FMC2, 2017.2
(Turma ♠N12♠ 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. $\forall x\big(\mathrm{Colar}(x) \to \neg\mathrm{Passar}(x, \mathrm{FMC2})\big)$.[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 $\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}$ 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 (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

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

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

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

(18) **A**

Definition I (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.*

Definition II (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.*

Proposição. As definições I e II são equivalentes, ou seja:

(9) **A1.** D é um domínio de integridade $\implies$ D é um domínio de cancelamento.

PROVA.

Sejam $a, x, y \in D$ tais que $a \neq 0$ e $ax = ay$.
Logo $ax - ay = 0$.
Logo $a(x - y) = 0$.
Logo $x - y = 0$. [pela hip. (NZD)]
Logo $x = y$.

(9) **A2.** D é um domínio de integridade $\impliedby$ D é um domínio de cancelamento.

PROVA.

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 (CL) concluimos $y = 0$.

(32) # B

(12) **B1.** Seja G grupo tal que:

$$\text{para todo } a, b \in G,\ (ab)^2 = a^2b^2.$$

Prove que G é abeliano.

Prova.

Sejam $a, b \in G$. Calculamos

$$\begin{aligned}(ab)^2 &= a^2b^2 = aabb \\ (ab)^2 &= (ab)(ab) = abab.\end{aligned}$$

Ou seja, $aabb = abab$, e cancelando o a pela esquerda e o b pela direita, chegamos no desejado $ab = ba$.

(20) **B2.** Seja G grupo abeliano. Prove por indução que para todo $n \in \mathbb{N}$, e todos os $a, b \in G$, temos:

$$(ab)^n = a^nb^n.$$

Prova.

Base $(n = 0)$: Calculamos:

$$(ab)^0 = e \qquad\qquad a^0b^0 = ee = e$$

Ou seja $(ab)^0 = a^0b^0$.

Passo indutivo: Suponha $k \in \mathbb{N}$ tal que $(ab)^k = a^kb^k$ (HI). Calculamos:

$$\begin{aligned}(ab)^{k+1} &= (ab)^k(ab) && \text{(def. exp.)} \\ &= (a^kb^k)(ab) && \text{(pela (HI))} \\ &= a^k(b^ka)b && \text{(ass.)} \\ &= a^k(ab^k)b && \text{(G abel.)} \\ &= (a^ka)(b^kb) && \text{(ass.)} \\ &= a^{k+1}b^{k+1} && \text{(def. exp.)}\end{aligned}$$

(32) **C**

Critérion. *Sejam* $\mathcal{G} = (G; \cdot_G, e_G), \mathcal{H} = (H; \cdot_H, e_H)$ *grupos e* $\varphi : G \to H$ *tal que*

$$\varphi(x \cdot_G y) = \varphi(x) \cdot_H \varphi(y) \quad \text{para todo } x, y \in G.$$

A φ *é um homomorfismo de grupos.*

PROVA.

Precisamos mostrar que φ respeita (1) a identidade; e (2) os inversos.

(1) Calculamos:

$$\begin{aligned} \varphi(e_A) &= \varphi(e_A e_A) && \text{(def. } e_A\text{)} \\ &= \varphi(e_A)\varphi(e_A). && \text{(hip.)} \end{aligned}$$

Operando nos dois lados pela direita com o $(\varphi(e_A))^{-1}$, ganhamos o desejado $e_B = \varphi(e_A)$.

(2) Precisamos mostrar que $\varphi(x^{-1})$ satisfaz a propriedade caraterística de ser inverso de $\varphi(x)$, ou seja, queremos $\varphi(x^{-1})\varphi(x) = e_B$. De fato:

$$\begin{aligned} \varphi(x^{-1})\varphi(x) &= \varphi(x^{-1}x) && \text{(hip.)} \\ &= \varphi(e_A) && \text{(def. } x^{-1}\text{)} \\ &= e_B. && \text{(pela (1))} \end{aligned}$$

(24) # D

(12) **D1.** Sejam $\mathcal{G}$ grupo e $H \leq G$. Prove que para todo $a \in G$, $aHa^{-1} \leq G$, onde lembramos que

$$aHa^{-1} \stackrel{\text{def}}{=} \left\{aha^{-1} \mid h \in H\right\}.$$

PROVA.

Basta provar que aHa^{-1} é fechado pela operação e pelos inversos:

FECHADO PELA OPERAÇÃO: Sejam $x, y \in aHa^{-1}$. Logo $x = ah_1a^{-1}$, $y = ah_2a^{-1}$, para alguns $h_1, h_2 \in H$. Calculamos

$$xy = (ah_1a^{-1})(ah_2a^{-1}) = ah_1(a^{-1}a)h_2a^{-1} = ah_1h_2a^{-1} \in aHa^{-1}$$

pois $h_1h_2 \in H$.

FECHADO PELOS INVERSOS: Seja $x \in aHa^{-1}$. Logo $x = aha^{-1}$ para algum $h \in H$. Calculamos

$$x^{-1} = \left(aha^{-1}\right)^{-1} = \left(a^{-1}\right)^{-1}h^{-1}a^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$$

pois $h^{-1} \in H$.

(12) **D2.** Sejam $\mathcal{G}$ grupo e $g \in G$. Defina a função $\varphi_g : G \to G$ pela

$$\varphi_g(x) = gxg^{-1}.$$

Prove que φ_g é um isomorfismo (e logo um automorfismo).
PROVA.

φ HOMOMORFISMO: Sejam $x, y \in G$. Temos

$$\varphi_g(x)\varphi_g(y) = (gxg^{-1})(gyg^{-1}) = gx(g^{-1}g)yg^{-1} = gxeyg^{-1} = g(xy)g^{-1} = \varphi_g(xy)$$

φ INJETORA: Sejam $x, y \in G$ tais que $\varphi_g(x) = \varphi_g(y)$. Logo $gxg^{-1} = gyg^{-1}$, e cancelando os g pela esquerda e os g^{-1} pela direita chegamos no desejado $x = y$.

φ SOBREJETORA: Seja $y \in G$. Uma preimagem de y é o $g^{-1}yg$, pois temos:

$$\varphi(g^{-1}yg) = g(g^{-1}yg)g^{-1} = (gg^{-1})y(gg^{-1}) = eye = y.$$

(48) **E**

Sejam G grupo e $N \trianglelefteq G$.

(12) **E1.** Defina o grupo quociente G/N.
DEFINIÇÃO.

$$G/N \stackrel{\text{def}}{=} \langle \{ Na \mid a \in G \} \; ; \, * \rangle,$$
$$\text{onde} \qquad C * D \stackrel{\text{def}}{=} CD.$$

(36) **E2.** Proves que G/N realmente é um grupo.
PROVA.

Primeiramente observe que:

$$\begin{aligned} (Na)(Nb) &= NaNb \\ &= N(aN)b \\ &= N(Na)b && (N \trianglelefteq G) \\ &= (NN)ab \\ &= Nab && (HH = H \text{ para todo } H \leq G) \end{aligned}$$

(G0): Sejam $A, B \in G/N$. Logo $A = Na$, $B = Nb$, para alguns $a, b \in G$. Queremos $AB \in G/N$. Calculamos

$$AB = (Na)(Nb) = N(ab) \in G/N$$

(G1): Sejam $A, B, C \in G/N$. Logo $A = Na$, $B = Nb$, $C = Nc$ para alguns $a, b, c \in G$. Calculamos:

$$(AB)C = (NaNb)Nc = N(ab)Nc = N(ab)c = Na(bc) = NaN(bc) = Na(NbNc) = A(BC).$$

(G2): Vamos verificar que $N = Ne$ é a identidade do G/N. Seja $A \in G/N$, logo $A = Na$ para algum $a \in G$. Calculamos:

$$NA = NeNa = N(ea) = Na = A.$$

(G3): Seja $X \in G/N$. Logo $X = Nx$ para algum $x \in G$. Confirmamos que o inverso de X no G/N é o Nx^{-1}:

$$X(Nx^{-1}) = NxNx^{-1} = N(xx^{-1}) = Ne = N.$$

Só isso mesmo.