FMC2, 2017.1
(Turma ♣T56♣ 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]

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. 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

(18) **A1.** Dado um grupo G, definimos seu *centro* $Z(G)$ como o conjunto dos membros de G que "comutam" com todos os elementos de G:

$$Z(G) \stackrel{\text{def}}{=} \{z \in G \mid \text{para todo } g \in G,\ zg = gz\}$$

Mostre que $Z(G) \leq G$.

PROVA.

Primeiramente observe que $Z(G) \neq \emptyset$: $e \in Z(G)$ pois para todo $g \in G$, $eg = e = ge$ pela definição de e. Como $\emptyset \neq Z(G) \subseteq G$, precisamos apenas mostrar que:

FECHADO SOBRE A OPERAÇÃO DO G:
Sejam $x, y \in Z(G)$. Para $xy \in Z(G)$ verificamos que o (xy) comuta com todos os elementos de G. Seja $g \in G$. Calculamos:

$$\begin{aligned}
(xy)g &= x(yg) && \text{(G1)}\\
&= x(gy) && (y \in Z(G))\\
&= (xg)y && \text{(G1)}\\
&= (gx)y && (x \in Z(G))\\
&= g(xy) && \text{(G1)}
\end{aligned}$$

FECHADO SOBRE OS INVERSOS:
Seja $x \in Z(G)$. Para $x^{-1} \in Z(G)$ verificamos que o x^{-1} comuta com todos os elementos de G. Seja $g \in G$. Calculamos:

$$\begin{aligned}
(x^{-1})g &= \left(g^{-1}x\right)^{-1} && (G \text{ grupo})\\
&= \left(xg^{-1}\right)^{-1} && (x \in Z(G))\\
&= \left(g^{-1}\right)^{-1}x^{-1} && (G \text{ grupo})\\
&= gx^{-1} && (G \text{ grupo})
\end{aligned}$$

(18) **A2.** Seja G grupo e $\emptyset \neq H \subseteq G$. Prove que:

$$H \leq G \iff \text{para todo } a, b \in H,\ ab^{-1} \in H.$$

PROVA.

"$\Rightarrow$": Sejam $a, b \in H$. Como $b \in H$ e $H \leq G$, $b^{-1} \in H$, e logo, $ab^{-1} \in H$.

"$\Leftarrow$": 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 pelos inversos.

Basta provar que é fechado pela operação de G também: tomando $a, b \in H$, ganhamos $a, b^{-1} \in H$, então pela hipótese $a(b^{-1})^{-1} \in H$, ou seja, $ab \in H$.

(36) B

Seja G grupo e denota com $\mathrm{Aut}(G)$ o conjunto estruturado de todos os automorfismos do G, com operação a $\circ$. Sabendo que $\mathrm{Bij}(G) \stackrel{\text{def}}{=} \langle (G \rightarrowtail\!\!\!\!\twoheadrightarrow G)\ ;\ \circ \rangle$ é um grupo, mostre que

$$\mathrm{Aut}(G) \leq \mathrm{Bij}(G).$$

Dica: *Se F é injetora, então $x = y \implies F(x) = F(y)$.*

Prova.

Como $\mathrm{Aut}(G) \subseteq \mathrm{Bij}(G)$, precisamos verificar apenas que:

$\mathrm{Aut}(G)$ é fechado pela $\circ$:
Tome $\varphi, \psi \in \mathrm{Aut}(G)$, e $x, y \in G$. Calculamos:

$$\begin{aligned}
(\varphi \circ \psi)(x \cdot y) &= \varphi\left(\psi(x \cdot y)\right) && \text{(def. } \circ\text{)} \\
&= \varphi\left(\psi(x) \cdot \psi(y)\right) && (\psi \text{ homo}) \\
&= \varphi\left(\psi(x)\right) \cdot \varphi\left(\psi(y)\right) && (\varphi \text{ homo}) \\
&= (\varphi \circ \psi)\,(x) \cdot (\varphi \circ \psi)\,(y) && \text{(def. } \circ\text{)}
\end{aligned}$$

$\mathrm{Aut}(G)$ é fechado pelos inversos:
Tome $\varphi \in \mathrm{Aut}(G)$. Precisamos verificar que a bijeção 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 provar que

$$\varphi\left(\varphi^{-1}(x \cdot y)\right) = \varphi\left(\varphi^{-1}(x) \cdot \varphi^{-1}(y)\right)$$

O lado esquerdo é igual ao $x \cdot y$. Calculamos o lado direito:

$$\begin{aligned}
\varphi\left(\varphi^{-1}(x) \cdot \varphi^{-1}(y)\right) &= \varphi\left(\varphi^{-1}(x)\right) \cdot \varphi\left(\varphi^{-1}(y)\right) && (\varphi \text{ homo}) \\
&= x \cdot y && \text{(def. } \varphi^{-1}\text{)}
\end{aligned}$$

(36) # C

Sejam A e B grupos. Se φ homomorfismo de A para B, definimos

$$\ker\varphi \stackrel{\text{def}}{=} \{x \in A \mid \varphi(x) = e_B\}.$$

Mostre que:

(18) **C1.** $\ker\varphi \leq A$

Prova.

Como $\ker\varphi \subseteq A$ precisamos mostrar que:

$\ker\varphi$ fechado pela operação de A:
Tome $x, y \in \ker\varphi$. Queremos provar que $xy \in \ker\varphi$, ou seja, que $\varphi(xy) = e_B$. Fácil:

$$\begin{aligned} \varphi(xy) &= \varphi(x)\varphi(y) && (\varphi \text{ homo}) \\ &= e_B e_B && (x, y \in \ker\varphi) \\ &= e_B && (\text{G2}) \end{aligned}$$

Logo, $xy \in \ker\varphi$, pela definição de $\ker\varphi$.

$\ker\varphi$ fechado pelos inveros:
Tome $x \in \ker\varphi$. Basta provar $\varphi(x^{-1}) = e_b$. Temos:

$$\begin{aligned} \varphi\left(x^{-1}\right) &= (\varphi(x))^{-1} && (\text{propr. de homo}) \\ &= {e_B}^{-1} && (x \in \ker\varphi) \\ &= e_B && (\text{propr. de grupos}) \end{aligned}$$

Ou seja, $x^{-1} \in \ker\varphi$.

(18) **C2.** $\ker\varphi \trianglelefteq A$

Prova.

Vamos mostrar que $\ker\varphi$ é fechado pelos conjugados, ou seja, que para todo $k \in \ker\varphi$, e todo $a \in A$, temos $aka^{-1} \in \ker\varphi$. Basta verificar então que $\varphi(aka^{-1}) = e_B$. Calculamos:

$$\begin{aligned} \varphi\left(aka^{-1}\right) &= \varphi(a)\varphi(k)\varphi\left(a^{-1}\right) && (\varphi \text{ homo}) \\ &= \varphi(a)e_B\varphi\left(a^{-1}\right) && (k \in \ker\varphi) \\ &= \varphi(a)\varphi\left(a^{-1}\right) && (\text{G2}) \\ &= \varphi\left(aa^{-1}\right) && (\varphi \text{ homo}) \\ &= \varphi(e_A) && (\text{G3}) \\ &= e_B && (\text{propr. de homo}) \end{aligned}$$

Ou seja, $aka^{-1} \in \ker\varphi$ e logo $\ker\varphi \trianglelefteq A$.

(36) **D**

Sejam G grupo, $a \in G$, e $m \in \mathbb{Z}$. Prove que:

$$a^m = e \iff o(a) \mid m$$

onde $o(a)$ denota a ordem de a no G.

PROVA.

"$\Leftarrow$": Usando a hipótese tome $q \in \mathbb{Z}$ tal que $o(a)q = m$. Calcule:

$$a^m = a^{o(a)q} = \left(a^{o(a)}\right)^q = e^q = e.$$

"$\Rightarrow$": Dividimos (lema da divisão de Euclides) o m por $o(a)$, ganhando assim inteiros $q, r \in \mathbb{Z}$ tais que:

$$m = o(a)q + r\,, \qquad 0 \leq r < o(a).$$

Basta mostrar que $r = 0$, ou seja, que r não pode ser positivo. Usando a hipótese temos

$$e = a^m = a^{o(a)q+r} = a^{o(a)q}a^r = \left(a^{o(a)}\right)^q a^r = \left(a^{o(a)}\right)^q a^r = e^q a^r = ea^r = a^r.$$

Mas $r < o(a)$ e pela definição de $o(a)$, r não pode ser positivo, ou seja, $r = 0$ como queriamos.

(36) **E**

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

$$HK = KH \implies HK \leq G.$$

Prova/Refutação.

Vamos provar a afirmação. Suponha $HK = KH$. Como $HK \subseteq G$ precisamos:

HK fechado pela operação de G:
Tome $hk, h'k' \in G$. Calculamos:

$$\begin{aligned}
(hk)(h'k') &= h(kh')k' && \text{(G1)}\\
&= h(h''k'')k', \text{ para alguns } h'' \in H,\ k'' \in K && (kh' \in KH = HK)\\
&= (hh'')(k''k') && \text{(G1)}\\
&\in HK && (\text{(G0)},\ hh'' \in H,\ k''k' \in K)
\end{aligned}$$

HK fechado pelos inversos:
Tome $hk \in HK$ e observe: $(hk)^{-1} = k^{-1}h^{-1} \in KH$.

(18) **E2.** Seja $\langle R\,;\, 0, +, \cdot\rangle$ anel. Prove que:

(i) $0x = 0 = x0$; (ii) $(-x)y = -(xy) = x(-y)$; (iii) $(-x)(-y) = xy$.

Prova.

(i) Facilmente,

$$0x \overset{\text{(A2)}}{=} (0+0)x \overset{\text{(DR)}}{=} 0x + 0x.$$

Sommando $(-(0x))$ nos dois lados pela direita ganhamos $0 = 0x$. O $x0 = 0$ é similar.

(ii) Vamos verificar que o $(-x)y$ é realmente o negativo do xy. Realmente,

$$xy + (-x)y \overset{\text{(DR)}}{=} (x + (-x))y \overset{\text{(A3)}}{=} 0y \overset{\text{(i)}}{=} 0.$$

Similarmente verificamos que o $x(-y)$ também é o negativo do xy.

(iii) Usando repetidamente a (ii) calculamos:

$$(-x)(-y) = -(x(-y)) = -(-(xy)) = xy$$

onde no último cálculo usamos o fato geral que em cada grupo aditivo, $-(-g) = g$ (e um anel com sua operação aditiva forma um grupo).

Só isso mesmo.