FMC2, 2018.2
(Turma N12 do Thanos)

Prova 2.1
(points: 100; bonus: $0^\flat$; time: 64')

Nome: Θάνος **Gabarito**

16/11/2018

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

XII. **Responda em até 2 dos A, B, C, D, E.**[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 $\mathcal{G} = \langle G\,;\,*, {}^{-1}, e\rangle$ é um *grupo* sse:

$$(\forall a, b \in G)\,[\,a * b \in G\,] \tag{G0}$$
$$(\forall a, b, c \in G)\,[\,a * (b * c) = (a * b) * c\,] \tag{G1}$$
$$(\forall a \in G)\,[\,e * a = a = a * e\,] \tag{G2}$$
$$(\forall a \in G)\,\left[\,a^{-1} * a = e = a * a^{-1}\,\right] \tag{G3}$$

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*.

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 $a = gbg^{-1}$. Escrevemos $a \approx b$.

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

(iii) $\varphi(e_A) = e_B$.

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**

Prove “from scratch” (usando apenas os (G0)–(G3)) que o inverso de inverso dum membro de grupo é o próprio membro.

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

PROVA.

Seja a membro dum grupo $\langle G\ ;\ *, {}^{-1}, e\rangle$. Quero demonstrar que

$$\left(a^{-1}\right)^{-1} = a.$$

DEMONSTRAÇÃO DIRETA (SEM LÉMMATA).

$$\begin{array}{lrl}
\text{Temos} & \left(a^{-1}\right)^{-1}a^{-1} = e. & \text{(pela (G3))} \\
\text{Logo} & \left(\left(a^{-1}\right)^{-1}a^{-1}\right)a = ea. & \text{(operando } (\cdot\ a)\text{)} \\
\text{Logo} & \left(\left(a^{-1}\right)^{-1}a^{-1}\right)a = a. & \text{(pela (G2))} \\
\text{Logo} & \left(a^{-1}\right)^{-1}\left(a^{-1}a\right) = a. & \text{(pela (G1))} \\
\text{Logo} & \left(a^{-1}\right)^{-1}e = a. & \text{(pela (G3))} \\
\text{Logo} & \left(a^{-1}\right)^{-1} = a. & \text{(pela (G2))}
\end{array}$$

Ou, numa linha só:

$$a \overset{\text{G2}}{=} ae \overset{\text{G3}}{=} a\left(a^{-1}\left(a^{-1}\right)^{-1}\right) \overset{\text{G1}}{=} \left(aa^{-1}\right)\left(a^{-1}\right)^{-1} \overset{\text{G3}}{=} e\left(a^{-1}\right)^{-1} \overset{\text{G2}}{=} \left(a^{-1}\right)^{-1}.$$

DEMONSTRAÇÃO INDIRETA.

Eu vou demonstrar que o inverso de a^{-1} é o a. Primeiramente eu vou provar que o a satisfaz a equação

$$a^{-1}\boxed{} = e. \qquad (\heartsuit)$$

Realmente, $a^{-1}a = e$ (pela (G3)). Agora basta provar que qualquer equação da forma

$$A\boxed{\mathrm{X}} = B$$

tem resolução única, pois já sabemos (pela (G3)) que $\left(a^{-1}\right)^{-1}$ satisfaz a equação ($\heartsuit$) acima.

LEMMA (Resolução única). Sejam $A, B, X, Y \in G$ tais que $AX = B$ e $AY = B$. Logo $AX = AY$. Logo $A^{-1}AX = A^{-1}AY$. Pela (G3) agora temos $eX = eY$, e logo pela (G2) $X = Y$.

(30) **B**

Seja G grupo e $(H_\alpha)_{\alpha\in A}$ uma família de subgrupos de G. Prove que

$$\bigcap_{\alpha\in A} H_\alpha \leq G.$$

PROVA.

Primeiramente observe que $\bigcap_{\alpha\in A} H_\alpha \neq \emptyset$, pois $e \in H_\alpha$ para todo $\alpha \in A$ (pois todos os H_α são subgrupos), e logo e pertence à intersecção.

Tome $x, y \in \bigcap_{\alpha\in A} H_\alpha$. Preciso mostrar que $xy^{-1} \in \bigcap_{\alpha\in A} H_\alpha$ pois pelo critério "single-shot" concluimos o que queremos provar. Seja $a \in A$. Logo $x \in H_a$ e $y \in H_a$ pois ambos pertencem a todos os H_α's. Como $y \in H_a \leq G$, logo $y^{-1} \in H_a$. Como H_a é fechado pela operação, $xy^{-1} \in H_a$ que foi o que bastava provar.

(30) **C**

Sejam G e H grupos, $\varphi : G \to H$ homomorfismo, e $B \leq H$. Prove que $\varphi^{-1}[\,B\,] \leq G$.

PROVA.

Como φ homo, ela respeita a identidade e logo $\varphi(e_G) = e_H$. Como $B \leq H$, $e_H \in B$ e logo $\varphi(e_G) \in B$, ou seja, $e_G \in \varphi^{-1}[\,B\,]$ e logo a preimagem é não-vazia.

Tome $x, y \in \varphi^{-1}[\,B\,]$. Basta provar que $xy^{-1} \in \varphi^{-1}[\,B\,]$ (graças ao critério "single-shot"). Ou seja, basta provar que $\varphi(xy^{-1}) \in B$. Calculamos:

$$\begin{aligned}
\varphi(xy^{-1}) &= (\varphi x)(\varphi(y^{-1})) && (\varphi \text{ homo: resp. op.})\\
&= (\varphi x)(\varphi y)^{-1} && (\varphi \text{ homo: resp. inv.})
\end{aligned}$$

Basta provar que $(\varphi x)(\varphi y)^{-1} \in B$.

Observe que $\varphi x \in B$ (pela escolha de x) e pela escolha de y temos $\varphi y \in B$ também, e logo seu inverso $(\varphi y)^{-1} \in B$ (pois B é fechado pelos inversos). Como B é fechado pela operação também, temos $(\varphi x)(\varphi y)^{-1} \in B$.

(34) **D**

Seja G grupo e $N \leq G$. Prove que:

$$N \trianglelefteq G \iff {}_N\!\equiv \,=\, \equiv_N$$

Onde ${}_N\!\equiv$ e $\equiv_N$ são as relações de congruência módulo-esquerdo e módulo-direito N.
PROVA.

($\Rightarrow$): Sejam $x, y \in G$. Quero mostrar que

$$x \;{}_N\!\equiv y \iff x \equiv_N y.$$

Suponha $x \;{}_N\!\equiv y$, ou seja $x^{-1}y \in N$, ou seja $y^{-1}x \in N$. Preciso mostrar $x \equiv_N y$, ou seja $xy^{-1} \in N$. Basta mostrar que xy^{-1} é conjugado de algum membro de N. Como $y^{-1}x \in N$ e $y \in G$, temos

$$\underbrace{y\left(y^{-1}x\right)y^{-1}}_{xy^{-1}} \in N$$

pois N é fechado pelos conjugados. A outra direção é similar.

($\Leftarrow$): Sejam $n \in N$ e $g \in G$. Preciso mostrar que $gng^{-1} \in N$. Mas

$$\begin{aligned}
(gn)g^{-1} \notin N &\implies (gn)^{-1}g \notin N && \text{(hipótese)}\\
&\implies n^{-1}g^{-1}g \notin N && \text{(inv. de inv.)}\\
&\implies n^{-1}e \notin N\\
&\implies n^{-1} \notin N\\
&\implies n \notin N && (N \leq G)
\end{aligned}$$

que contradiz a escolha de n, e logo $gng^{-1} \in N$.

(42) **E**

Sejam G grupo e $N \trianglelefteq G$. Logo existem grupo G' e homomorfismo $\varphi : G \to G'$ tal que N é o kernel de φ.

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.

(24) **L**

Definição. O conjunto estruturado $\mathcal{L} = \langle L\ ;\ \vee, \wedge\rangle$ onde *join* ($\vee$) e *meet* ($\wedge$) são operações binárias é um *reticulado* sse:

(`JA`)	$a \vee (b \vee c) = (a \vee b) \vee c$	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$	(`MA`)
(`JC`)	$a \vee b = b \vee a$	$a \wedge b = b \wedge a$	(`MC`)
(`JP`)	$a \vee a = a$	$a \wedge a = a$	(`MP`)
(`LJ`)	$a \vee (a \wedge b) = a$	$a \wedge (a \vee b) = a$	(`LM`)

Um conjunto estruturado $\mathcal{B} = \langle B\ ;\ \vee, \wedge, \bot, \top\rangle$ (onde $\bot, \top$ são constantes) que além das leis acima satisfaz também:

(`JI`)	$a \vee \bot = a$	$a \wedge \top = a$	(`MI`)

é chamado *reticulado limitado.*

(12) **L1.** **Teorema.** Seja $\mathcal{L} = \langle L\ ;\ \vee, \wedge\rangle$ um reticulado. Então para todo $a, b \in L$, temos

$$a \vee b = b \iff a \wedge b = a.$$

Prova.

Sejam $a, b \in L$. Suponha que $a \vee b = b$. Calculamos:

$$\begin{aligned} a \wedge b &= a \wedge (a \vee b) && \text{(pela hipótese } b = a \vee b) \\ &= a. && \text{(pela (LM))} \end{aligned}$$

Para a outra direção, suponha que $a \wedge b = a$. Calculamos:

$$\begin{aligned} a \vee b &= (a \wedge b) \vee b && \text{(pela hipótese } a = a \wedge b) \\ &= b \vee (a \wedge b) && \text{(pela (JC))} \\ &= b \vee (b \wedge a) && \text{(pela (MC))} \\ &= b. && \text{(pela (LJ))} \end{aligned}$$

(12) **L2.** Como definarias (formalmente, com texto completo!) a afirmação que dois reticulados limitados são isómorfos?

Definição.

Sejam $\langle L\ ;\ \vee, \wedge, \bot, \top\rangle$ e $\langle L'\ ;\ \vee', \wedge', \bot', \top'\rangle$ reticulados limitados. Chamamos os L, L' isómorfos sse existe isomorfismo de L para L', ou seja, função bijetora $\varphi : L \to L'$ tal que:

$$\begin{aligned} \text{para todo } x, y \in L, \quad & \varphi(x \vee y) = \varphi x \vee' \varphi y \\ \text{para todo } x, y \in L, \quad & \varphi(x \wedge y) = \varphi x \wedge' \varphi y \\ & \varphi(\bot) = \bot' \\ & \varphi(\top) = \top'. \end{aligned}$$

Só isso mesmo.