FMC2, 2018.1
(Turma N12 do Thanos)

Prova 2.1
(points: 156; bonus: $0^\flat$; time: 60')

Nome: Θάνος **Gabarito**

11/06/2018

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. $\forall x\big(\mathrm{Colar}(x) \rightarrow \neg\mathrm{Passar}(x, \mathrm{FMC2})\big)$.[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 são considerados apenas para quem consiga passar sem.[3]

XII. **Responda em até 2 dos A, B, C, D, E, F.**[4]

---

[1] Ou seja, *desligue antes* da prova.
[2] Se essa regra não faz sentido, melhor desistir desde já.
[3] Por exemplo, 25 pontos bônus 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 três problemas não serão corrigidas (tirarão 0 pontos).

Lembram-se:

Definição 1 (grupo; grupo abeliano). 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.

Definição 2. 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 3 (subgrupo). Seja G grupo e $H \subseteq G$. O H é um subgrupo de G (escrevemos $H \leq G$) sse H forma um grupo com a mesma operação (restrita no $H \times H$).

Definição 4 (conjugação). Seja G grupo e $a, b \in G$. Chamamos o b conjugado de a sse existe $g \in G$ tal que

$$a = gbg^{-1}.$$

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

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

Definição 6 (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 7 (kernel). Sejam A e B grupos e φ homomorfismo de A para B. Definimos

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

Boas provas!

(28) **A**

Seja G grupo e $\emptyset \neq H \subseteq G$. tal que para todo $a, b \in H$, $ab^{-1} \in H$. Prove que $H \leq G$.
PROVA.

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, $ab \in H$.

(32) **B**

Prove "from scratch" (usando apenas os (G0)–(G3)) a unicidade de inversos nos grupos.

Dica: *Pode provar lémmata (resultados intermediários) para te ajudar.*

Prova.

Unicidade de identidade. Suponha e, e' identidades. Logo temos $ee' = e$ (pois e' identidade) e tambem $ee' = e'$ (pois e identidade). Logo $e = e'$.

Cancelamento pela esquerda (GCL): $ax = ay \implies x = y$
Suponha $ax = ay$ e seja a' um inverso de a (pela G3). Logo temos:

$$a'(ax) = a'(ay)$$

Pelassociatividade agora temos

$$(a'a)x = (a'a)y$$

mas pela definição de a', $a'a = e$, ou seja, $ex = ey$, e pela definição de e, $x = y$.

Unicidade de inversos. Seja $a \in G$ e a', a'' inversos de a. Logo temos

$$aa' = e = aa''$$

e pela (GCL) ganhamos o desejado $a' = a''$.

(38) **C**

Definição. Um *monóide* é um conjunto estruturado $\mathcal{M} = \langle M\ ;\ \cdot, \epsilon \rangle$ que satisfaz as (G0)–(G2). Uma função $\phi : A \to B$ entre monóides é um homomorfismo sse ϕ respeita a estrutura:

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

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

Teorema. Sejam M, N monóides e $\phi : M \twoheadrightarrow N$ função *sobrejetora* tal que respeita a operação:

$$\text{para todo } x, y \in M, \quad \phi(x \cdot_M y) = \phi(x) \cdot_N \phi(y)$$

Então ϕ é um homomorfismo.

Prova.

Precisamos provar que $\phi(\epsilon_M) = \epsilon_N$, ou seja, que para todo $n \in N$,

$$n \cdot_N \phi(\epsilon_M) = n = \phi(\epsilon_M) \cdot_N n.$$

Seja $n \in N$. Logo $n = \phi(m)$ para algum $m \in M$. Calculamos:

$$\begin{aligned}
n \cdot_N \phi(\epsilon_M) &= \phi(m) \cdot_N \phi(\epsilon_M) && \text{(pela escolha do } m\text{)} \\
&= \phi(m \cdot_M \epsilon_M) && (\phi \text{ homo (oper.))} \\
&= \phi(m) && \text{(pela (G2))} \\
&= n && \text{(pela escolha do } m\text{)}
\end{aligned}$$

Similarmente, $n = \phi(\epsilon_M) \cdot_N n$.

(46) **D**

Sejam A e B grupos e $\varphi : A \to B$ homomorfismo.

(23) **D1.** $\ker\varphi \leq A$

Prova.

Observe primeiramente que $\ker\varphi \neq \emptyset$, pois $e_A \in \ker\varphi$ (pois φ homomorfismo). E como $\emptyset \neq \ker\varphi \subseteq A$ basta 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:

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

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

(23) **D2.** $\ker\varphi \trianglelefteq A$

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:

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

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

(56) **E**

Seja G grupo e $a, b \in G$ conjugados.

(32) **E1.** Para todo $n \in \mathbb{N}$, a^n e b^n também são conjugados;

Dica: *Indução.*

PROVA.

Sejam $x, g \in G$. Basta mostrar que:

$$\text{para todo } n \in \mathbb{N}, \quad (gxg^{-1})^n = gx^ng^{-1}.$$

Realmente, provamos por indução. Primeiramente observe que

$$(gxg^{-1})^0 = e \qquad\qquad gx^0g^{-1} = geg^{-1} = gg^{-1} = e$$

Agora seja $k \in \mathbb{N}$ tal que

$$(gxg^{-1})^k = gx^kg^{-1} \tag{H.I.}$$

Calculamos

$$\begin{aligned}
(gxg^{-1})^{k+1} &= (gxg^{-1})^k(gxg^{-1}) \\
&= (gx^kg^{-1})(gxg^{-1}) && \text{(pela H.I.)} \\
&= gx^k(g^{-1}g)xg^{-1} \\
&= gx^kxg^{-1} \\
&= gx^{k+1}g^{-1}
\end{aligned}$$

(24) **E2.** $o(a) = o(b)$.

PROVA.

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) Pela **E1**, temos que a^n e b^n são conjugados, mas $a^n = e$, e sabemos que a classe de conjugação de e é o $\{e\}$. Logo $b^n = e$.

(ii) Pela mesma observação cada suposto $b^m = e$ obrigaria $a^m = e$ também.

Logo $o(b) = n$.

Resolução 2. Pela **E1** 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 $o(a) = \infty$.

(100) **F**

Já provamos algo que informalmente falando podemos escrever assim:

$$\text{kernel} \implies \text{normal}$$

Formalize e prove o converso.

(16) TEOREMA.

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.

(84) PROVA.

Seja G' o grupo G/N e defina a $\varphi : G \to G/N$ pela

$$\varphi(x) = Nx.$$

Basta provar 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

$$\begin{aligned} x \in \ker\varphi &\iff \varphi(x) = e_{G/N} \\ &\iff \varphi(x) = N \\ &\iff Nx = N \\ &\iff x \in N. \end{aligned}$$

Ou seja, $\ker\varphi = N$.

Com isso concluimos que na teoria de grupos, "subgrupo normal" e "kernel" são dois lados da mesma moeda.

Só isso mesmo.