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

(a) $\lambda_g : G \to G$
$x \to gx$

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

$$\lambda_g(x_1) = \lambda_g(x_2) \Rightarrow gx_1 = gx_2$$
$$\Rightarrow \exists g^{-1} \in G \text{ t.q. } g^{-1}gx_1 = g^{-1}gx_2$$
$$\Rightarrow ex_1 = ex_2$$
$$\Rightarrow x_1 = x_2.$$

(b) $\lambda_g : G \to G$
$x \to xg$

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 $x^3 = y^2 = (xy)^2 = e$, qual é a ordem de G?

Temos que $y^3 = x^2 = e$, logo, $ord(x) = 3$ e $ord(x) = 2$ 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.

Seja $a, b \in G$, temos que, $\exists\, ab \in G$, logo,

~~$(ab)^2 = abab$~~

$(ab)^2 = e$, de forma análoga $ba \in G$, logo,
$(ab)^2 = (ba)^2 = e$. Pelo problema (5) é abeliano.

(19) Em $GL_2(\mathbb{Z})$, considere 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.

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

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

Mas olhando para ab

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

Por indução, vamos provar que

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

Para $n=1$ temos acima 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. Prove que G é um grupo finito de ordem prima.

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 sabemos que todos os grupos tem forma $n\mathbb{Z}$ (portanto, um número infinito de subconjuntos. Para provar que a cardinalidade primo. Suponha que seja $n = ?$ para alguns inteiros ≥ 2.

$$x^n = x^? x^? = e$$

Ou seja, ou $x^? = e$ ou $x^? = e$ absurdo.

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

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

Prove que $Z(G)$ é um subgrupo de G}.

Note que $e \in Z(G)$, pois $eg = ge \ \forall g$.
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) $\begin{pmatrix} \cos \alpha & \operatorname{sen} \alpha \\ \operatorname{sen} \alpha & -\cos \alpha \end{pmatrix}$ e $\begin{pmatrix} \cos \alpha & -\operatorname{sen} \alpha \\ \operatorname{sen} \alpha & \cos \alpha \end{pmatrix}$ em $GL_2(\mathbb{R})$ $\alpha = \frac{2\pi}{17}$

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

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

$\vdots$

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

Logo, $B^{17} = A^2 = e$ e a ordem do grupo é $2.17 = 34$.

(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 $ord(g^2)$ é finita:
Seja $g \in G$, para que g^2 tenha ordem infinita $\exists m$ tal que $(g^2)^m = g^{2m} = e$. Se escolhermos $m = (n+1)/2$, onde $n = ord(g)$; $g^{2m} = g^{n+1} = g^n g = e \cdot g = g$. Então temos que a ordem de g^2 is finite.

Second, vamos provar que $ord(g^2) = ord(g)$.
• Suponha por absurdo que $ord(g^2) = m > n = ord(g)$.
Então $g^{2m} = g^{qn+r}$, com $q, r \in \mathbb{N}$ e $r < n$

$$
\begin{aligned}
&= (g^n)^q \cdot g^r \\
&= (e)^q \cdot g^r \\
&= g^r
\end{aligned}
$$

Mas, daí $g^r = e$ absurdo pois $r < 2m$.
• Suponha agora que seja $ord(g^2) = m < n = ord(g)$
Então $\exists q \in \mathbb{N}$ t.q. $2m = qn$, como n é ímpar $2 | q$ seja $a \in \mathbb{N}$ t.q. $q = 2a$, ou seja

$$2m = 2an$$
$$\Rightarrow m = an$$

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

CamScanner

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

Solução: Seja por exemplo, a nesse subgrupo S. Suponha por absurdo que S não cíclico, ~~então~~, mas $a+a \in S$, $a+a+a \in S, \dots, a+na \in S$, $\forall n \in \mathbb{N}$. Porém daí S tem infinitos elementos absurdo.

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

Prova: Seja, $H = \langle g \rangle = \{e, g, \dots, g^{m-1}\}$, como $H \leq G$, por Lagrange $|G| = k|H| = km$, com $k \in \mathbb{N}$. daí
$$g^m = e$$
$$\Rightarrow (g^m)^k = e^k$$
$$\Rightarrow g^{mk} = e$$
$$\Rightarrow g^{|G|} = e \quad //$$

Voltando ao problema, seja k t.q. $|G| = 2k+1$, então pelo lema, $\forall g \in G$
$$\Rightarrow g^{2k+1} = e$$
$$\Rightarrow g^{2k+2} = g$$
$$\Rightarrow g^{2(k+1)} = g$$
$$\Rightarrow (g^{k+1})^2 = g \in G \quad \blacksquare$$

(27) Seja G um ~~ta~~ grupo com 9 elementos. Neste exercício vamos mostrar que G é abeliano.

(a) Se G possui um elemento de ordem 9, então G é abeliano.

(b) Caso contrário, todo elemento diferente de e tem ordem 3 e existe um subgrupo $H = \{e, h, h^2\}$ cíclico de ordem 3. Mostre que $G = H \cup gH \cup g^2H$ para algum $g \in G$.

(c) Mostre que $g^{-1}hg \neq h^2$, logo $hg \neq gh^2$. E também que $hg \neq g^2h$.

(d) Mostre que $hg \neq g^2h^2 = (hg)^{-1}$

(e) Conclua que a única possibilidade é $hg = gh$ e que G é portanto abeliano.

(a) Se $\text{ord}\, a = 9$, então
$$\langle a \rangle = \{e, a, a^2, \dots, a^8\} \Rightarrow G \text{ é abeliano.}$$

(b) Tome $g \in G/H$ e $g \notin H$, logo, $H = \{e, h, h^2\}$, $gH = \{g, gh, gh^2\}$ e $g^2H = \{g^2, g^2h, g^2h^2\}$, como $\text{ord}\, h = \text{ord}\, g = 3$ e $g \in G/H$, mas $g \notin H$, vale que
$$H \cap gH = H \cap g^2H = gH \cap g^2H = \emptyset$$
$$\Rightarrow H \cup gH \cup g^2H = G.$$

(c), (d), (e) Como $|G| = 9$, uma das igualdades e apenas uma deve valer para todo g:
$$\underset{(I)}{hg = gh^2}, \quad \underset{(II)}{hg = g^2h}, \quad \underset{(III)}{hg = g^2h^2} \quad \text{ou} \quad \underset{(IV)}{hg = gh}$$

(I) $hg = gh^2 \overset{\text{ord}\, h = 3}{\Longleftrightarrow} hgh = g \Leftrightarrow hgh^2gh = g^2$
$\Leftrightarrow hhggh = g^2 \Leftrightarrow h^4g^2h = g^2$
$\Leftrightarrow g^2h = hg^2 \Leftrightarrow h = ghg^2$

$\Leftrightarrow h = g^2h^2g \Leftrightarrow gh = h^2g$

$\Leftrightarrow gh = hgh^2 \Leftrightarrow gh^2 = hg$

(II) $hg = g^2h \Leftrightarrow ghg = h \Leftrightarrow ghg^2hg = h^2$

$\Leftrightarrow gg^2hgg^2hg = h^2 \Leftrightarrow h^2g = h^2$

$\Leftrightarrow g = e$ Absurdo

(III) $hg = g^2h^2 \Rightarrow$ Absurdo

Logo, sobra (IV) $\Rightarrow hg = gh \Rightarrow G$ é abeliano.

/ /

(28) Mostre que

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

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

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

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

(c) Se $43 | x^2+y^2$ então $43 | x$ e $43 | y$

. $x^2+y^2 \equiv 0 \pmod{43}$. Se $y \neq 0$, $\exists y^{-1}$ ~~$\exists$~~ $\bar{e}$ como 43 é primo:

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

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

(29) Sejam G um grupo e H, K dois subgrupos. Mostre que

(a) A interseção de duas classes laterais $xH \cap yK$ é vazia ou uma classe lateral de $H \cap K$.

Se $z \in xH \cap yK$

$xH = zH$ e $yK = zK$

Se $w \in zH \cap zK$,

$w = zh = zk$, $h \in H$, $k \in K$

$\Rightarrow h = k$, logo $h \in H \cap K$

$\Rightarrow w = zh \in zH \cap K$

A recíproca é clara ($w \in zH \cap K \Rightarrow w \in xH \cap yK$)

(30) Seja G um grupo. Mostre que

(a) o mapa $\phi: G \to G$ dado por $\phi(g) = g^{-1}$ é sempre bijetora e é um automorfismo de G se e só se G é abeliano.

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

(a) ϕ é bijetora, pois $\forall g \in G, \exists g^{-1}$ e é única.

ϕ é automorfismo $\iff$ ϕ é um morfismo bijetor

$$\iff (ab)^{-1} = a^{-1}b^{-1}$$
$$\iff b^{-1}a^{-1} = a^{-1}b^{-1}$$
$$\iff ab = ba, \forall a, b \in G$$
$$\iff G \text{ é abeliano}$$

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

Pela questão (5) temos que se ϕ é morfismo, então G é abeliano. Daí vamos provar a volta. De fato se G é abeliano vale que

$$abab = aabb$$
$$\Rightarrow (ab)^2 = a^2b^2$$
$$\Rightarrow \phi(ab) = \phi(a).\phi(b)$$

31) Quais dos seguintes mapas $f: G \to H$ são morfismos de grupos? Dentre estes, quais são isomorfismos? Para cada um dos isomorfismos, descreva o seu kernel e imagem.

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

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

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

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

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

e) $G = H = S_3$ (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 $mdc(k, |G|) = 1$. Prove que $g \mapsto g^k$ é um automorfismo de G.

Pelo teorema de Lagrange

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

Como $mdc(k, |G|) = 1 \Rightarrow g^k \neq e, g \neq e$. ~~Pa~~ Basta para injetividade para que f seja isomorfa.

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

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

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

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

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

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

$$\Rightarrow g m^{-1} \neq e \quad \text{pois } g \neq m \text{ e } g^k \neq e, g \neq e.$$

$\Rightarrow f$ é isomorfismo.

(34) Seja $\varphi: G \to H$ um morfismo de grupos. Mostre:
(a) se φ é sobrejetora e $N \trianglelefteq G$, prove que $\varphi(N) \trianglelefteq H$.

$\varphi: G \to H$ e $N \trianglelefteq G \iff gng^{-1} \in N$

Como φ é sobrejetora $\forall h \in H, \exists g$ t.q. $\varphi(g) = h$

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

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

(b) Se G é simples então φ é injetora.
Se G é simples $N = G$ ou $N = \{e\}$, daí $\varphi(N) = \varphi(G)$ ou
$\varphi(N) = e$

(37) Sejam M e N subgrupos normais de G com $M \cap N = \{e\}$. Prove que $mn = nm$ para quaisquer $m \in M$ e $n \in N$.

$M \trianglelefteq G \rightarrow \forall g \in G \quad gM = Mg \quad gm = mg$
$N \trianglelefteq G \rightarrow \forall g \in G \quad gN = Ng \quad gn = ng$

Tomando $m \in M$ dado $M \cap N = \{e\}$, basta escolher qualquer elemento de G que pertence a N, assim, temos que $mn = nm$ $\forall m \in M$ e $n \in N$.

~~$mn = nm$, mn~~

(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). $a^i b^j = b^j a^i$.
Daí G deve possuir um elemento de ordem 15.

(45) Mostre que se $Aut(G)$ é cíclico então G é abeliano

$Aut(G) = \{f: G \to G \mid f$ é automorfismo$\}$

com operação de composição

Seja, $f, g \in Aut(G)$. $f \circ g$ é automorfismo.

$$\begin{aligned} f(g(ab)) &= f(g(a)g(b)) \\ &= f(g(a))f(g(b)) \\ &= g(f(a))g(f(b)) \\ &= g(f(a)f(b)) \\ &= g(f(ab)) \end{aligned}$$