(46) Se G é um grupo de ordem par, mostre que existe $a \neq e$ em G tal que $a^2 = e$.

~~Suponha por absurdo,~~ Combinando cada elemento com seu inverso

$$g^2 \neq e \Leftrightarrow g \neq g^{-1} \Leftrightarrow \text{temos um par } (g, g^{-1}).$$

Tal que, $g \neq g^{-1}$, temos um elemento que não tem par: o elemento neutro, pois $e^{-1} = e$, então ~~∃~~ ~~par~~ para termos um número par de elementos ~~par~~ precisa existir outro elemento que também não tenha par. No caso $\exists g_0$ t.q. $g_0^2 = e$.

(17) Se H é um subconjunto ~~de~~ finito de G que é fechado em relação à operação de G, prove que H é um subgrupo de G. Mostre ainda que a conclusão pode ser falsa se H é infinito.

Temos que provar primeiro que H é um grupo.

- Possui elemento neutro: Como H é finito $\forall h \in H$, $\exists k \in \mathbb{N}$ t.q. $h^k = e \in H$, pois $h \in H, h^2 \in H, \dots, h^k \in H$.
- H é fechado.
- Elemento inverso: $\forall h \in H$, temos que $\exists k \in \mathbb{N}$ t.q. $h^k = e \Rightarrow h^{k-1} \cdot h = e \Rightarrow h^{-1} = h^{k-1}$, ou seja h possui elemento inverso.

Logo, H é subgrupo de G. Se H fosse infinito não necessariamente possui inverso ou elemento neutro.

⑱ Sejam p um primo e $H = \{X \in GL_2(\mathbb{Z}_p) : \det(X) = 1\}$. Qual a ordem de H?

Pelo primeiro teorema de isomorfismos, se existe um morfismo $f: G \to G'$ então temos um isomorfismo $G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$. Aplicando isto para $\det: GL_2(\mathbb{Z}_p) \to \mathbb{Z}_p^*$ da um isomorfismo $GL_2(\mathbb{Z}_p)/H \to \mathbb{Z}_p^*$ pois $H = \mathrm{Ker}(\det: GL_2(\mathbb{Z}_p) \to \mathbb{Z}_p^*)$ e $\det$ é sobrejetora. Significa que

$$p-1 = |\mathbb{Z}_p^*| = |GL_2(\mathbb{Z}_p)/H| = \frac{|GL_2(\mathbb{Z}_p)|}{|H|} = \frac{(p^2-1)(p^2-p)}{|H|}$$

Daí, $|H| = p(p^2-1)$

(49) Seja G um grupo qualquer. Dados $a, b \in G$, mostre que

(a) as ~~ambas~~ ordens de b e $\varphi_a(b) = a b a^{-1}$ são iguais.

(b) as ordens de ab e ba são iguais.

(a) $K = ord(b)$, então $b^K = e$. Segue que

$$(aba^{-1})^K = (aba^{-1})(aba^{-1})\dots(aba^{-1})$$
$$= a b^K a^{-1}$$
$$= a e a^{-1} = e$$

(Volta analoga).

(b) Seja $K = ord(ab)$, $(ab)^K = e$

$$\cancel{(ab)^K} \; (ba)^K = e$$
$$\iff a(ba)^K b = ab$$

Daí, $a(ba)^K b = a(ba)(ba)\dots(ba)b$

$$= (ab)(ab)\dots(ab)ab$$
$$= (ab)^K ab = ab.$$

(Volta analoga).

(50) Mostre que o grupo multiplicativo $(\mathbb{Z}/p\mathbb{Z})^\times$ é cíclico para $p=3,5,7,11,13$. Quais são seus geradores em cada um destes casos?

Elementos de $(\mathbb{Z}/_3\mathbb{Z})$: 1, 2

geradores $e, 2^k$

·	1	2
1	1	2
2	2	1

$(\mathbb{Z}/_3\mathbb{Z})$: 1, 2, 3, 4

geradores: $2^0, 2^1, 2^3, 2^2$

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$(\mathbb{Z}/_7\mathbb{Z})$: 1, 2, 3, 4, 5, 6 7

geradores: $3^0, 3^2, 3^1, 3^4, 3^5, 3^3$

·	1	2	3	4	5	6	~~7~~
1	1	2	3	4	5	6	~~7~~
2	2	4	6	1	3	5	
3	3	6	2	5	1	4	
4	4	1	5	2	6	3	
5	5	3	1	6	4	2	
6	6	5	4	3	2	1	

(51) Em um grupo G, dois elementos $a, b \neq e$ satisfazem $a^5 = e$ e $aba^{-1} = b^2$. Determine a ordem de b.

$$b^2 = aba^{-1} \iff b = a^{-1}b^2a$$

Note que, $(aba^{-1})^n = (aba^{-1})(aba^{-1})\dots(aba^{-1})$

$$= ab^n a^{-1}$$

Daí,
$$\begin{aligned}
b^{32} &= (aba^{-1})^{16} \\
&= ab^{16}a^{-1} \\
&= a(aba^{-1})^8 a^{-1} \\
&= a^2(aba^{-1})^4 a^{-2} \\
&= a^3 b^4 a^{-3} \\
&= a^4 b^2 a^{-4} \\
&= a^5 b a^{-5} \\
&= b
\end{aligned}$$

Portanto $b^{31} = e$ e $\text{ord}(b) = 31$.

(52) Prove: Se um grupo G possui um único elemento a de ordem 2, então $a \in Z(G)$ (aqui $Z(G)$ é o centro de G).

$$Z(G) = \{z \in G \mid gzg^{-1} = z \ \forall g \in G\}$$

Tome g qualquer de G. Seja

$$x = gag^{-1}.$$

Então, $x^2 = gag^{-1} . gag^{-1} = \cancel{ga^2 g^{-1}}$

$$= ga^2 g^{-1}$$

$$= geg^{-1} = e$$

Logo, a $ord(x) = 2 \Rightarrow x = a \Rightarrow a \in Z(G)$, x não pode ter ordem 1, pois daí $gag^{-1} = e \Rightarrow ga = g \Rightarrow a = e$, absurdo pois daí $G = \{e\}$.

CamScanner

(S3) Seja G um grupo em que a interseção de todos os subgrupos distintos de $\{e\}$ é distinto de $\{e\}$. Prove que todo elemento de G tem ordem infinita.

Suponha que existe um elemento $g \in G$ de ordem infinita. Então, o subgrupo gerado por g é isomorfo a $\mathbb{Z}$, o grupo dos inteiros sob adição. Como $\mathbb{Z}$ é um grupo infinito, ele tem uma infinidade de subgrupos distintos, cada um gerado por um único inteiro. No entanto, a interseção desses subgrupos é $\{0\} = \{e\}$ o que contradiz a hipótese. Portanto, todo elemento em G deve ter ordem finita.

CamScanner

(54) Em cada item, escreva todas as classes laterais à direita e à esquerda de H em G:

(a) $G=\mathbb{Z}_{10}$ e $H=\langle 2\rangle$

(b) $G=S_3$, o grupo das permutações, e $H=\{\sigma\in S_3:\sigma(1)=1\}$.

(a) Note que, $H=\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8}\}$. Como $|H|=5$ e $|G|=10$. O número de classes laterais é 2 (Teorema de Lagrange). A esquerda:

$$\overline{0}+H=\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8}\}$$
$$\overline{1}+H=\{\overline{1},\overline{3},\overline{5},\overline{7},\overline{9}\}$$

e para direita: $H+\overline{0}=\overline{0}+H$ e $H+\overline{1}=\overline{1}+H$.

(b) $G=\{(1,2,3),(1,3,2),(2,1,3),(2,3,1),(3,1,2),(3,2,1)\}$ e $H=\{(1,2,3),(1,3,2)\}$. Pelo Teorema de Lagrange temos 3 classes laterais:

$$(1,2,3)H=(1,3,2)H=\{(1,2,3),(1,3,2)\}$$
$$(2,1,3)H=(3,1,2)H=\{(2,1,3),(3,1,2)\}$$
$$(2,3,1)H=(3,2,1)H=\{(2,3,1),(3,2,1)\}$$

Note que, é um grupo abeliano, então as classes à esquerda são iguais as à direita

(S8) Três grilos A, B, C brincam de pula-sela: um grilo pode saltar um outro, mas não sobre dois outros. É possível que os grilos, após 2016 pulos, voltem à posição relativa inicial? E com 2017 pulos?

Vamos considerar as permutações possíveis

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Note que, $\sigma_1 \circ \sigma_1 = \sigma_2 \circ \sigma_2 = e$. Para 2016, o problema é resolvido com

$$(\sigma_1)^{2016} = (\sigma_1^2)^{1008} = (e)^{1008} = e$$

Para 2017, considere o grupo $\{-1, 1\}$ com a operação de produto, seja o morfismo

$$\varphi : S_3 \to \{-1, 1\}$$

dado por $\varphi(\sigma_1) = \varphi(\sigma_2) = -1$. Daí, sendo π_i o i-ésimo pulo

$$\varphi(\pi_1 \cdot \pi_2 \cdots \pi_{2017}) = 1 \iff \varphi(\pi_1) \cdot \varphi(\pi_2) \cdots \varphi(\pi_{2017}) = 1$$

$$\iff (-1)^{2017} = 1 \quad \text{Abs.}$$

Logo, não é possível para 2017.

(61) Seja G um grupo. Dados dois elementos $x, y \in G$, o produto $xyx^{-1}y^{-1}$ é chamado de comutante de x e y. Definimos o comutador de G, $K(G)$ como conjunto de todos os produtos de um número finito de comutantes de elementos de G.

(a) Prove que $K(G)$ é um subgrupo normal de G.

(b) Prove que o grupo quociente $G/K(G)$ é abeliano.

(b) Seja $aK, bK \in G/K$,

$$(aK)(bK)(a^{-1}K)(b^{-1}K) = aba^{-1}b^{-1}K = eK$$

Ou seja, $(aK)(bK) = (bK)(aK)$

(a) ~~$\forall x, y$~~ $\forall x, y, z \in G$

$$xyx^{-1}y^{-1} \to zxyx^{-1}y^{-1}z^{-1}$$

$$\hookrightarrow zxz^{-1}zyz^{-1}zx^{-1}z^{-1}zy^{-1}z^{-1}$$

$$= (zxz^{-1})(zyz^{-1})(zx^{-1}z^{-1})(zy^{-1}z^{-1})$$

67 Seja D_4 o grupo de simetrias do ~~dos~~ quadrado (o qual é gerado por uma rotação ρ de 90º no sentido anti-horário e uma reflexão σ em relação a uma das diagonais).

(a) Quantos elementos de D_4 tem ordem 2?

(b) Liste todos os subgrupos de D_4.

(a) Temos que $D_4 = \{e, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$. Utilizando a relação $\sigma\rho^m = \rho^{-m}\sigma$, obtemos

$$(\rho^2)^2 = e, \quad (\sigma)^2 = e, \quad (\sigma\rho)^2 = (\sigma\rho)(\rho^{-1}\sigma)$$
$$(\sigma\rho^2)^2 = (\sigma\rho^2)(\rho^{-2}\sigma) = e, \quad (\sigma\rho^3)^2 = (\sigma\rho^3)(\rho^{-3}\sigma) = e$$

Portanto D_4 tem 5 elementos de ordem 2.

(b) Os seguintes conjuntos são subgrupos de D_4.

$\{e\}$, $\{e, \rho^2\}$, $\{e, \sigma\}$, $\{e, \sigma\rho\}$, $\{e, \sigma\rho^2\}$, $\{e, \sigma\rho^3\}$,

$\{e, \rho^2, \sigma, \sigma\rho^2\}$, $\{e, \rho, \rho^2, \rho^3\}$

(68) Se G é um grupo e $a \in G$, o centralizador de a em G é denotado por $C(a)$ e definido por

$$C(a) = \{x \in G : ax = xa\}$$

(a) Prove que $C(a)$ é um subgrupo de G para todo $a \in G$.

(b) Se $a, x \in G$, prove que $C(xax^{-1}) = x\,C(a)\,x^{-1}$.

(a) • elemento neutro: $e \in C(a) \therefore ae = ea = a$

• $\forall x y \in C(a)$ $\begin{matrix} ax = xa \\ ay = ya \end{matrix} \Rightarrow a(xy) = (xa)y = (xy)a \Rightarrow xy \in C(a)$

• $x \in C(a)$ $ax = xa \Rightarrow x^{-1}ax = a \Rightarrow x^{-1}a = ax^{-1} \Rightarrow x^{-1} \in C(a)$

Com as propriedades acima $C(a) \subset G$, $\forall a \in G$.

(b) Se $y \in C(xax^{-1})$, então

$(xax^{-1})y = y(xax^{-1}) \Rightarrow ax^{-1}y = x^{-1}yxax^{-1} \Rightarrow a(x^{-1}yx) = (x^{-1}yx)a$

$\Rightarrow x^{-1}yx \in C(a)$

$\Rightarrow y \in xC(a)x^{-1}$

$\Rightarrow C(xax^{-1}) \subseteq xC(a)x^{-1}$ (I)

Se $y \in C(a)$, então

$(xyx^{-1})(xax^{-1}) = xyax^{-1} = xayx^{-1} = (xax^{-1})(xyx^{-1})$

$\Rightarrow xyx^{-1} \in C(xax^{-1})$

$\Rightarrow xC(a)x^{-1} \subseteq C(xax^{-1})$ (II)

Por (I) e (II), $C(xax^{-1}) = xC(a)x^{-1}$.

CamScanner

69 Suponha que, no grupo G, os elementos a e b sejam distintos do elemento neutro e, $a^5 = e$ e $aba^{-1} = b^2$. Calcule a ordem de b.

Temos que, $b = a^{-1}b^2a$

Seguindo que, $(aba^{-1})^n = (aba^{-1})(aba^{-1})\dots(aba^{-1})$
$= ab^na^{-1}$.

Temos, $b^{32} = (aba^{-1})^{16}$
$= ab^{16}a^{-1}$
$= a(aba^{-1})^8a^{-1}$
$= a^2b^8a^{-2}$
$= a^2(ab^2a^{-1})^4a^{-2}$
$= a^3b^4a^{-3}$
$= a^4b^2a^{-4}$
$= a^5ba^{-5}$
$= b$

Daí, $ord(b) = 31$.

CamScanner

71) Seja G o grupo dos números complexos diferentes de zero com a operação de multiplicação e seja N o subgrupo de G dos números complexos de módulo 1: $N = \{a+bi \in \mathbb{C} : a^2+b^2 = 1\}$. Mostre que G/N é isomorfo ao grupo dos números reais positivos com a operação de multiplicação.

Se $z_1 = \alpha + \beta i$; $z_2 = \gamma + \delta i$

$$|z_1 . z_2| = \sqrt{(\alpha\gamma - \beta\delta)^2 + (\alpha\delta + \beta\gamma)^2}$$

$$= \sqrt{\alpha^2\gamma^2 + \beta^2\delta^2 + \alpha^2\delta^2 + \beta^2\gamma^2}$$

$$= \sqrt{(\alpha^2+\beta^2)(\gamma^2+\delta^2)} = |z_1||z_2|$$

Logo, se $G = \{\alpha + \beta i \mid \alpha, \beta \in \mathbb{R}^*\}$, então G/N são círculos de raio $r = \sqrt{\alpha^2+\beta^2}$. Definimos $G/N = \{gN : g \in G\}$, onde cada gN representa um círculo de raio $|g| = r$. A função $\varphi: G/N \to \mathbb{R}_{>0}$ dada por $\varphi(z_1 . z_2) = |z_1||z_2|$ tem as seguintes propriedades:

• $\varphi(z_1) = \varphi(z_2) \iff |z_1| = |z_2| = r \iff z_1, z_2 \in gN$, com $|g| = r$ i.e. $\varphi(z_1) = \varphi(z_2)$ se e somente se z_1 e z_2 estão na mesma classe lateral.

• φ é sobrejetiva. Para ver isso basta tomar $z = \alpha + 0i$, com $\alpha \in \mathbb{R}_{>0}$. Temos que $\varphi(z) = \sqrt{a^2} = a$, e $|a|$ percorre todo o conjunto $\mathbb{R}_{>0}$.

Como φ é injetiva e sobrejetiva, $\varphi: G/N \to \mathbb{R}_{>0}$ é isomorfi

(72) Seja H um subgrupo normal de um grupo finito G, e seja $m = (G:H)$. Prove que $a^m \in H$, para todo $a \in G$.

Como $H \subset G$ é um subgrupo normal, então G/H é um grupo de ordem m. Pelo Teorema de Lagrange, a ordem de qualquer elemento de G/H divide m. Em particular, se $gH \in G/H$, então $(gH)^m = H$. Daí

$$(gH)^m = g^m H = H, \text{ implicando que } g^m \in H.$$

CamScanner

(73) Um subgrupo H de um grupo G é dito característico se $\varphi(H) \subset H$ para todo automorfismo $\varphi: G \to G$.

(a) Prove que se H é um grupo característico de G, então H é normal em G.

(b) Prove que se M e N são subgrupos característicos de G, então MN também é um subgrupo característico de G.

(a) $\forall g \in G$, como H é característico em G. Queremos mostrar que $gHg^{-1} \subset H$. ~~Es~~ a uma função automorfismo de conjugação por g, φ_g, que mapeia H em si mesmo:

$$gHg^{-1} = \varphi_g(H) \subset H$$

Logo, H é normal.

(b) $\forall \varphi$, $\varphi(M) \subset M$ e $\varphi(N) \subset N \Rightarrow$

$$\Rightarrow \varphi(M.N) = \varphi(M).\varphi(N) \subset M.N.$$

(74) Seja G um grupo finito de ordem n. Uma função $f: G \to G$ é um pseudomorfismo de G se $f(xyz) = f(x)f(y)f(z)$, $\forall x,y,z \in G$.

(a) Se n é ímpar, prove que todo pseudomorfismo de G é um endomorfismo de G (morfismo de G em G)

(b) Se n é par, é verdade que todo pseudoendomorfismo de G é um endomorfismo de G?

(a) Temos que

$$f(e) = f(e.e.e) = f(e)^3 \Rightarrow (f(e))^2 = e$$

Como $n \equiv 1 \pmod 2$, G não tem um elemento de ordem 2, já que $2 \nmid n$. Portanto $f(e)^2 = e \Leftrightarrow f(e) = e$. Logo

$$f(xy) = f(xy.e) = f(x)f(y)f(e) = f(x)f(y) \Rightarrow f \text{ é endomorfismo.}$$

(b) Seja $f: \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ dado por $f(x) = x + \bar{1}$. Temos que

$$f(x)+f(y)+f(z) = x+\bar{1}+y+\bar{1}+z+\bar{1} = x+y+z+\bar{1} = f(x+y+z)$$

Logo é pseudoendomorfismo. Contudo

$$\left.\begin{array}{l} f(\bar{0}) = \bar{1} \\ f(\bar{1}) = \bar{0} \end{array}\right\} f(e) \neq e \Rightarrow f \text{ não é endomorfismo.}$$

CamScanner