FMC2, 2017.1
(Turma ♠N12♠ do Thanos)

Prova 2
(points: 108/100; bonus: $0^\flat$; time: 90')

Nome: Θάνος **Gabarito**

09/06/2017

Regras:

I. Não vires esta página antes do começo da prova.

II. Nenhuma consulta de qualquer forma.

III. Nenhum aparelho ligado (por exemplo: celular, tablet, notebook, *etc.*).[1]

IV. Nenhuma comunicação de qualquer forma e para qualquer motivo.

V. $\forall x\big(\text{Colar}(x) \to \neg\text{Passar}(x, \text{FMC2})\big)$.[2]

VI. Use caneta para tuas respostas.

VII. Responda dentro das caixas indicadas.

VIII. Escreva teu nome em *cada* folha de rascunho extra, antes de usá-la.

IX. Entregue *todas* as folhas de rascunho extra, juntas com tua prova.

X. Nenhuma prova será aceita depois do fim do tempo.

XI. Os pontos bônus serão considerados apenas para quem conseguir passar sem.[3]

XII. Escolha até 3 dos A, B, C, D, E para resolver.[4]

Boas provas!

[1] Ou seja, *desligue antes* da prova.
[2] Se essa regra não faz sentido, melhor desistir desde já.
[3] Por exemplo, 25 pontos bonus podem aumentar uma nota de 5,2 para 7,7 ou de 9,2 para 10,0, mas de 4,9 nem para 7,4 nem para 5,0. A 4,9 ficaria 4,9 mesmo.
[4] Provas com respostas em mais que 3 partes não serão corrigidas (tirarão 0 pontos).

Lembre-se:

Definição 1. Um conjunto estruturado $\mathcal{G} = \langle G\,;\, e, * \rangle$ é um *grupo* sse:

$$(\forall a, b \in G)\,[\,a * b \in G\,] \tag{G0}$$
$$(\forall a, b, c \in G)\,[\,a * (b * c) = (a * b) * c\,] \tag{G1}$$
$$(\forall a \in G)\,[\,e * a = a = a * e\,] \tag{G2}$$
$$(\forall a \in G)\,(\exists a' \in G)\,[\,a' * a = e = a * a'\,] \tag{G3}$$

Denotamos o inverso de $a \in G$ garantido pela (G3) com a^{-1} ou $(-a)$, dependendo se usamos notação multiplicativa ou aditiva para o grupo.

Definição 2. Um conjunto estruturado $\mathcal{R} = \langle R\,;\, 0, +, \cdot \rangle$ é um *anel* sse:

$$(\forall x, y \in R)\,[\,x + y \in R\,] \tag{A0}$$
$$(\forall x, y, z \in R)\,[\,x + (y + z) = (x + y) + z\,] \tag{A1}$$
$$(\forall x \in R)\,[\,0 + x = x = x + 0\,] \tag{A2}$$
$$(\forall x \in R)\,(\exists x' \in R)\,[\,x' + x = 0 = x + x'\,] \tag{A3}$$
$$(\forall x, y \in R)\,[\,x + y = y + x\,] \tag{A4}$$
$$(\forall x, y \in R)\,[\,x \cdot y \in R\,] \tag{M0}$$
$$(\forall x, y, z \in R)\,[\,x \cdot (y \cdot z) = (x \cdot y) \cdot z\,] \tag{M1}$$
$$(\forall x, y, z \in R)\,[\,x \cdot (y + z) = x \cdot y + x \cdot z\,] \tag{DL}$$
$$(\forall x, y, z \in R)\,[\,(y + z) \cdot x = y \cdot x + z \cdot x\,] \tag{DR}$$

Denotamos o inverso de $x \in R$ garantido pela (A3) com $(-x)$. Se no R existe elemento neutro da $\cdot$, o denotamos com 1 ou $1_{\mathcal{R}}$; ele é único e satisfaz:

$$(\forall x \in R)\,[\,i \cdot x = x = x \cdot i\,] \tag{M2}$$

Nesse caso chamamos o anel $\mathcal{R}$ *anel com unidade*. Se a $\cdot$ é comutativa, chamamos o $\mathcal{R}$ *anel comutativo*.

Definição 3. Sejam G grupo $g \in G$, e $A, B \subseteq G$. Definimos

$$gA \stackrel{\text{def}}{=} \{ga \mid a \in A\} \qquad AB \stackrel{\text{def}}{=} \{ab \mid a \in A,\ b \in B\} \qquad \ldots \text{etc.}$$

Definição 4. Um *homomorfismo* φ do grupo $\langle A\,;\, e_A, \cdot_A \rangle$ para o grupo $\langle B\,;\, e_B, \cdot_B \rangle$ é uma função $\varphi : A \to B$ tal que para todo $x, y \in A$, $\varphi\,(x \cdot_A y) = \varphi(x) \cdot_B \varphi(y)$.

Definição 5. Um subgrupo $N \leq G$ é *subgrupo normal* de G sse

$$N \trianglelefteq G \iff \text{para todo } g \in G \text{ e } n \in N,\ gng^{-1} \in N$$
$$\iff \text{para todo } g \in G,\ gN = Ng$$

(36) **A**

Seja G grupo e $H \leq G$. Defina:

$$a \sim b \overset{\text{def}}{\iff} ab^{-1} \in H.$$

(18) **A1.** Prove que $\sim$ é uma relação de equivalência.
PROVA.

REFLEXIVIDADE:
Seja $a \in G$. Temos $aa^{-1} = e \in H$, pois $H \leq G$, e logo $a \sim a$.

SIMETRIA:
Sejam $a, b \in G$ com $a \sim b$, equivalentemente $ab^{-1} \in H$. Logo, como $H \leq G$,

$$H \ni \left(ab^{-1}\right)^{-1} = \left(b^{-1}\right)^{-1} a^{-1} = ba^{-1}.$$

Ou seja, $b \sim a$.

TRANSITIVIDADE:
Seja, $a, b, c \in G$ com $a \sim b$ e $b \sim c$. Equivalentemente $ab^{-1}, bc^{-1} \in H$. Como $H \leq G$, também $H \ni ab^{-1}bc^{-1} = aec^{-1} = ac^{-1}$. Logo $a \sim c$.

(18) **A2.** Prove que para todo $a, b \in G$:

(i) se $a \in H$ e $b \in H$, então $a \sim b$;

(ii) se $a \in H$ e $b \notin H$, então $a \not\sim b$.

PROVA.

(i) Suponha $a, b \in H$. Como $b \in H$ e $H \leq G$, $b^{-1} \in H$. Logo $ab^{-1} \in H$ pela (G0).

(ii) Suponha $a, b \in G$ com $a \in H$ e $b \notin H$ (logo também temos $b^{-1} \notin H$ pois H sendo grupo é fechado pelos inversos). Para chegar num absurdo, suponha que $ab^{-1} \in H$. Agora, como $a \in H$, então $a^{-1} \in H$, e logo $a^{-1}\left(ab^{-1}\right) \in H$. Agora temos:

$$H \ni a^{-1}\left(ab^{-1}\right) = \left(a^{-1}a\right)b^{-1} = eb^{-1} = b^{-1} \notin H,$$

que é absurdo. Concluimos que $ab^{-1} \notin H$, logo $a \not\sim b$.

(36) # B

Um anel $\langle B\,;0,+,\cdot\rangle$ com unidade é *booleano* sse $p^2 = p$ para todo $p \in B$. Prove que:

(18) (i) $p + p = 0$ para todo $p \in B$;

(18) (ii) B é um anel comutativo.

Dica: Calcule o $(p+q)^2$.

Prova.

Seguindo a dica calculamos:

$$\begin{aligned}(p+q)^2 &= (p+q)(p+q)\\ &= (p+q)p + (p+q)q\\ &= pp + qp + pq + qq\\ &= p^2 + qp + pq + q^2\\ &= p + qp + pq + q. \qquad (B \text{ booleano})\end{aligned}$$

Mas como B é booleano temos também $(p+q)^2 = p+q$. Ou seja

$$p + q = p + qp + pq + q$$

e cancelando os p e q ganhamos

$$qp + pq = 0 \tag{1}$$

ou seja, $pq = -qp$

(i) Botando $p = q$ na (1) ganhamos: $p^2 + p^2 = 0$, e como B é booleano, $p + p = 0$.

(ii) Usando a (i) e a (1) ganhamos $pq + pq = 0 = qp + pq$ e cancelando os pq na direita chegamos no $pq = qp$.

(36) # C

(18) **C1.** Sejam A e B grupos. Prove que se φ é um homomorfismo de A para B, então:

(i) $\varphi(e_A) = e_B$ (ii) $\varphi(x^{-1}) = (\varphi(x))^{-1}$

PROVA.

(i) Usando a (G2) e a hipótese que φ é homomorfismo temos $\varphi(e_A) = \varphi(e_A e_A) = \varphi(e_A)\varphi(e_A)$ Multiplicando os dois lados pela direita com $(\varphi(e_A))^{-1}$ temos:

$$\varphi(e_A)(\varphi(e_A))^{-1} = \varphi(e_A)\varphi(e_A)(\varphi(e_A))^{-1}$$
$$\text{ou seja,} \qquad e_B = \varphi(e_A).$$

(ii) Graças a unicidade de inversos em grupos, basta apenas verificar que o $\varphi(x^{-1})$ realmente é o inverso de $\varphi(x)$. Calculamos então o

$$\begin{aligned} \varphi(x)\varphi\big(x^{-1}\big) &= \varphi\big(xx^{-1}\big) && (\varphi \text{ homo}) \\ &= \varphi(e_A) && (\text{G3}) \\ &= e_B. && (\text{pela (i)}) \end{aligned}$$

Ou seja, $(\varphi(x))^{-1} = \varphi(x^{-1})$.

(18) **C2.** Considere os grupos $\mathbf{R} = \langle \mathbb{R} \setminus \{0\} \,;\, \cdot \rangle$ e $\mathbf{Z} = \langle \mathbb{Z} \,;\, + \rangle$. Denota seus subgrupos cíclicos gerados por 2 com $\langle 2 \rangle_{\mathbf{R}}$ e $\langle 2 \rangle_{\mathbf{Z}}$ respectivamente. Ache um isomorfismo entre os $\langle 2 \rangle_{\mathbf{R}}$ e $\langle 2 \rangle_{\mathbf{Z}}$ (e prove que realmente é isomorfismo).

RESPOSTA & PROVA.

Observe que

$$\langle 2 \rangle_{\mathbf{Z}} = \{2m \mid m \in \mathbb{Z}\} \qquad \text{e} \qquad \langle 2 \rangle_{\mathbf{R}} = \{2^m \mid m \in \mathbb{Z}\}.$$

Naturalmente definimos a $F : \langle 2 \rangle_{\mathbf{Z}} \to \langle 2 \rangle_{\mathbf{R}}$ tal que $2m \mapsto 2^m$:

$$F(x) = 2^{x/2}.$$

A F É BIJETORA: Trivial: a preimagem do aleatorio $2^m \in \langle 2 \rangle_{\mathbf{R}}$ é o $2m$, e

$$2m \neq 2m' \implies m \neq m' \implies 2^m \neq 2^{m'}.$$

A F É UM HOMOMORFISMO DE $\langle 2 \rangle_{\mathbf{Z}}$ PARA $\langle 2 \rangle_{\mathbf{R}}$: Sejam $x, y \in \langle 2 \rangle_{\mathbf{Z}}$. Temos:

$$\begin{aligned} F(x+y) &= 2^{(x+y)/2} && (\text{def. } F) \\ &= 2^{x/2+y/2} && (\text{aritmética}) \\ &= 2^{x/2} \cdot 2^{y/2} && (\text{aritmética}) \\ &= F(x) \cdot F(y). && (\text{def. } F) \end{aligned}$$

Logo, a F é um isomorfismo de $\langle 2 \rangle_{\mathbf{Z}}$ para $\langle 2 \rangle_{\mathbf{R}}$.

(36) **D**

Seja G grupo e $N \trianglelefteq G$. Prove que o conjunto G/N de todos os right cosets[5] de N com a operação $\bullet$ definida pela

$$(Na) \bullet (Nb) \stackrel{\text{def}}{=} (Na)(Nb)$$

é um grupo.

PROVA.

Precisamos verificar os (G0)–(G3).

(G0): Tomamos $A, B \in G/N$ e logo $A = Na$ e $B = Nb$ para alguns $a, b \in G$. Calculamos

$$\begin{aligned} A \bullet B &= (Na)(Nb) && \text{(def. } \bullet\text{)} \\ &= N(aN)b && \text{(G1 \& Def. 3)} \\ &= N(Na)b && \text{(G1 \& Def. 3)} \\ &= (NN)(ab) && \text{(G1 \& Def. 3)} \\ &= N(ab) && \text{(Lemma*)} \\ &\in G/N && (ab \in G) \end{aligned}$$

(G1): Garantida pela associatividade de G (G1) e a Definição 3: tomando $A, B, C \in G/N$ temos $A = Na$, $B = Nb$, $C = Nc$ para alguns $a, b, c \in G$. Agora observe:

$$A \bullet (B \bullet C) = Na(NbNc) = NaN(bc) = Na(bc) = N(ab)c = (NaNb)Nc = (A \bullet B) \bullet C.$$

(G2): A identidade do G/N é a coclasse $N = Ne$, pois tome uma coclasse arbitraria $A \in G/N$ (logo $A = Na$ para algum $a \in G$) e calcule:

$$A \bullet N = (Na)(Ne) = N(ae) = Na.$$

(G3): Vamos achar o inverso do arbitrario $A \in G/N$. Temos então $A = Na$ para algum $a \in G$. Afirmamos que $A^{-1} = Na^{-1}$:

$$A \bullet A^{-1} = (Na)(Na^{-1}) = N(aa^{-1}) = Ne.$$

Lemma*. *Se $H \leq G$, então $HH = H$.*

PROVA.

"$H \subseteq HH$": Tome $h \in H$. Como $h = eh$ e $e \in H$ (pois $H \leq G$), temos $h = eh \in HH$.

"$HH \subseteq H$": Tome $x \in HH$. Pela definição de HH então $x = h_1h_2$ para alguns $h_1, h_2 \in H$, e como $H \leq G$, temos $H \ni h_1h_2 = x$.

[5] coclasses à direita

(36) **E**

(18) **E1.** Prove/refuta a afirmação: *Se G é um grupo e $H_1, H_2 \leq G$, então $H_1 \cup H_2 \leq G$.*

Prova/Refutação.

Contraexemplo: Tome

$$G := \langle \mathbb{Z} \,;\, + \rangle$$
$$H_1 := 2\mathbb{Z}$$
$$H_2 := 3\mathbb{Z}$$
$$\text{e logo} \qquad H_1 \cup H_2 = \{m \in \mathbb{Z} \mid 2 \mid m \text{ ou } 3 \mid m\}$$

Obviamente $H_1, H_2 \leq G$. Mas observe que $2, 3 \in H_1 \cup H_2 \not\ni 2 + 3$.

(18) **E2.** Sejam G grupo e $\mathscr{H}$ uma família não vazia de subgrupos de G. Prove que:

$$\bigcap \mathscr{H} \leq G.$$

Prova.

Obviamente $\bigcap \mathscr{H} \subseteq G$, então precisamos mostrar que:

$\bigcap \mathscr{H}$ fechado pela operação de G:
Tome $h_1, h_2 \in \bigcap H$. Pela definição da $\bigcap$, temos que $h_1, h_2 \in H$ para todo $H \in \mathscr{H}$. Como cada $H \leq G$, também temos que $h_1 h_2 \in H$ para todo $H \in \mathscr{H}$. Ou seja, $h_1 h_2 \in \bigcap \mathscr{H}$.

$\bigcap \mathscr{H}$ fechado pelos inversos:
Similar. Aqui a mesma ideia escrita num estilo diferente:

$$\begin{aligned} h \in \bigcap \mathscr{H} &\implies (\forall H \in \mathscr{H})\,[\, h \in H \,] && (\text{def. } \textstyle\bigcap) \\ &\implies (\forall H \in \mathscr{H})\,\big[\, h^{-1} \in H \,\big] && (H \leq G) \\ &\implies h^{-1} \in \bigcap \mathscr{H}. && (\text{def. } \textstyle\bigcap) \end{aligned}$$

Só isso mesmo.