FMC2, 2017.2 (Turma ♣T34♣ do Thanos)

Prova 2 (points: 112/100; bonus: $0^\flat$; time: 90')

Nome: Θάνος **Gabarito**

08/11/2017

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]

GABARITO

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 (grupo; grupo abeliano; monóide). Um conjunto estruturado $\mathcal{G} = \langle G\,;\, e, *\rangle$ é um *grupo* sse:

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

Se $\mathcal{G}$ satisfaz as (G0)–(G3) em cima e a

$$(\forall a, b \in G)\,[\,a * b = b * a\,] \tag{G4}$$

chamamos o $\mathcal{G}$ *grupo abeliano*. 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. Se o $\mathcal{G}$ satisfaz as (G0)–(G2) ele é um *monóide*.

Definição 2 (anel). Um conjunto estruturado $\mathcal{R} = \langle R\,;\, 0, 1, +, \cdot\rangle$ é um *anel* (com identidade) sse:

$$(\forall x, y \in R)\,[\,x + y \in R\,] \tag{A0}$$
$$(\forall x, y, z \in R)\,[\,x + (y + z) = (x + y) + z\,] \tag{A1}$$
$$(\forall x \in R)\,[\,0 + x = x = x + 0\,] \tag{A2}$$
$$(\forall x \in R)\,(\exists y \in R)\,[\,y + x = 0 = x + y\,] \tag{A3}$$
$$(\forall x, y \in R)\,[\,x + y = y + x\,] \tag{A4}$$
$$(\forall x, y \in R)\,[\,x \cdot y \in R\,] \tag{M0}$$
$$(\forall x, y, z \in R)\,[\,x \cdot (y \cdot z) = (x \cdot y) \cdot z\,] \tag{M1}$$
$$(\forall x \in R)\,[\,1 \cdot x = x = x \cdot 1\,] \tag{M2}$$
$$(\forall x, y, z \in R)\,[\,x \cdot (y + z) = x \cdot y + x \cdot z\,] \tag{DL}$$
$$(\forall x, y, z \in R)\,[\,(y + z) \cdot x = y \cdot x + z \cdot x\,] \tag{DR}$$

Denotamos o inverso de $x \in R$ garantido pela (A3) com $(-x)$. Se 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 (homomorfismo de grupo). 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:

(i) para todo $x, y \in A$, $\varphi(x \cdot_A y) = \varphi(x) \cdot_B \varphi(y)$;

(ii) $\varphi(e_A) = e_B$;

(iii) para todo $x \in A$, $\varphi(x^{-1}) = (\varphi(x))^{-1}$.

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

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

(18) **A**

Dado um grupo *finito* G e $H \leq G$, definimos o *normalizer* de H no G como o conjunto:

$$N(H) \stackrel{\text{def}}{=} \{g \in G \mid \text{para todo } h \in H,\ ghg^{-1} \in H\}$$

(9) **A1.** Mostre que $N(H) \leq G$.
PROVA.

Como G é finito, $N(H)$ também é, então basta verificar que ele é fechado pela operação para ser um subgrupo. Sejam $m, n \in N(H)$. Queremos $mn \in N(H)$, ou seja, basta provar que:

$$\text{para todo } h \in H, \quad (mn)h(mn)^{-1} \in H.$$

Seja $h \in H$. Calculamos

$$\begin{aligned}
(mn)h(mn)^{-1} &= (mn)hn^{-1}m^{-1} && \text{(inv. de prod.)}\\
&= m(nhn^{-1})m^{-1} && \text{(ass.)}\\
&= mh'm^{-1} \quad \text{para algum } h' \in H && (n \in N(H);\ h \in H)\\
&\in H && (m \in N(H);\ h' \in H).
\end{aligned}$$

Logo $N(H) \leq G$.

(9) **A2.** Mostre que $H \trianglelefteq N(H)$.
PROVA.

"$H \subseteq N(H)$": Seja $x \in H$. Para provar que $x \in N(H)$, basta verificar que

$$\text{para todo } h \in H, \quad xhx^{-1} \in H.$$

Seja $h \in H$. Observe que realmente $xhx^{-1} \in H$, como produto de membros de H.

"$H \leq N(H)$": Os H e $N(H)$ são grupos com a mesma operação, e $H \subseteq N(H)$.

"$H \trianglelefteq N(H)$": Vamos provar que H é fechado pelos conjugados no $N(H)$. Tome então $h \in H$ e $n \in N(H)$. Logo $nhn^{-1} \in N(H)$, que é o que queremos provar!

(32) # B

Definition. Sejam G grupo e $H \subseteq G$. Chamamos o H *subgrupo* de G sse H é um grupo com a mesma operação de G. Escrevemos $H \leq G$.

(12) **B1. Criterion.** *Sejam G grupo e $\emptyset \neq H \subseteq G$ tal que:*

(i) *H é fechado pela operação de G;*

(ii) *H é fechado pelos inversos de G.*

Então $H \leq G$.
Prova.

Como G é um grupo sua operação é associativa, então a (G0) é garantida para o H. As (i) e (ii) são as (G1) e (G3) respectivamente, então basta verificar que o $e \in H$. Seja $h \in H$. Logo $h^{-1} \in H$ [pela (ii)]. Logo $hh^{-1} \in H$ [pela (i)]. Mas $hh^{-1} = e$, logo $e \in H$.

(20) **B2. Criterion.** *Sejam G grupo e H um* finito e não vazio *subconjunto de G, tal que H é fechado pela operação de G. Então $H \leq G$.*
Prova.

Graças ao B1, basta mostrar que todos os membros de H têm seu inverso dentro do H. Tome $a \in H$. Considere todas as potências positívas de a:

$$a, a^2, a^3, \ldots$$

Sabemos que é uma quantidade finita pois todas pertencem no H que é finito. Ou seja, $a^i = a^j$ para alguns distintos $i, j \in \mathbb{N}$. Sem perda de generalidade, suponha $i < j$. Logo $e = a^{j-i}$. Separamos em dois casos:

Caso $j - i = 1$: Nesse caso então temos $e = a^1 = a$, e logo $a^{-1} = e^{-1} = e = a \in H$.

Caso $j - i > 1$: Nesse caso, temos $e = aa^{j-i-1}$, ou seja, achamos o inverso do a: é o a^{j-i-1}, e ele pertence no H, pois é potência positiva de a (e H é fechado pela operação).

Em ambos os casos mostramos que $a^{-1} \in H$. Logo $H \leq G$.

(32) C

Definition I (domínio de cancelamento). Um anel comutativo D tal que

$$\text{para todo } a, x, y \in D, \quad ax = ay \ \ \& \ \ a \neq 0 \implies x = y \tag{CL}$$

é chamado *domínio de cancelamento*.

Definition II (domínio de integridade). Um anel comutativo D tal que

$$\text{para todo } x, y \in D, \quad \text{se } xy = 0 \text{ então } x = 0 \text{ ou } y = 0 \tag{NZD}$$

é chamado *domínio de integridade*.

Fato. As definições I e II são equivalentes.

Definition III (corpo). Um anel comutativo F tal que

$$\text{para todo } a \in F \setminus \{0\}, \text{ existe } y \in F, \text{ tal que } ay = 1 = ya. \tag{M3}$$

é chamado *corpo*.

Critérion. *Se D é um domínio de integridade finito então D é um corpo.*

Prova.

Suponha que D é um domínio de integridade finito. Preciso 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:

$$dd_i = dd_j \overset{\text{(CL)}}{\implies} d_i = d_j \implies i = j.$$

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 provar.

(24) # D

Definition (homomorfismo de monóide). Sejam $\mathcal{M} = (M; \cdot_M, 1_M), \mathcal{N} = (N; \cdot_N, 1_N)$ monóides e $\varphi : M \to N$. A φ é um *homomorfismo de monóides* sse:

(i) para todo $x, y \in M$, $\varphi(x \cdot_M y) = \varphi(x) \cdot_N \varphi(y)$;

(ii) $\varphi(1_M) = 1_N$.

(12) **D1. Critérion.** *Sejam $\mathcal{M} = (M; \cdot_M, 1_M), \mathcal{N} = (N; \cdot_N, 1_N)$ monóides e $\varphi : M \twoheadrightarrow N$ surjeção tal que*

$$\varphi(x \cdot_M y) = \varphi(x) \cdot_N \varphi(y) \quad \textit{para todo } x, y \in M.$$

A φ é um homomorfismo de monóides.

Prova.

Como φ é sobrejetora, temos que existe $u \in M$ tal que $\varphi(u) = 1_M$. Agora temos:

$$\begin{aligned} \varphi(u1_N) &= \varphi(u)\varphi(1_N) && \text{(pela hip.)} \\ &= 1_M\varphi(1_N) && \text{(pela escolha do } u\text{)} \\ &= \varphi(1_N) && \text{(pela def. do } 1_M\text{)} \end{aligned}$$

e também

$$\begin{aligned} \varphi(u1_N) &= \varphi(u) && \text{(pela def. do } 1_N\text{)} \\ &= 1_M && \text{(pela escolha do } u\text{)} \end{aligned}$$

Ou seja, $\varphi(1_N) = 1_M$ que é o que queremos provar.

(12) **D2. Proposição.** Sejam $\mathcal{R}, \mathcal{S}$ aneis e $f : \mathcal{R} \to \mathcal{S}$ um homomorfismo de aneis. Prove que para todo $k \in \ker f$ e todo $r \in R$, $kr \in \ker f$.

Prova.

Sejam $k \in \ker f$, $r \in R$. Precisamos mostrar que $f(kr) = 0_S$. Calculamos:

$$\begin{aligned} f(kr) &= f(k)f(r) && (f \text{ homo } (\cdot)) \\ &= 0_S f(r) && (k \in \ker f) \\ &= 0_S && (0x = 0 \text{ em todo anel}) \end{aligned}$$

Ou seja, $kr \in \ker f$.

(48) # E

(24) **E1.** Sejam $\mathcal{A}, \mathcal{B}$ grupos e $\varphi : \mathcal{A} \to \mathcal{B}$ homomorfismo. Prove que:

$$\varphi \text{ monomorfismo} \iff \ker \varphi = \{e_A\}.$$

Prova.

"$\Rightarrow$": Suponha que $x \in \ker \varphi$. Queremos mostrar que $x = e_A$. Logo $\varphi(x) = e_B$. Mas $\varphi(e_A) = e_B$, ou seja $\varphi(x) = \varphi(e_A)$, e como φ é injetora, temos $x = e_A$.

"$\Leftarrow$": Sejam $x, y \in A$ tais que $\varphi(x) = \varphi(y)$. Queremos provar que $x = y$.
Temos $\varphi(x) = \varphi(y)$.
Logo $\varphi(x)(\varphi(y))^{-1} = \varphi(y)(\varphi(y))^{-1}$. $[\cdot(\varphi(y))^{-1}]$
Logo $\varphi(x)\varphi(y^{-1}) = \varphi(y)\varphi(y^{-1})$. [$\varphi$ homo (resp. inv.)]
Logo $\varphi(xy^{-1}) = \varphi(yy^{-1})$. [$\varphi$ homo (resp. op.)]
Logo $\varphi(xy^{-1}) = \varphi(e_A)$. [def. y^{-1}]
Logo $\varphi(xy^{-1}) = e_B$. [φ homo (resp. id.)]
Logo $xy^{-1} \in \ker \varphi$. [def. $\ker \varphi$]
Logo $xy^{-1} = e_A$. [$\ker \varphi = \{e_A\}$]
Logo $x = y$. $[\cdot y]$

(24) **E2.** Seja G grupo e defina a função $\varphi : G \to G$ pela $\varphi(x) = x^2$. Prove que:

$$\varphi \text{ homomorfismo} \iff G \text{ abeliano.}$$

Prova.

"$\Rightarrow$": Sejam $x, y \in G$. Calculamos

$$\begin{aligned} \varphi(xy) &= (xy)^2 && \text{(pela def. de } \varphi(xy)) \\ &= xyxy && \text{(pela def. de } (xy)^2) \end{aligned} \qquad \begin{aligned} \varphi(xy) &= \varphi(x)\varphi(y) && (\varphi \text{ homo}) \\ &= x^2y^2 && \text{(def. } \varphi) \\ &= xxyy \end{aligned}$$

Ou seja,

$$xyxy = xxyy$$

e cancelando os x pela esquerda e os y pela direita, chegamos no desejado $yx = xy$ e G é abeliano.

"$\Leftarrow$": Sejam $x, y \in G$. Calculamos

$$\varphi(xy) = (xy)^2 = (xy)(xy) = x(yx)y = x(xy)y = (xx)(yy) = x^2y^2 = \varphi(x)\varphi(y).$$

Ou seja, φ é um homomorfísmo.

Só isso mesmo.