

16 Seja  $G$  um grupo e seja  $g \in G$ . Prove que as seguintes funções são bijetivas:

(a)  $\lambda_g: G \rightarrow G$

$$x \rightarrow gx$$

Sobrejetiva, para cada elemento  $y \in G$  deve existir  $x \in G$  tal que  $\lambda_g(x) = gx = y$ . De fato, dado  $y \in G$ ,  $\exists g^{-1} \in G$  tal que  $g^{-1}g = e$ . Daí,  $\forall y \in G$ ,  $\exists x = g^{-1}y \in G$  tal que  $gx = gg^{-1}y = y \Rightarrow \lambda_g = gx = y$ .

Injetora, temos que provar que  $\forall x_1, x_2 \in G$  tal que  $x_1 \neq x_2$  temos  $\lambda_g(x_1) \neq \lambda_g(x_2)$ . Suponha que temos  $\lambda_g(x_1) = \lambda_g(x_2) \Rightarrow gx_1 = gx_2 \Rightarrow \exists g^{-1} \in G$  t.q.  $g^{-1}gx_1 = g^{-1}gx_2 \Rightarrow ex_1 = ex_2 \Rightarrow x_1 = x_2$ .

(b)  $\lambda_g: G \rightarrow G$

$$x \rightarrow xg$$

Análogo ao item (a) trocando o lado da operação.

(17) Seja  $G$  um grupo gerado por 2 elementos  $x, y$ .  
Se a única informação que temos é que  $x^3 \cdot y^2 = (xy)^2 = e$ , qual é a ordem de  $G$ ?

Temos que  $y^3 = x^2 = e$ , logo,  $\text{ord}(x) = 3$  e  $\text{ord}(y) = 2$  (um múltiplo comum de 2 e 3 é 6). Daí, a ordem de  $G$  é 6.

18) Se  $a^2 = e$   $\forall a \in G$ , mostre que  $G$  é abeliano.

Sfn  $a, b \in G$ , temos que,  $\forall ab \in G$ , logo,

$$\cancel{(ab)^2} = abab$$

$(ab)^2 = e$ , de forma anloga  $ba \in G$ , logo,

$(ab)^2 = (ba)^2 = e$ . Pelo problema 5) é abeliano.

19) Em  $GL_2(\mathbb{Z})$ , consider os elementos

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ e } b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

Mostre que  $a^4 = 1$  e  $b^3 = 1$ , mas que ab tem ordem infinita.

$$a^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}; \quad a^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; \quad a^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$b^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}; \quad b^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Mas ollando para ab

$$ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}; \quad (ab)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}; \quad (ab)^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$$

Por indução, vamos provar que

$$(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \quad \forall n \in \mathbb{N}$$

Para  $n=1$  temos achado que  $ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ . Suponha que vale que  $(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ . Verificamos agora  $n+1$

$$\begin{aligned} (ab)^{n+1} &= (ab)^n (ab) \\ &= \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix} \neq e \quad \forall n \in \mathbb{N}. \end{aligned}$$

(20) Suponha que os únicos subgrupos de  $G$  sejam  $\{e\}$  e  $G$ . Prouve que  $G$  é um grupo finito de ordem píma.

Seja  $x$  um elemento não trivial de  $G$ . Note que,  $\langle x \rangle = G$  daí não pode ser infinito (caso contrário  $G$  teria um isomorfismo com  $\mathbb{Z}$ ) e sabesse que tales os grupos têm forma  $n\mathbb{Z}$  (portanto, um número infinito de subgrupos). Para provar que a cardinalidade de píma. Suponha que seja  $n=nr$  para alguns inteiros  $\geq 2$ .

$$x^n = x^r x^r = e$$

Então, ou  $x^r = e$  ou  $x^r \neq e$  absurdio.

(21) O centro de um grupo  $G$  é definido por

$$Z(G) = \{z \in G : zx = xz \ \forall x \in G\}$$

Prouve que  $Z(G)$  é um subgrupo de  $G$ .

Note que  $e \in Z(G)$ , para  $eg = ge$ .

Dados  $x, y \in Z(G)$  e  $g \in G$ , temos que

$$\begin{aligned} g(xy) &= (gx)y \\ &= (xg)y \\ &= x(gy) \\ &= x(yg) \\ &= (xy)g \end{aligned}$$

Logo,  $x, y \in Z(G)$ . Dado  $x \in Z(G)$  e  $g \in G$  temos que

$$\begin{aligned} x^{-1}g &= x^{-1}(gx)x^{-1} \\ &= x^{-1}xgx^{-1} \\ &= gx^{-1} \end{aligned}$$

Logo,  $x^{-1} \in Z(G)$ .

22 Determine as ordens de

(a)  $\begin{pmatrix} \cos \cancel{2\pi} d & \operatorname{sen} d \\ \operatorname{sen} 2d & -\cos d \end{pmatrix}$  e  $\begin{pmatrix} \cos d & -\operatorname{sen} d \\ \operatorname{sen} d & \cos d \end{pmatrix}$  em  $GL_2(\mathbb{R})$   
 $d = \frac{2\pi}{12}$

a)

Seja  $A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ;  $B^2 = \begin{pmatrix} \cos 2d & -\operatorname{sen} 2d \\ \operatorname{sen} 2d & \cos 2d \end{pmatrix}$

$$B^3 = \begin{pmatrix} \cos 3d & -\operatorname{sen} 3d \\ \operatorname{sen} 3d & \cos 3d \end{pmatrix}$$

:

$$B^{17} = \begin{pmatrix} \cos 17d & -\operatorname{sen} 17d \\ \operatorname{sen} 17d & \cos 17d \end{pmatrix} = \begin{pmatrix} \cos 2\pi & -\operatorname{sen} 2\pi \\ \operatorname{sen} 2\pi & \cos 2\pi \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Logo,  $B^{17} = A^2 = e$  e a ordem do grupo é  $2 \cdot 17 = 34$ .

(23) Seja  $G$  um grupo. Se  $g \in G$  é um elemento de ordem ímpar, mostre que  $g$  e  $g^2$  têm mesma ordem.

Primeiro, vamos mostrar que  $\text{ord}(g^2)$  é finita.

Seja  $g \in G$ , para que  $g^2$  tenha ordem infinita

temos tal que  $(g^2)^m = g^{2m} = e$ . Se dividirmos  $m = \frac{(n+1)}{2}$ , onde  $n = \text{ord}(g)$ ;  $g^{2m} = g^{n+1} = g^n \cdot g = e \cdot g = g$ . Então temos que a ordem de  $g^2$  é finita.

Segundo, vamos provar que  $\text{ord}(g^2) = \text{ord}(g)$ .

Suponha por absurdo que  $\text{ord}(g^2) > m > n = \text{ord}(g)$ .

Então  $g^{2m} = g^{q(n+1)}$ ; com  $q, n \in \mathbb{N}$  e  $n < q$

$$= (g^n)^q \cdot g^2$$

$$= (e)^q \cdot g^2$$

$$= g^2$$

Mas, daí  $g^2 = e$  absurdo pois  $n < 2m$ .

Suponha agora que seja  $\text{ord}(g^2) = m < n = \text{ord}(g)$

Então  $\exists q \in \mathbb{N}$  t.q.  $2m = qn$ , como  $n$  é ímpar  $2 \nmid q$  refa a  $\mathbb{N}$  t.q.  $q = 2a$ . ou seja

$$2m = 2a \cdot n$$

$$\Rightarrow m = a \cdot n$$

Como  $m < n$ ,  $|a| < 1$ , mas  $a \in \mathbb{N}$  logo, absurdo.

(24) Prove: todo subgrupo finitamente gerado de  $(\mathbb{Q}, +)$  é cíclico.

Solução: Seja por exemplo, a esse subgrupo  $S$ . Suponha por absurdo que  $S$  não cíclico, entao, mas  $a+a \in S$ ,  $a+a+a \in S, \dots, a+na \in S, \forall n \in \mathbb{N}$ . Portanto  $S$  tem infinitos elementos absurdos.

(26) Se um grupo  $G$  tem ordem ímpar, mostre que todo elemento  $g \in G$  é um quadrado perfeito, i.e.,  $g = h^2$  para algum  $h \in G$ .

Lema: Se  $|G| < \infty$  e  $g \in G$ , então

$$g^{|G|} = e$$

Para: Seja,  $H = \langle g \rangle = \{e, g, \dots, g^{m-1}\}$ , como  $H \leq G$ , por Lagrange  $|G| = k |H| = km$ , com  $k \in \mathbb{N}$ . dai

$$\Rightarrow (g^m)^k = e^k$$

$$\Rightarrow g^{mk} = e$$

$$\Rightarrow g^{|G|} = e$$

Voltando ao problema, seja  $k$  t.q.  $|G| = 2k+1$ , então pelo lema,  $\forall g \in G$

$$\nexists g^{2k+1} = e$$

$$\Rightarrow g^{2k+2} = g$$

$$\Rightarrow g^{2(k+1)} = g$$

$$\Rightarrow (g^{k+1})^2 = g \in G$$

■

28

Mostre que

(a) não existe  $x \in \mathbb{Z}$  t.g.  ~~$43|x^2+1$~~   $43|x^2+1$

Suponha por absurdo que  $\exists x \in \mathbb{Z}$ , tal que

$$\begin{aligned}x^2 &\equiv -1 \pmod{43} \\ \Rightarrow (x^2)^{21} &\equiv (-1)^{21} \equiv -1 \pmod{43} \\ \Rightarrow x^{42} &\equiv -1 \pmod{43}\end{aligned}$$

$\cancel{\Rightarrow}$

Mas, por Fermat,  $x^{42} \equiv 1 \pmod{43}$   $\blacksquare$

(b) Se  $43|x^2+y^2$  então  $43|x = 43|y$

$x^2+y^2 \equiv 0 \pmod{43}$ . Se  $y \neq 0$ ,  $\exists y' \not\equiv \bar{y}$  como  
43 é primo:

$x^2 y'^2 + 1 \equiv 0 \pmod{43}$ , absurdo pelo item (a).

Logo,  $y \equiv 0 \Rightarrow x \equiv 0 \pmod{43}$ .

(30) Seja  $G$  um grupo. Mostre que

(b) o mapa  $\phi: G \rightarrow G$  dado por  $\phi(g) = g^2$  é um morfismo de grupos se, e só se,  $G$  for abeliano.

Para ser um morfismo devemos ter:  $\phi(ab) = \phi(a)\phi(b)$ , ou seja,  $(ab)^2 = a^2 \cdot b^2$ .

Pela questão (5) temos que se  $\phi$  é morfismo, então  $G$  é abeliano. Então vamos provar a volta. De fato, se  $G$  é abeliano, vale que

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

31) Quais dos seguintes mapas  $f: G \rightarrow H$  não são isomorfismos de grupos? Dentro destes, quais não são isomorfismos? Para cada um dos isomorfismos, descreva o seu kernel e imagem.

(C)  $G = (\mathbb{R}, +)$ ,  $H = (\mathbb{C}^*, \cdot)$  e  $f(x) = \cos x + i \sin(x)$

Temos que,  $f(x) = e^{ix}$ ,

$$f(x+y) = e^{i(x+y)} = e^{ix} \cdot e^{iy} = f(x) \cdot f(y) \quad \checkmark$$

$$\begin{aligned} \text{Ker } f &= \{x \in \mathbb{R} \mid f(x) = 1\} \\ &= \{x \in \mathbb{R} \mid e^{ix} = 1\} \\ &= \{2k\pi \mid k \in \mathbb{Z}\} \end{aligned}$$

$$\text{Im } f = S_1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

(C)  $G = H = S_3$  (grupos simétricos e  $f(x) = x^2$ .

Não é morfismo, pois  $S_3$  não é abeliano.

32) Seja  $G$  um grupo abeliano finito e seja  $k \in \mathbb{N}$  com  $\text{mdc}(k, |G|) = 1$ . Prove que  $g \mapsto g^k$  é um automorfismo de  $G$ .

Pelo teorema de Lagrange

$$g^{|G|} = e \text{ para } |G| < \infty,$$

Como  $\text{mdc}(k, |G|) = 1 \Rightarrow g^k \neq e, g \neq e$ . Por Barta prova injetividade para que  $f$  seja isomórfica.

Suponha que  ~~$g^k = m^k$~~  que  $g^k = m^k, g \neq m$ .

$$g^k(m^k)^{-1} = e$$

$$\Rightarrow g^k m^{|G|-k} = e$$

$$\Rightarrow g^k m^{-k} = e$$

$$\Rightarrow g \cdot g \dots g^{m_1} \dots m_1^{-1} = e$$

$$\text{obtemos} \Rightarrow (g \cdot m_1^{-1})^k = e$$

$$\Rightarrow g \cdot m_1^{-1} \neq e \text{ para } g \neq m \text{ e } g^k \neq e, g \neq e.$$

$\Rightarrow f$  é isomorfismo.

(34) Seja  $\varphi: G \rightarrow H$  um morfismo de grupos. Mostre:

(a) se  $\varphi$  é surjetora e  $N \trianglelefteq G$ , prove que  $\varphi(N) \trianglelefteq H$ .

$$\varphi: G \rightarrow H \text{ e } N \trianglelefteq G \Leftrightarrow gng^{-1} \in N$$

Como  $\varphi$  é surjetora,  $\forall h \in H, \exists g \text{ t.g. } \varphi(g) = h$ .

$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g^{-1}) = h\varphi(n)h^{-1}$$

Logo,  $\varphi(N) \trianglelefteq H$ .

(b) Se  $G$  é simples então  $\varphi$  é injetor.

Se  $G$  é simples  $N = G$  ou  $N = \{e\}$ , dai  $\varphi(N) = \varphi(G)$  ou  $\varphi(N) = e$ .

(38) Mostre que se  $G$  é um grupo contendo dois subgrupos normais de ordens 3 e 5 então  $G$  possui um elemento de ordem 15.

Seja  $N = \{e, a, a^2\}$

$M = \{e, b, b^2, b^3, b^4\}$ .

Pelo (37),  $\forall i, j$ , (nas nossas condições).  $a^i b^j = b^j a^i$ .  
Dai  $G$  deve possuir um elemento de ordem 15.