FMC2, 2023.1
(Turma N12 do Thanos)

Prova 3.2
(points: 45; bonus: $0^\flat$; time: 84')

Nome: Θάνος **Gabarito**

2023-06-05

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. $(\forall x)\,[\,\mathrm{Colar}(x) \implies \neg\mathrm{Passar}(x, \mathrm{FMC2})\,]$.[2]

VI. Responda dentro das caixas indicadas.

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

VIII. Nenhuma prova será aceita depois do fim do tempo—mesmo se for atraso de 1 segundo.

IX. Escolha exatamente 2 das $\mathbf{C}, \mathbf{H}, \mathbf{D}, \mathbf{S}$.[3]

Esclarecimento. Escreva suas demonstrações e definições em linguagem "high-level" sem comprometer rigor, clareza, e corretude. Escreva em texto compilável em português matemático, sem depender de conhecimento de gírias matemáticas. (Podes utilizar gírias sim—é bom!—mas o texto das definições precisa compilar até para quem não as conhece.)
Presente. Na tua demonstração de $\mathbf{X}n$ podes considerar demonstrados os teoremas $\mathbf{X}i$ com $i < n$.

Lembrete. Nas aulas demonstramos que, para certos subgrupos $H \leq G$, as relações de equivalência (R_H) e (L_H) são *congruências*—tais subgrupos acabamos chamando de *subgrupos normais*. Uma outra relação de equivalência que definimos para qualquer grupo G foi a $(\approx)$ de conjuga, definida pela

$$x \approx y \overset{\text{def}}{\iff} (\exists g \in G)\,[\,x = gyg^{-1}\,]\,.$$

Suas classes de equivalência chamamos de *classes de conjugação*. Denotamos por $\mathrm{Cls}(a)$ a classe de conjugação de a:

$$\mathrm{Cls}(a) \overset{\text{def}}{=} [a]_{(\approx)} \equiv \{\, g \in G \mid a \approx g \,\}\,.$$

Definição. Um *monóide* $\mathscr{M}$ é um conjunto estruturado $\mathscr{M} = (M\,;\,\cdot, e)$ onde

$$(\cdot) : M \times M \to M \qquad\qquad e : M$$

tal que: (M-ass) a $(\cdot)$ é associativa; (M-id) e é uma $(\cdot)$-identidade.

Boas provas!

---

[1] Ou seja, *desligue antes* da prova.
[2] Se essa regra não faz sentido, melhor desistir desde já.
[3] Provas violando essa regra (com respostas em mais problemas) não serão corrigidas (tirarão 0 pontos).

(24) # C

Escolha exatamente uma das **C1**, **C2**, **C3**, **C4**.

Seja G um grupo.

(8) **C1.** $\mathrm{Cls}(e) = \{e\}$.

(16) **C2.** G abeliano sse toda classe de conjugação de G é singleton.

(8) **C3.** Todo membro $a \in G$ conjuga com todos os seus conjugados: $(\forall a, g \in G)\left[a \approx gag^{-1}\right]$.

(24) **C4.** $(\approx)$ é uma congruência sse G é abeliano.

DEMONSTRAÇÃO DE _____ .

C1. Como $e \approx e$ (reflexividade da $(\approx)$), logo $e \in \mathrm{Cls}(e)$. Agora seja x tal que $e \approx x$, e logo $x \approx e$ (simetria da $(\approx)$). Logo seja g tal que $x = geg^{-1} = gg^{-1} = e$.

C2. $(\Rightarrow)$ Pela reflexividade da $(\approx)$ cada classe de conjugação é habitada, logo basta mostrar que quaisquer membros da mesma classe são iguais. Sejam u, v tais que $u \approx v$, e logo seja g tal que $u = gvg^{-1} \overset{(\mathrm{Ab})}{=} gg^{-1}v = ev = v$.
$(\Leftarrow)$ Pela hipótese, basta mostrar que $ab \approx ba$.
Realmente: $ab = abe = ab(aa^{-1}) = a(ba)a^{-1}$.

C3. Sejam $a, g \in G$ tais que $a = gag^{-1}$. Preciso $a \approx gag^{-1}$, que segue pela reflexividade da $(\approx)$.

C4. Pela **C2**, basta mostrar que $(\approx)$ é uma congruência sse toda classe de conjugação é singleton.
$(\Rightarrow)$ Sejam u, v da mesma classe de conjugação, ou seja, $u \approx v$ $^{(1)}$.
Também temos $u^{-1} \approx v^{-1}u^{-1}\left(v^{-1}\right)^{-1}$ $^{(2)}$ pela **C3**.
Como $(\approx)$ é uma congruência, pelas (1) e (2), temos

$$uu^{-1} \approx v(v^{-1}u^{-1}\left(v^{-1}\right)^{-1}),$$

e logo: $$e \approx u^{-1}v.$$

Pela **C1**, segue que $u^{-1}v = e$, e logo $u = v$.
$(\Leftarrow)$ (op)-compatibilidade.
Sejam a, b, u, v tais que $a \approx u$ e $b \approx v$.
Pela hipotese temos $a = u$ e $b = v$, e agora é imediato que $ab \approx uv$, pela reflexividade da $(\approx)$. (id)-compatibilidade. Imediata pela reflexividade.
(inv)-compatibilidade.
Sejam $a \approx b$, e logo seja g tal que $a = gbg^{-1}$.
Logo $a^{-1} = \left(g^{-1}\right)^{-1}b^{-1}g^{-1}$ e logo $a^{-1} \approx b^{-1}$.

(21) # H

(4) **H0.** Como definirias o que significa homomorfismo de monóides?

DEFINIÇÃO.

Sejam $\mathscr{M} = (M\,;\cdot_M, 1_M), \mathscr{N} = (N\,;\cdot_N, 1_N)$ monóides e $\varphi : M \to N$ função.
Chamamos a φ de *homomorfismo* sse φ respeita a operação e a identidade, i.e.:
(i) para todo $m, m' \in M$, $\varphi\,(m \cdot_M m') = (\varphi\, m) \cdot_N (\varphi\, m')$; (ii) $\varphi\, 1_M = 1_N$.

(5 + 12) **H1.** Desenhe o(s) diagrama(s) cuja comutatividade *significa* que $\varphi : \mathscr{M} \to \mathscr{N}$ é um homomorfismo.

DIAGRAMAS.

$$\begin{tikzcd}
M \times M \arrow[r, "\varphi\times\varphi"] \arrow[d, "(\cdot_M)"'] & N \times N \arrow[d, "(\cdot_N)"] \\
M \arrow[r, "\varphi"] & N
\end{tikzcd}$$

$$\begin{tikzcd}
& 1 \arrow[dl, "\lambda x.1_M"'] \arrow[dr, "\lambda x.1_N"] & \\
M \arrow[rr, "\varphi"] & & N
\end{tikzcd}$$

H2. Demonstre o seguinte critérion.
Sejam $\mathscr{M}, \mathscr{N}$ monóides e $\varphi : M \to N$ uma função. Logo:
φ homomorfismo se φ é sobrejetiva e respeita a operação.

DEMONSTRAÇÃO.

Preciso mostrar que φ respeita a identidade: $\varphi\, 1_M = 1_N$.
Seja $m_1 \in M$ tal que $m_1 \overset{\varphi}{\longmapsto} 1_N$. Calculamos:

$$\begin{aligned}
\varphi\, 1_M &= (\varphi\, 1_M)1_N && (\mathscr{N}.(\mathrm{id}))\\
&= (\varphi\, 1_M)(\varphi\, m_1) && (\text{pela escolha de } m_1)\\
&= \varphi\,(1_M m_1) && (\varphi \text{ resp. op.})\\
&= \varphi\, m_1 && (\mathscr{M}.(\mathrm{id}))\\
&= 1_N. && (\text{pela escolha de } m_1)
\end{aligned}$$

(14) **D** *Escolha exatamente uma das* **D1**, **D2**, **D3**, **D4**.

(12) **D1.** Sejam H, K subgrupos de um grupo G. Logo $HK = KH \implies HK \leq G$.
(14) **D2.** Seja $\varphi : \mathscr{A} \to \mathscr{B}$ homomorfismo de grupos. Logo $\ker \varphi \trianglelefteq \mathscr{A}$.
(12) **D3.** Seja $\varphi : \mathscr{A} \to \mathscr{B}$ homomorfismo de grupos. Logo $\mathrm{im}\varphi \leq \mathscr{B}$.
(12) **D4.** Seja $\varphi : \mathscr{A} \to \mathscr{B}$ homomorfismo de grupos. Logo φ preserve a $(\approx)$.

Demonstração de ______ .

D1. Sejam $h_1, h_2 \in H$ e $k_1, k_2 \in K$. Basta verificar que $(h_1k_1)(h_2k_2)^{-1} \in HK$. Calculamos: $(h_1k_1)(h_2k_2)^{-1} = h_1k_1{k_2}^{-1}{h_2}^{-1} \overset{(*)}{=} h_1h_3k_3h_3{h_2}^{-1}$.
$(*)$: Como $k_1{k_2}^{-1}{h_2}^{-1} \in KH = HK$, logo sejam $h_3 \in H$ e $k_3 \in K$ tais que $k_1{k_2}^{-1}{h_2}^{-1} = h_3k_3$.

D3. Como $\varphi\, e_A \in \mathrm{im}\varphi$, logo $\mathrm{im}\varphi$ habitado; basta utilizar o one-test. Sejam $u, v \in A$. Preciso $(\varphi\, u)(\varphi\, v)^{-1} \in \mathrm{im}\varphi$. Calculamos: $(\varphi\, u)(\varphi\, v)^{-1} = (\varphi\, u)(\varphi\,(v^{-1})) = \varphi\,(uv^{-1}) \in \mathrm{im}\varphi$.

D4. Sejam $u \approx v$. Logo seja g tal que $u = gvg^{-1}$. Logo $\varphi\, u = \varphi\,(gvg^{-1}) = (\varphi\, g)(\varphi\, v)(\varphi\,(g^{-1})) = (\varphi\, g)(\varphi\, v)(\varphi\, g)^{-1}$.

D2. Obviamente $\ker \varphi \subseteq A$.
Parte $\ker \varphi \leq A$.
Como $\varphi\, e_A = e_A$, logo $\ker \varphi$ habitado e assim basta utilizar o one-test: Sejam $k, \ell \in \ker \varphi$. (Preciso $k\ell^{-1} \in \ker \varphi$.) Temos: $\varphi\,(k\ell^{-1}) = (\varphi\, k)(\varphi\, \ell^{-1}) = e_B(\varphi\,(\ell^{-1})) = (\varphi\,(\ell^{-1})) = (\varphi\, \ell)^{-1} = {e_B}^{-1} = e_B$.
Parte $\ker \varphi \trianglelefteq A$.
Sejam $k \in \ker \varphi$, $a \in A$. Preciso $aka^{-1} \in \ker \varphi$.
$\varphi\,(aka^{-1}) = (\varphi\, a)(\varphi\, k)(\varphi\,(a^{-1}) = (\varphi\, a)e_B(\varphi\,(a^{-1})) = (\varphi\, a)(\varphi\,(a^{-1}) = (\varphi\, a)(\varphi\, a)^{-1} = e_B$.

(21) **S** *Escolha exatamente uma das* **S2**, **S3**, **S4**.

(3) **S0.** Defina o que significa submonóide dum monóide.

Definição.

Sejam $\mathscr{M} = (M\ ; \cdot_M, 1_M)$ um monóide e $S \subseteq M$.
Chamamos o S de *submonóide de* $\mathscr{M}$ sse S é fechado pela operação e pela identidade, i.e.:
(i) para quaisquer $s, t \in S$, $s \cdot_M t \in S$; (ii) $1_M \in S$.

(6) **S1.** Sejam $\mathscr{M}$ monóide e $A \subseteq \mathscr{M}$.
Defina o submonóide gerado por $A \subseteq M$ em duas maneiras: uma top-down e uma bottom-up.

Definição de $\langle A \rangle^{\triangledown}$ (top-down).

$$\langle A \rangle^{\triangledown} \overset{\text{def}}{=} \bigcap \{\, H \leq M \mid H \supseteq A \,\}$$

Definição de $\langle A \rangle_{\vartriangle}$ (bottom-up).

$$A_0 \overset{\text{def}}{=} A \qquad \langle A \rangle_{\vartriangle} \overset{\text{def}}{=} \bigcup\nolimits_n A_n$$
$$A_{n+1} \overset{\text{def}}{=} A_n \cup \{\, uv \mid u, v \in A_n \,\} \cup \{1_M\}$$

(8 | 10 | 12) **S2.** $\langle A \rangle^{\triangledown} \leq M$. **S3.** $\langle A \rangle_{\vartriangle} \leq M$. **S4.** $\langle A \rangle_{\vartriangle} = \langle A \rangle^{\triangledown}$.

Demonstração de ______ .

S2. Como $\langle A \rangle^{\triangledown}$ foi definido como interseção de submonóides de M, obtemos $\langle A \rangle^{\triangledown} \leq M$ como corolário imediato de (inter-submonoid).

S3. Parte (id)-fechado.
Temos $1_M \in A_1 = A_0 \cup \{\dots\} \cup \{1_M\}$.
Parte (op)-fechado.
Sejam $x, y \in \langle A \rangle_{\vartriangle}$.
Logo sejam $n_x, n_y \in \mathbb{N}$ tais que $x \in A_{n_x}$ e $y \in A_{n_y}$.
Seja $n = \max\{n_x, n_y\}$.
Pelo (bu-monotone) temos $A_{n_x}, A_{n_y} \subseteq A_n$.
Logo $x, y \in A_n$.
Logo $xy \in A_{n+1} = \mathscr{A}_n \cup \{\, uv \mid u, v \in A_n \,\} \cup 1_M$.

S4. Parte $\langle A \rangle_{\vartriangle} \subseteq \langle A \rangle^{\triangledown}$. Seja $x \in \langle A \rangle_{\vartriangle}$.
Logo seja n_x tal que $x \in A_{n_x} \subseteq \langle A \rangle^{\triangledown}$, pelo (td-contains-bu-stages), com $n := n_x$ e $A' := \langle A \rangle^{\triangledown}$, já que $A \subseteq \langle A \rangle^{\triangledown}$ (interseção de superconjuntos de A) e $\langle A \rangle^{\triangledown} \leq M$ (pela **S3**).
Parte $\langle A \rangle_{\vartriangle} \supseteq \langle A \rangle^{\triangledown}$. Seja $x \in \langle A \rangle^{\triangledown}$.
Ou seja, x pertence a todos os submonoides de M que contêm o A. Logo basta verificar que $\langle A \rangle_{\vartriangle}$ é um submonoide de M que contem o A.
Pela **S3**, é um submonoide sim.
Para verificar que $\langle A \rangle_{\vartriangle} \supseteq A$, seja $a \in A = A_0$. Logo $a \in \bigcup_n A_n = \langle A \rangle_{\vartriangle}$.

Só isso mesmo.

(inter-submonoid).
A interseção de submonóides de um monóide M, é submonoide de M.

Demonstração.
Seja $\mathcal{S}$ coleção de submonóides de M.
Parte $\bigcap \mathcal{S}$ é (op)-fechado:
Sejam $u, v \in \bigcap \mathcal{S}$.
Seja $S \in \mathcal{S}$.
Logo $u \in S$ e $v \in S$, pela escolha dos u, v.
Logo $uv \in S$, pois S é $(\cdot_M)$-fechado como submonóide de M.
Parte $\cap \mathcal{S}$ é (id)-fechado:
Seja $S \in \mathcal{S}$.
Logo $1 \in S$, pois S é 1_M-fechado como submonóide de M.

(bu-monotone).
$(\forall i \in \mathbb{N})\,(\forall n \in \mathbb{N})\,[\,A_i \subseteq A_{i+n}\,]$.

Demonstração.
Seja $i \in \mathbb{N}$.
Por indução.
Base: $(A_i \subseteq A_{i+0})$.
Imediato.
Passo indutivo.
Seja k tal que $A_i \subseteq A_{i+k}$.
Seja $x \in A_i$.
Logo $x \in A_{i+k}$ (pela H.I.).
Logo $x \in A_{i+k} \cup \{\, uv \mid u, v \in A_{i+k} \,\} \cup \{1_M\} = A_{i+k+1}$.

(td-contains-bu-stages).
$(\forall n \in \mathbb{N})\,(\forall A \subseteq A' \leq M)\,[\,A_n \subseteq A'\,]$.

Demonstração.
Por induçaõ.
Base.
Seja A' tal que $A \subseteq A' \leq M$.
Imediato pois $A_0 = A \subseteq A'$.
Passo Indutivo. Seja k tal que $(\forall A \subseteq A' \leq M)\,[\,A_k \subseteq A'\,]$.
Seja A' tal que $A \subseteq A' \leq M$.
Preciso mostrar que $A_{k+1} \subseteq A'$.
Seja $x \in A_{k+1}$, ou seja, $x \in A_k \cup \{\, uv \mid u, v \in A_k \,\} \cup \{1_M\}$.
Logo separamos em casos:
Caso $x \in A_k$.
Pela H.I. temos $x \in A'$.
Caso $x \in \{\, uv \mid u, v \in A_k \,\}$.
Sejam $u, v \in A_k$ tais que $x = uv$.
Logo, $u, v \in A'$ (pela H.I.), e logo $x = uv \in A'$ (pois A' é $(\cdot_M)$-fechado).
Caso $x \in \{1_M\}$.
Logo $x = 1_M \in A'$ pois A' é 1_M-fechado.