Parent} \diamond \text{Child}) \, y \overset{\text{def}}{\iff} x \text{ e } y \text{ tem um filho ou uma filha juntos}$$
$$x \, (\text{Child} \diamond \text{Parent}) \, y \overset{\text{def}}{\iff} x \text{ e } y \text{ são irmã(o)s ou a mesma pessoa}$$

x10.11S. ($\Rightarrow$): Suponha $a \in A$ e $d \in D$ tais que $a \, ((R \diamond S) \diamond T) \, d$. Logo, para algum $c \in C$, temos $a \, (R \diamond S) \, c$ (1) e $c \, T \, d$ (2), e usando a (1) ganhamos um $b \in B$ tal que $a \, R \, b$ (3) e

$b\ S\ c$ (4). Juntando as (4) e (2) temos $b\ (S \diamond T)\ d$, e agora junto com a (3) chegamos em $a\ ((R \diamond S) \diamond T)\ d$.

A direção ($\Leftarrow$) é similar.

x10.12S. Temos $\text{Child} \diamond \text{Parent} \neq \text{Parent} \diamond \text{Child}$:

Tome $x, y \in \mathcal{P}$ dois irmãos que não têm filhos (juntos). Logo

$$x\ (\text{Parent} \diamond \text{Child})\ y \qquad \text{mas não} \qquad x\ (\text{Child} \diamond \text{Parent})\ y.$$

Demonstramos assim que as duas relações são diferentes.

x10.13S. Existe sim: a I é a igualdade $=_A$ no A. Vamos mostrar que para todos $a, b \in A$

$$a\ R\ b \iff a\ (I \diamond R)\ b.$$

Tratamos cada direção separadamente.

($\Rightarrow$). Suponha que $a\ R\ b$. Precisamos mostrar que existe $w \in A$ tal que $a\ I\ w$ e $w\ R\ b$. Tome $w := a$. Realmente temos $a\ I\ a$ (pois I é a igualdade), e $a\ R\ b$ que é nossa hipótese.

($\Leftarrow$). Suponha que $a\ (I \diamond R)\ b$. Logo, existe $w \in A$ tal que $a\ I\ w$ (1) e $w\ R\ b$ (2). Mas, como I é a igualdade, o único w que satisfaz a (1) é o próprio a. Ou seja, $w = a$. Substituindo na (2), ganhamos o desejado $a\ R\ b$.

A outra equivalência,

$$a\ R\ b \iff a\ (R \diamond I)\ b,$$

é similar.

x10.14S. Definimos:

$$\begin{aligned} x\ \left(R^0\right)\ y &\stackrel{\text{def}}{\iff} x = y \\ x\ \left(R^{n+1}\right)\ y &\stackrel{\text{def}}{\iff} x\ (R \diamond R^n)\ y \end{aligned}$$

ou, diretamente, em estilo "point-free":

$$\begin{aligned} R^0 &\stackrel{\text{def}}{=} \text{Eq} \\ R^{n+1} &\stackrel{\text{def}}{=} R^n \diamond R, \end{aligned}$$

onde escrevemos Eq para a relação $=_A$ de igualdade no A.

x10.15S. Não, como o contraexemplo do Exercício x10.12 mostra, pois

$$\text{Parent} = \text{Child}^\partial \qquad \& \qquad \text{Child} = \text{Parent}^\partial.$$

x10.16S. Considerando que um escritor é coescritor com ele mesmo,

$$\text{Coauthors} = \text{Author} \diamond \text{Author}^\partial\ .$$

x10.17S. Vou demonstrar que $(R \diamond S)^\partial = S^\partial \diamond R^\partial$. Calculo:

$$\begin{aligned}
x\ (RS)^\partial\ y &\iff y\ RS\ x && \text{(def. } (RS)^\partial\text{)}\\
&\iff \text{existe } w \text{ tal que } y\ R\ w\ \ \&\ \ w\ S\ x && \text{(def. } RS\text{)}\\
&\iff \text{existe } w \text{ tal que } w\ R^\partial\ y\ \ \&\ \ x\ S^\partial\ w && \text{(def. } R^\partial \text{ e } S^\partial\text{)}\\
&\iff \text{existe } w \text{ tal que } x\ S^\partial\ w\ \ \&\ \ w\ R^\partial\ y\\
&\iff x\ S^\partial R^\partial\ y. && \text{(def. } S^\partial R^\partial\text{)}
\end{aligned}$$

x10.20S. Mostramos o contrapositivo. Suponha que R não é irreflexiva. Então existe s com $R(s,s)$, e logo é impossível que a R seja assimétrica, pois achamos x e y $(x, y := s)$ que satisfazem ambas $R(x,y)$ e $R(y,x)$.

x10.21S. Para demonstrar a $(\Rightarrow)$, observe que R não é antissimétrica sse existem x e y tais que:

$$\underbrace{R(x,y) \wedge R(y,x)}_{\text{impossível por assimetria}} \quad \wedge \quad x \neq y.$$

Para refutar a $(\Leftarrow)$, considere o contraexemplo da antissimétrica $(\leq)$ no $\mathbb{N}$, que não é assimétrica, pois é reflexiva.

x10.22S. $(\Rightarrow)$. Suponha R simétrica.

$$\begin{aligned}
x\ R\ y &\implies y\ R\ x && \text{(hipótese)}\\
&\implies x\ R^\partial\ y. && \text{(def. } R^\partial\text{)}
\end{aligned}$$

$(\Leftarrow)$. Suponha $R = R^\partial$.

$$\begin{aligned}
x\ R\ y &\implies y\ R^\partial\ x && \text{(def. } R^\partial\text{)}\\
&\implies y\ R\ x. && \text{(hipótese)}
\end{aligned}$$

x10.25S. Fechando através da totalidade a gente deveria tomar umas decisões injustas. Fechando através da irreflexividade a gente deveria retirar setinhas quando fechando podemos apenas adicionar. Fechando através da assimetria, a gente deveria retirar setinhas também e inclusive isso seria numa maneira injusta: dadas setinhas $(0,1)$ e $(1,0)$ qual das duas tu vai escolher para retirar?

x10.27S. Tome a relação R nos $\mathbb{N}$ com gráfico $\{(0,1)\}$. Aplicando essa suposta definição da R_{S} então temos:

$$x\ R_{\mathrm{S}}\ y \iff x\ R\ y\ \ \&\ \ y\ R\ x \iff \mathsf{False}$$

ou seja, a $x\ R_{\mathrm{S}}\ y$ acaba sendo a relação vazia. Assim acabamos apagando setinhas, algo contra do nosso conceito de fecho!

x10.28S. A relação definida é a R^2, ou seja, a $R \diamond R$.

x10.36S. Esqueceu o Teorema Θ3.162?

x10.38S. Não, pois não é transitiva. Tome os $\langle 0,0,0\rangle$, $\langle 0,1,0\rangle$, e $\langle 2,1,0\rangle$. Observe que

$$\langle 0,0,0\rangle \sim \langle 0,1,0\rangle \quad \& \quad \langle 0,1,0\rangle \sim \langle 2,1,0\rangle$$

mas $\langle 0,0,0\rangle \not\sim \langle 2,1,0\rangle$.

x10.39S. A identidade $=_A$, a trivial True, e a vazia False.

x10.40S. Encontramos a resposta dessa pergunta no Exercício x10.60.

x10.42S. Não é. Uma resolução já foi rescunhada nas dicas. Para um contraexemplo direto, pode tomar os reais 0, $\sqrt{\varepsilon}/2$, e $\sqrt{\varepsilon}$. Observe que $0 \approx_\varepsilon \sqrt{\varepsilon}/2$ e $\sqrt{\varepsilon}/2 \approx_\varepsilon \sqrt{\varepsilon}$ mas não temos $0 \approx_\varepsilon \sqrt{\varepsilon}$.

x10.43S. Escrevemos os tipos:

$$\begin{aligned}[-]_\sim &: A \to \wp A\\ [a]__ &: E \to \wp A\\ [-]__ &: (A \times \mathrm{EqRel}\,(A)) \to \wp A.\end{aligned}$$

x10.44S. Vamos demonstrar primeiro a ((i) ⇔ (iii)).

(⇒). Suponha que $a \sim b$. Precisamos achar um elemento que pertence nos dois conjuntos $[a]$ e $[b]$. Tome o próprio a. Temos $a \in [a]$ pois $a \sim a$ (pela reflexividade da $\sim$). Também temos $a \in [b]$, pois $a \sim b$ (hipótese). Logo $a \in [a] \cap [b] \neq \emptyset$.

(⇐). Suponha que $[a] \cap [b] \neq \emptyset$ e tome $w \in [a] \cap [b]$. Logo $w \in [a]$ e $w \in [b]$, ou seja $w \sim a$ e $w \sim b$ pela definição de classe de equivalência. Pela simetría da $\sim$ temos $a \sim w$. Agora como $a \sim w$ e $w \sim b$, pela transitividade da $\sim$ ganhamos o desejado $a \sim b$.

Agora vamos demonstrar a ((i) ⇔ (ii)).

(⇒). Suponha que $a \sim b$. Tome $x \in [a]$. Logo $x \sim a$. Mas $a \sim b$ e logo pela transitividade da $\sim$ temos $x \sim b$, e logo $x \in [b]$.

(⇐). Suponha que $[a] = [b]$. Pela reflexividade da $\sim$, sabemos que $a \in [a]$. Logo $a \in [b]$, e logo $a \sim b$ pela definição de $[b]$.

x10.46S. Sim! Pois como $\mathscr{A}$ é uma família de subconjuntos de A, já sabemos que $\bigcup \mathscr{A} \subseteq A$. Logo, afirmar $\bigcup \mathscr{A} = A$ ou afirmar $\bigcup \mathscr{A} \supseteq A$ nesse caso é a mesma coisa. Escolhemos o (P1) pois fica mais natural (e porque se retirar a hipótese que $\mathscr{A} \subseteq \wp A$, o (P1) vira necessário).

x10.47S. A $\mathscr{A}_5 \subseteq \wp A$ do Exercício x8.71 satisfaz as

$$\bigcup \mathscr{A}_5 = A, \qquad \bigcap \mathscr{A}_5 = \emptyset,$$

mas não é uma partição: o $2 \in A$ por exemplo, pertenceria em duas classes diferentes, algo contra da nossa idéia de "partição".

Π10.1S. Vamos demonstrar as duas direções separadamente.
$x\ R\ y \implies x\ (R \diamond R)\ y$: Suponha $x\ R\ y$. Como R é reflexiva, logo $x\ R\ x$. Pelas $x\ R\ x$ e $x\ R\ y$ concluimos que $x\ (R \diamond R)\ y$.
$x\ (R \diamond R)\ y \implies x\ R\ y$: Suponha $x\ (R \diamond R)\ y$. Logo $x\ R\ w$ e $w\ R\ y$ para algum $w \in A$ (pela def. de $\diamond$), e logo pela transitividade da R temos $x\ R\ y$.

Π10.2S. $\text{graph}(S) = \emptyset$.

Pois, supondo que tem membros, tome $(x, y) \in \text{graph}(S)$, e agora: $x\ S\ y$ e logo $y\ S^\partial\ x$ (pela def. de S^∂). Logo $x\ \left(S \diamond S^\partial\right)\ x$, que contradiza a irreflexividade da $S \diamond S^\partial$.

Π10.4S. Por indução.
Base. Calculamos:

$$\begin{aligned}
\left(R^0\right)^\partial &= (=_X)^\partial && \text{(def. } R^0\text{)} \\
&= (=_X) && \text{(pelo Exercício x10.22)} \\
&= \left(R^\partial\right)^0. && \text{(def. } \left(R^\partial\right)^0\text{)}
\end{aligned}$$

Passo indutivo. Seja $k \in \mathbb{N}$ tal que $\left(R^k\right)^\partial = \left(R^\partial\right)^k$ (HI). Calculamos:

$$\begin{aligned}
\left(R^{k+1}\right)^\partial &= \left(RR^k\right)^\partial && \text{(def. } R^{k+1}\text{)} \\
&= \left(R^k R\right)^\partial && \text{(Lemma)} \\
&= R^\partial \left(R^k\right)^\partial && \text{(Exercício x10.17)} \\
&= R^\partial \left(R^\partial\right)^k && \text{(HI)} \\
&= \left(R^\partial\right)^{k+1} && \text{(def. } R^{k+1}\text{)}
\end{aligned}$$

Onde devemos demonstrar o Lemma: *para todo* $t \in \mathbb{N}$, $R^t R = RR^t$.
Demonstração do Lemma. Por indução.
Base: $R^0 R \stackrel{?}{=} RR^0$. Imediato pois $R^0 = (=_X)$ e $=_X$ é uma $\diamond$-identidade (Exercício x10.13).
Passo indutivo. Seja $w \in \mathbb{N}$ tal que $R^w R = RR^w$ (HI). Calculamos:

$$\begin{aligned}
R^{w+1} R &= (R^w R) R && \text{(def. } R^{w+1}\text{)} \\
&= (RR^w) R && \text{(HI)} \\
&= R(R^w R) && \text{(assoc. } \diamond \text{ (10.33))} \\
&= R(RR^w) && \text{(HI)} \\
&= RR^{w+1}. && \text{(def. } R^{w+1}\text{)}
\end{aligned}$$

Π10.5S. Não. Sejam $P = \{p, q, r\}$ e $C = \{a, b, c\}$. Considere que as pessoas do P em ordem de preferência de melhor para pior têm:

$$\begin{aligned}
p &: a, b, c \\
q &: c, a, b \\
r &: b, c, a.
\end{aligned}$$

Assim temos:

$$\begin{aligned} a \succcurlyeq b, \quad & \text{(pois os } p, q \text{ preferem } a \text{ que } b) \\ b \succcurlyeq c, \quad & \text{(pois os } p, r \text{ preferem } b \text{ que } c) \end{aligned}$$

mas $a \not\succcurlyeq c$ pois apenas o p prefere a que c. De fato, $c \succcurlyeq a$, pois os q, r preferem c que a.

Π10.6S. Não, e vamos ver um contraexemplo. Considere:

$$\begin{aligned} A &= \{1, 2, 3, 4\} \\ B &= \{5, 6, 7\} \end{aligned}$$

e a $\rightsquigarrow$ relacionando apenas os:

$$\begin{aligned} 1 &\rightsquigarrow 2 \\ 3 &\rightsquigarrow 4. \end{aligned}$$

Defina a $f : A \to B$ pelas

$$\begin{aligned} 1 &\overset{f}{\longmapsto} 5 \\ 2 &\overset{f}{\longmapsto} 6 \\ 3 &\overset{f}{\longmapsto} 6 \\ 4 &\overset{f}{\longmapsto} 7. \end{aligned}$$

Primeiramente observe que realmente $\rightsquigarrow$ é transitiva. Vamos verificar que: $5 \mathrel{R} 6$ e $6 \mathrel{R} 7$ mas mesmo assim $5 \not\mathrel{R} 7$. Os testemunhos de $5 \mathrel{R} 6$ são os 1 e 2; e os testemunhos de $6 \mathrel{R} 7$ são os 3 e 4. Mas os únicos candidados para testemunhos de $5 \mathrel{R} 7$ são os 1 e 4, e $1 \not\rightsquigarrow 4$; e logo $5 \not\mathrel{R} 7$.

Π10.8S. Seja $n \in \mathbb{N}$. Temos:

$$a \to^n b \iff a + n = b.$$

Sejam $a, b \in \mathbb{N}$. Vou demonstrar por indução que para todo $n \in \mathbb{N}$,

$$a \to^n b \iff a + n = b.$$

Base. Temos

$$\begin{aligned} a \to^0 b &\iff a = b && \text{(pela def. } \to^0) \\ &\iff a + 0 = b. \end{aligned}$$

Passo Indutivo. Seja $k \in \mathbb{N}$ tal que

$$a \to^k b \overset{\text{HI}}{\iff} a + k = b.$$

Calculamos:

$$\begin{aligned} a \to^{k+1} b &\iff a \, (\to^k \diamond \to) \, b && \text{(def. } \to^{k+1}) \\ &\iff (\exists w)\big[\, a \to^k w \;\; \& \;\; w \to b \,\big] && \text{(def. } \diamond) \\ &\iff (\exists w)[\, a + k = w \;\; \& \;\; w + 1 = b \,] && \text{(HI; def. de } \to) \\ &\iff (a + k) + 1 = b \\ &\iff a + (k + 1) = b. \end{aligned}$$

Π10.9S. Não é. Sejam $s, t, u \in A$ distintos dois-a-dois. Tome

$$\begin{aligned} a &:= \langle s, s, \ldots, s, t, t, \ldots, t \rangle \\ b &:= \langle s, s, \ldots, s, u, u, \ldots, u \rangle \\ c &:= \langle t, t, \ldots, t, u, u, \ldots, u \rangle \end{aligned}$$

como contraexemplo, pois temos $a \sim b$ e $b \sim c$ mas $a \not\sim c$.

Π10.10S. Primeiramente tentamos entender essas relações bem informalmente. As $\sim$ e $\approx$ envolvem um movimento horizontal, e as $\wr$ e $\wr\!\!\wr$ um movimento vertical. Especificamente $f \sim g$ [$f \wr g$] sse f e g são a mesma função depois de um "shift" horizontal [vertical] para qualquer direção. As $\approx$ e $\wr\!\!\wr$ são parecidas so que $f \approx g$ [$f \wr\!\!\wr g$] sse a f "coincide" com a g depois de um "shift" da f para a direita [para baixo] 0 ou mais "posições".

Reflexividade. Todas são reflexivas, algo que mostramos tomando $u := 0$. Vamos ver em detalhe apenas para a $\sim$.
Reflexividade da $\approx$.
Seja $f : \mathbb{Z} \to \mathbb{Z}$. Temos para todo $x \in \mathbb{Z}$, $f(x) = f(x + 0)$, e como $0 \in \mathbb{Z}_{\geq 0}$, logo $f \approx f$.

Transitividade. Todas são transitivas, e parecida em todas: usando nossas hipoteses ganhamos dois números i, j e o número que procuramos acaba sendo o $i + j$. Vamos ver em detalhe apenas para a $\wr\!\!\wr$:
Transitividade da $\wr\!\!\wr$.
Sejam $f, g, h : \mathbb{Z} \to \mathbb{Z}$ tais que $f \sim g$ e $g \sim h$. Sejam então $i, j \in \mathbb{Z}$ tais que:

(1) para todo $x \in \mathbb{Z}$, $f(x) = g(x + i)$
(2) para todo $x \in \mathbb{Z}$, $g(x) = h(x + j)$.

Seja $z \in \mathbb{Z}$ e calcule:

$$\begin{aligned} f(z) &= g(z + i) && \text{(pela (1) com } x := z) \\ &= h((z + i) + j) && \text{(pela (2) com } x := z + i) \\ &= h(z + (i + j)). \end{aligned}$$

Ou seja, o inteiro $i + j$ mostra que $f \sim h$. Já demonstramos então que todas essas relações são preordens! Vamos pesquisar sobre as outras propriedades agora.

(A(nti)s)simetria. As $\sim$ e $\wr$ são simétricas, algo que mostramos para as duas no mesmo jeito: nossa hipótese fornece um $i \in \mathbb{Z}$ que satisfaz algo, e o inteiro que procuramos acaba sendo o $-i$. As $\wr\!\!\wr$ é antissimétrica, mas a $\approx$ não satisfaz nenhuma dessas propriedades. Vamos demonstrar a simetria da $\sim$, a antissimetria da $\wr\!\!\wr$, e refutar a simetria e a antissimetria da $\approx$.
Simetria da $\sim$.
Sejam $f, g : \mathbb{Z} \to \mathbb{Z}$ tais que $f \sim g$. Então seja $i \in \mathbb{Z}$ tal que para todo $x \in \mathbb{Z}$, $f(x) = g(x + i)$ (1). Observe que para todo $x \in \mathbb{Z}$, temos:

$$\begin{aligned} g(x) &= g(x + (i - i)) \\ &= g((x - i) + i) \\ &= f(x - i). && \text{(pela (1) com } x := x - i) \end{aligned}$$

Ou seja, o $-i \in \mathbb{Z}$ mostra que $g \sim f$.

Antissimetria da $\wr$.
Sejam $f, g : \mathbb{Z} \to \mathbb{Z}$ tais que $f \wr g$ e $g \wr f$. Sejam então $i, j \in \mathbb{Z}_{\geq 0}$ tais que para todo $x \in \mathbb{Z}$ $f(x) = g(x) + i$ e $g(x) = f(x) + j$. Seja $x \in \mathbb{Z}$ e calcule:

$$f(x) = g(x) + i = f(x) + j + i.$$

Logo $i + j = 0$, e sendo ambos naturais, temos $i = j = 0$. Ou seja, para todo $x \in \mathbb{Z}$, $f(x) = g(x)$, e logo $f = g$.

A $\wr$ não é nem relação de equivalência nem de ordem.
Refutação da simetria da $\approx$.
Como contraexemplo tome as funções $f, g : \mathbb{Z} \to \mathbb{Z}$ definidas pelas:

$$\begin{aligned} f(0) &= 1 & \qquad g(1) &= 1 \\ f(x) &= 0 \quad (x \neq 0) & \qquad g(x) &= 0 \quad (x \neq 1) \end{aligned}$$

Observe que realmente $f \approx g$ pois temos que para todo $x \in \mathbb{Z}$, $f(x) = g(x+1)$. Mas $g \not\approx f$. Suponha que tem $u \in \mathbb{Z}_{\geq 0}$ tal que para todo $x \in \mathbb{Z}$, $g(x) = f(x + u)$. Basta ou achar um absurdo. Pela nossa hipótese, $g(1) = f(1 + u)$. Mas $g(1) = 1$, ou seja $f(1 + u) = 1$. Pela definição da f então $u + 1 = 0$, Absurdo, pois o 0 não é sucessor de nenhum natural.
Refutação da antissimetria da $\approx$.
Como contraexemplo tome as funções $f, g : \mathbb{Z} \to \mathbb{Z}$ definidas pelas:

$$f(x) = \begin{cases} 0, & \text{se } x \text{ é par;} \\ 1, & \text{se } x \text{ é ímpar;} \end{cases} \qquad g(x) = \begin{cases} 1, & \text{se } x \text{ é par;} \\ 0, & \text{se } x \text{ é ímpar;} \end{cases}$$

Observe que realmente $f \approx g$ (tome $u := 1$) e $g \approx f$ (tome $u := 1$ de novo). Mesmo assim, $f \neq g$. Logo $\approx$ não é uma relação antissimétrica.

Concluimos então que: as $\sim$ e $\wr$ são relações de equivalência, a $\wr$ é uma relação de ordem, e a $\approx$ apenas uma preordem.

Π10.11S. (i) A $\overset{\infty}{=}$ não é. Considere o seguinte contraexemplo. Sejam as $\alpha, \beta, \gamma : \mathbb{N} \to \mathbb{N}$ (como seqüências):

$$\begin{aligned} \alpha &= \langle 0, 1, 0, 1, 0, 1, \ldots \rangle \\ \beta &= \langle 0, 2, 0, 2, 0, 2, \ldots \rangle \\ \gamma &= \langle 1, 2, 1, 2, 1, 2, \ldots \rangle . \end{aligned}$$

Trivialmente, $\alpha \overset{\infty}{=} \beta$ e $\beta \overset{\infty}{=} \gamma$ mas $\alpha \overset{\infty}{\neq} \gamma$.
(ii) Correto. Sejam $f, g \in (\mathbb{N} \to \mathbb{N})$. Vamos mostrar que $f \left(\overset{\text{e}}{=} \diamond \overset{\text{o}}{=}\right) g$. Pela definição da $\diamond$ temos:

$$f \left(\overset{\text{e}}{=} \diamond \overset{\text{o}}{=}\right) g \iff \text{existe } h \in (\mathbb{N} \to \mathbb{N}) \text{ tal que } f \overset{\text{e}}{=} h \text{ e } h \overset{\text{o}}{=} g.$$

A função $h : \mathbb{N} \to \mathbb{N}$ definida pela

$$h(n) = \begin{cases} f(n), & \text{se } n \text{ par} \\ g(n), & \text{se } n \text{ ímpar} \end{cases}$$

satisfaz as $f \overset{\text{e}}{=} h \overset{\text{o}}{=} g$ pela sua construção. Logo, $f \left(\overset{\text{e}}{=} \diamond \overset{\text{o}}{=}\right) g$.

Π10.12S. A $\sim$ é uma relação de equivalência:

Reflexiva. Seja $f : \mathbb{R} \to \mathbb{R}$. Calculamos:

$$\{\, x \in \mathbb{R} \mid f(x) \neq f(x) \,\} = \emptyset,$$

que, sendo finito, mostra que $f \sim f$.
Simétrica. Trivial, pois para quaisquer $f, g : \mathbb{R} \to \mathbb{R}$ temos

$$\{\, x \in \mathbb{R} \mid f(x) \neq g(x) \,\} = \{\, x \in \mathbb{R} \mid g(x) \neq f(x) \,\}$$

e logo um é finito sse o outro é finito.
Transitiva. Sejam $f, g, h : \mathbb{R} \to \mathbb{R}$ tais que $f \sim g$ e $g \sim h$. Logo:

$$A \stackrel{\text{def}}{=} \{\, x \in \mathbb{R} \mid f(x) \neq g(x) \,\} \text{ finíto} \tag{1}$$

$$B \stackrel{\text{def}}{=} \{\, x \in \mathbb{R} \mid g(x) \neq h(x) \,\} \text{ finíto} \tag{2.}$$

Seja $w \in \mathbb{R}$. Vamos demonstrar que

$$w \notin A \cup B \implies f(w) = h(w).$$

Calculamos:

$$\begin{aligned} f(w) &= g(w) && (\text{pois } w \notin A) \\ &= h(w). && (\text{pois } w \notin B) \end{aligned}$$

Contrapositivamente,

$$f(w) \neq h(w) \implies w \in A \cup B.$$

Mas $A \cup B$ é finito, (sendo uma união finita de conjuntos finitos) e mostramos que

$$\{\, x \in \mathbb{R} \mid f(x) \neq h(x) \,\} \subseteq A \cup B$$

e logo também finito, ou seja, $f \sim h$.
A $\approx$ não é uma relação de equivalência. Vamos refutar a sua transitividade. Como contraexemplo, tome as $f, g, h : \mathbb{R} \to \mathbb{R}$ definidas pelas:

$$f(x) = 1 \qquad g(x) = \cos(x) \qquad h(x) = -1.$$

Observe que $f \approx g$ pois concordam nos pontos $2k\pi$ para todo $k \in \mathbb{Z}$. Também $g \approx h$ pois concordam nos pontos $(2k+1)\pi$ para todo $k \in \mathbb{Z}$. Mesmo assim, $f \not\approx h$ pois não concordam em ponto nenhum.

Π10.14S. Seguem umas idéias.
Função como relação. Sejam A, B conjuntos. Uma relação f de A para B tal que f é *left-total* e *right-unique* (veja o glossário 10.44) é chamada uma *função de A para B*. Escrevemos $f(x) = y$ em vez de $f(x, y)$ ou de $x\ f\ y$ e para todo $a \in A$ denotamos com $f(a)$ o único $b \in B$ tal que $a\ f\ b$.
Relação binária como função. Sejam A, B conjuntos. Uma função $R : A \to \wp B$ é chamada uma *relação de A para B*. Escrevemos $a\ R\ b$ quando $b \in R(a)$, e $a \not R\ b$ quando $b \notin R(a)$.
Relação geral como função. Seja W conjunto. Uma função $R : W \to \mathbb{B}$ é chamada uma *relação no W*. Escrevemos $R(w)$ como afirmação, quando $R(w) = \mathsf{True}$, e $\neg R(w)$ ou "não $R(w)$" quando $R(w) = \mathsf{False}$.

x10.48S. Seguindo as dicas, faltou escrever a ultima linha:

$$\begin{aligned} C \in \mathscr{A}_R \iff^{\mathsf{def}} & C \subseteq A \\ & \& \;\; C \neq \emptyset \\ & \& \;\; (\forall c, d \in C)[\, c \mathrel{R} d \,] \\ & \& \;\; (\forall a \in A)(\forall c \in C)[\, a \mathrel{R} c \implies a \in C \,]. \end{aligned}$$

x10.49S. Definir uma família de subconjuntos de A. Definimos $\mathscr{A}_\sim$ para ser a família de todas as classes de equivalência através da $\sim$. Formalmente:

$$\mathscr{A}_\sim \stackrel{\mathsf{def}}{=} \{\, [a] \mid a \in A \,\}.$$

Demonstrar que a família $\mathscr{A}_\sim$ é uma partição. Primeiramente observe que cada membro de $\mathscr{A}_\sim$ é um subconjunto de A. Agora basta verificar as (P1)–(P3) da Definição D10.88.
(P1) Mostrar que $A \subseteq \bigcup(\mathscr{A}_\sim)$. Tome $a \in A$. Como $a \sim a$ (reflexividade), então $a \in [a]$. Agora como $[a] \in \mathscr{A}_\sim$, temos que $a \in \bigcup(\mathscr{A}_\sim)$.
(P2) Os membros de $\mathscr{A}_\sim$ são disjuntos dois-a-dois. Sejam $C, D \in \mathscr{A}_\sim$. Logo sejam $c, d \in A$ tais que $C = [c]$ e $D = [d]$. Precisamos demonstrar *qualquer uma* das duas implicações (são contrapositivas):

$$\begin{aligned} C \neq D &\implies C \cap D = \emptyset; \\ C \cap D \neq \emptyset &\implies C = D. \end{aligned}$$

Vamos demonstrar a segunda. Suponha $C \cap D \neq \emptyset$ e seja logo $w \in C \cap D$. Ou seja, $w \in C$ e $w \in D$, e logo $w \sim c$ e $w \sim d$. Queremos demonstrar que $C = D$. ($\subseteq$). Tome $x \in C = [c]$. Temos:

$$x \sim c \sim w \sim d$$

(simetria e transitividade da $\sim$) e logo $x \in [d] = D$ e $C \subseteq D$. A ($\supseteq$) é similar.
(P3) $\emptyset \notin \mathscr{A}_\sim$. Basta demonstrar que para cada $a \in A$, $[a] \neq \emptyset$. Isso é uma conseqüência da reflexividade da $\sim$, pois para todo $a \in A$, $a \in [a]$.

Se escolher a primeira implicação na parte de (P2), a gente continua assim: Suponha $C \neq D$ e logo sem perda de generalidade, tome $c_0 \in C \setminus D$. Logo $c_0 \sim c$ e $c_0 \not\sim d$. Isso já mostra que não pode ter nenhum elemento $w \in C \cap D$, pois nesse caso usando a simetria e transitividade da $\sim$ teriamos $c_0 \sim c \sim w \sim d$ que obrigaria $c_0 \sim d$; impossível.

x10.50S. Veja a resolução do Exercício x10.49.

x10.51S. $A/- : \mathrm{EqRel}\,(A) \to \wp\wp A$.

x10.54S. O $\mathbb{R}^3/\!\sim_3$ parece lasanha: é composto por todos os planos horizontais. O $\mathbb{R}^3/\!\sim_{1,2}$ é composto pelas todas as retas verticais (perpendiculares no xy-plano). O $\mathbb{R}^3/\!\sim_{\mathrm{N}}$ é composto pelas todas as sferas com centro na origem. Informalmente temos as "equações" seguintes:

$$\mathbb{R}^3/\!\sim_3 \text{“}=\text{”}\, \mathbb{R} \qquad \mathbb{R}^3/\!\sim_{1,2} \text{“}=\text{”}\, \mathbb{R}^2 \qquad \mathbb{R}^3/\!\sim_{\mathrm{N}} \text{“}=\text{”}\, \mathbb{R}_{\geq 0}.$$

Na primeira identificamos cada plano com sua altura; na segunda cada reta com sua sombra no xy-plano; na terceira casa sfera com seu raio.

x10.56S. Temos:

$$\begin{aligned} a \equiv_0 b &\iff 0 \mid a-b \iff a-b=0 \iff a=b \\ a \equiv_1 b &\iff 1 \mid a-b \iff \mathsf{True}. \end{aligned}$$

Ou seja: $(\equiv_0) = (=_{\mathbb{Z}})$ e $(\equiv_1) = (\mathsf{True})$.

x10.58S. Definimos a $\sim_{\mathscr{A}}$ pela

$$x \sim_{\mathscr{A}} y \overset{\text{def}}{\iff} (\exists C \in \mathscr{A})[\, x, y \in C \,].$$

A relação $\sim_{\mathscr{A}}$ é uma relação de equivalência.

Reflexiva. Tome $a \in A$. Precisamos mostrar que existe $C \in \mathscr{A}$ tal que $a \in C$. Mas, como $\mathscr{A}$ é uma partição (P1), temos que $\bigcup \mathscr{A} = A$. Seja então C tal que $a \in C \in \mathscr{A}$. Logo $a \sim_{\mathscr{A}} a$.

Simétrica. Trivial pois $x, y \in C \iff y, x \in C$.

Transitiva. Suponha $x \sim_{\mathscr{A}} y$ e $y \sim_{\mathscr{A}} z$. Logo sejam $C, D \in \mathscr{A}$ tais que $x, y \in C$ e $y, z \in D$. Agora, como $y \in C \cap D$ e $\mathscr{A}$ é uma partição (P2), temos $C = D$. Ou seja, $x, z \in C \in \mathscr{A}$ e logo $x \sim_{\mathscr{A}} z$.

O conjunto quociente $A/\!\sim_{\mathscr{A}}$ é a partição $\mathscr{A}$.

($\subseteq$). Tome $C \in A/\!\sim_{\mathscr{A}}$. Seja $c \in A$ tal que $C = [c]$. Como $c \in \bigcup \mathscr{A}$ ($\mathscr{A}$ partição (P1)), seja C' o único ($\mathscr{A}$ partição (P2)) membro da $\mathscr{A}$ tal que $c \in C'$. Basta mostrar que $C = C'$. Tome $x \in C = [c]$. logo $x \sim_{\mathscr{A}} c$, e logo existe $D' \in \mathscr{A}$ tal que $x, c \in D'$. Mas pela escolha do C', temos $D' = C'$, e logo $x \in C'$ e $C \subseteq C'$. Conversamente, tome $x' \in C'$. Logo $x', c \in C'$, logo $x' \sim_{\mathscr{A}} c$, e logo $x' \in [c] = C$. Ou seja, $C' \subseteq C$.

($\supseteq$). Tome $C' \in \mathscr{A}$. Como $C' \neq \emptyset$ (pois $\mathscr{A}$ é partição (P3)), seja $c' \in C'$. Basta demonstrar que $[c'] = C'$. Tome $x \in [c']$. Logo $x \sim_{\mathscr{A}} c'$, e logo seja $D' \in \mathscr{A}$ tal que $x, c' \in D'$. Mas, como $c' \in C' \cap D'$, concluimos que $C' = D'$ (pela (P2)). Ou seja, $x \in C'$. Conversamente, tome $x' \in C'$. Como $c' \in C'$, logo $x' \sim_{\mathscr{A}} c'$ pela definição da $\sim_{\mathscr{A}}$, ou seja $x' \in [c']$.

x10.59S. Veja a resolução do Exercício x10.58.

x10.61S. $\approx_f$ é uma relação de equivalência. Cada uma das três propriedades é uma conseqüência direta da propriedade correspondende da igualdade. Em detalhe:

Reflexiva. Seja $x \in X$. Temos $x \approx_f x$ pois $f(x) = f(x)$ (reflexividade da $(=)$).

Transitiva. Sejam $a, b, c \in X$ tais que $a \approx_f b$ e $b \approx_f c$. Logo $f(a) = f(b)$ e $f(b) = f(c)$. Logo $f(a) = f(c)$ (transitividade da $(=)$), ou seja, $a \approx_f c$.

Simétrica. Sejam $a, b \in X$ tais que $a \approx_f b$, e logo $f(a) = f(b)$ e logo $f(b) = f(a)$ (simetria da $(=)$), ou seja, $b \approx_f a$.

Descripção do conjunto quociente. O conjunto quociente "é" a imagem $\operatorname{im} f$. Caso que f é injetora a relação acaba sendo a igualdade e logo o conjunto quociente acaba sendo o próprio $\operatorname{dom} f$. Caso que f é sobrejetora nada demais muda, só que agora $\operatorname{im} f = \operatorname{cod} f$.

x10.62S. A $\approx_{f,\sim_B}$ é uma relação de equivalência sim. Isso já foi demonstrado, pois a resolução do Exercício x10.61 usou apenas o fato que a igualdade é uma relação de equivalência.

Π10.21S. Seguindo todas as dicas, basta definir:

$$B_0 = 1$$
$$B_{n+1} = \sum_{i=0}^{n} N_i = \sum_{i=0}^{n} C(n,i)B_i$$

Essa seqüência de números é conhecida como *números Bell*.

Π10.23S. (i) Defina a partição de $\mathbb{R}$

$$\mathscr{C} \stackrel{\text{def}}{=} \underbrace{\{\,(n,n+1) \mid n \in \mathbb{Z}\,\}}_{\mathcal{I}} \cup \underbrace{\{\,\{n\} \mid n \in \mathbb{Z}\,\}}_{\mathcal{S}}.$$

Basta demonstrar que $\mathscr{C} = \mathbb{R}/\breve{\smile}$, ou seja:

$$x \breve{\smile} y \iff (\exists C \in \mathscr{C})[\, x \in C \ \ \&\ \ y \in C\,].$$

($\Leftarrow$). Trivial nos dois casos $C \in \mathcal{I}$ e $C \in \mathcal{S}$.
($\Rightarrow$). Pela hipótese, $x = y$ ou $x \smile y$ ou $y \smile x$. Separamos então em casos:
Caso $x = y$: Caso $x \in \mathbb{Z}$ tome $C = \{x\} \in \mathcal{S}$. Caso $x \notin \mathbb{Z}$ tome $C = (\lfloor x \rfloor, \lfloor x \rfloor + 1) \in \mathcal{I}$.
Caso $x \smile y$: Nesse caso $[x,y] \cap \mathbb{Z} = \emptyset$. Facilmente, $\lfloor x \rfloor < x \leq y < \lfloor x \rfloor + 1$. Tome novamente $C = (\lfloor x \rfloor, \lfloor x \rfloor + 1) \in \mathcal{I}$.
Caso $y \smile x$: Similar.

(ii) Não é, pois não é transitiva. Observe que $0 \breve{\frown} 1$, pois não existe inteiro no $(0,1)$, e similarmente $1 \breve{\frown} 2$. Mas $0 \not\breve{\frown} 2$, pois 1 é inteiro e $1 \in (0,2)$.

Π10.25S. Definimos:

$$x\ R_{\mathfrak{t}}\ y \iff x\ R\ y \ \text{ ou } \ (\exists w \in A)\big[\, x\ R\ w \ \ \&\ \ w\ R_{\mathfrak{t}}\ y\,\big].$$

Pense para visualizar como isso "funciona".

Capítulo 11

x11.2S. Qualquer uma das duas seria suficiente nesse caso! A injetividade obrigaria a imagem de 3 evitar tanto o 1 quanto o 3 (pois o primeiro é imagem do 1 e o segundo do 2), e logo só sobra uma opção para ser a imagem do 3: o 2. A sobrejetividade obrigaria a imagem de 3 ser o 2 também, pois por enquanto ninguém foi mapeado a ele.

x11.3S. Calculamos:

$$1 \xmapsto{\psi^2} 3 \xmapsto{\psi} 1$$
$$2 \xmapsto{\psi^2} 1 \xmapsto{\psi} 2$$
$$3 \xmapsto{\psi^2} 2 \xmapsto{\psi} 3$$

ou seja, $\psi \circ \psi^2 = \mathrm{id}$. A igualdade é imediata pela associatividade da $(\circ)$. (E ambas são iguais à ψ^3.)

x11.6S. Pois elas discordam em pelo menos um valor: tome o 1. Agora

$$(\varphi \circ \psi)(1) = \varphi(\psi(1)) = \varphi(2) = 1 \neq 3 = \psi(2) = \psi(\varphi(1)) = (\psi \circ \varphi)(1).$$

Logo $\varphi \circ \psi \neq \psi \circ \varphi$.

x11.8S. Sim! Veja também a Observação 11.20.

x11.14S. Não é, pois quebra a (G0):

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{\in (M;+)} + \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\in (M;+)} = \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}}_{\notin (M;+)}.$$

x11.19S. Precisamos verificar as leis (G0)–(G3).
(G0). Tome $\langle x_1, x_2\rangle, \langle y_1, y_2\rangle \in G_1 \times G_2$. Calculamos

$$\begin{aligned} \langle x_1, x_2\rangle * \langle y_1, y_2\rangle &= \langle x_1 *_1 y_1, x_2 *_2 y_2\rangle && \text{(def. } *\text{)} \\ &\in G_1 \times G_2. && (G_1 \text{ e } G_2 \text{ fechados sob suas operações}) \end{aligned}$$

e logo $G_1 \times G_2$ é $*$-fechado.
(G1). Tome $\langle x_1, x_2\rangle, \langle y_1, y_2\rangle, \langle z_1, z_2\rangle \in G_1 \times G_2$. Calculamos:

$$\begin{aligned} (\langle x_1, x_2\rangle * \langle y_1, y_2\rangle) * \langle z_1, z_2\rangle &= \langle x_1 *_1 y_1, x_2 *_2 y_2\rangle * \langle z_1, z_2\rangle \\ &= \langle (x_1 *_1 y_1) *_1 z_1, (x_2 *_2 y_2) *_2 z_2\rangle \\ &= \langle x_1 *_1 (y_1 *_1 z_1), x_2 *_2 (y_2 *_2 z_2)\rangle \\ &= \langle x_1, x_2\rangle * (\langle y_1 *_1 z_1, y_2 *_2 z_2\rangle) \\ &= \langle x_1, x_2\rangle * (\langle y_1, y_2\rangle * \langle z_1, z_2\rangle). \end{aligned}$$

(G2). Afirmação: o $\langle e_1, e_2\rangle \in G_1 \times G_2$ é a $*$-identidade. Prova da afirmação: tome $\langle x_1, x_2\rangle \in G_1 \times G_2$ e calcule:

$$\langle e_1, e_2\rangle * \langle x_1, x_2\rangle = \langle e_1 *_1 x_1, e_2 *_2 x_2\rangle = \langle x_1, x_2\rangle = \langle x_1 *_1 e_1, x_2 *_2 e_2\rangle = \langle x_1, x_2\rangle * \langle e_1, e_2\rangle.$$

(G3). Seja $\langle x_1, x_2\rangle \in G_1 \times G_2$. Afirmação: o $\langle {x_1}^{-1}, {x_2}^{-1}\rangle$ é o $*$-inverso dele. Realmente temos:

$$\begin{aligned} \langle x_1, x_2\rangle * \langle {x_1}^{-1}, {x_2}^{-1}\rangle &= \langle x_1 *_1 {x_1}^{-1}, x_2 *_2 {x_2}^{-1}\rangle = \langle e_1, e_2\rangle \\ \langle {x_1}^{-1}, {x_2}^{-1}\rangle * \langle x_1, x_2\rangle &= \langle {x_1}^{-1} *_1 x_1, {x_2}^{-1} *_2 x_2\rangle = \langle e_1, e_2\rangle \end{aligned}$$

Assim concluimos nossa demonstração.

x11.21S. É apenas escrever

(1) $$\text{para todo } a \in G, \quad e_1 * a \overset{\text{L}}{=} a \overset{\text{R}}{=} a * e_1$$

(2) $$\text{para todo } a \in G, \quad e_2 * a \overset{\text{L}}{=} a \overset{\text{R}}{=} a * e_2$$

e depois

$$\begin{aligned} e_1 &= e_1 * e_2 && \text{(pela (2R), com } a := e_1\text{)} \\ &= e_2. && \text{(pela (1L), com } a := e_2\text{)} \end{aligned}$$

Observe que os a que aparecem nas instanciações $a := \ldots$ são completemante independentes. Ou seja, nada muda mesmo!

x11.22S. Se $x = y$ isso quis dizer que podemos substituir à vontade em cada *expressão* que envolve x e y, uns x's por y's, e vice versa. Nesse caso, começa com o

$$a * x$$

e troca a única ocorrência de x nessa expressão por y, e já chegamos no

$$a * y$$

ou seja, $a * x = a * y$.

x11.23S. No S_3, temos

$$\varphi(\psi\varphi) = (\varphi\psi)\varphi$$

e mesmo assim

$$\psi\varphi \neq \varphi\psi.$$

x11.26S. Precisamos mosrar que

$$\text{para todo } a \in G,\ e^{-1} * a = e = a * e^{-1}.$$

Seja $a \in G$. Vamos mostrar que o e^{-1} "deixa o a em paz" pelos dois lados. Calculamos:

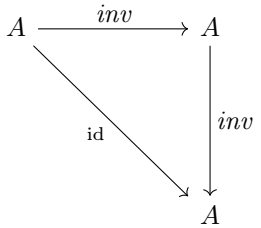
$$\begin{aligned} e^{-1} * a &= e^{-1} * (e * a) && (a = e * a) \\ &= (e^{-1} * e) * a && \text{(G1)} \\ &= e * a && \text{(def. de } e^{-1}\text{)} \\ &= a && \text{(def. de } e\text{)} \end{aligned}$$

Ou outro lado é similar.

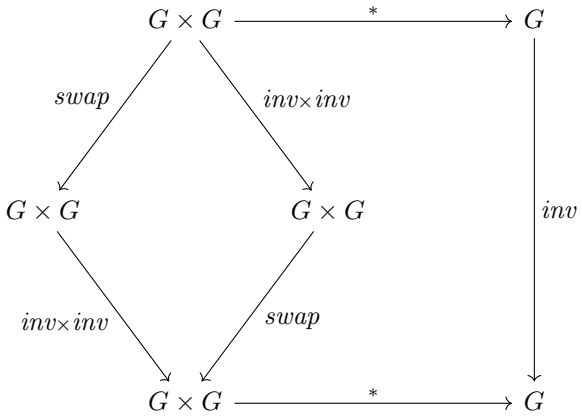
x11.27S. Calculamos:

$$\begin{aligned} e^{-1} &= e^{-1} * e && \text{(def. } e\text{)} \\ &= e && \text{(def. } e^{-1}\text{)} \end{aligned}$$

x11.28S.



x11.29S. Um tal diagrama é o seguinte:



onde $swap(x, y) = \langle y, x \rangle$.

x11.31S. ($\Rightarrow$). Calculamos:

$$\begin{aligned} (ab)^{-1} &= b^{-1}a^{-1} && \text{(pelo Lema Λ11.58)} \\ &= a^{-1}b^{-1}. && (G \text{ abeliano}) \end{aligned}$$

($\Leftarrow$). Calculamos:

$$\begin{aligned} ab &= \left((ab)^{-1}\right)^{-1} && \text{(pelo Lema Λ11.56)} \\ &= \left(b^{-1}a^{-1}\right)^{-1} && \text{(pelo Lema Λ11.58)} \\ &= \left(b^{-1}\right)^{-1}\left(a^{-1}\right)^{-1} && \text{(pela hipótese)} \\ &= ba. && \text{(pelo Lema Λ11.56 (×2))} \end{aligned}$$

x11.32S. Veja Problema Π11.2.

x11.34S. Seja $A = \left\{ 1_{\mathrm{R}}, a \right\}$ um conjunto com dois membros. Definimos a operação $*$ pela:

$$x * y = x.$$

Confirmamos que $(A \; ; *)$ satisfaz todas as (G0),(G1),(G2R),(G3L), mas mesmo assim não é um grupo: não tem identidade, pois a 1_{R} não serve como L-identidade:

$$1_{\mathrm{R}} * a = 1_{\mathrm{R}} \neq a.$$

x11.36S. Só tem uma maneira:

e	a	b
a	b	e
b	e	a

Realmente não temos nenhuma opção em nenhum dos ?. O Exercício x11.37 investiga o porquê.

x11.38S. *Essencialmente* são apenas 2:

e	a	b	c
a	b	c	e
b	c	e	a
c	e	a	b

e	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

O primeiro é conhecido como o grupo cíclico de ordem 4; o segundo como Klein four-group. Se tu achaste mais, verifique que renomeando seus membros umas viram iguais, e só tem dois que realmente não tem como identificá-las, mesmo renomeanos seus membros. Tudo isso vai fazer bem mais sentido daqui umas secções onde vamos estudar o conceito de isomorfia (§258).

x11.39S. De ordem 1 sim. Cada um tem a mesma forma: seu único elemento é sua identidade. De ordem 0, não: a lei (G2) *manda a existência* de um certo membro do grupo (a sua identidade).

x11.40S. Seja $a \in G$. Vamos demonstrar que para todo $n \in \mathbb{N}$, $a \uparrow_1 n = a \uparrow_2 n$ por indução no n.
Bases $n := 0, 1$: Temos

$$\begin{aligned} a \uparrow_1 0 &= e && \text{(def. } \uparrow_1\text{)} \\ &= a \uparrow_2 0 && \text{(def. } \uparrow_2\text{)} \end{aligned}$$

$$\begin{aligned} a \uparrow_1 1 &= a * (a \uparrow_1 0) && \text{(def. } \uparrow_1\text{)} \\ &= a * e && \text{(def. } \uparrow_1\text{)} \\ &= a && \text{(def. } e\text{)} \\ &= e * a && \text{(def. } e\text{)} \\ &= (a \uparrow_2 0) * a && \text{(def. } \uparrow_2\text{)} \\ &= a \uparrow_2 1 && \text{(def. } \uparrow_2\text{)} \end{aligned}$$

Passo indutivo: Seja $k \in \mathbb{N}$, tal que $k \geq 2$ e:

(HI1) $a \uparrow_1 (k-1) = a \uparrow_2 (k-1)$
(HI2) $a \uparrow_1 (k-2) = a \uparrow_2 (k-2)$.

Precisamos demonstrar que $a \uparrow_1 k = a \uparrow_2 k$. Calculamos:

$$\begin{aligned} a \uparrow_1 k &= a * (a \uparrow_1 (k-1)) && \text{(def. } \uparrow_1\text{)} \\ &= a * (a \uparrow_2 (k-1)) && \text{(HI1)} \\ &= a * ((a \uparrow_2 (k-2)) * a) && \text{(def. } \uparrow_2\text{)} \\ &= a * ((a \uparrow_1 (k-2)) * a) && \text{(HI2)} \\ &= (a * (a \uparrow_1 (k-2))) * a && \text{(associatividade (G1))} \\ &= (a \uparrow_1 (k-1)) * a && \text{(def. } \uparrow_1\text{)} \\ &= (a \uparrow_2 (k-1)) * a && \text{(HI1)} \\ &= a \uparrow_2 k. && \text{(def. } \uparrow_2\text{)} \end{aligned}$$

Pelo principio da indução segue que para todo $n \in \mathbb{N}$, $a \uparrow_1 n = a \uparrow_2 n$. Como a foi arbitrário membro de G, isso termina nossa demonstração que $\uparrow_1 = \uparrow_2$.

x11.43S. Graças ao Corolário 11.61, basta demonstrar que para todo $a \in G$, $\left(a^{-1}\right)^2 * a^2 = e$. Seja $a \in G$ então. Calculamos:

$$\begin{aligned}
\left(a^{-1}\right)^2 * a^2 &= (a^{-1} * a^{-1}) * a^2 && \text{(def. } \left(a^{-1}\right)^2\text{)} \\
&= (a^{-1} * a^{-1}) * (a * a) && \text{(def. } a^2\text{)} \\
&= \big((a^{-1} * a^{-1}) * a\big) * a && \text{(ass.)} \\
&= \big(a^{-1} * (a^{-1} * a)\big) * a && \text{(ass.)} \\
&= \big(a^{-1} * e\big) * a && \text{(def. } a^{-1}\text{)} \\
&= a^{-1} * a && \text{(def. } e\text{)} \\
&= e && \text{(def. } a^{-1}\text{)}
\end{aligned}$$

Logo $\left(a^{-1}\right)^2$ é o inverso de a^2.

Mas, um segundo! Nessa maneira fizemos bem mais trabalho do que precisamos. Observe que praticamente repetimos aqui a demonstração do Lema Λ11.58! Seria melhor simplesmente usá-lo, chegando assim nessa demonstração bem mais simples:

$$\begin{aligned}
\left(a^2\right)^{-1} &= (aa)^{-1} && \text{(def. } a^2\text{)} \\
&= a^{-1}a^{-1} && \text{(inv. prod. (Lema Λ11.58))} \\
&= \left(a^{-1}\right)^2. && \text{(def. } \left(a^{-1}\right)^2\text{)}
\end{aligned}$$

x11.45S. Sejam $x, y \in G$. Pela hipótese temos:

$$(xy)^2 = x^2y^2 = xxyy;$$

e pela definição de $(xy)^2$ temos

$$(xy)^2 = xyxy.$$

Ou seja

$$xxyy = xyxy$$

e cancelando os x pela esquerda e os y pela direita, chegamos no desejado:

$$xy = yx.$$

x11.47S. Precisamos mostrar que existe $n \in \mathbb{N}_{>0}$ com $a^n = e$. Se $m > 0$, o conjunto $N := \{\, n \in \mathbb{N}_{>0} \mid a^n = e \,\}$ não é vazio, então pelo princípio da boa ordem (PBO) possui elemento mínimo e logo $o(a) = \min N < \infty$. Se $m < 0$, observe que $-m > 0$, e calcule:

$$a^{-m} = (a^m)^{-1} = e^{-1} = e,$$

e novamente $N \neq \emptyset$ e $o(a) < \infty$.

x11.48S. Sejam $i, j \in \{0, \ldots, n-1\}$ tais que $a^i = a^j$. Preciso mostrar que $i = j$. Sem perda de generalidade suponha que $i \leq j$, ou seja:

$$0 \leq i \leq j < n.$$

Agora temos

$$\underbrace{aa\cdots a}_{i} = \underbrace{aa\cdots aaa\cdots a}_{j}$$

E como $i \leq j$, quebramos o lado direito assim:

$$\underbrace{aa\cdots a}_{i} = \underbrace{\overbrace{aa\cdots a}^{i}\overbrace{aa\cdots a}^{j-i}}_{j}$$

Ou seja,

$$a^i = a^i a^{j-i}$$

e logo

$$e = a^{j-i}$$

pelo Corolário 11.62. Achamos então uma potência de a igual à identidade e: $a^{j-i} = e$. Logo $j - i \geq n$ ou $j - i = 0$, pela definição da $o(a)$. A primeira alternativa é impossível pela escolha dos i, j, e logo concluimos que $j - i = 0$, ou seja, $i = j$.

x11.49S. Sejam $a, b, c \in G$. Calculamos:

$$\begin{aligned}
\Big(\Big(c(ab)^{-1}\Big)^{-1}(cb^{-1})\Big)(b^{-1}b)^{-1} &= \Big(\Big(c(ab)^{-1}\Big)^{-1}(cb^{-1})\Big)(b^{-1}(b^{-1})^{-1}) \\
&= \Big(\Big(c(ab)^{-1}\Big)^{-1}(cb^{-1})\Big)(b^{-1}b) \\
&= \Big(\Big(c(ab)^{-1}\Big)^{-1}(cb^{-1})\Big)e \\
&= \Big(c(ab)^{-1}\Big)^{-1}(cb^{-1}) \\
&= \Big(\Big((ab)^{-1}\Big)^{-1}c^{-1}\Big)(cb^{-1}) \\
&= \big((ab)c^{-1}\big)(cb^{-1}) \\
&= (ab)(c^{-1}c)b^{-1} \\
&= (ab)eb^{-1} \\
&= (ab)b^{-1} \\
&= a(bb^{-1}) \\
&= ae \\
&= a.
\end{aligned}$$

x11.50S. Basta achar um *modelo* (ou seja, algo que satisfaz as leis) que não satisfaz a proposição que queremos mostrar sua indemonstrabilidade.
Para a (GA) tome o S_3, que é grupo mas não abeliano ($\varphi\psi \neq \psi\varphi$).
Para a (G3) tome o S do Nãoexemplo 11.27 que ja verificámos que não satisfaz a (G3), e que tu já demonstrou (Exercício x11.11) que ele goza das outras: (G0)–(G2).
Para a (G2) considere um conjunto $A = \{a, b\}$ com operação $*$ a *outl*:

$$x * y = x.$$

Facilmente o $(A\,; *)$ satisfaz as (G0)–(G1) mas não possui identidade.
Para a (G1) tome o $\mathbb{N}$ com a exponenciação: o conjunto obviamente é fechado, mas a operação não é associativa:

$$2^{(1^2)} \neq (2^1)^2.$$

x11.51S. Reflexividade: Seja $a \in G$. Procuramos $g \in G$ tal que $a = gag^{-1}$. Como $a = eae^{-1}$, temos que realmente $a \approx a$.
Simetria: Sejam $a, b \in G$ tais que $a \approx b$. Daí, seja $x \in G$ tal que $a = xbx^{-1}$. Operando pela esquerda com x^{-1} e pela direita com x, temos:

$$x^{-1}ax = x^{-1}xbx^{-1}x = b.$$

Mas $x = \big(x^{-1}\big)^{-1}$, ou seja $b = x^{-1}a\big(x^{-1}\big)^{-1}$ e logo $b \approx a$.
Transitividade: Sejam $a, b, c \in G$ tais que $a \approx b$ e $b \approx c$. Daí, sejam $x, y \in G$ tais que:

$$\begin{aligned} a &= xbx^{-1} \\ b &= ycy^{-1}. \end{aligned}$$

Substituindo a segunda na primeira, temos

$$\begin{aligned} a &= x\big(ycy^{-1}\big)x^{-1} \\ &= (xy)c\big(y^{-1}x^{-1}\big) && \text{(ass.)} \\ &= (xy)c(xy)^{-1}. && \text{(inverso de produto (}\Lambda\text{11.58))} \end{aligned}$$

Ou seja, $a \approx c$.

x11.54S. Demonstramos primeiramente por indução que para todo $n \in \mathbb{N}$, $\big(gag^{-1}\big)^n = ga^ng^{-1}$. Observe que

$$\begin{aligned} (gag^{-1})^0 &= e \\ ga^0g^{-1} &= geg^{-1} = gg^{-1} = e. \end{aligned}$$

Agora seja $k \in \mathbb{N}$ tal que

(H.I.) $$(gag^{-1})^k = ga^kg^{-1}.$$

Calculamos

$$\begin{aligned} (gag^{-1})^{k+1} &= (gag^{-1})^k(gag^{-1}) \\ &= (ga^kg^{-1})(gag^{-1}) && \text{(pela H.I.)} \\ &= ga^k(g^{-1}g)ag^{-1} \\ &= ga^kag^{-1} \\ &= ga^{k+1}g^{-1}. \end{aligned}$$

Para terminar a demonstração basta observar que para qualquer $n \in \mathbb{N}$ temos:

$$\begin{aligned}(gag^{-1})^n = ga^n g^{-1} &\implies \left((gag^{-1})^n\right)^{-1} = (ga^n g^{-1})^{-1} \\ &\implies (gag^{-1})^{-n} = (g^{-1})^{-1}(a^n)^{-1}g^{-1} \\ &\implies (gag^{-1})^{-n} = ga^{-n}g^{-1}.\end{aligned}$$

x11.55S. Isso é um corolário imediato do Exercício x11.54: Como x, y conjugados, temos $x = gyg^{-1}$ para algum $g \in G$. E agora calculamos:

$$\begin{aligned}x^n &= (gyg^{-1})^n \\ &= gy^n g^{-1}. \qquad \text{(pelo x11.54)}\end{aligned}$$

e logo x^n, y^n conjugados também.

Π11.1S. Injectividade:

$$f(x) = f(y) \implies ax = ay \implies x = y.$$

Sobrejectividade: Seja $y \in G$. Considere o $a^{-1}y \in G$. Observe que

$$f(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y = y.$$

A f^{-1} é definida pela:

$$f^{-1}(y) = a^{-1}y$$

pois, de fato, $f(a^{-1}y) = aa^{-1}y = y$. Similar para a g. Sobre a h, observe que $h = g \circ f$ e logo ela é bijetora como composição de bijetoras, e sua inversa é dada pela Exercício x9.64.

Π11.2S. Na demonstração do fato que as leis de cancelamento implicam a existência de inversos únicos, *usamos* a (G3) que garanta a existência, e demonstramos a unicidade. No caso do $(\mathbb{N}\,;+)$ não temos a (G3) (existência de inversos). Então nossa demonstração nesse caso mostra que cada membro de $(\mathbb{N}\,;+)$ tem *no máximo* um inverso, algo que realmente é verdade: o 0 tem exatamente um, e nenhum dos outros tem.

Π11.4S. Vamos demonstrar em detalhe o critério unilateral direito. A demonstração do esquerdo é simétricamente análoga. Demonstração da (G2'). Preciso demonstrar que a identidade direita 1_{R} é uma identidade esquerda. Seja $a \in G$. Basta verificar que $1_{\mathrm{R}}a \stackrel{?}{=} a$.

Calculamos:

$$\begin{aligned}
{}^{1}\mathrm{R}a &= {}^{1}\mathrm{R}a\,{}^{1}\mathrm{R} && (\text{def. } {}^{1}\mathrm{R})\\
&= {}^{1}\mathrm{R}a({a}^{\mathrm{R}}{a}^{\mathrm{R}{}^{\mathrm{R}}}) && (\text{def. } {a}^{\mathrm{R}{}^{\mathrm{R}}})\\
&= {}^{1}\mathrm{R}(a{a}^{\mathrm{R}}){a}^{\mathrm{R}{}^{\mathrm{R}}}\\
&= {}^{1}\mathrm{R}\,{}^{1}\mathrm{R}{a}^{\mathrm{R}{}^{\mathrm{R}}} && (\text{def. } {a}^{\mathrm{R}})\\
&= ({}^{1}\mathrm{R}\,{}^{1}\mathrm{R}){a}^{\mathrm{R}{}^{\mathrm{R}}}\\
&= {}^{1}\mathrm{R}{a}^{\mathrm{R}{}^{\mathrm{R}}} && (\text{def. } {}^{1}\mathrm{R})\\
&= (a{a}^{\mathrm{R}}){a}^{\mathrm{R}{}^{\mathrm{R}}} && (\text{def. } {a}^{\mathrm{R}})\\
&= a({a}^{\mathrm{R}}{a}^{\mathrm{R}{}^{\mathrm{R}}})\\
&= a\,{}^{1}\mathrm{R} && (\text{def. } {a}^{\mathrm{R}{}^{\mathrm{R}}})\\
&= a. && (\text{def. } {}^{1}\mathrm{R})
\end{aligned}$$

onde botei parenteses apenas para ajudar a leitura; seu uso sendo opcional graças a (G1).

Para demonstrar o (G3'), eu vou usar o Lemma:

$$(\forall g \in G)\Big[\, gg = g \implies g = {}^{1}\mathrm{R} \,\Big].$$

Demonstração do Lemma. Seja $g \in G$. Temos

$$\begin{aligned}
gg = g &\implies (gg)g^{\mathrm{R}} = gg^{\mathrm{R}} && ((\cdot g))\\
&\implies g(gg^{\mathrm{R}}) = {}^{1}\mathrm{R} && ((\mathrm{G1});\ \text{def. } g^{\mathrm{R}})\\
&\implies g\,{}^{1}\mathrm{R} = {}^{1}\mathrm{R} && (\text{def. } g^{\mathrm{R}})\\
&\implies g = {}^{1}\mathrm{R} && (\text{def. } {}^{1}\mathrm{R})
\end{aligned}$$

Demonstração da (G3'). Vou demonstrar que para todo $a \in G$, o ${a}^{\mathrm{R}}$ é um inverso esquerdo do a. Seja $a \in G$ então; preciso mostrar que ${a}^{\mathrm{R}}a \stackrel{?}{=} {e}^{\mathrm{R}}$. Verificamos que $({a}^{\mathrm{R}}a)({a}^{\mathrm{R}}a) = ({a}^{\mathrm{R}}a)$:

$$\begin{aligned}
({a}^{\mathrm{R}}a)({a}^{\mathrm{R}}a) &= {a}^{\mathrm{R}}(a{a}^{\mathrm{R}})a && ((\mathrm{G1}))\\
&= {a}^{\mathrm{R}}({}^{1}\mathrm{R})a && (\text{def. } {a}^{\mathrm{R}})\\
&= ({a}^{\mathrm{R}}\,{}^{1}\mathrm{R})a && ((\mathrm{G1}))\\
&= {a}^{\mathrm{R}}a. && (\text{def. } {}^{1}\mathrm{R})
\end{aligned}$$

e logo pelo Lemma concluimos que $({a}^{\mathrm{R}}a) = {}^{1}\mathrm{R}$.

Π11.7S. Sejam a, b conjugados.

Caso que $o(a) < \infty$.
Resolução 1. Preciso mostrar: (i) $b^n = e$; (ii) para todo m com $0 < m < n$, $b^m \neq e$.

(i) Pelo Exercício x11.55, temos que a^n e b^n são conjugados, mas $a^n = e$, e a classe de conjugação de e é o singleton $\{e\}$ (Exercício x11.52). Logo $b^n = e$.

(ii) Pela mesma observação cada suposto $b^m = e$ obrigaria $a^m = e$ também. Logo $o(b) = n$.
Resolução 2. Pelo Exercício x11.55 temos $a^{o(a)}$ conjugado com $b^{o(a)}$. Logo $b^{o(a)} = e$ e logo $o(b) \mid o(a)$. Similarmente $o(a) \mid o(b)$ e logo $o(a) = o(b)$ pois ambos são naturais.
Caso que $o(a) = \infty$. Tenho que para todo $n > 0$, $a^n \neq e$, e preciso mostrar a mesma coisa sobe os b^n. De novo, de qualquer suposto contraexemplo $m \in \mathbb{N}$ com $b^m = e$ concluimos $a^m = e$ que é absurdo pois $o(a) = \infty$.

Para uma resolução mais poderosa e simples, veja o Problema Π11.23.

x11.60S. Como $H \neq \emptyset$, tome $h \in H$. Pela hipótese, $hh^{-1} \in H$, ou seja $e \in H$. Como $e, h \in H$, de novo pela hipótese temos $eh^{-1} \in H$, ou seja $h^{-1} \in H$. Temos então que o H é fechado sob inversos. Basta demonstrar que é fechado sob a operação de G também: tomando $a, b \in H$, ganhamos $a, b^{-1} \in H$, então pela hipótese $a\big(b^{-1}\big)^{-1} \in H$, ou seja, $ab \in H$.

x11.63S. Os seguintes são todos os subgrupos do S_3:

$$\{\mathrm{id}\} \qquad \{\mathrm{id}, \varphi\} \qquad \{\mathrm{id}, \varphi\psi\} \qquad \{\mathrm{id}, \psi\varphi\} \qquad \big\{\mathrm{id}, \psi, \psi^2\big\} \qquad S_3.$$

x11.64S. O $H = \{\emptyset, X, A\}$ em geral não é um subgrupo, pois pode violar a lei (G0) no caso que $A \setminus X \notin H$, pois $A \triangle X = A \setminus X$.

x11.65S. Temos $H_1 \cap H_2 \subseteq G$. Observe primeiramente que $H_1 \cap H_2 \neq \emptyset$, pois $e \in H_1$ e $e \in H_2$ (os dois sendo subgrupos de G). Agora mostramos que o $H_1 \cap H_2$ é fechado sob a operação:

Sejam $a, b \in H_1 \cap H_2$.	
Logo $a, b \in H_1$ e $a, b \in H_2$.	(def. $\cap$)
Logo $ab \in H_1$ e $ab \in H_2$.	(H_1 e H_2 grupos)
Logo $ab \in H_1 \cap H_2$.	(def. $\cap$)

e sob inversos:

Seja $a \in H_1 \cap H_2$.	
Logo $a \in H_1$ e $a \in H_2$.	(def. $\cap$)
Logo $a^{-1} \in H_1$ e $a^{-1} \in H_2$.	(H_1 e H_2 grupos)
Logo $a^{-1} \in H_1 \cap H_2$.	(def. $\cap$)

e o resultado segue graças ao Critérion 11.99.

x11.68S. Reflexiva: Seja $a \in G$. Calculamos:

$$\begin{aligned} a \mathrel{R_H} a &\iff aa^{-1} \in H \\ &\iff e \in H \end{aligned}$$

que é verdadeiro pois $H \leq G$.
TRANSITIVA: Sejam $a, b, c \in G$ tais que $a \; R_H \; b$ e $b \; R_H \; c$. Precisamos mostrar que $a \; R_H \; c$, ou seja, mostrar que $ac^{-1} \in H$. Temos

$$\begin{aligned}
&(1) && ab^{-1} \in H && (a \; R_H \; b)\\
&(2) && bc^{-1} \in H && (b \; R_H \; c)\\
& && (ab^{-1})(bc^{-1}) \in H && (\text{pelas (1) e (2) pois } H \leq G)
\end{aligned}$$

Logo $ab^{-1}bc^{-1} = ac^{-1} \in H$.
SIMÉTRICA: Sejam $a, b \in G$ tais que $a \; R_H \; b$, ou seja, $ab^{-1} \in H$ (1). Vamos demonstrar que $b \; R_H \; a$, ou seja, queremos $ba^{-1} \in H$. Mas como H é fechado sob inversos, pela (1) temos que $\left(ab^{-1}\right)^{-1} \in H$. Mas calculando

$$\begin{aligned}
\left(ab^{-1}\right)^{-1} &= \left(b^{-1}\right)^{-1}a^{-1} && (\text{inv. de op.})\\
&= ba^{-1} && (\text{inv. de inv.})
\end{aligned}$$

ou seja, $ba^{-1} \in H$.

x11.69S. Graças ao Critério 11.99, precisamos verificar que $\langle a \rangle$ é fechado sob a operação e sob inversos.
FECHADO PELA OPERAÇÃO: Sejam $h_1, h_2 \in \langle a \rangle$. Logo $h_1 = a^{k_1}$ (1) e $h_2 = a^{k_2}$ (2) para alguns $k_1, k_2 \in \mathbb{Z}$. Precisamos mostrar que $h_1h_2 \in \langle a \rangle$. Calculamos:

$$\begin{aligned}
h_1h_2 &= a^{k_1}a^{k_2} && (\text{pelas (1),(2)})\\
&= a^{k_1+k_2} && (\text{pela Propriedade 11.78 (1)})\\
&\in \langle a \rangle\,. && (\text{def. } \langle a \rangle, \text{ pois } k_1 + k_2 \in \mathbb{Z})
\end{aligned}$$

FECHADO SOB INVERSOS: Seja $h \in \langle a \rangle$, logo $h = a^k$ para algum $k \in \mathbb{Z}$. Pela Propriedade 11.78 (3),

$$h^{-1} = \left(a^k\right)^{-1} = a^{-k} \in \langle a \rangle\,.$$

x11.70S. $\langle e \rangle = \{e\}$.

x11.73S. O problema é que não podemos chamar isso *subgrupo*, pois não é garantidamente fechado sob a operação. Por exemplo, sabendo que $a \in \langle a, b \rangle$ e $a * b \in \langle a, b \rangle$, deveriamos ter $(ab)a \in \langle a, b \rangle$, mas o $(ab)a$ *em geral* não pode ser escrito na forma $a^m b^n$. Uma outra observação similar que serve também é que o inverso de $ab \in \langle a, b \rangle$ é o $b^{-1}a^{-1}$ que também *em geral* não pode ser escrito na forma $a^m b^n$.

x11.74S. Pela sua forma, já é óbvio que

$$a^3b^{-2}cb^3d^{-1} \in \left\{\, a_0^{m_0} * \cdots * a_{k-1}^{m_{k-1}} \;\middle|\; k \in \mathbb{N};\; i \in \overline{k};\; m_i \in \mathbb{Z};\; a_i \in A \,\right\}.$$

Basta tomar $k := 5$ e

$$\begin{aligned}
a_0 &:= a & m_0 &:= 3\\
a_1 &:= b & m_1 &:= -2\\
a_2 &:= c & m_2 &:= 1\\
a_3 &:= b & m_3 &:= 3\\
a_4 &:= d & m_4 &:= -1
\end{aligned}$$

e pronto! Mas para mostrar que

$$a^3b^{-2}cb^3d^{-1} \in \left\{ a_0^{m_0} * \cdots * a_{k-1}^{m_{k-1}} \;\middle|\; k \in \mathbb{N};\ i \in \overline{k};\ m_i \in \{-1,1\};\ a_i \in A \right\}$$

não podemos fazer a mesma escolha, pois cada um dos m_i pode ser ou 1 ou -1. Basta só aumentar o k, e tomando $k := 10$ e

$$\begin{aligned}
a_0 &:= am_0 := 1 \quad a_5 := cm_5 := 1\\
a_1 &:= am_1 := 1 \quad a_6 := bm_6 := 1\\
a_2 &:= am_2 := 1 \quad a_7 := bm_7 := 1\\
a_3 &:= bm_3 := -1 a_8 := bm_8 := 1\\
a_4 &:= bm_4 := -1 a_9 := dm_9 := -1.
\end{aligned}$$

Finalmente para demonstrar que

$$a^3b^{-2}cb^3d^{-1} \in \left\{ a_0 * \cdots * a_{k-1} \;\middle|\; k \in \mathbb{N};\ i \in \overline{k};\ a_i \in A \text{ ou } {a_i}^{-1} \in A \right\}.$$

o k é o mesmo, $k := 10$, e basta escolher nossos a_i's em tal forma que cada um deles ou é membro de A ou seu inverso é. Fácil:

$$\begin{aligned}
a_0 &:= a \quad a_5 := c\\
a_1 &:= a \quad a_6 := b\\
a_2 &:= a \quad a_7 := b\\
a_3 &:= b^{-1} a_8 := b\\
a_4 &:= b^{-1} a_9 := d^{-1}.
\end{aligned}$$

x11.75S. Temos

$$\begin{aligned}
\langle \emptyset \rangle &= \{e\}\\
\langle G \rangle &= G.
\end{aligned}$$

x11.77S. A parte esquerda parece assim:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{b \in A}{b \in A_0}\,(1) \quad \dfrac{b \in A}{b \in A_0}\,(2)}{b^2 \in A_1}\,(3) \quad \dfrac{\dfrac{b \in A}{b \in A_0}\,(4)}{b \in A_1}\,(5)}{b^3 \in A_2}\,(6) \quad \dfrac{\vdots}{b \in A_2}\,(7)}{b^4 \in A_3}\,(8) \quad *}{\dfrac{\vdots}{b^7 \in A_6}\,*} \quad \dfrac{\vdots}{b \in A_6}\,(9)}{b^8 \in A_7}\,(10)}{b^{-8} \in A_8}\,(11)$$

Onde as justificativas são:

(1) def. A_0;

(2) def. A_0;
(3) def. A_1 (G0);
(4) def. A_0;
(5) $A_0 \subseteq A_1$ (Θ11.120);
(6) def. A_2 (G0);
(7) $A \subseteq A_2$ (Θ11.120);
(8) def. A_3 (G0);
(9) $A \subseteq A_6$ (Θ11.120);
(10) def. A_7 (G0);
(11) def. A_8 (G3).

Nas (*) usamos a regra inferida:

$$\frac{x^k \in A_m}{x^{k+1} \in A_{m+1}}\, x \in A \qquad \rightsquigarrow \qquad \frac{x^k \in A_k \qquad \dfrac{x \in A_0}{x \in A_k}\, A_0 \subseteq A_k}{x^2 \in A_{k+1}}\ \text{def. } A_{k+1}\ \text{(G0)}$$

O resto da árvore é justificado numa maneira parecida.

x11.78S.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{b \in A}{b \in A_0}*}{b^2 \in A_1}*}{b^4 \in A_2}* \qquad \dfrac{\dfrac{a \in A}{a \in A_0}*}{a^2 \in A_1} \qquad \dfrac{\dfrac{a \in A}{a \in A_0}}{a \in A_1}}{b^8 \in A_3} \qquad \dfrac{a^3 \in A_2}{a^3 \in A_4}}{b^{-8} \in A_4 \qquad\qquad a^3 b^{-8} \in A_5}$$

Onde explicamos a regra inferida (*):

$$\frac{x \in A_m}{x^2 \in A_{m+1}}\,* \qquad \rightsquigarrow \qquad \frac{x \in A_k \qquad x \in A_k}{x^2 \in A_{k+1}}$$

A parte esquerda com pouco mais detalhe parece assim:

$$\dfrac{\dfrac{\dfrac{\dfrac{b \in A}{b \in A_0} \qquad \dfrac{b \in A}{b \in A_0}}{b^2 \in A_1} \qquad \dfrac{\vdots}{b^2 \in A_1}}{b^4 \in A_2} \qquad \dfrac{\vdots}{b^4 \in A_2}}{b^8 \in A_3}$$

x11.79S. Precisamos verificar que a família $\mathscr{H}$ tem pelo menos um membro antes de intersectar (veja a resolução do Exercício x8.40). Fato, pois já temos um membro dela: o próprio G! É imediato verificar que $G \in \mathscr{H}$, e logo $\mathscr{H} \neq \emptyset$.

x11.80S. Imediato pelo Exercício x11.67, pois $\mathscr{H}$ e não vazia e todos os seus membros são subgrupos.

x11.81S. Pela definição da $\mathscr{H}$, para todo $H \in \mathscr{H}$ temos $A \subseteq H$. Logo $A \subseteq \bigcap \mathscr{H}$. Isso deveria ser óbvio, e resolvido desde Exercício x8.43.

x11.82S. Seja K tal que $A \subseteq K \leq G$. Como já demonstramos que $\bigcap \mathscr{H}$ é um grupo, e como K também é grupo, basta demonstrar $\bigcap \mathscr{H} \subseteq K$. Mas, pela sua escolha, K é um dos membros da família $\mathscr{H}$, e logo $\bigcap \mathscr{H} \subseteq K$. Se isso não é óbvio, resolva o Exercício x8.44.

x11.83S. Isso não é nada demais do que unicidade do mínimo, se existe, algo fácil para demonstrar num contexto geral para qualquer ordem (Exercício x14.1). Mas vamos ver essa demonstração nesse contexto especifico aqui. Suponha que $\overline{A}, A'$ ambos satisfazem a (i)–(ii). Vamos demonstrar que $\overline{A} = A'$. Como $\overline{A}$ satisfaz a (ii) e A' satisfaz a (i), temos

$$\overline{A} \leq A'.$$

No outro lado, A' satisfaz a (ii) e $\overline{A}$ satisfaz a (i), logo

$$A' \leq \overline{A}.$$

Logo $\overline{A} = A'$, pois a relação de subgrupo é antissimétrica (Exercício x11.61).

x11.84S. O $(\mathbb{R}\,;+)$ não é. O $(\mathbb{Q}\,;+)$ também não. O $(\mathbb{Z}\,;+)$ é: $\langle 1\rangle = (\mathbb{Z}\,;+)$. O $(\mathbb{R}_{\neq 0}\,;\cdot)$ não é. O $(\mathbb{Q}_{\neq 0}\,;\cdot)$ também não é. O $(\mathbb{Z}_6\,;+_6)$ é: $\langle 1\rangle = (\mathbb{Z}_6\,;+_6)$ O $(\mathbb{Z}_6 \setminus \{0\}\,;\cdot_6)$ nem é grupo! O S_3 não é.

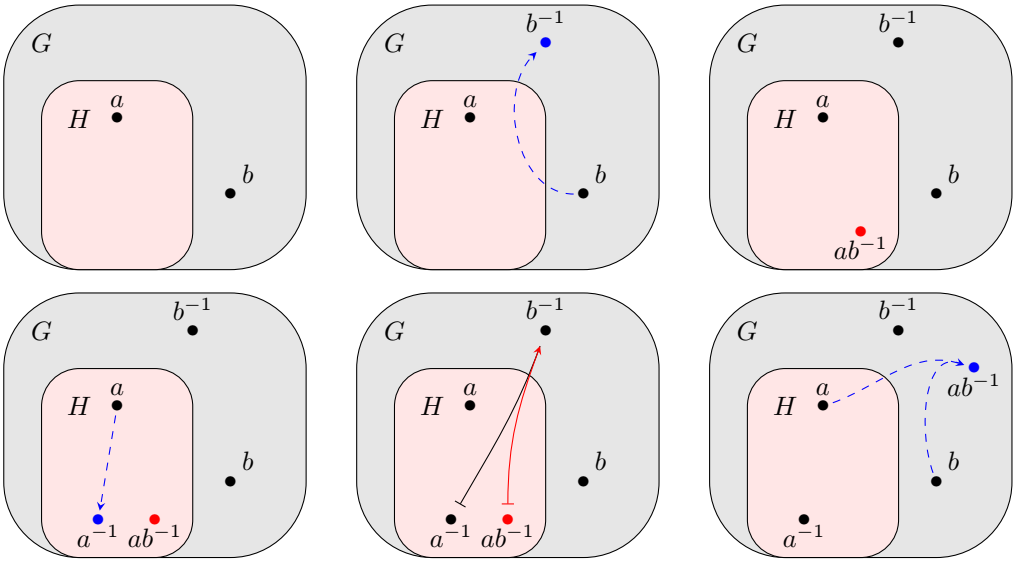
x11.85S. $\langle 1\rangle = \langle 5\rangle = \mathbb{Z}_6$.

Π11.11S. Primeiramente observe que $\mathrm{Z}(G) \neq \emptyset$: $e \in \mathrm{Z}(G)$ pois para todo $g \in G$, $eg = e = ge$ pela definição de e. Como $\emptyset \neq \mathrm{Z}(G) \subseteq G$, precisamos apenas mostrar que:
Fechado pela operação: Sejam $x, y \in \mathrm{Z}(G)$. Para demonstrar que $xy \in \mathrm{Z}(G)$, verificamos que o (xy) comuta com todos os elementos de G. Seja $g \in G$. Calculamos:

$$\begin{aligned}
(xy)g &= x(yg) && ((\mathrm{G1})) \\
&= x(gy) && (y \in \mathrm{Z}(G)) \\
&= (xg)y && ((\mathrm{G1})) \\
&= (gx)y && (x \in \mathrm{Z}(G)) \\
&= g(xy). && ((\mathrm{G1}))
\end{aligned}$$

Fechado sob inversos: Seja $x \in \mathrm{Z}(G)$. Para demonstrar que $x^{-1} \in \mathrm{Z}(G)$, verificamos que o x^{-1} comuta com todos os elementos de G. Seja $g \in G$. Calculamos:

$$\begin{aligned}
x^{-1}g &= \left(\left(x^{-1}g\right)^{-1}\right)^{-1} && (\text{inv. de inv.}) \\
&= \left(g^{-1}\left(x^{-1}\right)^{-1}\right)^{-1} && (\text{inv. de prod.}) \\
&= \left(g^{-1}x\right)^{-1} && (\text{inv. de inv.}) \\
&= \left(xg^{-1}\right)^{-1} && (x \in \mathrm{Z}(G)) \\
&= \left(g^{-1}\right)^{-1}x^{-1} && (\text{inv. de prod.}) \\
&= gx^{-1}. && (\text{inv. de inv.})
\end{aligned}$$



Os passos da resolução do Exercício x11.94.

Π11.12S. Sejam $G =: \{a_1, \ldots, a_n\}$ os $n > 0$ membros de G. O inteiro N que procuramos é o

$$N := \prod_{i=1}^{n} o(a_i).$$

Para confirmar, seja $w \in \{1, \ldots, n\}$ (assim temos uma arbitrário membro de G, o a_w). Basta mostrar que $a_w^N = e$:

$$\begin{aligned}
a_w^N &= a_w^{o(a_1)\cdots o(a_n)} && \text{(def. } N\text{)} \\
&= a_w^{o(a_w)(o(a_1)\cdots o(a_{w-1})o(a_{w+1})\cdots o(a_n))} && \text{(ensino fundamental)} \\
&= \left(a_w^{o(a_w)}\right)^{o(a_1)\cdots o(a_{w-1})o(a_{w+1})\cdots o(a_n)} && \text{(Propriedade 11.78-(2))} \\
&= e^{\text{coisa}} && \text{(def. } o(a_w)\text{)} \\
&= e. && \text{(Propriedade 11.78-(3))}
\end{aligned}$$

x11.94S. Sem perda de generalidade, suponha $a \in H$ e $b \notin H$. Primeiramente mostramos que $b^{-1} \notin H$:

$$b^{-1} \in H \implies \left(b^{-1}\right)^{-1} \in H \implies b \in H,$$

logo $b^{-1} \notin H$. Para chegar num absurdo, vamos supor que $ab^{-1} \in H$.
Vamos deduzir a contradição $b^{-1} \in H$. Para conseguir isso, observamos que $a^{-1} \in H$ (pois $a \in H$), e logo

$$\overbrace{\underbrace{a^{-1}}_{\in H}\underbrace{(ab^{-1})}_{\in H}}^{b^{-1}} \in H.$$

Achamos assim nossa contradição:

$$b^{-1} = eb^{-1} = (a^{-1}a)b^{-1} = a^{-1}(ab^{-1}) \in H.$$

Concluimos então que $ab^{-1} \notin H$, ou seja $a \not\equiv b \pmod{H}$.

x11.95S. No grupo $G := (\mathbb{Z}\,;+)$ considere seu subgrupo $H := 5\mathbb{Z}$. Temos:

$$\left.\begin{array}{l} G := (\mathbb{Z}\,;+) \\ H := 5\mathbb{Z} \\ a := 1 \\ b := 6 \end{array}\right\} \implies a \equiv b \pmod{H} \qquad \left.\begin{array}{l} G := (\mathbb{Z}\,;+) \\ H := 5\mathbb{Z} \\ a := 1 \\ b := 3 \end{array}\right\} \implies a \not\equiv b \pmod{H},$$

porque $1 + (-6) = -5 \in 5\mathbb{Z}$ e $1 + (-3) = -2 \notin 5\mathbb{Z}$ respectivamente.

x11.96S. Que $a = b$ (pela (GCL))—e logo que *para todo* i, $h_i a = h_i b$.

x11.97S. Qualquer coclasse de H tem a forma Ha ou aH para algum $a \in G$. Observe que o proprio $a \in Ha$, pois

$$a = \underbrace{e}_{\in H} a \in Ha,$$

e similarmente $a \in aH$.

x11.98S. ($\Rightarrow$). Suponha $Ha = H$. Como $e \in H$, então $ea \in Ha$, mas $ea = a$ e pronto. Numa linha só:

$$a = ea \in Ha = H.$$

($\Leftarrow$). Suponha $a \in H$. Para demonstrar $Ha = H$ separamos as duas direcções: ($\subseteq$). Seja $x \in Ha$, e logo seja $h \in H$ tal que $x = ha$. Mas $a \in H$ e logo $ha \in H$ pois H é fechado sob a operação do grupo. Ou seja, $x \in H$. ($\supseteq$). Seja $h \in H$. Para mostrar que $h \in Ha$ procuramos $h' \in H$ tal que $h = h'a$. Tome $h' := ha^{-1}$ e confirma que $h = ha^{-1}a$, e logo $h \in Ha$ pois $ha^{-1} \in H$. Sabemos disso pois H sendo subgrupo de G é fechado sob inversos (logo $a^{-1} \in H$) e pela operação também, e logo $ha^{-1} \in H$.

x11.99S. Podemos concluir que: *se $a \notin H \leq G$ então H e Ha são disjuntos:* Suponha que H e Ha tem algum membro em comum h. Vamos chegar numa contradição, demonstrando assim que $H \cap Ha = \emptyset$. Como $h \in Ha$, logo seja $h_1 \in H$ tal que $h = h_1 a$. Passando o h_1 para o outro lado, temos

$$\underbrace{(h_1)^{-1}h}_{\in H} = \underbrace{a}_{\notin H}$$

que é absurdo.

x11.100S. Suponha que Ha e Hb tem algum membro em comum w. Logo sejam $h_a, h_b \in H$ tais que $w = h_a a$ e $w = h_b b$. Logo

$$h_a a = h_b b$$

e passando o h_b para o outro lado temos:

$$\underbrace{\underbrace{(h_b)^{-1}h_a}_{\in H}\, a}_{\in Ha} = b$$

que contradiz que $b \notin Ha$.

x11.101S. Um nome que faz sentido pensar aqui seria *divisão*, se pensar multiplicativamente; e *subtraição*, se pensar aditivamente. Mas pra ser mais específicos ainda deveriamos mudar incluir como adjectivo o lado: *divisão direita* ou *subtraição direita*. Como assim divisão/subtraição "direita"? Nunca escutamos isso antes, mas isso é porque nossa operação (multiplicação de números ou adição de números) foi comutativa, então ab^{-1} e $b^{-1}a$ eram sempre o mesmo número. Mas aqui no contexto geral de grupo podem ser diferentes, então faz sentido incluir os lados mesmo!

x11.102S. Sejam $a, b \in G$. Calculamos:

$$\begin{aligned}
(a_b)x &= axb && \text{(def. } (a_b)\text{)} \\
&= a(xb) && \text{(assoc.)} \\
&= a((_b)x) && \text{(def. } (_b)\text{)} \\
&= (a_)((_b)x) && \text{(def. } (a_)\text{)} \\
&= ((a_) \circ (_b))(x). && \text{(def. } \circ\text{)}
\end{aligned}$$

Demonstramos a outra igualdade similarmente.

x11.105S. Se $H \leq G$, pelo teorema de Lagrange temos que $o(H) \mid o(G) = p$, logo $o(H) = 1$ ou p. No primeiro caso $H = \{e\}$, no segundo, $H = G$. Ou seja: *um grupo com ordem primo não tem subgrupos não-triviais.*

x11.106S. Sabemos que $\langle a \rangle$ é um subgrupo de G, com ordem $o(\langle a \rangle) = o(a)$, e pelo teorema de Lagrange, como $\langle a \rangle \leq G$ e G é finito temos

$$o(a) = o(\langle a \rangle) \mid o(G).$$

x11.107S. Graças ao Corolário 11.163 temos que $o(a) \mid o(G)$, ou seja, $o(G) = ko(a)$ para algum $k \in \mathbb{Z}$. Agora calculamos:

$$a^{o(G)} = a^{ko(a)} = a^{o(a)k} = \left(a^{o(a)}\right)^k = e^k = e.$$

x11.114S. Suponha $H \leq G$ com Precisamos mostrar que $aH = Ha$ para todo $a \in G$. Como o índice de H é 2, só tem 2 cosets, logo, fora do próprio H, seu complemento $G \setminus H$ tem que ser um coset. Agora para qualquer aH com $a \notin H$, temos

$$aH = G \setminus H = Ha.$$

x11.115S. Sejam a, a', b, b' tais que $aN = a'N$ e $bN = b'N$, e como $N \trianglelefteq G$ temos $aN = a'N = Na'$ e $bN = b'N = Nb'$. Basta demonstrar que $(ab)N = (a'b')N$. Demonstramos apenas a direção $(\subseteq)$(a outra é similar).

($\subseteq$): Precisamos mostrar que um arbitrario membro do $(ab)N$ pertence ao $(a'b')N$. Seja $n \in N$. O abn então já é um arbitrário membro do $(ab)N$. Basta demonstrar que $abn \in (a'b')N$, ou seja escrevê-lo na forma:

$$abn = a'b' \underbrace{?}_{\in N} .$$

Calculamos:

$$\begin{aligned} abn &= an'b' && \text{(onde } n' \in N \text{ tal que } bn = n'b' \text{ (pela } bN = Nb')) \\ &= a'n''b' && \text{(onde } n'' \in N \text{ tal que } an' = a'n'' \text{ (pela } aN = a'N)) \\ &= a'b'n''' && \text{(onde } n''' \in N \text{ tal que } n''b' = b'n''' \text{ (pela } Nb' = b'N)) \end{aligned}$$

x11.118S. A $(\forall g \in G)\big[\, gNg^{-1} = N \,\big]$, pois escolhendo a $(\forall g \in G)\big[\, gNg^{-1} \subseteq N \,\big]$, a gente teria menos trabalho pra fazer.

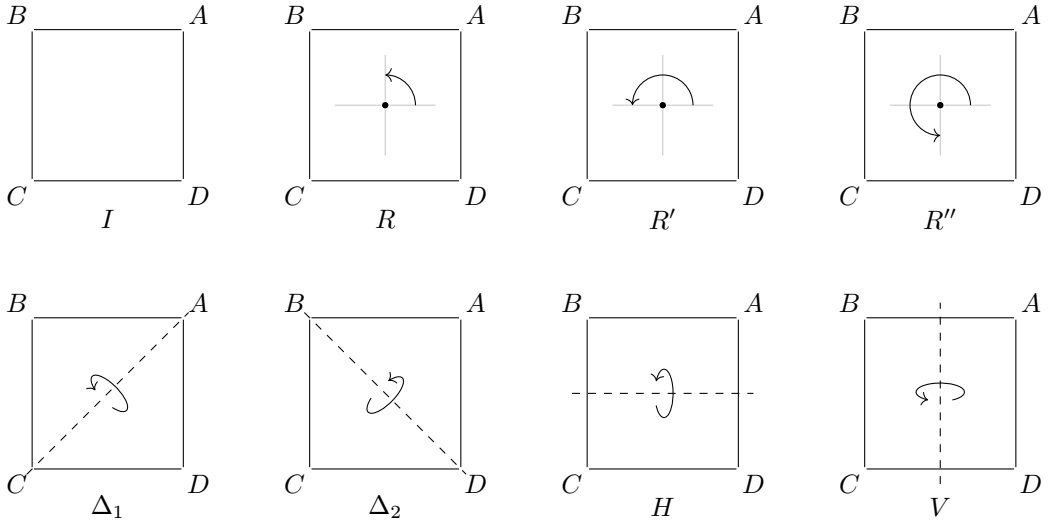
x11.122S. Temos $S \cap N \leq N \leq G$ como intersecção de subgrupos (veja exercícios x11.65 e x11.61). Basta mostrar que $S \cap N \trianglelefteq S$, ou seja, que $S \cap N$ é fechado pelos conjugados no S. Tome $x \in S \cap N$ e $h \in S$. Temos:

$$\begin{aligned} hxh^{-1} &\in S && (S \leq G) \\ hxh^{-1} &\in N && (N \trianglelefteq G) \end{aligned}$$

Logo $hxh^{-1} \in S \cap N$.

Π11.20S. Seja $a \in G$. Basta demonstrar que Ha e H têm a mesma quantidade de elementos (a demonstração sobre as coclasses esquerdas é similar). Vamos fazer isso mostrando uma bijecção entre os dois conjuntos. Primeiramente observe que a função $(_a) : G \to G$ é injetora (Lema Λ11.149) e logo sua restricção $(_a)\restriction H$ também é. Basta mostrar que ela é sobrejetora no Ha. Seja $d \in Ha$, e logo pela definição de Ha seja $h \in H$ tal que $d = ha$. Temos então $(_a)\restriction H(h) = d$, e logo $(_a)\restriction H$ é sobrejetora no Ha.

x11.125S. Aqui todas as simetrias dum quadrado:

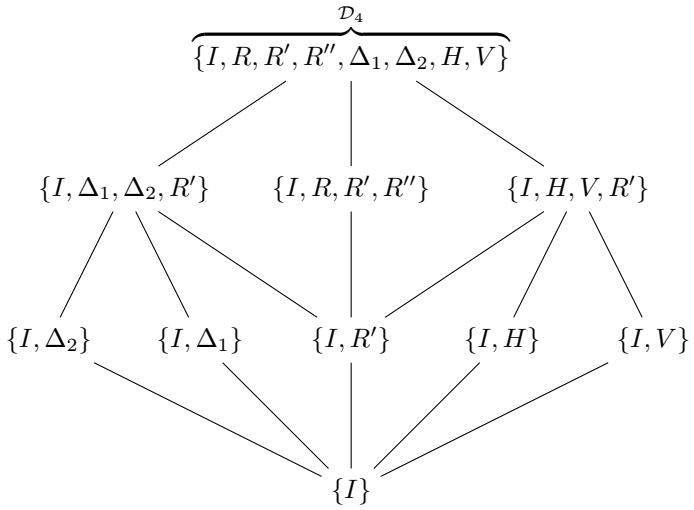


x11.127S. Basta achar uma propriedade grupoteórica que um dos dois grupos tem e o outro não. Uns exemplos:

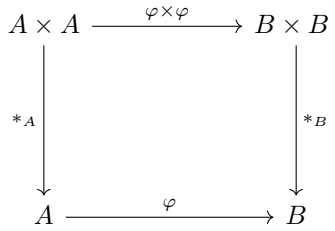
- «__ é abeliano»: satisfeita por $\mathbb{Z}_8$ mas não por $\mathcal{D}_4$;
- «__ é cíclico»: satisfeita por $\mathbb{Z}_8$ mas não por $\mathcal{D}_4$;
- «__ tem 3 membros de ordem 2»: satisfeita por $\mathcal{D}_4$ mas não por $\mathbb{Z}_8$;

etc.

x11.128S.



x11.134S.



x11.138S. Sejam $x, y \in G$. Calculamos

$$\mathrm{id}(xy) = xy = \mathrm{id}(x)\,\mathrm{id}(y)$$

e logo id é um homomorfismo, e como id é bijetora e endomapa, id é um automorfismo.

x11.141S. Considere a propriedade seguinte:

$$\text{Para todo } w, \text{ existe } u \text{ tal que } u + u = w.$$

Ela é uma propriedade grupoteórica, válida no $(\mathbb{Q}\,;+)$ e inválida no $(\mathbb{Z}\,;+)$. Em outras palavras, suponha para chegar num absurdo que temos um isomorfismo desses grupos $\varphi : \mathbb{Z} \to \mathbb{Q}$. Olhe para o $w := \varphi(1)$ (qualquer número ímpar serveria em vez do 1). Sendo racional, o $u := \varphi(1)/2$ também é racional e temos:

$$w = u + u.$$

Qual inteiro é o φ^{-1}? Deve ser um inteiro que satisfaz

$$\varphi^{-1}(u) + \varphi^{-1}(u) = \varphi^{-1}(u + u) = \varphi^{-1}(w) = 1$$

mas tal inteiro não existe. Logo, não pode existir nenhum isomorfismo entre os $(\mathbb{Z}\,;+)$ e $(\mathbb{Q}\,;+)$.

Usando uma outra propriedade grupoteórica para diferenciar os dois grupos seria observar que um é cíclico, mas o outro não é.

x11.142S. Primeiramente observamos que $\ker\varphi \neq \emptyset$: $e_A \in \ker\varphi$, pois φ é um homomorfismo e logo leva a e_A para a e_B. Então graças ao Critérion 11.99, basta demonstrar:
$\ker\varphi$ É FECHADO SOB A OPERAÇÃO: Sejam $x, y \in \ker\varphi$. Precisamos mostrar que $xy \in \ker\varphi$, ou seja, que $\varphi(xy) = e_B$. Calculamos:

$$\begin{aligned} \varphi(xy) &= \varphi(x)\varphi(y) && (\varphi \text{ homo (oper.)}) \\ &= e_B e_B && (x, y \in \ker\varphi) \\ &= e_B. && (\text{def. } e_B) \end{aligned}$$

$\ker\varphi$ É FECHADO SOB INVERSOS: Seja $x \in \ker\varphi$. Precisamos mostrar que $x^{-1} \in \ker\varphi$, ou seja, que $\varphi(x^{-1}) = e_B$. Calculamos:

$$\begin{aligned} \varphi(x^{-1}) &= (\varphi(x))^{-1} && (\varphi \text{ homo (inv.)}) \\ &= {e_B}^{-1} && (x \in \ker\varphi) \\ &= e_B. && (\text{inverso da identidade (Lema A11.55)}) \end{aligned}$$

x11.143S. Seja $k \in \ker\varphi$ e tome $a \in A$. Precisamos demonstrar que o a-conjugado de k também está no $\ker\varphi$: $aka^{-1} \in \ker\varphi$. Calculamos:

$$\begin{aligned}
\varphi(aka^{-1}) &= \varphi(a)\varphi(k)\varphi(a^{-1}) && (\varphi \text{ homo}) \\
&= \varphi(a)e_B\varphi(a^{-1}) && (k \in \ker\varphi) \\
&= \varphi(a)\varphi(a^{-1}) && (\text{def. } e_B) \\
&= \varphi(a)(\varphi(a))^{-1} && (\varphi \text{ homo}) \\
&= e_B && (\text{def. } (\varphi(a))^{-1})
\end{aligned}$$

Logo $aka^{-1} \in \ker\varphi$ como queremos demonstrar.

x11.144S. Calculamos:

$$\begin{aligned}
\varphi(aka^{-1}) &= \varphi(a)\varphi(k)\varphi(a^{-1}) && (\varphi \text{ homo (oper.)}) \\
&= \varphi(a)e_B\varphi(a^{-1}) && (k \in \ker\varphi) \\
&= \varphi(a)\varphi(a^{-1}) && (\text{def. } e_B) \\
&= \varphi(aa^{-1}) && (\varphi \text{ homo (oper.)}) \\
&= \varphi(e_A) && (\text{def. } a^{-1}) \\
&= e_B && (\varphi \text{ homo (iden.)})
\end{aligned}$$

x11.145S. $\operatorname{im}\varphi$ FECHADO SOB A OPERAÇÃO: Sejam $x', y' \in \operatorname{im}\varphi$. Logo, sejam $x, y \in A$ tais que $\varphi x = x'$, e $\varphi y = y'$. Calculamos:

$$\begin{aligned}
\varphi(xy) &= \varphi(x)\varphi(y) && (\varphi \text{ homo (oper.)}) \\
&= x'y'. && (\text{pela escolha dos } x, y)
\end{aligned}$$

Ou seja, $x'y' \in \operatorname{im}\varphi$.
$\operatorname{im}\varphi$ FECHADO SOB INVERSOS: Seja $x' \in \operatorname{im}\varphi$. Logo, seja $x \in A$ tal que $\varphi x = x'$. Calculamos:

$$\begin{aligned}
\varphi(x^{-1}) &= (\varphi x)^{-1} && (\varphi \text{ homo (inv.)}) \\
&= (x')^{-1}. && (\text{pela escolha do } x)
\end{aligned}$$

Ou seja, $x' \in \operatorname{im}\varphi$.

Π11.24S. Primeiramente precisamos demonstrar que $\operatorname{Hom}(G, G')$ é $(+)$-fechado. Então sejam $\varphi, \psi \in \operatorname{Hom}(G, G')$ e $x, y \in G$. Calculamos:

$$\begin{aligned}
(\varphi + \psi)(x + y) &= \varphi(x + y) + \psi(x + y) && (\text{pointwise } (+)) \\
&= \varphi(x) + \varphi(y) + \psi(x) + \psi(y) && (\varphi, \psi \text{ homo}) \\
&= \varphi(x) + \psi(x) + \varphi(y) + \psi(y) && (G' \text{ abeliano}) \\
&= (\varphi + \psi)(x) + (\varphi + \psi)(y). && (\text{def. } \varphi + \psi)
\end{aligned}$$

Agora basta só confirmar que realmente é abeliano. Fácil:

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x) = \psi(x) + \varphi(x) = (\psi + \varphi)(x).$$

Observe que precisamos a comutatividade apenas no G', ou seja, $(\mathrm{Hom}(G, G')\ ;\ +)$ é abeliano se G' é.

Π11.26S. Como $\mathrm{Aut}\, G \subseteq \mathrm{Bij}\, G$ precisamos verificar apenas que $\mathrm{Aut}\, G$ é:
NÃO VAZIO: $\mathrm{id} : G \to G$ é um automorfismo (Exercício x11.138) e logo $\mathrm{Aut}\, G \neq \emptyset$.
FECHADO PELA OPERAÇÃO: Tome $\varphi, \psi \in \mathrm{Aut}\, G$, e $x, y \in G$. Calculamos:

$$\begin{aligned}(\varphi \circ \psi)(x \cdot y) &= \varphi(\psi(x \cdot y)) && \text{(def. } \circ\text{)}\\ &= \varphi(\psi(x) \cdot \psi(y)) && (\psi \text{ homo})\\ &= \varphi(\psi(x)) \cdot \varphi(\psi(y)) && (\varphi \text{ homo})\\ &= (\varphi \circ \psi)(x) \cdot (\varphi \circ \psi)(y). && \text{(def. } \circ\text{)}\end{aligned}$$

FECHADO SOB INVERSOS: Tome $\varphi \in \mathrm{Aut}\, G$. Precisamos verificar que a bijecção φ^{-1} é realmente um homomorfismo. Ou seja, precisamos mostrar que

$$\varphi^{-1}(x \cdot y) = \varphi^{-1}(x) \cdot \varphi^{-1}(y)$$

para todos os $x, y \in G$. Seguindo a dica, basta demonstrar que

$$\varphi\big(\varphi^{-1}(x \cdot y)\big) = \varphi\big(\varphi^{-1}(x) \cdot \varphi^{-1}(y)\big)$$

O lado esquerdo é igual ao $x \cdot y$. Calculamos o lado direito:

$$\begin{aligned}\varphi\big(\varphi^{-1}(x) \cdot \varphi^{-1}(y)\big) &= \varphi\big(\varphi^{-1}(x)\big) \cdot \varphi\big(\varphi^{-1}(y)\big) && (\varphi \text{ homo})\\ &= x \cdot y. && (\text{def. } \varphi^{-1})\end{aligned}$$

Π11.27S. Precisamos demonstrar: $\mathrm{Inn}\, G \subseteq \mathrm{Aut}\, G$; $\mathrm{Inn}\, G \leq \mathrm{Aut}\, G$; $\mathrm{Inn}\, G \trianglelefteq \mathrm{Aut}\, G$.

$\mathrm{Inn}\, G \subseteq \mathrm{Aut}\, G$. Seja $f \in \mathrm{Inn}\, G$. Logo seja $g \in G$ tal que $f = (g_g^{-1})$. Precisamos mostrar que f é um automorfismo. Já demonstramos que é bijetora (Lema Λ11.149) então basta demonstrar que é um homomorfismo. Pelo Critério 11.219, é suficiente mostrar que f respeita a operação. Calculamos:

$$\begin{aligned}f(x)f(y) &= \big((g_g^{-1})x\big)\big((g_g^{-1})y\big)\\ &= \big(gxg^{-1}\big)\big(gyg^{-1}\big)\\ &= gxg^{-1}gyg^{-1}\\ &= gxeyg^{-1}\\ &= g(xy)g^{-1}\\ &= f(xy).\end{aligned}$$

$\mathrm{Inn}\, G \leq \mathrm{Aut}\, G$. Vamos usar o Critério 11.99. Primeiramente mostramos que $\mathrm{Inn}\, G \neq \emptyset$: de fato, $\mathrm{id}_G \in \mathrm{Inn}\, G$, pois id_G é um inner:

$$\mathrm{id}_G = \big(e_e^{-1}\big).$$

$\mathrm{Inn}\, G$ $\circ$-FECHADO. Agora sejam $f_1, f_2 \in \mathrm{Inn}\, G$. Vou demonstrar que $f_1 \circ f_2$ é um inner. Como f_1, f_2 são inners, sejam g_1, g_2 tais que

$$f_1 = \big(g_1_{g_1}^{-1}\big) \qquad\qquad f_2 = \big(g_2_{g_2}^{-1}\big).$$

Para um arbitrário $x \in G$ temos:

$$\begin{aligned}(f_1 \circ f_2)x &= f_1(f_2 x)\\ &= f_1(g_2 x {g_2}^{-1})\\ &= g_1(g_2 x {g_2}^{-1}){g_1}^{-1}\\ &= (g_1 g_2)x({g_2}^{-1}{g_1}^{-1})\\ &= (g_1 g_2)x(g_1 g_2)^{-1}.\end{aligned}$$

Ou seja, $f_1 \circ f_2 \in \operatorname{Inn} G$.

$\operatorname{Inn} G$ $^{-1}$-FECHADO. Seja $f \in \operatorname{Inn} G$, e logo seja $g \in G$ tal que $f = (g_g^{-1})$. Observe que (g^{-1}_g) é a inversa da f, e que realmente é um inner, pois

$$(g^{-1}_g) = \left(g^{-1}_(g^{-1})^{-1}\right),$$

ou seja, $f^{-1} \in \operatorname{Inn} G$.

$\operatorname{Inn} G$ FECHADO SOB CONJUGADOS. Seja $f \in \operatorname{Inn} G$ e logo seja $g \in G$ tal que $f = (g_g^{-1})$. Vou mostrar que todos os conjugados de f são inners. Seja então $\alpha \in \operatorname{Aut} G$. Basta demonstrar que $\alpha f \alpha^{-1} \in \operatorname{Inn} G$. Ou seja, basta resolver o

$$\alpha f \alpha^{-1} = \left(\,?\,_\,?\,^{-1}\right).$$

Para um arbitrário $x \in G$ temos:

$$\begin{aligned}(\alpha \circ f \circ \alpha^{-1})x &= \alpha\big(f(\alpha^{-1}x)\big) && \text{(def. } \circ\text{)}\\ &= \alpha\big(g * (\alpha^{-1}x) * g^{-1}\big) && \text{(pela escolha de } g\text{)}\\ &= \alpha g * \alpha(\alpha^{-1}x) * \alpha(g^{-1}) && (\alpha \text{ homo: resp. op.})\\ &= \alpha g * (\alpha \circ \alpha^{-1})x * \alpha(g^{-1}) && \text{(def. } \circ\text{)}\\ &= \alpha g * x * \alpha(g^{-1}) && \text{(def. } \alpha^{-1}\text{)}\\ &= \alpha g * x * (\alpha g)^{-1} && (\alpha \text{ homo: resp. inv.})\end{aligned}$$

e logo $\alpha f \alpha^{-1} \in \operatorname{Inn} G$.

Π11.29S. Formalização: *Seja G grupo e $N \trianglelefteq G$. Logo existem grupo G' e homomorfismo $\varphi : G \to G'$ tal que N é o kernel de φ.*

DEMONSTRAÇÃO. Considere o grupo G/N e defina a $\varphi : G \to G/N$ pela

$$\varphi(x) = Nx.$$

Basta demonstrar que:

(i) φ é um homomorfismo;
(ii) $\ker \varphi = N$.

(i) Basta verificar que φ respeita a operação. Sejam $x, y \in G$. Calculamos

$$\varphi(xy) = N(xy) = (Nx)(Ny) = \varphi(x)\varphi(y).$$

(ii) Temos

$$\begin{aligned}x \in \ker\varphi &\iff \varphi(x) = e_{G/N} && \text{(def. } \ker\varphi\text{)}\\ &\iff \varphi(x) = N && (N \text{ é a identidade do } G/N)\\ &\iff Nx = N && \text{(def. } \varphi\text{)}\\ &\iff x \in N. && \text{(Exercício x11.98)}\end{aligned}$$

Ou seja, $\ker \varphi = N$.

Com isso concluimos que na teoria dos grupos, "subgrupo normal" e "kernel" são dois lados da mesma moeda.

Capítulo 12

x12.1S. Temos:

$$\psi(1+1) = \mathsf{01} \neq \mathsf{00} = \psi(1) +\!\!+ \psi(1).$$

x12.3S. Vamos demonstrar que $\varphi(\varepsilon_M) = \varepsilon_N$, ou seja, que para todo $n \in N$,

$$n \cdot_N \varphi(\varepsilon_M) = n = \varphi(\varepsilon_M) \cdot_N n.$$

Seja $n \in N$. Logo $n = \varphi(m)$ para algum $m \in M$ (pois φ sobre N). Calculamos:

$$\begin{aligned} n \cdot_N \varphi(\varepsilon_M) &= \varphi(m) \cdot_N \varphi(\varepsilon_M) && \text{(pela escolha do } m) \\ &= \varphi(m \cdot_M \varepsilon_M) && (\varphi \text{ homo: resp. op.}) \\ &= \varphi(m) && \text{(pela (G2))} \\ &= n && \text{(pela escolha do } m) \end{aligned}$$

Similarmente, $n = \varphi(\varepsilon_M) \cdot_N n$.

Alternativamente, podemos começar assim: seja $m \in M$ tal que $\varphi(m) = e_N$; e agora

$$\begin{aligned} \varphi(e_M) &= \varphi(e_M)e_N && \text{(def. } e_N) \\ &= \varphi(e_M)\varphi(m) && \text{(pela escolha de } m) \\ &= \varphi(e_M m) && (\varphi \text{ homo: resp. op.}) \\ &= \varphi(m) && \text{(def. } e_M) \\ &= e_N. && \text{(pela escolha de } m) \end{aligned}$$

x12.4S. A estrutura mais completa:

$$(R\,;+,\cdot,-,0,1)$$

onde seus símbolos têm as aridades $(2,2,1,0,0)$ respectivamente. A estrutura mais pobre:

$$(R\,;+,\cdot)$$

com assinatura $(2,2)$.

x12.5S. Seja $\mathcal{R} = (R\ ;+,\cdot,-,0,1)$ um conjunto estruturado, onde $0,1$ são constantes, $+,\cdot$ são operações binárias, e $-$ unária. O $\mathcal{R}$ é um *anel* sse:

(i) $(R\,;+,-,0)$ é um grupo abeliano;
(ii) $(R\,;\cdot,1)$ é um monóide;
(iii) as seguintes leis são satisfeitas:

$$\begin{aligned} &\text{(RDL)} && (\forall a,b,c \in R)[\,a\cdot(b+c) = (a\cdot b)+(a\cdot c)\,] \\ &\text{(RDR)} && (\forall a,b,c \in R)[\,(b+c)\cdot a = (b\cdot a)+(c\cdot a)\,]. \end{aligned}$$

x12.10S. Se é pra ter tal anel R, qual seria o inverso de 0? Pelo Lema Λ12.22 temos que

$$0x = 0$$

para todo $x \in R$, e logo para $x := 0^{-1}$ também:

$$00^{-1} = 0$$

Mas $00^{-1} = 1$ pela definição de 0^{-1}, e logo

$$0 = 00^{-1} = 1.$$

Necessariamente então, em tal ring temos $0 = 1$. Pode ter mais membros além do 0? Não! Seja $r \in R$. Temos então

$$\begin{aligned} r &= 1r && \text{(def. 1)} \\ &= 0r && \text{(pois 0=1)} \\ &= 0 && \text{(pelo Lema Λ12.22)} \end{aligned}$$

e logo $R = \{0_R\}$.

x12.12S. Seja $p \in R$. Calculamos:

$$\begin{aligned} p + p &= (p+p)^2 && (R \text{ booleano}) \\ &= (p+p)(p+p) \\ &= (p+p)p + (p+p)q \\ &= pp + pp + pp + pp \\ &= p^2 + p^2 + p^2 + p^2 \\ &= p + p + p + p && (R \text{ booleano}) \\ &= p + p + (p+p) \end{aligned}$$

e logo $p + p = 0$, ou seja, $p = -p$.

x12.13S. Sejam $p, q \in R$. Calculamos:

$$\begin{aligned} (p+q)^2 &= (p+q)(p+q) \\ &= (p+q)p + (p+q)q \\ &= pp + qp + pq + qq \\ &= p^2 + qp + pq + q^2 \\ &= p + qp + pq + q. && (B \text{ booleano}) \end{aligned}$$

Mas como B é booleano temos também $(p+q)^2 = p + q$. Ou seja

$$\begin{aligned} p + q &= p + qp + pq + q \\ &= p + q + (qp + pq) \end{aligned}$$

e logo (Corolário 11.62)

(1) $$0 = qp + pq$$

ou seja, $pq = -qp$.

Para ganhar o Exercício x12.12 como corolário, é so tomar $q := 1$.

x12.14S. Sejam p, q membros dum anel booleano. Temos

$$\begin{aligned} pq &= -qp && \text{(Exercício x12.13, com } p := p \text{ e } q := q\text{)} \\ &= qp. && \text{(Exercício x12.12, com } p := qp\text{)} \end{aligned}$$

x12.19S. Seja $a \in L$. Calculamos

$$a \vee ((a \vee a) \wedge a) = a \vee a \qquad (\wedge\text{-abs.})$$

e também

$$\begin{aligned} a \vee ((a \vee a) \wedge a) &= ((a \vee a) \wedge a) \vee a && (\vee\text{-com.}) \\ &= (a \wedge (a \vee a)) \vee a && (\wedge\text{-com.}) \\ &= a && (\vee\text{-abs.}) \end{aligned}$$

Logo $a \vee a = a$.

x12.20S. ($\Rightarrow$): Suponha $b = a \vee b$. Calculamos

$$\begin{aligned} a \wedge b &= a \wedge (a \vee b) && \text{(hipótese)} \\ &= (a \vee b) \wedge a && (\wedge\text{-com.}) \\ &= a. && (\wedge\text{-abs.}) \end{aligned}$$

($\Leftarrow$): Similar.

x12.21S. O conjunto estruturado $\mathcal{L} = (L\,;\vee,\wedge)$ é um *lattice* sse os conjuntos estruturados $(L\,;\vee)$ e $(L\,;\wedge)$ são semilattices, e as leis de absorção são satisfeitas. $\mathcal{L} = (L\,;\vee,\wedge)$ é um *reticulado* sse $(L\,;\vee)$ e $(L\,;\wedge)$ são semirreticulados. Similarmente $(L\,;\vee,\wedge,0,1)$ é um reticulado limitado sse $(L\,;\vee,0)$ e $(L\,;\wedge,1)$ são semirreticulados limitados.

Capítulo 13

x13.1S. Definimos

$$\overline{n} \stackrel{\text{def}}{=} \{\, i \in \mathbb{N} \mid 0 \leq i < n \,\}.$$

x13.2S. Qualquer uma das definições abaixo serve:

$$\begin{aligned} \overline{0} &\stackrel{\text{def}}{=} \emptyset && & \overline{0} &\stackrel{\text{def}}{=} \emptyset \\ \overline{n} &\stackrel{\text{def}}{=} \overline{n-1} \cup \{n-1\} && (n > 0) & \overline{Sn} &\stackrel{\text{def}}{=} \overline{n} \cup \{n\}. \end{aligned}$$

x13.7S. Usamos as bijecções seguintes: identidade, composição, inversa.

x13.8S. Defina $F : A \times B \to A' \times B'$ pela $F(a,b) = (f(a), g(b))$. Ou seja, $F = f \times g$. Injectividade. Tome $\langle a_1, b_1\rangle \neq \langle a_2, b_2\rangle$ no $A \times B$. Logo $a_1 \neq a_2$ ou $b_1 \neq b_2$ (pela definição de $(=)$ nas tuplas). Logo

$$F(a_1, b_2) = \langle f(a_1), g(b_1)\rangle \neq \langle f(a_2), g(b_2)\rangle = F(a_2, b_2).$$

onde a $(\neq)$ segue pelas injectividades das f, g: pois se $a_1 \neq a_2$ então $f(a_1) \neq f(a_2)$, e se $b_1 \neq b_2$ então $g(b_1) \neq g(b_2)$. Sobrejectividade. Tome $\langle a', b'\rangle \in A' \times B'$. Logo $a' \in A'$ e $b' \in B'$, e como f e g são sobrejetoras, sejam $a \in A$ e $b \in B$ tais que $f(a) = a'$ e $g(b) = b'$. Observe que $F(a,b) = \langle f(a), g(b)\rangle = \langle a', b'\rangle$.

x13.9S. Defina $F : \wp A \to \wp A'$ pela $F(X) = f[X]$. Injectividade. Tome $X, Y \in \wp A$ tais que $X \neq Y$. Ou seja, existe $z \in X \mathbin{\triangle} Y$. Tome tal z e considere os $F(X)$ e $F(Y)$. Como f é injetora, o $f(z) \in F(X) \mathbin{\triangle} F(Y)$. Ou seja: $F(X) \neq F(Y)$. Sobrejectividade. Tome $X' \in \wp A'$. Observe que o $f_{-1}[X']$ é mapeado no X' através da F, graças ao Teorema Θ9.176.

x13.10S. Defina $F : (A \to B) \to (A' \to B')$ pela $F(t) = g \circ t \circ f^{-1}$. Injectividade. Sejam $s, t \in (A \to B)$ com $s \neq t$. Logo existe $a_0 \in A$ tal que $s(a_0) \neq t(a_0)$. Calcule:

$$\begin{aligned}
(F(s))(f(a_0)) &= (g \circ s \circ f^{-1})(f(a_0)) \\
&= (g \circ s \circ f^{-1} \circ f)(a_0) \\
&= (g \circ s)(a_0) \\
&= g(s(a_0)) \\
&\neq g(t(a_0)) && (g \text{ injetora e } s(a_0) \neq t(a_0)) \\
&= (g \circ t)(a_0) \\
&= (g \circ s \circ f^{-1} \circ f)(a_0) \\
&= (g \circ s \circ f^{-1})(f(a_0)) \\
&= (F(t))(f(a_0)).
\end{aligned}$$

Sobrejectividade. Seja $t' \in (A' \to B')$. Defina a $t \in (A \to B)$ pela

$$t = g^{-1} \circ t' \circ f$$

e observe que $F(t) = t'$.

x13.12S. Nenhuma! Como contraexemplo, tome os

$$A := \{\{0\}, \{1\}\} =_{\mathrm{c}} B := \{\{0,1\}, \{1,2\}\}$$

e calcule

$$\bigcup \{\{0\}, \{1\}\} = \{0,1\} \qquad \bigcap \{\{0\}, \{1\}\} = \emptyset$$
$$\bigcup \{\{0,1\}, \{1,2\}\} = \{0,1,2\} \qquad \bigcap \{\{0,1\}, \{1,2\}\} = \{1\}.$$

Ou seja, $\bigcup A \neq_{\mathrm{c}} \bigcup B$ e $\bigcap A \neq_{\mathrm{c}} \bigcap B$.

x13.13S. Defina $F : ((A \times B) \to C) \to (A \to (B \to C))$, pela

$$F(t) = \lambda a \,.\, \lambda b \,.\, t(a, b).$$

Injectividade. Tome $s, t \in ((A \times B) \to C)$ tais que $s \neq t$. Ou seja, para alguma entrada $\langle a_0, b_0\rangle \in (A \times B)$, as saídas são diferentes elementos de C:

$$s(a_0, b_0) \neq t(a_0, b_0).$$

Observe então que $F(s) \neq F(t)$, pois para a entrada a_0, elas retornam valores diferentes: a $F(s)$ retorna a função $\lambda b \,.\, s(a_0, b)$, e a $F(t)$ retorna a função $\lambda b \,.\, t(a_0, b)$. Para confirmar que realmente

$$\lambda b \,.\, s(a_0, b) \neq \lambda b \,.\, t(a_0, b)$$

basta observar que seus valores para a entrada $b := b_0$ são diferentes. Sobrejectividade. Toma um $f \in (A \to (B \to C))$. Defina a $t : (A \times B) \to C$ pela

$$t(a, b) = (f(a))(b)$$

e observe que realmente $F(t) = f$.

x13.19S. Vendo as expansões como strings (infinitos) feitos pelo alfabeto $0, \ldots, 9$ já temos que o conjunto de todos eles não é contável.

x13.20S. Os únicos conflitos de expansões envolvem reais com exatamente duas expansões: uma que a partir duma posição só tem 0's, e uma que a partir duma posição só tem 9's. Logo basta determinar uma maneira de trocar os digitais da diagonal que garanta que cada dígito mudou mesmo e que o número criado não termina nem em 0's nem em 9's: Mandamos todos os dígitos diferentes de 5 para o 4 e o 4 para o 5.

x13.31S. Seja A conjunto. Definimos a $f : a \rightarrowtail \wp a$ pela

$$f(x) = \{x\}\,.$$

Facilmente ela é injetora (Exercício x13.32).

Π13.3S. (1) Precisamos disso para que f seja bem-definida. Sem essa restricção, para onde f manda o $\langle 1/2, 1/3\rangle$? O $1/3$ realmente *determina* os b_j's, mas o $1/2$ não determina os a_i's pois:

$$0.4999\ldots = 1/2 = 0.5000\ldots$$

e logo a f não seria bem-definida sem essa restricção, já que seu valor dependeria (e mudaria) dependendo dessa escolha.
(2) A f não é bijetora! Basta só criar um exemplo que sua preimagem precisaria dum número cuja expansão termina em $000\ldots$:

$$f(?) = 0.5303030303\ldots$$

Nenhuma entrada (a, b) pode ser mapeada nesse número, pois pela definição da f o b só pode ser o $0.333\ldots = 1/3$ (e nenhum problema com isso), e agora o a só pode ser ser o $0.5000\ldots$, ou seja, $a = 1/2 = 0.5000\ldots = 0.4999\ldots$. Calculamos

$$f(\frac{1}{2}, \frac{1}{3}) = 0.43939393 \neq 0.530303\ldots$$

e logo f não é sobrejetora!

Π13.7S. Cada relação de equivalência corresponde numa partição e vice-versa, então descrevemos as três partições diretamente:

$$\begin{aligned}\mathscr{C}_1 &= \{(-\infty, 0), \{0\}, (0, +\infty)\}\\ \mathscr{C}_2 &= \{\, [n, n+1) \mid n \in \mathbb{Z} \,\}\\ \mathscr{C}_3 &= \{\, \{a\} \mid a \in \mathbb{R} \setminus \mathbb{Q} \,\} \cup \{\mathbb{Q}\}\,.\end{aligned}$$

Sem usar partições poderiamos definir as relações diretamente assim:

$$\begin{aligned}x \sim_1 y &\overset{\text{def}}{\iff} x = y \text{ ou } xy > 0\\ x \sim_2 y &\overset{\text{def}}{\iff} \lfloor x \rfloor = \lfloor y \rfloor\\ x \sim_3 y &\overset{\text{def}}{\iff} x = y \text{ ou } x, y \in \mathbb{Q}.\end{aligned}$$

Π13.8S. Seja $T \subseteq A$ o conjunto de todos os terminantes elementos de A. Basta demonstrar que $T \notin \varphi[A]$, ou seja, que para todo $x \in A$, $A_x \neq T$, demonstrando assim que φ não é bijetora. Suponha para chegar num absurdo que $T \in \varphi[A]$ e logo seja $a \in A$ tal que $T = A_a$ (1). Observe que $T \neq \emptyset$, pois se fosse vazio o a seria terminante e logo pertenceria ao T; absurdo. Vamos demonstrar que qualquer caminho de a é terminante. Seja α um caminho de a:

$$\alpha = (\alpha_0, \alpha_1, \alpha_2, \ldots)$$

Logo $\alpha_1 \in A_{\alpha_0} = A_a = T$, ou seja α_1 é terminante, e logo o caminho $(\alpha_1, \alpha_2, \ldots)$ é finito! Logo o $(\alpha_0, \alpha_1, \alpha_2, \ldots)$ também é. Mostramos então que o arbitrário caminho de a é finito; ou seja, todos são; ou seja, a é terminante (2) e logo $a \in T$ (3). Mas aqui um caminho infinito de a:

$$\begin{aligned}a_0 &:= a\\ a_1 &:= a\\ a_2 &:= a\\ a_3 &:= a\\ &\vdots\end{aligned}$$

ou seja, o caminho seguinte:

$$(a, a, a, \ldots)$$

Isso realmente é um caminho de a pois pelos (1) e (3), $a \in A_a$ e logo substituindo iguais por iguais,

$$\underbrace{a_{n+1}}_{a} \in A \underbrace{a_n}_{a}.$$

Concluimos então que a não é terminante, contradizendo o (2). Chegamos assim num absurdo, e logo nossa hipótese que $T \in \varphi[A]$ não é válida, ou seja, $T \notin \varphi[A]$ e logo φ não é sobrejetora.

Capítulo 14

x14.2S. Seja $m \in U$ o único membro do U. Vamos confirmar que satisfaz a definição de mínimo. Já temos que m é um membro do U, então basta verificar que

$$(\forall u \in U)[\, m \leq u \,].$$

Seja $u \in U$ então. Como U unitário, temos $m = u$. Portanto $m \leq u$ (pela reflexividade da $(\leq)$).

x14.3S. Já resolvido no Lema Λ4.112, pois na sua resolução não usamos nenhuma propriedade de números: todo que precisamos foi que A é totalmente ordenado pela $(\leq)$. Assim temos que todo conjunto finito, não vazio, e linearmente ordenado possui mínimo. Para concluir que é bem ordenado basta observar que qualquer subconjunto dum conjunto finito, é finito.

x14.6S. Vamos demonstrar usando um caminho "round-robin":

(i) ⇒ (ii). Seja $a \in {\downarrow}x$. Logo $a \leq x$, e como $x \leq y$ (hipótese), pela transitividade da $(\leq)$ temos $a \leq y$. Logo $a \in {\downarrow}y$. Ou seja, ${\downarrow}x \subseteq {\downarrow}y$.

(ii) ⇒ (iii). Seja D downset de P com $y \in D$. Logo ${\downarrow}y \subseteq D$. Pela hipótese ${\downarrow}x \subseteq {\downarrow}y$ e logo ${\downarrow}x \subseteq D$. Como $x \in {\downarrow}x$, então $x \in D$.

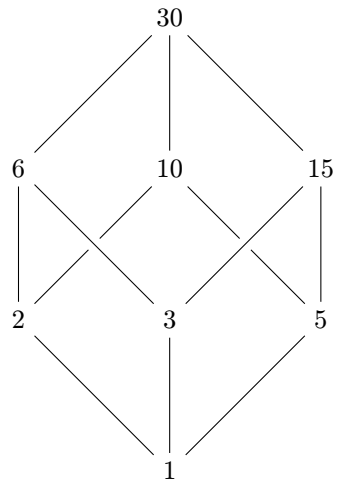
(iii) ⇒ (i). Observe que ${\downarrow}y$ é um downset tal que y pertence nele. Logo $x \in {\downarrow}y$ (pela hipótese). Logo $x \leq y$ (pela def. de ${\downarrow}y$).

x14.9S. $P_\perp \stackrel{\text{def}}{=} \mathbf{1} \oplus P$.

x14.15S. $\varphi(X) = P \setminus X$

x14.16S. $\psi(D) = \langle D \cap P_1, D \cap P_2 \rangle$.

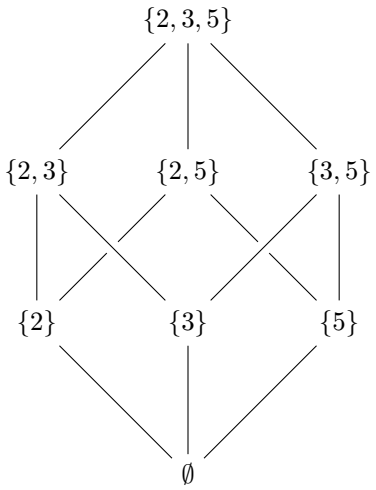
x14.17S. (i) Primeiramente calculamos: $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$.



(ii) Tome o $A = \{2, 3, 5\}$ e defina a função $\varphi : \wp A \to D_{30}$ pelas equações:

$$\begin{aligned}
\varphi(30) &= A \\
\varphi(15) &= \{3, 5\} \\
\varphi(10) &= \{2, 5\} \\
\varphi(6) &= \{2, 3\} \\
\varphi(2) &= \{2\} \\
\varphi(3) &= \{3\} \\
\varphi(5) &= \{5\} \\
\varphi(1) &= \emptyset
\end{aligned}$$

Seu diagrama Hasse parece assim:



Obs: qualquer conjunto A com $|A| = 3$ serve! Uma avantagem desse é que podemos bem elegantemente definir a bijecção inversa, mandando cada subconjunto de $\{2, 3, 5\}$ para seu produtório!
(iii) Não existe, pois $D_0 = \mathbb{N}$ (contável) e logo não pode ser equinúmero com o powerset de nenhum conjunto B.
(iv) Verdade, a função $\varphi : D_0 \to \{\, D_n \mid n \in \mathbb{N} \,\}$ definida pela

$$\varphi(n) = D_n$$

é um isomorfismo, pois:

$$n \mid m \iff D_n \subseteq D_m.$$

x14.19S. Como já definimos as iterações de qualquer endomapa (Definição D9.150), podemos simplesmente definir a órbita do $\bot$ como a seqüência $(f^n(\bot)_n)_n$. Alternativamente definimos diretamente por recursão:

$$\begin{aligned}
x_0 &= \bot \\
x_{n+1} &= f(x_n).
\end{aligned}$$

x14.20S. O $\emptyset$ é uma chain—como poderia não ser?—e logo o $\bigvee \emptyset$ existe. Mas o $\bigvee \emptyset$ é o bottom pela sua definição como menor de todos os upper bounds. (Já observamos que todo membro de p é trivialmente um upper bound do $\emptyset$.)

Π14.2S. Sobre o $\mathscr{L}_1$. Sejam $A, B \in \mathscr{L}_1$. Pela definição então $\mathbb{N} \setminus A$ e $\mathbb{N} \setminus B$ são finitos. Vou mostrar que $A \cup B$ e $A \cap B$ são cofinitos, e logo pertencem ao $\mathscr{L}_1$ também. Calculamos

$$\mathbb{N} \setminus (A \cup B) = (\mathbb{N} \setminus A) \cap (\mathbb{N} \setminus B)$$
$$\mathbb{N} \setminus (A \cap B) = (\mathbb{N} \setminus A) \cup (\mathbb{N} \setminus B),$$

logo os dois conjuntos no lado esquerdo são finitos como intersecção e união de finitos respectivamente.

Sobre o $\mathscr{L}_2$. Sejam $A, B \in \mathscr{L}_2$. Separamos em casos:
Caso ambos finitos: Facilmente $A \cup B$ e $A \cap B$ são finitos também, como intersecção e união de conjuntos finitos. Logo ambos pertencem ao $\mathscr{L}_2$.
Caso ambos cofinitos: Fechamos isso na demonstração sobre o $\mathscr{L}_1$.
Caso contrário: Temos um dos A, B finito e o outro cofinito. Sem perda de generalidade, suponha que A finito, B cofinito. O $A \cap B$ é trivialmente finito como intersecção de finito com qualquer conjunto. Logo $A \cap B \in \mathscr{L}_2$. O $A \cup B$ é cofinito, pois

$$\mathbb{N} \setminus (A \cup B) = (\mathbb{N} \setminus A) \cap (\mathbb{N} \setminus B)$$

que é finito para o mesmo motivo (intersecção com o $\mathbb{N} \setminus B$ que é finito). Logo $A \cup B \in \mathscr{L}_2$.

Π14.3S. Vamos demonstrar primeiramente a afirmação seguinte: *se $B \subseteq A_n$ para todo $n \in \mathbb{N}$, então B não é cofinito.*

demonstração da afirmação: Suponha que para todo $n \in \mathbb{N}$, $B \subseteq A_n$. Logo

$$B \subseteq \bigcap_{i=0}^{\infty} A_i$$

e complementando os dois lado,

$$\begin{aligned}
\mathbb{N} \setminus B &\supseteq \mathbb{N} \setminus \bigcap_{i=0}^{\infty} A_i \\
&= \bigcup_{i=0}^{\infty} (\mathbb{N} \setminus A_i) \\
&= \bigcup_{i=0}^{\infty} (\{0, 2, \dots, 2n-2\}) \\
&= 2\mathbb{N}.
\end{aligned}$$

Como $2\mathbb{N}$ é infinito, o B não é cofinito.

Agora voltamos a demonstrar que nenhum dos $\mathscr{L}_1, \mathscr{L}_2$ é completo. Considere o conjunto

$$\mathcal{S} := \{A_0, A_1, A_2, \dots\}$$

Observe que $\mathcal{S} \subseteq \mathscr{L}_1, \mathscr{L}_2$ pois todos os seus elementos são claramente cofinitos. Mesmo assim, o $\bigcap \mathcal{S}$ não é cofinito $\bigcap \mathcal{S}$ é o conjunto de todos os ímpares) e logo não pertence em nenhum dos $\mathscr{L}_1, L_2$.

Capítulo 16

x16.2S. Graças ao Emptyset (ZF2) temos o $\emptyset$. Aplicamos iterativamente o operador $\{-\}$ (Teorema Θ16.23) e assim construimos a seqüência infinita de singletons

$$\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \{\{\{\{\emptyset\}\}\}\}, \dots$$

Para os doubletons, uma abordagem seria aplicar o $\{\emptyset, -\}$ em todos os membros da seqüência acima começando com o segundo. Construimos assim a seqüência seguinte de doubletons:

$$\{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\{\emptyset\}\}\}, \{\emptyset, \{\{\{\emptyset\}\}\}\}, \{\emptyset, \{\{\{\{\emptyset\}\}\}\}\}, \dots$$

Outra idéia simples de descrever para criar uma infinidade de doubletons é a seguinte: começa com o doubleton dos dois primeiros singletons que construimos acima:

$$D_0 \stackrel{\text{def}}{=} \{\emptyset, \{\emptyset\}\}$$

e fique aplicando o operador $\{-\}$ em cada um dos membros:

$$\begin{aligned} D_1 &\stackrel{\text{def}}{=} \{\{\emptyset\}, \{\{\emptyset\}\}\} \\ D_2 &\stackrel{\text{def}}{=} \{\{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}\} \\ &\vdots \end{aligned}$$

x16.4S. A construção dum conjunto com cardinalidade finita n só pode ter sido garantida ou pelo Emptyset, se $n = 0$ (nesse caso o conjunto construido é o próprio $\emptyset$), ou pelo Pairset, se $n > 0$. Mas o Pairset só constrói conjuntos de cardinalidade 1 ou 2, dependendo se o aplicamos em conjuntos iguais ou não (respectivamente). Para concluir: nossos axiomas não são suficientemente poderosos para garantir a existência de conjuntos com cardinalidades maiores que 2.

x16.5S. Veja a discussão no 16.26.

x16.7S. Usando o (ZF4) definimos:

$$a \setminus b \stackrel{\text{def}}{=} \{\, x \in a \mid x \notin b \,\}.$$

x16.8S. Não tem como! Os axiomas que temos por enquanto não são suficientemente poderosos para definir nenhuma dessas operações!

x16.10S. Queremos mostrar que dado conjunto a, a classe

$$\big\{\, \{x\} \mid x \in a \,\big\}$$

é conjunto. Basta só achar um conjunto W tal que todos os $\{x\} \in W$. Botamos apenas o $W := \wp a$ que sabemos que é conjunto pelo Powerset (ZF5), assim ganhando o conjunto

$$\{\, z \in \wp a \mid (\exists x \in a)[\, z = \{x\}\,]\,\}.$$

pelo Separation (ZF4).

x16.11S. Sim. Seja $n \in \mathbb{N}$. Precisamos construir um conjunto A com $|A| \geq n$. Se $n = 0$, graças ao Emptyset (ZF2) tomamos $A := \emptyset$. Se $n > 0$, iteramos o operador $\wp -$ até chegar num conjunto cuja cardinalidade supera o n.

x16.12S. Não. Por exemplo, não temos como construir conjunto com cardinalidade 3, pois uma tal construção deveria "terminar" com uma aplicação do Powerset (o Emptyset constrói conjuntos com cardinalidade 0, e o Pairset com 1 ou 2). Mas aplicando o Powerset para conjunto com cardinalidade finita n, construimos conjunto com cardinalidade 2^n, e 3 não é uma potência de 2.

x16.15S. Sejam conjuntos a, b. Definimos:

$$a \cup b \stackrel{\text{def}}{=} \bigcup \{a, b\}$$
$$a \triangle b \stackrel{\text{def}}{=} \{\, x \in a \cup b \mid x \notin a \cap b \,\}$$

x16.16S. Não podemos. Dado conjunto a, se seu complemento a^{c} também fosse conjunto, poderiamos aplicar o $\cup$ para construir o $a \cup a^{\mathsf{c}}$. Mas pela definição dos $\cup$ e a^{c}, temos agora

$$x \in a \cup a^{\mathsf{c}} \iff x \in a \vee x \notin a$$

ou seja, todos os objetos x satisfazem a condição na direita! Em outras palavras $a \cup a^{\mathsf{c}}$ seria o próprio universo $\mathbb{V}$ que sabemos que não é um conjunto.

x16.17S. Dado conjunto $A \neq \emptyset$, definimos

$$\bigcap A \stackrel{\text{def}}{=} \left\{ x \in \bigcup A \mid (\forall a \in A)[\, x \in a \,] \right\}.$$

x16.18S. Como a, b são conjuntos, pelo Pairset o $\{a, b\}$ também é. Similarmente o $\{c, d\}$ é conjunto, e aplicando mais uma vez o Pairset neles temos que o $\{\{a, b\}, \{c, d\}\}$ é conjunto. Agora aplicando o Union nele o ganhamos o A.

Aqui uma construção do B pelos axiomas, em forma de árvore:

$$\dfrac{\dfrac{\dfrac{a \quad b}{\{a,b\}}\,\textsc{Pair} \qquad \dfrac{\dfrac{c \quad d}{\{c,d\}}\,\textsc{Pair}}{\{\{c,d\}\}}\,\textsc{Singleton}}{\{\{a,b\},\{c,d\}\}}\,\textsc{Pair}}{\{a,b,c,d\}}\,\textsc{Union}$$

Para o C, usamos o Separation (ZF4) no $\wp(\bigcup A)$, que é conjunto graças aos Union (ZF6) & Powerset (ZF5):

$$\dfrac{\dfrac{\dfrac{A}{\bigcup A}\,\textsc{Union}}{\wp \bigcup A}\,\textsc{Powerset}}{C}\,\textsc{Separation}, \varphi$$

onde na aplicação do Separation (ZF4) usamos a fórmula

$$\varphi(x) := \underbrace{\exists u \exists v (u \neq v \wedge \forall w (w \in x \leftrightarrow w = u \vee w = v))}_{\text{Doubleton}(x)} .$$

x16.19S. A direção '$\Longleftarrow$' é garantida pela nossa lógica: podemos substituir iguais por iguais em qualquer expressão.

x16.22S. Primeiramente verificamos que, dados objetos x, y, o $\langle x, y\rangle$ realmente é um conjunto:

$$\dfrac{\dfrac{}{\emptyset}\,\textsc{Empty} \quad \dfrac{x}{\{x\}}\,\textsc{Singleton}}{\{\emptyset, \{x\}\}}\,\textsc{Pair} \qquad \dfrac{\dfrac{y}{\{y\}}\,\textsc{Singleton}}{\{\{y\}\}}\,\textsc{Singleton}}{\{\{\emptyset, \{x\}\}, \{\{y\}\}\}}\,\textsc{Pair}$$

(TUP2): Sejam A, B conjuntos. Queremos demonstrar que a classe

$$A \times B = \{\, \langle x, y\rangle \mid x \in A \;\&\; y \in B \,\}$$

é um conjunto. Como na demonstração da Propriedade 16.51, Basta achar um conjunto W que contem o arbitrário $\langle a, b\rangle \in A \times B$, pois depois aplicamos o Separation (ZF4) com a mesma fórmula da Propriedade 16.51 para ganhar o $A \times B$. Um conjunto que serve como W é o $\wp\wp\wp(A \cup B)$, como verificamos aqui, escrevendo a derivação em forma de árvore:

$$\dfrac{\dfrac{}{\emptyset \in \wp(A \cup B)} \quad \dfrac{\dfrac{a \in A}{a \in A \cup B}}{\{a\} \in \wp(A \cup B)}}{\{\emptyset, \{a\}\} \in \wp\wp(A \cup B)} \qquad \dfrac{\dfrac{\dfrac{b \in B}{b \in A \cup B}}{\{b\} \in \wp(A \cup B)}}{\{\{b\}\} \in \wp(A \cup B)}}{\{\{\emptyset, \{a\}\}, \{\{b\}\}\} \in \wp\wp\wp(A \cup B)}$$

x16.24S. Seja o qualquer conjunto (tome $o := \emptyset$ por exemplo). Considere o $\{\{o\}, \{\{o\}\}\}$. Ele representa algum par ordenado? Calculamos:

$$\begin{aligned} \langle \{o\}, \{o\}\rangle &= \{\{o\}, \{\{o\}\}\} \\ \langle \{\{o\}\}, o\rangle &= \{\{\{o\}\}, \{o\}\} \end{aligned}$$

Observe que os conjuntos nos lados direitos são iguais:

$$\{\{o\}, \{\{o\}\}\} = \{\{\{o\}\}, \{o\}\}$$

e logo

$$\langle \{o\}, \{o\}\rangle = \langle \{\{o\}\}, o\rangle .$$

Isso já mostra que a (TUP1) não é satisfeita, pois $\{o\} \neq \{\{o\}\}$. (E nem $\{o\} = o$ mas só precisamos uma das duas ser falsa para concluir que a propriedade não é satisfeita.) ↯

A demonstração que acabamos de escrever tem um roubo sutil, que é muito fácil corrigir, mas difícil identificar! Para corrigi-lo, basta tomar o conjunto $\emptyset$ onde tomamos um arbitrário conjunto o, e a demonstração vira correta! O Problema II16.13 pede identificar o problema.

x16.32S. Fácil, como na demonstração da Propriedade 16.66:

$$(a \rightharpoonup b) = \{\, f \in \mathrm{Rel}\,(a,b) \mid f : A \rightharpoonup B \,\}$$

que é conjunto.

x16.34S. Usando o Separation (ZF4) escrevemos

$$\{\, f \in (A \rightharpoonup B) \mid f \subseteq F \,\}.$$

x16.35S. (i) Tome $\langle x, y\rangle \in F$. Para concluir que $\langle x, y\rangle \in \bigcup \mathscr{F}$ precisamos achar uma aproximação $f \in \mathscr{F}$ tal que $\langle x, y\rangle \in f$. Aqui uma: a aproximação $\{\langle x, y\rangle\} \subseteq F$. Conversamente, tome $\langle x, y\rangle$ in $\bigcup \mathscr{F}$. Pela definição de $\bigcup$ então temos que $\langle x, y\rangle \in f$ para alguma aproximação $f \in \mathscr{F}$. Pela definição de aproximação agora, $f \subseteq F$, ou seja: $\langle x, y\rangle \in f \subseteq F$.

(ii) Sim. A direção $\bigcup \mathscr{F}_{\mathrm{f}} \subseteq F$ é trivial graças ao (i), e a direção oposta também demonstramos no (i) pois a aproximação $\{\langle x, y\rangle\}$ que escolhemos nessa direção é realmente finita.

Π16.3S. (1) Dados os objetos a, b, queremos construir o $\{a, b\}$. Aplicando o (CONS) com $h := b$ e $t := \emptyset$ ganhamos o $\{b\}$, e agora aplicando novamente o mesmo axioma com $h := a$ e $t := \{b\}$ ganhamos o desejado $\{a, b\}$.
(2) Observe que com os axiomas (ZF1)+(ZF2)+(CONS) conseguimos construir conjuntos de qualquer cardinalidade finita, mas com os (ZF1)+(ZF2)+(ZF3) conseguimos construir apenas conjuntos com cardinalidades 0, 1, ou 2. Basta realmente construir um conjunto com cardinalidade maior que 2 então. Aplique o (CONS) com $h, t := \emptyset$ ganhando assim o $\{\emptyset\}$. Agora com $h := \{\emptyset\}$ e $t := \emptyset$ ganhando o $\{\{\emptyset\}\}$. Com $h := \emptyset$ e $t := \{\{\emptyset\}\}$ ganhamos o $\{\emptyset, \{\emptyset\}\}$. E finalmente, com $h, t := \{\emptyset, \{\emptyset\}\}$ construimos o $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, que tem cardinalidade 3.
(3) Sejam h, t conjuntos. Pelo singleton (Teorema Θ16.23) ganhamos o $\{h\}$, e usando a união binária (Exercício x16.15) nos $\{h\}$ e t ganhamos o desejado conjunto.

x16.41S. Para definir I como *o* conjunto que satisfaz tal propriedade precisamos: *existência & unicidade*. Existência é o que (ZF7) garanta; mas não temos—e nem podemos demonstrar—unicidade. Então precisamos definir o I como *um* conjunto que satisfaz aquela condição.

x16.42S. Tome

$$\begin{aligned} I_0 &:= I \\ I_1 &:= I \setminus \{\emptyset\} \\ I_2 &:= I \setminus \{\emptyset, \emptyset^+\} \\ I_3 &:= I \setminus \{\emptyset, \emptyset^+, \emptyset^+\} \\ &\vdots \end{aligned}$$

x16.43S. Pois $I \in \mathscr{I}$.

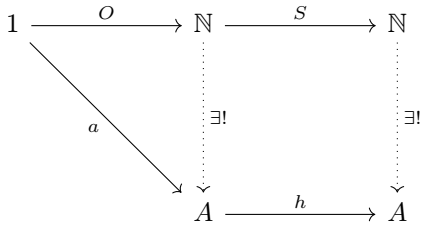
x16.50S. Como $\varphi[\mathbf{N}_1] \subseteq \mathbf{N}_2$, demonstramos a igualdade usando o princípio da indução (P5). Base. $\mathsf{O}_2 \in \varphi[\mathbf{N}_1]$: Imediato pois $\varphi(\mathsf{O}_1) = \mathsf{O}_2$. Passo indutivo. Suponha $k \in \varphi[\mathbf{N}_1]$. Precisamos mostrar que $\mathsf{S}_2 k \in \varphi[\mathbf{N}_1]$. Pela escolha de k, tome $k' \in \mathbf{N}_1$ tal que $\varphi(k') = k$. Calculamos:

$$\begin{aligned} \varphi(\mathsf{S}_1 k') &= \mathsf{S}_2(\varphi(k')) && \text{(pela def. } \varphi) \\ &= \mathsf{S}_2 k && \text{(pela escolha de } k') \end{aligned}$$

ou seja, $\mathsf{S}_2 k \in \varphi[\mathbf{N}_1]$.

x16.51S. Não temos demonstrado que dando equações recursivas como na demonstração desse teorema podemos realmente definir uma função. Fazemos isso no Teorema da Recursão Θ16.92, assim realmente botando o ∎ no Teorema Θ16.91.

x16.52S.



Π16.8S. (i) Um *multiset* é uma tupla $\mathcal{M} = \langle M; f\rangle$ onde M é um conjunto e $f : M \to \mathbb{N}_{>0}$.

$$\begin{aligned} \wr\wr &= \langle \emptyset; \emptyset\rangle \\ \wr 0, 1, 2, 2, 1\wr &= \langle \{0, 1, 2\}\,; f\rangle \\ \wr 1, 2, 2, 3, 3, 3, \ldots\wr &= \langle \mathbb{N}_{>0}; \mathrm{id}_{\mathbb{N}_{>0}}\rangle \end{aligned}$$

onde $f : \{0, 1, 2\} \to \mathbb{N}_{>0}$ é a função definida pela

$$f(n) = \begin{cases} 1, & \text{se } n = 0 \\ 2, & \text{se } n = 1 \\ 2, & \text{se } n = 2. \end{cases}$$

(ii)

$$\begin{aligned} \langle A; \alpha\rangle \uplus \langle B; \beta\rangle &\stackrel{\text{def}}{=} \langle A \cup B\ ;\ \lambda x.\max\{\alpha(x), \beta(x)\}\rangle \\ \langle A; \alpha\rangle \Cap \langle B; \beta\rangle &\stackrel{\text{def}}{=} \langle A \cap B\ ;\ \lambda x.\max\{\alpha(x), \beta(x)\}\rangle \\ \langle A; \alpha\rangle \oplus \langle B; \beta\rangle &\stackrel{\text{def}}{=} \langle A \cup B\ ;\ \lambda x.(\alpha(x) + \beta(x))\rangle \\ x \mathrel{\varepsilon} \langle A; \alpha\rangle &\stackrel{\text{def}}{\iff} x \in A \\ \langle A; \alpha\rangle \Subset \langle B; \beta\rangle &\stackrel{\text{def}}{\iff} A \subseteq B \ \&\ (\forall x \in A)[\alpha(x) \leq \beta(x)] \end{aligned}$$

(iii) A (MS1) é obviamente satisfeita graças à nossa definição de múltiset como tupla de conjunto e função: ganhamos assim a (MS1) pelas definições de (=) nos três tipos envolvidos: conjunto; tupla; função. Vamos verificar a (MS2). Seja A conjunto. O arbitrário multiset $\mathcal{M}$ com membros de A tem a forma $\mathcal{M} = \langle X, f\rangle$ para algum $X \subseteq A$ e

$f : X \to \mathbb{N}_{>0}$. Então $\mathcal{M} \in \wp A \times (A \rightharpoonup \mathbb{N}_{>0})$ e construimos o conjunto de todos os multisets com membros de A usando o ZF4:

$$\text{Multisets}(A) \stackrel{\text{def}}{=} \{\mathcal{M} \in \wp A \times (A \rightharpoonup \mathbb{N}_{>0}) \mid \mathcal{M} \text{ é um multiset.}\}$$

Para mostrar que o $\wp A \times (A \rightharpoonup \mathbb{N} \setminus \{0\})$ é um conjunto, precisamos os operadores $\wp$, $\times$, $\rightharpoonup$, $\setminus$, e o próprio $\mathbb{N}$, que já temos construido pelos ZF1–ZF7.

x16.67S. Definimos o operador $\Phi(-)$ assim:

$$\Phi(x) \stackrel{\text{def}}{=} \{x\}\,.$$

Facilmente, pelo Replacement (ZF8) aplicado no a com esse Φ temos que $\Phi[\![\, a \,]\!]$ é um conjunto: o conjunto que procuramos!

x16.75S. Seja $A \subseteq \omega^2 + 1$ com $A \neq \emptyset$. Temos a seguinte ordem no $\omega^2 + 1$:

$$\underbrace{\underbrace{\langle 0,0\rangle < \langle 1,0\rangle < \langle 2,0\rangle < \cdots}_{\omega} < \underbrace{\langle 0,1\rangle < \langle 1,1\rangle < \langle 2,1\rangle < \cdots}_{\omega} < \cdots}_{\omega^2} < \{\top\}\,.$$

Caso $A = \{\top\}$: $\min A = \top$.
Caso $A \neq \{\top\}$: Como $A \neq \emptyset$, concluimos que $A \cap \omega^2 \neq \emptyset$. Sejam:

$$\begin{aligned} y_0 &:= \min\{\, y \in \mathbb{N} \mid (\exists x \in \mathbb{N})[\, \langle x, y\rangle \in A \,]\,\} \\ x_0 &:= \min\{\, x \in \mathbb{N} \mid \langle x, y_0\rangle \in A\,\} \end{aligned}$$

onde os dois mínima existem graças ao PBO dos naturais. Facilmente, $\min A = \langle x_0, y_0\rangle$.

x16.76S.

(i) $\alpha = 0$
(ii) α é finito
(iii) $\alpha = 1$
(iv) α finíto & $\alpha \neq 0$
(v) ou $\begin{cases} \alpha \text{ finíto } \& \ \beta = \omega \\ \alpha = \omega \ \& \ \beta = 0 \end{cases}$
(vi) ou $\begin{cases} 1 \leq \alpha < \omega \ \& \ \beta = \omega \\ \alpha = \omega \ \& \ \beta = 1 \end{cases}$

Π16.11S. Seja A conjunto e $\varphi(x)$ fórmula. Definimos a class-function

$$\Phi(x) = \begin{cases} \{x\}\,, & \text{se } \varphi(x) \\ \emptyset, & \text{se não.} \end{cases}$$

Agora aplicamos o Replacement com essa class-function no conjunto A, ganhando assim como conjunto o $\Phi[\![\, A \,]\!]$, cujos elementos são exatamente os *singletons* $\{a\}$ de todos os $a \in A$ que satisfazem a $\varphi(a)$, e o $\emptyset$. Usando o ZF6 chegamos no $\bigcup \Phi[\![\, A \,]\!]$ que realmente é o desejado conjunto $\{\, a \in A \mid \varphi(a)\,\}$.

Π16.12S. Sejam a, b objetos. Considere a class-function

$$\Phi(x) := \begin{cases} a, & \text{se } x = \emptyset \\ b, & \text{se } x \neq \emptyset. \end{cases}$$

Agora precisamos apenas construir um conjunto S tal que: $\emptyset \in S$, e $|S| \geq 2$. Pelo Emptyset, temos o $\emptyset$. Pelo Powerset aplicado no $\emptyset$ ganhamos o $\{\emptyset\}$, e aplicando mais uma vez o Powerset chegamos no $\{\emptyset, \{\emptyset\}\}$. Usando o Replacement com a $\Phi(x)$ nesse conjunto, construimos o desejado $\{a, b\}$.

Em forma de árvore:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\emptyset}\,\text{Empty}}{\{\emptyset\}}\,\text{Power}}{\{\emptyset, \{\emptyset\}\}}\,\text{Power}}{\{a, b\}}\,\text{Repl; }\Phi$$

Π16.14S. Considere um x mal-fundamentado, que satisfaz a

$$x = \{o, \{x, y\}\}$$

para alguns y, o onde $o \neq y$. Calculamos o

$$\begin{aligned} \langle \{x, y\}, o \rangle &= \{\{x, y\}, \{\{x, y\}, o\}\} \\ &= \{\{x, y\}, x\} \\ &= \langle x, y \rangle \end{aligned}$$

mesmo com $o \neq y$, ou seja, achamos um contraexemplo mesmo.

Referências

[Abb15] Stephen D. Abbott.
Understanding Analysis.
Undergraduate Texts in Mathematics. Springer New York, 2015.

[Acz77] Peter Aczel.
An introduction to inductive definitions.
In Jon Barwise, editor, *Handbook of Mathematical Logic*, pages 739–782. North-Holland, Amsterdam, 1977.

[AHS09] J. Adamek, H. Herrlich, and G. E. Strecker.
Abstract and Concrete Categories: The Joy of Cats.
Dover books on mathematics. Dover Publications, 2009.

[Alu09] Paolo Aluffi.
Algebra: Chapter 0.
Graduate studies in mathematics. American Mathematical Society, 2009.

[AM75] Michael A. Arbib and Ernest G. Manes.
Arrows, structures, and functors: the categorical imperative.
Academic Press rapid manuscript reproductions. Academic Press, 1975.

[And94] George E. Andrews.
Number Theory.
Dover Books on Mathematics. Dover Publications, 1994.

[Apo67] Tom M. Apostol.
Calculus: One-variable calculus, with an introduction to linear algebra.
Calculus. Wiley, 1967.

[Apo69] Tom M. Apostol.
Calculus: Multi-variable calculus and linear algebra, with applications to differential equations and probability.
Calculus. Wiley, 1969.

[Apo76] Tom M. Apostol.
Introduction to analytic number theory.
Undergraduate Texts in Mathematics. Springer, 1976.

[AR10] Peter Aczel and Michael Rathjen.
Constructive set theory.
book draft: http://www1.maths.leeds.ac.uk/~rathjen/book.pdf, 2010.

[Awo10] Steve Awodey.
Category Theory.
Oxford Logic Guides. OUP Oxford, 2010.

[Bar13] Henk P. Barendregt.
The Lambda Calculus: Its Syntax and Semantics.
Studies in Logic and the Foundations of Mathematics. Elsevier Science, 2013.

[Bar14] Robert G. Bartle.
The Elements of Integration and Lebesgue Measure.
Wiley Classics Library. Wiley, 2014.

[Bim11] Katalin Bimbó.
Combinatory Logic: Pure, Applied and Typed.
Discrete Mathematics and Its Applications. Taylor & Francis, 2011.

[Bim14] Katalin Bimbó.
Proof Theory: Sequent Calculi and Related Formalisms.
Discrete Mathematics and Its Applications. Taylor & Francis, 2014.

[Bir98] Richard Bird.
Introduction to functional programming using Haskell.
Prentice Hall series in computer science. Prentice Hall Europe, 1998.

[Bir14] Richard Bird.
Thinking Functionally with Haskell.
Cambridge University Press, 2014.

[BM76] John Adrian Bondy and U. S. R. Murty.
Graph Theory with Applications.
American Elsevier Publishing Company, 1976.

[BM77a] John Bell and Moché Machover.
A Course in Mathematical Logic.
Elsevier Science & Technology, 1977.

[BM77b] Garrett Birkhoff and Saunders Mac Lane.
A Survey of Modern Algebra.
AKP classics. Taylor & Francis, 1977.

[BM11] John Adrian Bondy and U. S. R. Murty.
Graph Theory.
Graduate Texts in Mathematics. Springer London, 2011.

[Bol98] Béla Bollobás.
Modern Graph Theory.
Graduate Texts in Mathematics. Springer New York, 1998.

[Bor94] Francis Borceux.
Handbook of Categorical Algebra: Volume 1, Basic Category Theory.
Cambridge University Press, 1994.

[BW88] Richard Bird and Philip Wadler.
An Introduction to Functional Programming.
Prentice Hall International (UK) Ltd., 1988.

[BW90] Michael Barr and Charles Wells.
Category Theory for Computing Science.
Prentice Hall international series computer science. Prentice Hall, 1990.

[Can84] Georg Cantor.
Ueber unendliche, lineare punktmannichfaltigkeiten.
Math. Ann., 23, pages 453–488, 1884.

[Can91] Georg Cantor.
Ueber eine elementare frage der mannigfaltigkeitslehre.
Jahresbericht der DeutschenMathematiker-Vereinigung, pages 75–78, 1891.

[Can55] Georg Cantor.
Contributions to the founding of the theory of transfinite numbers.
Dover Books on Mathematics. Dover Publ., New York, 1955.

[Car00] N. L. Carothers.
Real Analysis.
Cambridge University Press, 2000.

[CD37] Georg Cantor and Richard Dedekind.
Briefwechsel cantor–dedekind.
1937.

[CG67] H. S. M. Coxeter and S. L. Greitzer.
Geometry Revisited.
Number v. 19 in Anneli Lax New Mathematical Library. Mathematical Association of America, 1967.

[CL00] René Cori and Daniel Lascar.
Mathematical Logic, Part 1: Propositional Calculus, Boolean Algebras, Predicate Calculus, Completeness Theorems.
Oxford University Press, 2000.

[CLRS09] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein.
Introduction to Algorithms, Third Edition.
The MIT Press, 3rd edition, 2009.

[Coh12] Paul J. Cohen.
Set Theory and the Continuum Hypothesis.
Dover books on mathematics. Dover Publications, 2012.

[Cur12] Haskell B. Curry.
Foundations of Mathematical Logic.
Dover Books on Mathematics. Dover Publications, 2012.

[Cut80] Nigel Cutland.
Computability: An Introduction to Recursive Function Theory.
Cambridge University Press, 1980.

[CZ12] G. Chartrand and P. Zhang.
A First Course in Graph Theory.
Dover books on mathematics. Dover Publications, 2012.

[Dav58] M.D. Davis.
Computability and Unsolvability.
Dover Books on Computer Science Series. Dover Publications, 1958.

[Die05] Reinhard Diestel.
Graph Theory.
Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2005.

[DP02] Brian A. Davey and Hilary A. Priestley.
Introduction to Lattices and Order (2nd ed.).
Cambridge University Press, 2002.

[DPV06] Sanjoy Dasgupta, Christos Papadimitriou, and Umesh Vazirani.
Algorithms.
McGraw-Hill Education, 2006.

[DW83] M.D. Davis and E.J. Weyuker.
Computability, Complexity and Languages: Fundamentals of Theoretical Computer Sciences.
Computer Science and Applied Mathematics Series. Academic Press, 1983.

[Esc04] Martín Escardó.
Synthetic topology of data types and classical spaces.
Electronic Notes in Theoretical Computer Science. Elsevier, 2004.

[Euc02] Euclid.
Euclid's Elements: all thirteen books complete in one volume.
Green Lion Press, 2002.

[Fer93] José Ferreirós.
On the relations between georg cantor and richard dedekind.
Historia Mathematica, 20:343–363, 1993.

[Fré06] Maurice Fréchet.
Sur quelques points de calcul fonctionnel.
PhD thesis, 1906.

[Gau66] Carl Friedrich Gauss.
Disquisitiones Arithmeticae.
Yale paperbound. Yale University Press, 1966.

[Gir95] Jean-Yves Girard.
Linear logic: Its syntax and semantics.
In *Proceedings of the Workshop on Advances in Linear Logic*, pages 1–42, New York, NY, USA, 1995. Cambridge University Press.

[Gir11] Jean-Yves Girard.
The Blind Spot: Lectures on Logic.
European Mathematical Society, 2011.

[GJ79] M.R. Garey and D.S. Johnson.
Computers and Intractability: A Guide to the Theory of NP-completeness.
Books in mathematical series. W. H. Freeman, 1979.

[GLT89] Jean-Yves Girard, Yves Lafont, and Paul Taylor.
Proofs and Types.
Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 1989.

[Gol06] Robert Goldblatt.
Topoi: The Categorial Analysis of Logic.
Dover books on mathematics. Dover Publications, 2006.

[Gou11] Fernando Quadros Gouvêa.
Was cantor surprised?
Amer. Math. Monthly, 118(3):198–209, 2011.

[Gra94] Robert Gray.
Georg cantor and transcendental numbers.
Amer. Math. Monthly, 101(9):819–832, 1994.

[Grä09] George Grätzer.
Lattice Theory: First Concepts and Distributive Lattices.
Dover Books on Mathematics Series. Dover Publications, 2009.

[Grä11] George Grätzer.
Lattice Theory: Foundation.
SpringerLink : Bücher. Springer Basel, 2011.

[Gun92] Carl A. Gunter.
Semantics of Programming Languages: Structures and Techniques.
Foundations of Computing. MIT Press, 1992.

[Hal60] Paul R. Halmos.
Naive set theory.
Litton Educational Publishing, Inc., 1960.

[Hal63] Paul R. Halmos.
Lectures on Boolean algebras.
Van Nostrand mathematical studies. Van Nostrand, 1963.

[Hal93] Paul R. Halmos.
Finite-Dimensional Vector Spaces.
Undergraduate Texts in Mathematics. Springer New York, 1993.

[Hal95] Paul R. Halmos.
Linear Algebra Problem Book.
Number v. 16 in Dolciani Mathematical Expositions. Mathematical Association of America, 1995.

[Hal13] Paul R. Halmos.
Measure Theory.
Graduate Texts in Mathematics. Springer New York, 2013.

[Har08] G. H. Hardy.
A Course of Pure Mathematics: Centenary Edition.
Cambridge Mathematical Library. Cambridge University Press, 2008.

[Har10] Robin Hartshorne.
Geometry: Euclid and Beyond.
Undergraduate Texts in Mathematics. Springer New York, 2010.

[Hau78] Felix Hausdorff.
Set Theory.
Chelsea Publishing Company, 1978.

[Her75] I. N. Herstein.
Topics in Algebra.
Wiley, 1975.

[HS08] J. R. Hindley and J. P. Seldin.
Lambda-Calculus and Combinators: An Introduction.
Cambridge University Press, 2008.

[HU79] J. E. Hopcroft and J. D. Ullman.
Introduction to Automata Theory, Languages, and Computation.
Addison–Wesley Series in Computer Science and Information Processing. Addison–Wesley, 1979.

[Hut16] Graham Hutton.
Programming in Haskell.
Cambridge University Press, 2016.

[HW79] G. H. Hardy and E. M. Wright.
An Introduction to the Theory of Numbers.
Oxford science publications. Clarendon Press, 1979.

[Jec13] Thomas Jech.
Set Theory.
Perspectives in Mathematical Logic. Springer Berlin Heidelberg, 2013.

[Joh86] P.T. Johnstone.
Stone Spaces.
Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1986.

[Jon97] Neil D. Jones.
Computability and Complexity: From a Programming Perspective.
Datalogisk Institut København: DIKU-Rapport. Datalogisk Inst., Univ., 1997.

[Jä95] Klaus Jänich.
Topology.
Undergraduate Texts in Mathematics. Springer New York, 1995.

[Kan03] Akihiro Kanamori.
The Higher Infinite: Large Cardinals in Set Theory from Their Beginnings.
2003.

[KF99] A. N. Kolmogorov and S. V. Fomin.
Elements of the Theory of Functions and Functional Analysis (two volumes in one).
Dover books on mathematics. Dover, 1999.

[Kle52] Stephen Cole Kleene.
Introduction to Metamathematics.
Bibliotheca Mathematica. Wolters–Noordhoff, 1952.

[Knu74] Donald E. Knuth.
Surreal numbers: how to ex-students turned on to pure mathematics and found total happiness: a mathematical novelette.
Addison–Wesley Professional, 1974.

[Knu97] Donald E. Knuth.
The Art of Computer Programming, Volume 2: Seminumerical Algorithms.
Addison–Wesley Longman Publishing Co., Inc., Boston, MA, USA, 3rd edition, 1997.

[Kol56] A. N. Kolmogorov.
Foundations of the Theory of Probability.
Chelsea, 1956.
Orig.: Grundbegriffe der Wahrscheinlichkeitsrechnung (1933).

[Koz97] Dexter C. Kozen.
Automata and Computability.
Undergraduate Texts in Computer Science. Springer, 1997.

[Koz06] Dexter C. Kozen.
Theory of Computation.
Springer, 2006.

[Kri71] Jean-Louis Krivine.
Introduction to axiomatic set theory.
D. Reidel publishing company, 1971.

[Kri93] J. L. Krivine.
Lambda-calculus, types and models.
Ellis Horwood series in computers and their applications. Ellis Horwood, 1993.

[Kun80] Kenneth Kunen.
Set Theory: An Introduction to Independence Proofs.
Mathematical Programming Study. North-Holland Publishing Company, 1980.

[Kun92] Kenneth Kunen.
Single axioms for groups.
Journal of Automated Reasoning, 9(3):291–308, Dec 1992.

[Kun09] Kenneth Kunen.
The Foundations of Mathematics.
Mathematical logic and foundations. College Publications, 2009.

[Kun11] Kenneth Kunen.
Set Theory.
Studies in logic. College Publications, 2011.

[Lan98] Serge Lang.
Basic Mathematics.
Springer New York, 1998.

[Lau08] Olivier Laurent.
Théorie de la démonstration (lecture notes).
2008.

[Lip12] Miran Lipovača.
Learn You a Haskell for Great Good.
No Starch Press, 2012.

[Llo87] John Wylie Lloyd.
Foundations of Logic Programming.
Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1987.

[LR03] F. William Lawvere and Robert Rosebrugh.
Sets for Mathematics.
Cambridge University Press, 2003.

[LS09] F. William Lawvere and Stephen H. Schanuel.
Conceptual Mathematics: A First Introduction to Categories.
Cambridge University Press, 2009.

[LS14] L. H. Loomis and S. Sternberg.
Advanced Calculus.
World Scientific, 2014.

[Mac13] Saunders Mac Lane.
Categories for the Working Mathematician.
Graduate Texts in Mathematics. Springer New York, 2013.

[MB99] Saunders Mac Lane and Garrett Birkhoff.
Algebra.
AMS Chelsea Publishing Series. Chelsea Publishing Company, 1999.

[MN12] Dale Miller and Gopalan Nadathur.
Programming with Higher-Order Logic.
Cambridge University Press, June 2012.

[Mon57] Richard Montague.
Contributions to the axiomatic foundations of set theory, 1957.

[Mos05] Yiannis N. Moschovakis.
Notes on set theory (2nd ed.).
Springer-Verlag New York, Inc., New York, NY, USA, 2005.

[Mos14] Yiannis N. Moschovakis.
Elementary Induction on Abstract Structures.
Dover Publications, 2014.

[Mos16] Yiannis N. Moschovakis.
Recursion and Computation (lecture notes v2.0).
2016.

[Mun00] James Raymond Munkres.
Topology.
Featured Titles for Topology Series. Prentice Hall, Incorporated, 2000.

[NG14] Rob Nederpelt and Herman Geuvers.
Type Theory and Formal Proof: An Introduction.
Cambridge University Press, New York, NY, USA, 1st edition, 2014.

[Niv65] Ivan Niven.
Mathematics of Choice: How to Count Without Counting.
Anneli Lax New Mathematical Library. Random House, 1965.

[Niv05] Ivan Niven.
Irrational Numbers.
Carus Mathematical Monographs. Mathematical Association of America, 2005.

[NPS90] Bengt Nordström, Kent Petersson, and Jan M. Smith.
Programming in Martin-Löf type theory: an introduction.
Clarendon, 1990.

[NvP08] Sara Negri and Jan von Plato.
Structural Proof Theory.
Cambridge University Press, 2008.

[NZ80] I. Niven and H. S. Zuckerman.
An Introduction to the Theory of Numbers.
Wiley, 1980.

[Pas65] Blaise Pascal.
Traité du triangle arithmétique avec quelques autres petits traitez sur la mesme matière.
G. Desprez, 1665.

[PdAC+17] Benjamin C. Pierce, Arthur Azevedo de Amorim, Chris Casinghino, Marco Gaboardi, Michael Greenberg, Cătălin Hriţcu, Vilhelm Sjöberg, and Brent Yorgey.
Software Foundations, Vol. 1.
Electronic textbook, 2017.

[Pie02] Benjamin C. Pierce.
Types and Programming Languages.
MIT Press, 2002.

[Pin10] Charles C. Pinter.
A Book of Abstract Algebra, 2nd ed.
Dover Books on Mathematics. Dover Publications, 2010.

[Poo14] Bjorn Poonen.
Why all rings should have a 1, 2014.

[Pra06] Dag Prawitz.
Natural Deduction: A Proof-Theoretical Study.
Dover Books on Mathematics. Dover Publications, 2006.

[Rie16] Emily Riehl.
Category Theory in Context.
Aurora: Dover Modern Math Originals. Dover Publications, 2016.

[Rog67] Hartley Rogers.
Theory of Recursive Functions and Effective Computability.
McGraw-Hill series in higher mathematics. McGraw-Hill, 1967.

[Ros13] John S. Rose.
A Course on Group Theory.
Dover Books on Mathematics. Dover Publications, 2013.

[Rot99] Joseph J. Rotman.
An Introduction to the Theory of Groups.
Graduate Texts in Mathematics. Springer New York, 1999.

[Rud76] Walter Rudin.
Principles of Mathematical Analysis.
International series in pure and applied mathematics. McGraw-Hill, 1976.

[Ser73] Jean-Pierre Serre.
A course in arithmetic.
Graduate Texts in Mathematics. Springer, 1973.

[Sha87] David Sharpe.
Rings and Factorization.
Cambridge University Press, 1987.

[Sho01] Joseph R. Shoenfield.
Recursion Theory.
Lecture Notes in Logic. Association for Symbolic Logic, 2001.

[Sim68] George F. Simmons.
Introduction to Topology and Modern Analysis.
International Series in pure and applied Mathematics. McGraw-Hill, 1968.

[Sim03] George F. Simmons.
Precalculus Mathematics in a Nutshell: Geometry, Algebra, Trigonometry: Geometry, Algebra, Trigonometry.
Resource Publications, 2003.

[Smu85] Raymond Smullyan.
To mock a mockingbird and other logic puzzles.
Knopf, 1985.

[Smu92] Raymond Smullyan.
Satan, Cantor, and Infinity.
Knopf, 1992.

[Smu14] Raymond Smullyan.
A Beginner's Guide to Mathematical Logic.
Dover Books on Mathematics. Dover Publications, 2014.

[Spi06] Michael Spivak.
Calculus.
Calculus. Cambridge University Press, 2006.

[Sri14] S. M. Srivastava.
How did cantor discover set theory and topology?
Resonance, 19(11):977–999, Nov 2014.

[SS94] Leon Sterling and Ehud Shapiro.
The art of Prolog (2nd ed.): advanced programming techniques.
MIT Press, Cambridge, MA, USA, 1994.

[Sto77] Joseph Stoy.
Denotational Semantics: The Scott–Strachey Approach to Programming Language

Theory.
The MIT Press Series in Computer Science. MIT Press, 1977.

[Str06] Thomas Streicher.
Domain-theoretic Foundations of Functional Programming.
World Scientific, 2006.

[SU06] Morten Heine Sørensen and Paweł Urzyczyn.
Lectures on the Curry–Howard Isomorphism, volume 149 of *Studies in Logic and the Foundations of Mathematics*.
Elsevier Science, 2006.

[Tak13] Gaisi Takeuti.
Proof Theory.
Dover books on mathematics. Dover, 2013.

[Tao16] Terrence Tao.
Analysis I: Third Edition.
Texts and Readings in Mathematics. Springer Nature Singapore, 2016.

[Tay12] A. E. Taylor.
General Theory of Functions and Integration.
Dover Books on Mathematics Series. Dover Publications, Incorporated, 2012.

[Ten76] R. D. Tennent.
The denotational semantics of programming languages.
Commun. ACM, 19(8):437–453, August 1976.

[Ten91] R. D. Tennent.
Semantics of Programming Languages.
PHI series in computer science. Prentice Hall, 1991.

[TW95] Richard Taylor and Andrew Wiles.
Ring-theoretic properties of certain hecke algebras.
Annals of Mathematics, 141(3):553–572, 1995.

[Uni13] The Univalent Foundations Program.
Homotopy Type Theory: Univalent Foundations of Mathematics.
https://homotopytypetheory.org/book, Institute for Advanced Study, 2013.

[vdW03a] Bartel Leendert van der Waerden.
Algebra.
Number vol 1. Springer New York, 2003.

[vdW03b] Bartel Leendert van der Waerden.
Algebra.
Number vol 2. Springer New York, 2003.

[Vel06] D. J. Velleman.
How to prove it: A structured approach (2nd ed.).
Cambridge University Press, Cambridge, 2006.

[VH67] J. Van Heijenoort.
From Frege to Gödel: A Source Book in Mathematical Logic, 1879–1931.
Source books in the history of the sciences. Harvard University Press, 1967.

[Vic96] S. Vickers.
Topology Via Logic.
Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 1996.

[vP14] Jan von Plato.
Elements of Logical Reasoning.
Cambridge University Press, 2014.

[Wik20] Wikipedia.
List of fallacies — Wikipedia, the free encyclopedia.
http://en.wikipedia.org/w/index.php?title=List_of_fallacies&oldid=946516412, 2020.

[Wil95] Andrew Wiles.
Modular elliptic curves and Fermat's last theorem.
Annals of Mathematics, 141(3):443–551, 1995.

[Wil12] S. Willard.
General Topology.
Dover Books on Mathematics. Dover Publications, 2012.

[Win93] Glynn Winskel.
The Formal Semantics of Programming Languages: An Introduction.
MIT Press, Cambridge, MA, USA, 1993.

[WK18] Philip Wadler and Wen Kokke.
Programming Language Foundations in Agda.
Electronic textbook, 2018.

Glossário de símbolos

$A \overset{\text{def}}{\iff} B$ — A tá sendo definida para ser equivalente a B 1.12, 23

$A \overset{\text{def}}{=} B$ — A tá sendo definido para ser igual a B 1.12, 23

$A = B$ — igualdade extensional D1.30, 27

$A \iff B$ — equivalência extensional D1.30, 27

$A \equiv B$ — igualdade intensional D1.30, 27

$A \iff B$ — equivalência intensional D1.30, 27

$A \equiv B$ — igualdade sintáctica 1.73, 43

$A \overset{\text{sug}}{\equiv} B$ — açúcar sintáctico de objeto 1.78, 46

$A \overset{\text{sug}}{\iff} B$ — açúcar sintáctico de proposição 1.78, 46

$A \overset{\heartsuit}{=} B$ — os A, B são sinônimos no nível coração, com palavras de rua D1.94, 51

$A \overset{\heartsuit}{\iff} B$ — as A, B são sinônimas no nível coração, com palavras de rua D1.94, 51

$a \mid b$ — a divide b D3.22, 74

$x = \min A$ — x é membro mínimo do A D3.54, 84

$x = \max A$ — x é membro máximo do A D3.54, 84

$\sum_{i=s}^{t} \tau(i))$ — o somatório $\tau(s) + \cdots + \tau(t)$ 3.74, 92

$\prod_{i=s}^{t} \tau(i))$ — o produtório $\tau(s) \cdot \cdots \cdot \tau(t)$ 3.74, 92

$\sum_{i=s}^{t} \tau(i))$ — o somatório $\tau(s) + \cdots + \tau(t)$ D3.75, 92

$\prod_{i=s}^{t} \tau(i))$ — o produtório $\tau(s) \cdot \cdots \cdot \tau(t)$ D3.77, 93

$\prod_{i=s}^{t} \tau(i))$ — o produtório $\tau(s) \cdot \cdots \cdot \tau(t)$ x3.65, 93

$quot(a, b)$ — o quociente de a dividido por b D3.83, 98

$rem(a, b)$ — o resto de a dividido por b D3.83, 98

$d = (a, b)$ — d é um mdc dos a e b D3.98, 108

(a, b) — o máximo divisor comum de a e b D3.104, 109

$a \equiv b \pmod{m}$	a é congruente com b módulo m	D3.155, 127
a^{-1}	o inverso (multiplicativo) do a (módulo m)	D3.167, 130
ϕ	a função totiente de Euler	D3.213, 147
$\mathrm{length}\,\ell$	o tamanho da ListNat ℓ	D4.60, 179
$\mathsf{List}\ \alpha$	o tipo de dados $\mathsf{List}\ \alpha$	D4.63, 180
$\mathrm{length}\,\ell$	o tamanho da lista ℓ	D4.65, 181
$\mathrm{reverse}\ \ell$	a reversa da lista ℓ	D4.66, 181
$\ell_1 +\!\!+\, \ell_2$	a concatenação da lista ℓ_1 com a ℓ_2	D4.67, 181
$\mathsf{Maybe}\ \alpha$	o tipo de dados $\mathsf{Maybe}\ \alpha$	D4.79, 187
$\mathsf{Either}\ \alpha\ \beta$	o tipo de dados $\mathsf{Either}\ \alpha\ \beta$	D4.80, 187
$\mathsf{Konst}\ \kappa$	o functor constante κ	D4.84, 189
Id	o functor identidade	x4.47, 189
$\mathsf{BinTree}\ \alpha$	o tipo de árvores binárias $\mathsf{Tree}\ \alpha$	D4.86, 191
Tree	um construtor de tipos de árvores inferível pelo contexto	4.87, 191
$\mathrm{nodes}\ t$	a quantidade de nós na árvore t	x4.53, 191
$\mathrm{leaves}\ t$	a quantidade de folhas na árvore t	x4.53, 191
$\mathrm{depth}\ t$	a quantidade de andares (a profundidade) da árvore t	x4.53, 191
$\mathrm{revcat}\,\ell_1\,\ell_2$	a reversa da ℓ_1, concatenada na ℓ_2	D4.95, 196
$C(n, r)$	o número de r-combinações de n objetos	D5.6, 206
$P(n, r)$	o número de r-permutações de n objetos	D5.6, 206
$P_{\mathsf{tot}}(n)$	o número de permutações (totais) de n objetos	D5.6, 206
a^{-1}	o inverso multiplicativo do real a	D6.14, 225
$A \leq x$	x é uma cota superior de A	D6.55, 243
$x \leq A$	x é uma cota inferior de A	D6.55, 243
$\mathrm{glb}\ A$	o greatest lower bound de $A \subseteq \mathbb{R}$	D6.56, 244
$\mathrm{lub}\ A$	o least upper bound de $A \subseteq \mathbb{R}$	D6.56, 244
$\inf A$	o infimum de $A \subseteq \mathbb{R}$	D6.56, 244

$\sup A$	o supremum de $A \subseteq \mathbb{R}$	D6.56, 244
$\overline{\mathbb{R}}$	os reais estendidos: $\{-\infty\} \cup \mathbb{R} \cup \{+\infty\}$	D6.56, 244
$\mathcal{B}_\varepsilon(x_0)$	a ε-bola do x_0	D6.71, 248
$\operatorname{diam} A$	a diâmetro do conjunto de reais A	D6.75, 249
$(a_n)_n \to \ell$	a seqüência $(a_n)_n$ tende ao ℓ	D6.83, 251
$(a_n)_n \to +\infty$	a seqüência $(a_n)_n$ tende ao $+\infty$	D6.83, 251
$(a_n)_n \to -\infty$	a seqüência $(a_n)_n$ tende ao $-\infty$	D6.83, 251
e	constante de Euler	Π6.6, 271
Unit	o tipo Unit	S7.11, 279
Empty	o tipo Empty	S7.12, 279
Bool	o tipo Bool	S7.15, 281
$\{ x : \alpha \mid \varphi(x) \}$	o conjunto de todos os $x : \alpha$ tais que $\varphi(x)$	D8.7, 285
$A \subseteq B$	A é um subconjunto de B	D8.26, 290
$\emptyset$	o conjunto vazio	D8.32, 291
$\mathcal{U}$	o conjunto universal	D8.35, 292
$A \cup B$	a união dos A e B	D8.49, 297
$A \cap B$	a intersecção dos A e B	D8.51, 297
A^{c}	o complemento de A	D8.55, 298
$A \setminus B$	o complemento relativo de B no A	D8.56, 298
$A \triangle B$	a diferença simétrica dos A e B	D8.57, 299
$\lvert A \rvert$	a cardinalidade de A	D8.68, 302
$\wp A$	o powerset de A (conjunto de partes)	D8.70, 303
$\wp_{\mathsf{f}} A$	o powerset finito de A	D8.70, 303
$\subseteq_{\mathsf{fin}} B$	A é um subconjunto finito de B	D8.70, 303
$\bigcap \mathscr{A}$	a intersecção de $\mathscr{A}$	D8.77, 306
$\bigcup \mathscr{A}$	a união de $\mathscr{A}$	D8.77, 306
$A \times B$	o produto cartesiano dos A, B	D8.93, 311

$(a_n)_n$ a seqüência $a_0, a_1, a_2, \ldots$ P8.120, 320

$(a_i)_{i\in\mathcal{I}}$ a família indexada dos a_i's D8.139, 326

$\prod_{i\in\mathcal{I}} A_i$ o produto cartesiano da família indexada de conjuntos $(A_i)_{i\in\mathcal{I}}$. D8.158, 332

$\lim_n A_n$ o limite da seqüência $(A_n)_n$ D8.168, 335

$\liminf_n A_n$ o limite inferior da seqüência de conjuntos $(A_n)_n$ D8.168, 335

$\limsup_n A_n$ o limite superior da seqüência de conjuntos $(A_n)_n$ D8.168, 335

$\operatorname{src} f$ o source da função f D9.3, 337

$\operatorname{tgt} f$ o target da função f D9.3, 337

$\operatorname{dom} f$ o domínio da função f D9.3, 337

$\operatorname{cod} f$ o codomínio da função f D9.3, 337

$A \xrightarrow{f} B$ f é uma função de A para B D9.3, 337

$f : A \to B$ f é uma função de A para B D9.3, 337

$f \mathbin{@} x$ notação explícita para o $f(x)$ 9.4, 338

$(A \to B)$ o conjunto das funções de A para B D9.10, 339

$\operatorname{range} f$ o range (também: imagem) da função f D9.18, 342

$\operatorname{im} f$ o range (também: imagem) da função f 9.19, 342

$\operatorname{graph} f$ o gráfico da função f D9.21, 342

$f : A \rightarrowtail\!\!\!\!\!\to B$ $f : A \to B$ bijectiva D9.44, 347

$f : A \rightarrowtail B$ $f : A \to B$ injectiva D9.44, 347

$f : A \twoheadrightarrow B$ $f : A \to B$ sobrejectiva D9.44, 347

$(A \rightarrowtail\!\!\!\!\!\to B)$ o conjunto de todas as bijecções de A para B D9.47, 348

$(A \rightarrowtail B)$ o conjunto de todas as injecções de A para B D9.47, 348

$(A \twoheadrightarrow B)$ o conjunto de todas as surjecções de A para B D9.47, 348

ι descritor definitivo 9.57, 350

$\lambda x\,.\,__$ λ-abstracção D9.80, 357

$(x \mapsto __)$ função anônima D9.81, 357

$eval_{A\to B}$ a operação que aplica funções de tipo $A \to B$ em objetos de tipo A ... D9.114, 368

$f\,;g$ composição escrita na ordem diagramática 9.138, 376

id_A a identidade do conjunto A D9.142, 379

1_A a identidade do conjunto A D9.142, 379

$\imath_{A\hookrightarrow B}$ a inclusão do A no B D9.144, 379

$i : A \hookrightarrow B$ i é a inclusão do A no B (ou uma injecção) D9.144, 379

$i : A \subseteq B$ $A \xhookrightarrow{\subseteq} B$ (notação alternativa) D9.144, 379

$i : A \xhookrightarrow{\subseteq} B$ i é a inclusão do A no B D9.144, 379

f^n a n-ésima iteração da f D9.150, 381

χ_C a função característica do C (com domínio implícito) D9.156, 382

χ_C^A a função característica do C no A D9.156, 382

$f \restriction X$ a restricção de f no X D9.161, 384

$f|_X$ $f \restriction X$ (notação alternativa) D9.161, 384

f^{-1} a função inversa da f D9.162, 384

$f[X]$ a imagem de X através da f D9.170, 388

$f_{-1}[Y]$ a preimagem de Y através da f D9.170, 388

$f \times g$ a função-produto das f, g D9.199, 403

$\langle f, g\rangle$ a função-par f "pair" g D9.201, 404

Δ_A a função diagonal do A D9.205, 405

Δ a função diagonal do conjunto implicito pelo contexto D9.205, 405

$A \amalg B$ o coproduto de A e B D9.210, 408

$A \uplus B$ a união disjunta de A e B D9.210, 408

$(A \rightharpoonup B)$ o conjunto das funções parciais de A para B D9.213, 409

$f : A \rightharpoonup B$ f é uma função parcial de A para B D9.213, 409

$f(x)\uparrow$ f diverge no x D9.213, 409

$f(x)\downarrow$ f converge no x D9.213, 409

$A \cong B$ os conjuntos A, B são isómorfos D9.254, 424

$f : A \cong B$ $f : A \xrightarrow{\cong} B$ (notação alternativa) D9.254, 424

$f : A \xrightarrow{\cong} B$	f é um isomorfismo do A para o B	D9.254, 424
Set	a categoria dos conjuntos e suas funções	9.263, 428
$R : \mathrm{Rel}\,(A_1, \ldots, A_n)$	R é uma relação entre os conjuntos $A_1, \ldots, A_n$	D10.6, 433
$\mathrm{graph}\, R$	o gráfico da relação R	D10.13, 435
R^{∂}	a relação oposta da R	D10.25, 438
$R^{=}$	o fecho reflexivo da R	D10.56, 452
R_{r}	o fecho reflexivo da R	D10.56, 452
$R^{\leftrightarrow}$	o fecho simétrico da R	D10.57, 452
R_{s}	o fecho simétrico da R	D10.57, 452
R^{*}	o fecho reflexivo-transitivo da R	D10.59, 452
R_{rt}	o fecho reflexivo-transitivo da R	D10.59, 452
R^{+}	o fecho transitivo da R	D10.59, 452
R_{t}	o fecho transitivo da R	D10.59, 452
$[a]_R$	a classe de equivalência do a através da R	D10.86, 459
$[a]$	a classe de equivalência do a (relação implícita pelo contexto)	D10.86, 459
A/R	o conjunto quociente do A por R	D10.89, 463
$\mathrm{coim}\, f$	a coimagem da f	D10.99, 468
$\ker f$	o kernel da f	D10.99, 468
R°	o fecho cíclico da R	II10.24, 472
$R^{\triangleright}$	o fecho left-euclideano da R	II10.24, 472
$R^{\triangleleft}$	o fecho right-euclideano da R	II10.24, 472
$o(G)$	a ordem do grupo G	D11.23, 481
$\mathbb{Z}_n$	o grupo aditivo dos inteiros módulo	D11.30, 483
S_n	o grupo simétrico S_n	D11.32, 483
e_G	a identidade do grupo G	D11.43, 487
e	a identidade dum grupo implicito pelo contexto	D11.43, 487

a^{-1} o inverso de a num grupo D11.44, 487

a^m $a * \cdots * a$ (m vezes) D11.72, 495

$o(a)$ a ordem do elemento a num grupo D11.79, 497

$a \approx b$ conjugação de grupo D11.91, 501

$\mathrm{Cls}\,(a)$ a classe de conjugação de a D11.92, 501

σ_g o g-conjugador D11.93, 501

$H \leq G$ H é um subgrupo de G D11.94, 503

$m\mathbb{Z}$ o conjunto de todos os múltiplos do m x11.58, 504

$\langle a \rangle$ o subgrupo gerado por o elemento a D11.109, 507

$\langle A \rangle$ o subgrupo gerado por o conjunto A D11.112, 509

$\mathrm{Z}(G)$ o centro do grupo G D11.130, 515

Ha o right-coset do $H \leq G$ através do $a \in G$ D11.133, 517

aH o left-coset do $H \leq G$ através do $a \in G$ D11.133, 517

$\mathcal{L}_H$ a família das coclasses esquerdas do subgrupo H (grupo implícito) .. D11.139, 520

$\mathcal{R}_H$ a família das coclasses direitas do subgrupo H (grupo implícito) D11.139, 520

$a \equiv b \pmod{_{\mathrm{L}}\ H}$ a, b são equivalentes módulo-esquerdo $H \leq G$ D11.144, 521

$a \equiv b \pmod{_{\mathrm{R}}\ H}$ a, b são equivalentes módulo-direito $H \leq G$ D11.144, 521

$a \ {}_H\!\equiv b$ $a \equiv b \pmod{_{\mathrm{L}}\ H}$ D11.144, 521

$a \equiv_H b$ $a \equiv b \pmod{_{\mathrm{R}}\ H}$ D11.144, 521

$i_G(H)$ $|G : H|$ (notação alternativa) D11.156, 524

$|G : H|$ o índice do subgrupo H no grupo G D11.156, 524

$N \trianglelefteq G$ N é um subgrupo normal de G D11.172, 530

$a \equiv b \pmod{}N$ a, b são congruentes módulo o subgrupo normal N D11.174, 531

G/N o grupo quociente de G módulo N D11.180, 535

$\varphi : A \xrightarrow{\text{hom}} B$ φ é um homomorfismo do A para o B D11.217, 546

$\varphi : \mathcal{A} \to \mathcal{B}$ φ é um homomorfismo do $\mathcal{A}$ para o $\mathcal{B}$ D11.217, 546

$\mathrm{im}\,\varphi$ a image do homomorfismo φ D11.222, 548

$\ker \varphi$	o kernel do homomorfismo φ	D11.222, 548
Group	a categoria dos grupos e seus homomorfismos	D11.227, 550
Abel	a categoria dos grupos abelianos e seus homomorfismos	D11.229, 551
$\mathrm{Aut}(G)$	o grupo de automorfismos no G	Π11.25, 552
$\mathrm{Inn}(G)$	os inner automorfismos de G	D11.231, 552
$\overline{n}$	o conjunto $\{0, \ldots, n-1\}$	D13.8, 574
$A =_{\mathrm{c}} B$	os A e B são equinúmeros	D13.9, 574
$A \leq_{\mathrm{c}} B$	o A é menor-ou-igual em cardinalidade que o B	D13.10, 574
$A <_{\mathrm{c}} B$	o A é menor em cardinalidade que o B	D13.10, 574
$\aleph_0$	a cardinalidade do $\mathbb{N}$	D13.54, 593
$\mathfrak{c}$	a cardinalidade do $\wp\mathbb{N}$ e do $\mathbb{R}$	D13.54, 593
$x \prec y$	o x é coberto por o y	D14.5, 604
$\max A$	o máximo de A	D14.9, 605
$\min A$	o mínimo de A	D14.9, 605
0_P	o zero (o mínimo elemento dum poset)	D14.10, 605
1_P	o um (o máximo elemento dum poset)	D14.10, 605
$\bot_P$	o bottom (o mínimo elemento dum poset)	D14.10, 605
$\top_P$	o top (o máximo elemento dum poset)	D14.10, 605
$\mathrm{lbs}\, A$	o conjunto dos lower bounds de A	D14.12, 606
$\mathrm{ubs}\, A$	o conjunto dos upper bounds de A	D14.12, 606
$\bigvee A$	o join de A	D14.14, 606
$\bigwedge A$	o meet de A	D14.14, 606
$\mathrm{glb}\, A$	o greatest lower bound de A	D14.14, 606
$\inf A$	o infimum de A	D14.14, 606
$\mathrm{lub}\, A$	o least upper bound de A	D14.14, 606
$\sup A$	o supremum de A	D14.14, 606
$\mathcal{O}(P)$	o conjunto de downsets de P	D14.16, 606

$\downarrow a$ o down de a D14.17, 606

$\uparrow a$ o up de a D14.17, 606

P^{∂} o poset dual de P D14.19, 607

$P_{\perp}$ o lifting do poset P D14.21, 607

$P \oplus Q$ a soma do poset P com o poset Q D14.23, 608

$\mathrm{Fix}\, f$ o conjunto dos fixpoints de f D14.38, 612

$\mathrm{gfp}\, f$ o maior fixpoint de f D14.38, 612

$\mathrm{lfp}\, f$ o menor fixpoint de f D14.38, 612

$x \in A$ x é um membro do conjunto A P16.1, 618

$x \Subset C$ o objeto x está na classe C D16.15, 621

$\emptyset$ o conjunto vazio D16.19, 622

$\{a, b\}$ o conjunto doubleton de a e b D16.21, 622

$\{a\}$ o conjunto singleton de a, com membro único o a D16.24, 623

$\wp a$ o conjunto de partes (powerset) de a D16.37, 626

$\bigcup a$ a união de a (operação unária) D16.40, 627

$A \uplus B$ a união disjunta de A com B D16.54, 633

$\mathrm{Infinite}(a)$ o conjunto a é Dedekind-infinito D16.78, 641

x^{+} o conjunto-sucessor de x D16.80, 641

ZF a teoria dos conjuntos Zermelo–Fraenkel (without Choice) 16.112, 655

ZFC a teoria dos conjuntos Zermelo–Fraenkel with Choice 16.120, 657

$(a_n)_n \to \ell$ a seqüência $(a_n)_n$ tende ao ℓ D17.9, 665

$\mathrm{deriv}\, A$ o conjunto derivado de A D17.14, 667

$\mathcal{O}\mathcal{S}$ a topologia do espaço $\mathcal{S}$ D18.6, 670

Índice de pessoas

Abel, Niels Henrik, 474, 480
Ackermann, Wilhelm, 175, 176
Aczel, Peter Henry George
  anti-foundation, 662
  CZF, 662
Arquimedes, de Siracusa
  propriedade, 266
Artin, Emil, 553

Backus, John
  BNF, 197
Baire, René-Louis, 287, 596
Banach, Stefan, 287
  paradoxo –Tarski, 658
Bell, Eric Temple
  números, 845
Bernays, Paul Isaac
  NBG, 662
Bernoulli, Jacob
  constante e "de Euler", 271
  convergêcia de série, 271
  desigualdade, 231, 232
  divergência da série harmônica, 271
Bernstein, Felix, 589, 590
Birkhoff, Garrett, 553
Bolzano, Bernard
  –Weierstrass, teorema, 264
  teorema de função real contínua, 272
Boole, George
  álgebra, 614
Borel, Émile, 287, 596
Bézout, Étienne
  lemma, 110

Cantor, Georg, 268, 287, 303, 572, 576, 583, 586–589, 595, 596, 600, 603, 664, 679
  aritmética transfinita, 595
  CH, 595
  conjunto de Cantor, 586
  construção dos reais, 650
  descrição de conjunto, 284
  diagonalização, 581
  intervalos aninhados, 265
  teorema, 824
  teorema de powerset, 593
Carmichael, Robert Daniel
  números, 144
Cauchy, Augustin-Louis, 474
  seqüência, 259
  seqüência Cauchy, 650
  seqüências autoconvergentes, 259
Cayley, Arthur, 480
  tabela, 493
Church, Alonzo
  numeral, 682
  teorema Church–Rosser, 360
Collatz, Lothar
  conjectura, 124, 290, 831
Condorcet, Nicolas de
  paradoxo, 461
Curry, Haskell, 371
  –Howard, 339
  currificação, 371

De Morgan, Augustus
  leis para conjuntos, 301
Dedekind, Richard, 587, 596, 600, 603, 641, 643
  construção dos reais, 650
  cut, 651
  Dedekind cut, 651
  infinito, 641
  unicidade dos naturais, 645
Dirichlet, Johann Peter Gustav Lejeune
  teorema, 141

Eilenberg, Samuel, 553
Eratosthenes, de Cyrene
  crivo, 120
Euclides, de Alexandria, 122, 287, 445, 528
  algoritmo, 111
  algoritmo estendido, 114
  divisão, 498, 697
  Elementos, 121
  geometria euclideana, 42
  infinidade dos primos, 120, 539
  lemma, 118
  lemma da divisão, 98

lemma de mdc, 113
medir, 106
Euler, Leonhard, 124, 149
constante e, 271
demonstração do pequeno Fermat, 149
divergência da série harmônica, 271
função totiente, 147
primeira demonstração de Fermatinho, 141
resolução de Basel, 271
teorema de congruência, 149, 527, 528
transcendentais, 572

Fermat, Pierre de, 141
conjectura, 124
Fermatinho, 527
inverso modular, 142
teorema pequeno, 142
teorema pequeno (Fermatinho), 141
Fibonacci, Leonardo, 417
função, 417
números, 100
Fourier, Joseph
séries, 572
Fraenkel, Abraham, 558, 653
carta para Zermelo, 653
teoria dos conjuntos, 599
ZF, 655, 662
Frege, Gottlob
currificação, 371
Fréchet, Maurice, 287, 596, 664

Galois, Évariste, 474, 480
Gauss, Carl Friedrich, 122
definição de congruência, 127
Disquisitiones Arithmeticæ, 121
somatório, 94
Gentzen, Gerhard
cálculo de seqüentes, 684
dedução natural, 684
Goldbach, Christian, 124
conjectura, 124
Gödel, Kurt
CH, 595
diagonalização, 582
NBG, 662

Hadamard, Jacques
teorema dos números primos, 145
Halmos, Paul, 17, 52
Hardy, Godfrey Harold, 67
Hasse, Helmut, 446, 544, 605
Hausdorff, Felix, 287, 576, 596
par, 633
Hermite, Charles, 587
transcendentalidade do e, 572
Heyting, Arend
álgebra, 614
Hilbert, David, 287
estilo de sistema de demonstração, 684
Howard, William Arvin
–Curry, 339

Keeler, Ken, 503
Kelley, John L.
MK, 662
Kleene, Stephen Cole
strongly least fixpoint, 613
Klein, Felix
four-group, 849
Knaster, Bronisław, 612
Knuth, Donald
index loop, 25
Kolmogorov, Andrey Nikolaevich, 596
Kunen, Kenneth, 500
Kuratowski, Kazimierz, 632
par, 631

Lagrange, Joseph-Louis, 474, 526, 528
corolário, 525, 527, 528, 539
teorema, 524, 525
Lambert, Johann Heinrich, 474
irracionalidade, 572
Lebesgue, Henri, 596
Legendre, Adrien-Marie
conjectura, 124
conjecura, 141
Leibniz, Gottfried Wilhelm
algébrico, 572
demonstração do pequeno Fermat, 149
primeira demonstração de Fermatinho, 141
Lindelöf, Ernst Leonard
space, 676
teorema, 675
Liouville, Joseph, 587
constantes transcendentais, 572
Lucas, François Édouard Anatole
números, 100
Łukasiewicz, Jan
notação, 200

Mac Lane, Saunders, 553
Mengoli, Pietro
  divergência da série harmônica, 271
  problema de Basel, 271
Mirimanoff, Dmitry
  teoria dos conjuntos, 599
Montague, Richard, 285
  teorema, 658
Morse, Anthony
  MK, 662

Naur, Peter
  BNF, 197
Noether, Emmy, 553

Pascal, Blaise
  triângulo, 213
Peano, Giuseppe, 643
Poussin, Charles Jean de la Vallée
  teorema dos números primos, 145
Pythagoras, de Samos
  métrica euclideana, 665

Quine, Willard van Orman
  ML, 662
  NF, 662

Riemann, Bernhard, 596
  função zeta, 145
  integral, 370
  teorema de rearranjo, 323, 324
Rivest, John Barkley
  teorema Church–Rosser, 360
Rondogiannis, Panos, 603
Ruffini, Paolo, 474
Russell, Bertnard, 625
  de paradoxo para teorema, 626
  operador, 626
  paradoxo, 598, 662
  teoria dos tipos, 599

Schröder, Ernst, 589
Schönfinkel, Moses Ilyich
  currificação, 371
Sierpiński, Wacław Franciszek
  espaço, 671

Singmaster, David
  conjectura, 214
Skolem, Thoralf, 653
  MK, 662
  paradoxo, 661
  teoria dos conjuntos, 599
  ZF, 662
Smullyan, Raymond, 589
  jogo, 577
Stone, Marshall Harvey, 287

Tarski, Alfred, 612
  paradoxo Banach–, 658

Urysohn, Pavel Samuilovich
  lema, 678

van der Waerden, Bartel Leendert, 553
Venn, John, 300
von Lindemann, Ferdinand, 474, 603
  teorema –Weierstrass, 572
von Neumann, John, 576
  conjunto-sucessor, 641
  NBG, 662
  teoria dos conjuntos, 599

Wang, Hao
  MK, 662
Wantzel, Pierre, 474
Weierstrass, Karl
  Bolzano–, teorema, 264
  teorema Lindemann–, 572
Wiener, Norbert, 632
  par, 632
Wiles, Andrew
  teorema, 124
Wilson, John
  teorema, 540

Zermelo, Ernst, 653
  conjunto-sucessor, 641
  teoria axiomática dos conjuntos, 599
  teoria dos conjuntos, 599
  ZF, 655, 662
Zwicker, William
  hypergame, 601, 602

Índice geral

aberto
  mapa, **674**
abreviação, **46**
abuso, 660
abuso notacional, 80, 229
acumulação, *veja também* ponto
Agda, 368
agnóstico, **632**
  implementação, **315**
aleph 0, **593**
algarismo, *veja* dígito
algebra
  linear, **566**
algoritmo
  de Euclides, **111**
  estendido de Euclides, **114**
anel, **558**
  booleano, **562**
  comutativo, **558**
aninhada
  recursão, *veja* recursão
anticadeia, **604**
análise
  real, **570**
aplicação
  parcial, 433
archimedeano, **266**
aridade, 340
aritmética, *veja também* expressão
arity
  primeiro contato, **39**
arranjo, *veja* permutação
artigo
  (in)definido, 292, 379, 416, 481, 485
associatividade
  sintáctica, **44**, **68**, **224**
autoconvergente, *veja* seqüência
automorfismo
  de grupos, **547**
  inner, **552**
axioma
  vs. lei, 479
  Choice (AC), **657**
  Dedekind–Peano, **643**
  Emptyset, **622**
  Extensionality, **622**
  Foundation, **654**
  Infinity, **641**
  Pairset, **622**
  Powerset, **626**
  Regularity, *veja* Foundation.
  Replacement (schema), **653**
  Separation (schema), **624**
  Unionset, **627**
açúcar
  sintáctico, 629
açúcar sintáctico, **46**

Backus–Naur form, *veja* BNF
bag, *veja* multiset
base, **674**, *veja* indução
base local, **674**
Basel, 271
  problema de, 271
Bell
  números, *veja* Bell
bem-ordem, **176**
bijecção, *veja* função bijectiva
binomial
  teorema, *veja* teorema
black box, **287**, *veja também* white box
  de conjunto, **287**
  de funcção, **337**
  de relação, **432**
  de tupla, **309**, 630
BNF, *veja* gramática
bola
  ε-, de real, **249**
Bool, **177–179**
bottom, **605**
bound
  lower, **243**
  upper, **243**
boundary, **672**

bounded
  above, **243**
  below, **243**
  por baixo, **605**
  por cima, **605**
buraco, **355**, *veja também* função

C, 339, 368, 384
C++, 339, 368
cadeia, **604**
calculus, **570**
caminho
  em espaço topológico, **677**
Cantor
  conjunto de, **586**
canônico, **156**
capturada, *veja* variável
característica, *veja* função
  de corpo, **565**
cardinalidade
  ingenuamente, **303**
Carmichael
  número, *veja* número
Cauchy
  seqüência, *veja* autoconvergente
cercado, **250**
chinês
  teorema do resto, *veja* teorema chinês
cidadão da primeira classe, 368
classe, **287**, **621**, **660**
  própria, **621**
classe de conjugação, **501**
classe de equivalência, **459**
Clojure, 368
cluster, *veja também* ponto
cobertura, **604**
coclasse, **518**
codomínio
  de função, *veja* função
cofinito, **614**
coimagem, **469**
colecção, **286**, **287**, **660**
combinação, **207**
combinação linear, **110**, 131
compacto, **676**
complemento, **298**
  relativo, **298**
composição
  de função parcial see: função, **410**
  de funções, *veja* função
  de relações, *veja* relação
  diagramática, **376**
composto, *veja também* redutível
condição definitiva, **285**, 288
conexo, **677**
  por caminho, **677**
congruência, **127**
  módulo subgrupo, **531**
  sistema, 137
conjectura, **40**, 290
  de Collatz, **124**
  de Goldbach, **124**
  de Legendre, **124**
  dos primos gêmeos, **124**
conjugado
  de elemento de grupo, **501**
conjugador, **502**
conjugação
  de grupo, **501**
conjunto, **618**, **660**
  (+)-fechado, **76**
  bem-ordenado, *veja* woset
  como black box, *veja* black box
  contável, **577**
  de Cantor, *veja* Cantor
  de partes, *veja* powerset
  de índices, **326**
  definição intuitiva, **284**
  denso nos reais, **268**
  dirigido, **255**
  gerado, **233**
  heterogêneo, **285**
  homogêneo, **285**
  incontável, **269**, **577**
  indexado, **233**
  indexado por conjunto, **328**, **375**
  multiplicidade, 289
  naturalmente indutivo, *veja* indutivo
  notação, **285**
  ordem de membros, 289
  perfeito, 679
  potência, *veja* powerset
  primeiro contato, **38**
  quociente, **463**, 531
  vazio, **622**
conjunto derivado, **667**
conjunto-escolha, **656**
conjunto-sucessor, **641**, 641
constante
  e, de Euler, **271**
constructivismo, *veja* intuicionismo
construtor, **156**
  de tuplas, **310**
continuum, **593**
contraexemplo, **24**

convergente, *veja* seqüência
convergência
  pointwise, **273**
  uniforme, **273**
coprimos, **108**, 271
coproduto, **408**
corollary, **40**
corolário
  de Lagrange, 527
corpo, **564**
  ordenado, completo, **568**
coset, *veja* coclasse
cota
  inferior, **243**, **606**
  superior, **243**, **606**
cotado
  inferiormente, **243**
  superiormente, **243**
covering, **329**
crescente, *veja* seqüência
crivo
  de Eratosthenes, **120**
cross, *veja* produto
currificação, **371**
Curry–Howard
  teaser, 339
CZF, *veja* teoria dos conjuntos

Dedekind cut, **651**
Dedekind-infinito, **641**
definitiva, *veja* condição
definição circular, **25**
demonstração, **41**, *veja também* proof
  estado, *veja* estado
  por intimidação, **63**
  REPL, *veja* REPL
  script, *veja* script
denso
  em topologia, **672**
derivado, **671**
derivação, *veja também* árvore
descripção definitiva, **350**
descritor definitivo, **350**
diagrama
  comutativo, **257**, **401**
  externo, **345**
  interno, **344**
  linha pontilhada, **259**
diagrama de Venn, **300**
diagramática, *veja* composição
diferença simétrica, **299**
dihedral, *veja* grupo dihedral
dirigido, *veja* conjunto
discreta, *veja também* topologia
disjuntos, **297**
distância, **247**, *veja também* métrica
  função, 124
divergente, *veja* seqüência
divide, **75**
  nos naturais, **175**
divisibilidade
  critéria, 139
divisor, **75**
  máximo comum, o, **109**
  máximo comum, um, **108**
divisor de zero, *veja* zerodivisor
divisão, **98**, *veja também* Euclides
  lemma, 98
divisível, **75**
diâmetro, **250**
dominar, **255**
domínio
  de função, *veja* função
domínio de cancelamento, **563**
domínio de integridade, **563**
doubleton, **622**
downset, **606**
dual, 244
dualidade, 302, 322
dummy, *veja* variável ligada
dígito, **37**

eficiência
  de Fermatinho, 144
endomapa, **344**, *veja* função
endomorfismo
  de grupo, **547**
entry point, **27**
enumeração, **577**
epimorfismo
  de grupo, **547**
  split (de grupo), **547**
epsilon, **246**
equiconsistente, **661**
equinúmeros, **574**
equivalência
  módulo subgrupo, **522**
erro
  de aestética, **49**
  de ética, **49**
escolhedor
  coproduto, **408**
  produto, **332**

Espaço
  de Fréchet, **678**
  de Hausdorff, **678**
  de Kolmogorov, **678**
  normal, **678**
  regular, **678**
espaço, **287**
esquema axiomático, **624**, 657, 658
estado
  de demonstração, **53**
estratégia
  de evaluação, **160**
  vencedora, 577, 627
estratégia vencedora, **253**
Euclid : lemma da divisão, 498
Euler
  função, *veja* função totiente
exemplo, **24**
expansão
  binária de 1, **271**
explode, **61**
expressão
  vs. statement, **384**
  aritmética, **43**
extensão, **27**
  de conjunto, **289**

falácia, **48**, 64
família, **286**
  indexada, **326**
fatoração
  de função, **397**
fechado
  pelos conjugados, **537**
fecho, **672**
  cíclico, **472**
  de relação, **450**
  left-euclideano, **472**
  reflexivo, **452**
  reflexivo-transitivo, **453**
  right-euclideano, **472**
  simétrico, **452**
  transitivo, **453**
Fermatinho, *veja* teorema, Fermatinho
Fibonacci, 100
  números, **100**, *veja também* Lucas
  seqüência, 111
finitamente axiomatizáve, **658**
finitamente axiomatizável, 658
finito, **576**
first-class citizen, *veja* cidadão
fixpoint, **410**
  greatest, **612**
  least, **612**
  strongly least, **613**
forma fechada, 271
Fourier, *veja* séries
fracção
  nos reais, **226**
funcionalidade
  condições, **340**
functor, **188**
funcção
  como black box, *veja* black box
função
  algébrica, 572
  anônima, **357**, 366
  aplicação, **338**
  bem-definida, 534, 550
  bijectiva, **347**
  característica, **382**
  codomínio, **337**
  composição, **376**
  constante, **380**
  contínua, **673**
  contínua em ponto, **673**
  convergir, **409**
  cross, **403**
  de ordem superior, **365**
  definição intuitiva, **337**
  determinabilidade, **340**
  diagonal, **406**
  divergir, **409**
  domínio, **337**
  endomapa, 344, 345
  epi, **423**
  epônima, **357**
  eval, **369**
  fixpoint, *veja* fixpoint
  gráfico, **342**
  idempotente, **382**
  identidade, **379**
  imagem, **342**, **388**, *veja também* range
  inclusão, **379**
  injectiva, **347**
  invariável, **380**
  inversa, **384**
  inversa direita, **425**
  inversa esquerda, **425**
  iteração, **381**
  mono, **423**
  multiplicativa, **148**
  não-determinística, **418**
  par, **404**

parcial, 257, **409**
aproximação, **637**
compatibilidade, **637**, 646
composição, **410**
conflito, **637**, 646
partial, **418**
pointwise operação, *veja* pointwise
preimagem, **388**
primeiro contato, **39**
produto, **403**
range, **342**, *veja também* imagem
restricção, **384**
retracção, **425**
secção, **425**
sinônimos, **340**
sobrecjetiva, **347**
steady, *veja* invariável
tipo de, **280**
totalidade, **340**
totiente de Euler, **147**
valor, **337**
vazia, **354**
função-escolha
de conjunto, **657**
de família, **657**
Futurama, 503

geometria
euclideana, **42**
gerado
conjunto, *veja também* indexado, *veja* conjunto
gerador
de conjunto, **233**
gramática
BNF, **197**
grande, *veja* infinitamente
greatest lower bound, **606**
reais, **244**
Grupo
cíclico, **513**
grupo, **478**, **481**
abeliano, **480**
aditivo, **479**
centro, **515**
dihedral, **542**
isomórficos, **548**
multiplicativo, **479**
quociente, **535**
simétrico, **484**
subgrupo
gerado por elemento, **508**
gerado por subconjunto, **509**
teorema de isomorfismo, *veja* teorema de isomorfismo
índice de subgrupo, **524**
Grupoku, **494**
gráfico, *veja* função, *veja* relação

H.I., *veja* hipótese indutiva
Halmos
túmulo, **17**
Haskell, 368, 384
Hasse
diagrama, 446, **544**, **605**
heterogeneidade, **285**
hipótese indutivo, *veja* indução
homogeneidade, **285**
homomorfismo
de anel, **561**
de grupo, **547**
de grupos, **546**
de monóide, **556**
hypergame, **601**

idempotente
função, *veja* função idempotente
idempotência, 562
identidade, *veja* função
Idris, 368
igualdade
extensional, **289**
intensional, **289**
semântica, **44**
sintáctica, **44**
image de homomorfismo, **548**
imagem, *veja* função, imagem
implementação, 315
agnóstico, *veja* agnóstico
implicação, **58**
incomparável, **604**
indexado
conjunto, *veja* conjunto
indiscreta, *veja também* topologia
indutivo
naturalmente, **241**
indução
base, **165**
como usar, 90
forte, 122
hipótese indutiva, **165**
para o tipo List α, **181**
para o tipo ListNat, **180**
para o tipo Nat, **164**, **165**
para os inteiros positivos, **90**, **91**
passo indutivo, **165**

infimum, **606**
  reais, **244**
infinidade
  dos primos, 120
infinitamente
  grande, **266**
  pequeno, **266**
infinito, **576**, *veja também* infinidade
infix, *veja* notação
injecção, *veja* função injectiva
inner automorfismo, *veja* automorfismo
inteiros, **68**, **74**, **80**, **84**
intensão, **27**
  de conjunto, **289**
interior, **672**
  ponto, **672**
intersecção, **297**
  de conjuntos de reais, **239**
  grande, **306**
intervalos
  de reais, **234**
intuicionismo, 21
inverso
  multiplicativo módulo m, **130**
invertível
  inteiro, **106**
involução, **439**
irredutível, **118**, *veja também* primo
iso, **429**
isolado, *veja* ponto
isometria, **541**
isomorfismo, *veja também* teorema de isomorfismo
  de conjuntos, **424**
  de grupo, **547**
  de ordem, **610**

Java, 339, 368
jogo
  de quantificadores, **253**
  terminante, **601**
justaposição, **69**, 378

kernel, **469**
kernel de homomorfismo, **548**

lattice, **568**, *veja* reticulado
  como algebra, **611**
  como poset, **611**
least upper bound, **606**
  reais, **244**
lei, **479**
  de functor, **188**
leis de grupo, **479**
lema
  de Urysohn, 678
lemma, **40**
ligador, 296
  de variável, **34**, 358
  lambda, **358**
limit point, **667**
limitante, *veja* cota
limite
  de seqüência de conjuntos, **335**
  espaço métrico, **665**
  reais, **251**
Lindelöf, **676**
linguagem
  de demonstração, **41**
linguagem-objeto, **45**
LISP, 55
ListNat, **179**
lower bound, **606**
Lucas, 100
  números, **100**, *veja também* Fibonacci
lógica
  de relevância, **21**

main, 383
mal-tipado, **22**
map, *veja* função
mapa, *veja* função
mapeamento, *veja* função
matemalhar, **252**
maximal, **606**
mdc, *veja* divisor, máximo comum
  lemma, 113
melhor
  divisor comum, **108**
metademonstração, 262
metalinguagem, **45**, 660
metavariável, **45**
minimal, **606**
mixfix, *veja* notação
MK, *veja* teoria dos conjuntos
modelo, **242**
modus ponens, **59**

monomorfismo
  de grupo, **547**
  split (de grupo), **547**
monóide, **555**
monótona, **610**
morfismo
  grupo, **547**
multiplicativa, *veja* função
multiplo, **75**
multiset, 324, 652
máximo, **84**, **605**
máximo divisor, *veja* divisor
métrica, **247**, *veja também* distância
mínimo, **84**, **605**
módulo, **127**
  subgrupo, **522**, **531**
mônica, *veja* função, mono

Nat, **153**
NBG, *veja* teoria dos conjuntos
negativo
  inteiro, **80**
New Foundations, *veja* NF
NF, *veja* teoria dos conjuntos
normal, *veja* subgrupo normal
notação
  diagramática, *veja* composição
  funcional, 378
  infix, **40**
  mixfix, **40**
  postfix, **40**
  prefix, **40**
  sobrecarregar, *veja* sobrecarregamento
numeral, **37**
nãœxemplo, **24**
número, **37**
  Carmichael, **144**

one
  dum poset, **605**
operador, *veja também* função
operação, *veja também* função
ordem
  antilexicográfica, **609**
  assimétrica, **82**
  componentwise, **608**
  conectada, **82**
  coordinatewise, *veja* componentwise
  de grupo, **482**
  de membro em grupo, **497**
  estrita, **82**, **456**
  fraca, **456**
  irreflexiva, **82**
  lexicográfica, **609**
  nos naturais, **174**
  pointwise, **609**
  preservar, **231**
  refletir, **231**
order-embedding, **610**
order-isomorfismo, **610**

P.I., *veja* passo indutivo
par
  de Hausdorff, **633**
  de Kuratowski, 631, 632
  de Wiener, **632**
paradoxo
  Banach–Tarski, 658
  de Condorcet, 461
  de Russell, **598**
    vira teorema, 625
parsing, **47**
partição, **330**, **460**, 520
  induzida, **467**
passo indutivo, *veja* indução
PBO, *veja* princípio da boa ordem
pela escolha de, **77**
pequeno, *veja* infinitamente
perfeito
  conjunto, *veja* conjunto
permutação, **207**, 475
  total, **207**
perto
  ε-, de um real, **248**
  em espaço métrico, **665**
PIF, 102
PIFF, 102
PNT, *veja* teorema dos números primos
pointwise, 240, *veja também* convergência
  operação, **405**, 559, 563, 570
  order, *veja* ordem
Polonesa
  notação, **200**, *veja também* Łukasiewicz
ponto
  de acumulação, **671**
  de cluster, **671**
  de conjunto, **338**
  isolado, **671**
ponto de acumulação, *veja* limit point
poset, **604**
  discreto, **607**
  dual, **607**
  lift, **607**
  soma, **608**
postfix, *veja* notação
postfixpoint, **612**

powerset, **303**, **626**
precedência, **43**
  sintáctica, **69**
predicado, **639**
prefix, *veja* notação
prefixpoint, **612**
preordem, **457**
preservar, *veja também* respeitar
  as distincções, 348
  estrutura, **545**
primeiro-contável, **675**
primo, **118**, *veja também* irredutível
  informalmente, 116
princípio
  da adição, **205**
  da boa ordem, **89**, 565, 850
  da indução, Peano, **643**
  da multiplicação, **205**
  da puridade, **618**
probabilidade, 271
problema
  de Basel, 271
procedimento, *veja também* função
produto
  binário de tipos, **275**
  finito de tipos, **276**
  nulário de tipos, **277**
  nívelo coração, **332**
produto cartesiano, **312**
  generalizado, **332**
  tripla, 315
produtório iterativo, **92**, **93**
programação, 55
proof
  script, **53**
  state, **53**
propriedade
  archimedeana, **266**
  grupoteórica, **543**
pré-distância, **247**
pré-métrica, **247**
própria
  classe, *veja* classe própria
pseudométrica, *veja* pré-métrica
PureScript, 368
puridade, *veja* princípio
Python, 55, 341, 357, 366, 368, 371

quasiordem, *veja* preordem
quociente
  conjunto, *veja* conjunto quociente
  divisão, **98**

Racket, 368
reais, **223**, **229**, **263**
  estendidos, **244**
real
  algébrico, **228**
  inteiro, **228**
  irracional, **228**
  natural, **242**
  racional, **228**
  transcendental, **228**
recursão
  aninhada, **175**, **176**
  teorema, *veja* teorema de recursão
redutível, **118**, *veja também* composto
regra
  de inferência, 92
relação
  antissimétrica, **444**
  assimétrica, **444**
  circular, **445**
  como black box, *veja* black box
  composição, **441**
  conjugação, *veja* conjugação
  de equivalência, 129, **457**, 520
  dual, **438**
  gráfico, **435**
  induzida, **467**
  inversa, *veja* oposta
  irreflexiva, **444**
  left-euclidean, **445**
  oposta, **438**
  primeiro contato, **39**
  reflexiva, **444**
  right-euclidean, **445**
  simétrica, **444**
  total, **445**
  transitiva, **445**
  tricotômica, **445**
relação-classe, **639**
REPL, **55**
  de demonstração, **53**
representação canônica
  de inteiro, **122**, 691
respeitar, *veja também* preservar
  as distincções, 348
  estrutura, **545**
resto
  divisão, **98**
resíduo, **146**

reticulado
  como álgebra, **567**
  cubo, **605**
  de conjuntos, **614**
  limitado, como álgebra, **567**
rng, **558**

s.c.r., *veja* sistema completo de resíduos
s.r.r., *veja* sistema reduzido de resíduos
Scala, 368
script
  de demonstração, **53**
segundo-contável, **675**
semirreticulado, **567**
  limitado, **567**
semântica, 43
  denotacional, **43**
separável
  espaço, **672**
seqüência, **320**
  autoconvergente, **259**
  Cauchy, *veja* autoconvergente
  convergente, **251**
  crescente, **238**
  de reais, **236**
  divergente, **251**
  ordem, **240**
set
  comprehension, *veja também* set builder
set builder, **285**, 662
set comprehension, **285**
set-builder, **233**
setas : topologia, 673
setinha barrada, **358**
sintáxe, 43
sistema
  de congruências, 137
sistema completo de resíduos, **146**
sistema Peano, **643**
sistema reduzido de resíduos, **146**
sobrecarregamento
  notação, **70**, 224
sobrejecção, *veja* função sobrejectiva
soma
  binária de tipos, **277**
  de poset, *veja* poset
  finita de tipos, **278**
  nulária de tipos, **279**
somatório iterativo, **92**, **93**
sonho do calouro, 140
source
  de função, *veja* função
sse, 20
state, *veja* estado
statement
  vs. expressão, **384**
subanel, **561**
subconjunto, **290**
  próprio, **290**
subgrupo, **503**
  normal, **531**, **537**, 538
  trivial, **503**
subjuntivo, 21
submonóide, **556**
subtração
  nos inteiros, **70**
  nos reais, **224**
supremum, **606**
  reais, **244**
série
  harmônica, **271**
séries
  Fourier, 572
sócios, **106**

tabela
  Cayley, **493**
target
  de função, *veja* função
tende, **251**
  uniformemente, **273**
teorema, **40**
  binomial, 96
    por indução, 97
  Cantor, 593
  chinês do resto, 137
  da bem-ordenação, 658
  de intervalos aninhados de Cantor, **265**
  de rearranjo de Riemann, **324**
  de recursão, 417, **646**
  dos números primos, 145
  expansão em base, 99
  fatoração única, *veja* fundamental da aritmética
  Fermatinho, 141, 142, 149, 527
  fundamental da aritmética, 122
  Futurama, **503**
  Knaster–Tarski fixpoint, 612
  Lagrange, **525**
  pequeno de Fermat, *veja* Fermatinho
  sanduíche, **258**
  Schröder–Bernstein, 590
  squeeze, *veja* sanduíche
teorema de isomorfismo
  primeiro (de grupos), 549

teoria dos conjuntos, **658**
  CZF, **662**
  MK, **662**
  NBG, **662**
  NF, **662**
  ZF, **655**
  ZFC, **657**, 658
teoria dos grupos, **658**
testemunha, 300
tetração, **176**
tijolo, **25**, *veja* tijolo
tipo
  duma relação, **434**
  primitivo, 314
TOC
  matemático, 419
top, **605**
topologia, **670**
  discreta, **675**
  indiscreta, **675**
totiente, *veja* função totiente
transformação, *veja* função
trivial, **63**
trivialmente, **59**
triângulo
  de Pascal, **213**
truth set, **435**
tupla
  $\mathcal{I}$-tupla, **326**
  como black box, *veja* black box
  primeiro contato, **38**
  zero, **319**
type error, **22**
túmulo, *veja também* Halmos

unicidade, 108
  da identidade, 485
  do $\emptyset$, 292, 622
  do universal, 292
  dos inversos, 485
  dos naturais, 645
uniformemente, *veja também* convergência
unionset, **627**
unit
  inteiro, **106**
universal
  conjunto, **292**
universo, *veja também* universal
univocidade, *veja* determinabilidade
Unix
  shell, 383
união, **297**
  de conjuntos de reais, **239**
  disjunta, **633**, 633
  grande, **306**
união disjunta, **408**
upper bound, **606**
upset, **606**
urelemento, **618**

valor absoluto, **85**
valuação, **123**, *veja também* primo
variável, **29**
  capturada, **32**, **286**, 286, 362
  dummy, 286
  fresca, **32**
  instância, *veja* ocorrência
  ligada, **30**, **286**, 485
  livre, **30**, **286**
  ocorrência, **30**
  sombreamento, **32**
vazia
  função, *veja* função
vazio, **291**

white box, **287**, *veja também* black box
working mathematician, 655, 657
woset, **655**

zero
  dum poset, **605**
zerodivisor, **563**
ZFC, *veja* teoria dos conjuntos

árvore
  de derivação, **47**
  sintáctica, **47**
átomo, *veja também* urelemento
épica, *veja* função, epí
óbvio, **63**

λ-abstracção, **358**
  corpo, **358**

Depois de 1074 exercícios e 227 problemas, let's call it a day (year?).