Teoria de Grupos

Definição 1: Um conjunto $G \neq \emptyset$ munido com uma operação $* : G \times G \longrightarrow G$ (fechada)

$$(x, y) \longmapsto x * y$$

satisfazendo

C1) Associatividade: $x * (y * z) = (x * y) * z$

C2) Existência de Elemento Neutro:

$$\exists\, e \in G \mid e * x = x = x * e, \ \forall\, x \in G$$

C3) Existência do elemento simétrico:

$$\forall\, x \in G \ \exists\, y \in G \mid x * y = e = y * x$$

é dito ser um grupo.

A notação usada é $(G, *)$.

Exemplos:

① $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ são grupos.

② $(\mathbb{N}, +)$ não é grupo, pois não há simétrico.

③ $(\mathbb{Z}, \cdot)$ não é grupo, pois não há simétrico.

④ $(\mathbb{Q}^*, \cdot)$ é grupo,

- o elemento neutro é 1
- o simétrico de $\frac{a}{b}$ é $\frac{b}{a}$, pois $\frac{a}{b}\frac{b}{a} = 1$.

⑤ $(\mathbb{R}^*, \cdot)$ é grupo

⑥ Os irracionais com $+$ e $\cdot$ não é grupo, pois não tem elemento neutro (1). Além disso, $+$ e $\cdot$ não são fechadas:

- $\sqrt{2} + (-\sqrt{2}) = 0 \in \mathbb{Q}$.
- $\sqrt{2} \cdot \sqrt{2} = \sqrt{4} = 2 \in \mathbb{Q}$

⑦ $(\mathbb{C}, +)$ é grupo.

$(\mathbb{C}, \cdot)$ também é, onde $z^{-1} = \frac{\overline{z}}{|z|^2}$, $z \in \mathbb{C}$.

⑧ $G = \{1, -1\}$ é grupo com $\cdot$.

⑨ $G = \{1, i, -1, -i\}$ é grupo com $\cdot$.

⑩ Considere $M_n(\mathbb{R})$ o conjunto das matrizes quadradas de ordem n com entradas reais.

$(M_n(\mathbb{R}), +)$ é grupo, pois

C1) $M_n(\mathbb{R})$ é associativo com $+$.

(2) o elemento neutro é $0 = (0)$.

C3) O simétrico de $A = (a_{ij})$ é $-A = (-a_{ij})$

(11) $(M_n^*(\mathbb{R}), \cdot)$ não é grupo, pois há matrizes que não possuem inversa:

$$A = \begin{pmatrix} 2 & 6 \\ 1 & 3 \end{pmatrix} \Rightarrow \det A = 0 \Rightarrow A \text{ não tem inversa.}$$

(12) Definamos

$$GL_n(\mathbb{R}) := \{ A \in M_n(\mathbb{R}) \mid \det A \neq 0 \}.$$

Esse conjunto é um grupo, chamado de grupo linear geral de $M_n(\mathbb{R})$, onde o neutro é $I_n = \text{diag}(1, \dots, 1)$, $A^{-1} = \dfrac{\text{Adj}(A)}{\det A}$, lembrando que $\det A^{-1} = \dfrac{1}{\det A}$ e $\det(AB) = \underbrace{\det A}_{\neq 0} \cdot \underbrace{\det B}_{\neq 0} \neq 0$ (fechamento)

(13) $\mathbb{R}^n = \{(x_1, x_2, \dots, x_n) \mid x_i \in \mathbb{R}\}$ é grupo com $+$, onde:

- elemento neutro é $0 = (0, \dots, 0)$
- simétrico de $v = (v_1, v_2, \dots, v_n)$ é $-v = (-v_1, \dots, -v_n)$

(14) Seja $P(\mathbb{R})$ o conjunto dos polinômios.
$(P(\mathbb{R}), +)$ é grupo, onde

- o elemento neutro é $0 = 0x^n + 0x^{n-1} + \dots + 0x + 0$.
- o simétrico de $p(x) = a_n x^n + \dots + a_1 x + a_0$ é $-p(x)$.

Já $(P(\mathbb{R}), \cdot)$ não é grupo, pois

$p(x) = x$ não possui inverso sendo polinômio, seria $\frac{1}{x} \notin P(\mathbb{R})$.

(15) Considere um grupo com 2 elementos:

$$G = \{e, g\}.$$

Temos que e é o elemento neutro.
Também, só há uma possibilidade:

$$g * g = e \Rightarrow g \text{ é o simétrico de } g.$$

Obs.: A partir de agora, chamaremos o simétrico de inverso e denotaremos por x^{-1}.

Definição 2: Seja G um grupo e considere $g \in G$, a potência de g de ordem $n \in \mathbb{N}$ é

$$g^n = \underbrace{g * g * \cdots * g}_{n \text{ vezes}}$$

Obs.: A partir de agora, vamos denotar a operação $*$ por justaposição: $x * y = xy$.

Propriedades

Sejam $x, y, z \in G$.

1) O elemento neutro é único.

2) O elemento simétrico é único.

3) $xy = xz \Rightarrow y = z$ (cancelamento)

4) $(x^{-1})^{-1} = x$

5) $(xy)^{-1} = y^{-1} x^{-1}$

6) $(x^n)^{-1} = (x^{-1})^n$

Prova:

1) Suponha que $e_1, e_2 \in G$ são neutros. Daí,

$$e_1 = e_1 e_2 = e_2 \quad \checkmark$$

2) Suponha que x', x'' são simétricos de x. Daí,

$$x x' = e$$

$$\overset{\cdot x''}{\Rightarrow} x''(x x') = x'' e$$

$$\overset{C1, C2}{\Rightarrow} (x'' x) x' = x''$$

$$\overset{C2}{\Rightarrow} e x' = x''$$

$$\Rightarrow x' = x'' \quad \checkmark$$

3) $xy = xz \overset{\cdot x^{-1}}{\Rightarrow} x^{-1}xy = x^{-1}xz$

$\Rightarrow ey = ez \Rightarrow y = z.$

4) Como $x^{-1}x = e = xx^{-1}$ e o inverso é único, temos que $(x^{-1})^{-1} = x$.

5) Veja que

$$xyy^{-1}x^{-1} = xex^{-1} = xx^{-1} = e.$$

Como o inverso é único, temos $(xy)^{-1} = y^{-1}x^{-1}$.

6) Veja que

$$(x^m)^{-1} = \underbrace{(x \cdot x \cdots x)^{-1}}_{m\times} \overset{5)}{=} \underbrace{x^{-1}x^{-1}\cdots x^{-1}}_{m\times} = (x^{-1})^m.$$

#

Grupos Finitos e Cíclicos

Definição 3: Um grupo é finito se ele possui um número finito de elementos.

A ordem de um grupo é sua cardinalidade:

$$|G| = \#(G)$$

Se G tem n elementos, $|G| = n$.

Se G é infinito, $|G| = \infty$.

Exemplos:

1) Finitos: $G = \{1, -1\}$, $|G| = 2$

$G = \{1, -1, i, -i\}$, $|G| = 4$.

2) Infinitos: $(\mathbb{Z}, +)$, $(M_n(\mathbb{R}), +)$, $(\mathbb{C}^*, \cdot)$, $(GL_n(\mathbb{R}), \cdot)$.

Definição4: Um grupo G é dito ser abeliano se satisfaz

C4) $xy = yx$, $\forall\, x, y \in G$.

Exemplo: $\mathbb{Z}$, $M_n(\mathbb{R})$, $\mathbb{C}^*$ são abelianos.

Já $GL_n(\mathbb{R})$ não é abeliano.

Exemplo: Grupo dos Quatérnios

Considere o grupo dado pelo conjunto

$$Q_8 := \{1, -1, i, -i, j, -j, k, -k\}$$

satisfazendo:

1) 1 é o neutro

2) $(-1)(-1) = 1$

3) $(-1)x = -x = x(-1)$, $x = i, j, k$

4) $i^2 = j^2 = k^2 = -1$

5) $ijk = -1$

Veja que

- $(-1)(-1) = 1 \Rightarrow (-1)^{-1} = -1$.
- $x(-x) = x\,x(-1) = x^2(-1) = (-1)(-1) = 1$

  $\Rightarrow x^{-1} = -x, \quad x = i, j, k$
- $ijk = -1$
  - $\Rightarrow ijk(-k) = (-1)(-k)$

    $\Rightarrow ij1 = (-1)(-1)k$

    $\Rightarrow \boxed{ij = k}$
  - $\Rightarrow (-i)ijk \Rightarrow (-i)(-1)$

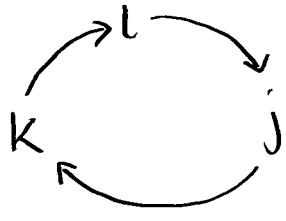
    $\Rightarrow \boxed{jk = i}$
  - $\Rightarrow kijk(-k)(-j) = k(-1)(-k)(-j)$

    $\Rightarrow kij(-j) = kk(-j)$

    $\Rightarrow ki = k^2(-j) = (-1)(-1)j$

    $\Rightarrow \boxed{ki = j}$

Para memorizar:



Resta obter ji, kj, ik:

- $i = jk \Rightarrow ji = j^2k \Rightarrow \boxed{ji = -k}$
- $k = ij \Rightarrow ik = i^2j \Rightarrow \boxed{ik = -j}$
- $j = ki \Rightarrow kj = k^2i \Rightarrow \boxed{kj = -i}$

Portanto, temos

$$\boxed{ij = -ji}, \quad \boxed{jk = -kj}, \quad \boxed{ki = -ik},$$

Isto é, Q_8 é anticomutativo.

Exemplo: Grupo de Klein (Klein-4)

Considere o grupo abeliano definido por

$$K_4 := \{e, a, b, c \mid a^2 = b^2 = c^2 = abc = e\}$$

Como $abc = e$, temos

- $abc^2 = c \Rightarrow \boxed{ab = c = ba}$
- $a^2bc = a \Rightarrow \boxed{bc = a = cb}$
- $a = bc \Rightarrow ac = bc^2 \Rightarrow \boxed{ac = b = ca}$

Observe que $x^{-1} = x$, $x = a, b, c$.

Exemplo: Existe grupo de ordem 3 não abeliano?

Considere o seguinte grupo não abeliano:

$$G = \{e, a, b\}$$

Temos as seguintes possibilidades:

1) $ab = e$

Como G não é abeliano, devemos ter $ba \neq ab = e$

Resta que:

- $ba = a \Rightarrow b = e$ ↯

ou

- $ba = b \Rightarrow a = e$ ↯

$\Rightarrow ab \neq e$

2) $ab = a \Rightarrow b = e$ ↯

3) $ab = b \Rightarrow a = e$ ↯

Logo, $ab \in G$, um absurdo. Logo, G deve ter ab.

Mesmo acrescentando ab, precisamos ter ba, que será diferente de ab e pelos casos anteriores também não pode ser e, a, b.

Portanto,

Não há grupos não abelianos de ordem 3 ou 4.

Proposição 5: Se G é abeliano, então

$$(ab)^n = a^n b^n, \quad \forall a, b \in G.$$

Prova: Veja que

$$(ab)^n = \underbrace{ab\,ab\cdots ab}_{n\times} \overset{\text{abeliano}}{=} \underbrace{a\cdots a}_{n\times}\cdot\underbrace{b\cdots b}_{n\times} = a^n b^n. \quad \#$$

Vamos estender nossa definição de função:

- $g^0 = e$
- $g^{-n} = (g^n)^{-1} = (g^{-1})^n$, $n \in \mathbb{N}$.

Definição 6: Seja G um grupo e tome $g \in G$. O seguinte conjunto

$$\langle g \rangle := \{ g^n \mid n \in \mathbb{Z} \}$$

é chamado de **gerado por g**.

Proposição 7: $\langle g \rangle$ é um grupo abeliano.

Prova: 1) Associatividade: G é grupo e $\langle g \rangle \subset G$.
2) O elemento neutro é $g^0 = e$.
3) O inverso de g^n é $g^{-n} = (g^{-1})^n$
4) $g^n g^m = g^{n+m} = g^m g^n$. $\#$

Com isso, dizemos que

$\langle g \rangle$ é o grupo gerado por g.

Exemplos:

1) Em $\mathbb{Z}$:

$$\langle 2 \rangle = \{ \underbrace{2 + \cdots + 2}_{n \times} \mid n \in \mathbb{Z} \}$$

$$= \{ 2n \mid n \in \mathbb{Z} \} = 2\mathbb{Z}$$

2) Em $\mathbb{Q}^*$:

$$\langle 2 \rangle = \{ 2^n \mid n \in \mathbb{Z} \} = \{ \ldots, \tfrac{1}{4}, \tfrac{1}{2}, 1, 2, 4, 8, \ldots \}$$

3) Em $M_2(\mathbb{R})$:

$$\langle I_2 \rangle = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \cdots + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{n \times} \mid n \in \mathbb{Z} \right\}$$

$$= \left\{ \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \mid n \in \mathbb{Z} \right\}$$

Já em $GL_2(\mathbb{R})$:

$$\langle I_2 \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^n \mid n \in \mathbb{Z} \right\} = \{ I_2 \}.$$

4) Em $\mathbb{Z}$:

$$\langle n \rangle = n\mathbb{Z}$$

Definição 8: O grupo gerado por $x, y \in G$ é

$$\langle x, y \rangle = \{ g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k} \mid g_1, g_2, \ldots, g_k \in \{x, y\} \}$$

Se G for abeliano, então

$$\langle x, y \rangle = \{ x^n y^m \mid m, n \in \mathbb{Z} \}$$

Exemplo: Em $\mathbb{Z}$ temos

$$\langle a, b \rangle = \{ na + mb \mid n, m \in \mathbb{Z} \}$$

$$= a\mathbb{Z} + b\mathbb{Z}$$

$$\overset{\text{TN}}{=} d\mathbb{Z},$$

onde $d = mdc(a, b)$.

Por exemplo:

- $\langle 6, 4 \rangle = mdc(6, 4)\,\mathbb{Z} = 2\mathbb{Z}$ em $\mathbb{Z}$.
- $\langle 2, 3 \rangle = mdc(2, 3)\,\mathbb{Z} = \mathbb{Z}$

Definição 9: A ordem de $g \in G$ é o menor inteiro positivo n tal que

$$g^n = e.$$ Notação: $o(g) = n$.

Exemplos:

1) $o(e) = 1$, $e^1 = e$

2) Em K_4,

$o(a) = o(b) = o(c) = 2$, pois $a^2 = b^2 = c^2 = e$.

3) Em Q_8, $o(i) = o(j) = o(k) = 4$, pois

$i^2 = -1$, $i^3 = -i$ e $\boxed{i^4 = 1}$, ...

4) Considere $A = \begin{pmatrix} 2 & 1 \\ -3 & -2 \end{pmatrix} \in GL_2(\mathbb{R})$. Veja que

$$A^2 = \begin{pmatrix} 2 & 1 \\ -3 & -2 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ -3 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow o(A) = 2.$$

Propriedades da ordem: Sejam $g, x, y \in G$, $o(g) = n$. Daí,

1) $n \mid m \Leftrightarrow g^m = e$.
2) $g^k = g^m \Leftrightarrow n \mid k-m$.
3) $o(g^{-1}) = o(g)$.
4) $g^{-1} = g^{n-1}$.
5) $o(xgx^{-1}) = o(g)$.
6) $o(xy) = o(yx)$.

Prova:

1) ($\Rightarrow$) $n \mid m \Rightarrow m = kn \Rightarrow g^m = g^{kn} = (g^n)^k = e^k = e$

($\Leftarrow$) Pelo TADE escrevemos

$$m = nq + r, \quad 0 \leq r < n.$$

Daí,

$$e = g^m = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r$$

$\Rightarrow g^r = e$, $r < n$ ↯ Pela minimalidade de n.

Logo, resta que $r = 0$. Assim, $m = nq \Rightarrow n \mid m$.

2) $g^k = g^m \Rightarrow g^{k-m} = e \Leftrightarrow n \mid k - m$.

3) Veja que

$$(g^{-1})^n = (g^n)^{-1} = e^{-1} = e$$

Suponha que existe $0 < k < n$ tal que $(g^{-1})^k = e$.

Daí,

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

$$\Rightarrow ((g^k)^{-1})^{-1} = ((g^n)^{-1})^{-1}$$

$$\Rightarrow g^k = g^n = e \text{ ↯ min. de } n.$$

Logo, $o(g^{-1}) = n = o(g)$.

4) $g^n = e \Rightarrow g g^{n-1} = e \Rightarrow g^{-1} = g^{n-1}$.

$$g g^{n-1} = g^{n-1} g$$

5) Observe que

$$(xgx^{-1})^n = \underbrace{x g \cancel{x^{-1}} \cancel{x} g \cancel{x^{-1}} \cdots \cancel{x} g \cancel{x^{-1}} \cancel{x} g x^{-1}}_{n\times}$$

$$= x \underbrace{g \cdots g}_{n\times} x^{-1}$$

$$= x g^n x^{-1} = x e x^{-1} = e.$$

Suponha que exista $0 < k < n$ tal que $(xgx^{-1})^k = e$
Daí,

$$(xgx^{-1})^k = x g^k x^{-1} = e = x g^n x^{-1}$$

$$\Rightarrow \cancel{x} g^k \cancel{x^{-1}} = \cancel{x} g^n \cancel{x^{-1}} \Rightarrow g^k = g^n = e \;\lightning$$

Logo, $o(xgx^{-1}) = n = o(g)$.

6) Seja $o(xy) = m$. Daí,

$$(yx)^m = y(xyx \cdots yxy)x = y(xy)^{m-1}x$$

$$= y(xy)^{-1}x = yy^{-1}x^{-1}x = e$$

Suponha que exista $0 < k < m$ tal que $(yx)^k = e$. Daí,

$$(xy)^k = x(yxy \cdots xyx)y = x(yx)^{k-1}y = x(yx)^{-1}y = e \;\lightning$$

Logo, $o(yx) = m = o(xy)$. #

Proposição 10: Seja G finito e $g \in G$. Então,

$$|\langle g \rangle| = o(g).$$

Prova: Considere $g^m \in \langle g \rangle$. Pelo TA DE

$$m = nq + r, \quad 0 \leq r < n,$$

para $n = o(g)$.

Daí,

$$g^m = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r.$$

Dessa forma,

$$\langle g \rangle = \{ g^m \mid m \in \mathbb{Z} \}$$

$$= \{ g^r \mid 0 \leq r < n \}$$

$$= \{ g^0 = e, g, g^2, \ldots, g^{n-1} \}$$

Sejam $0 \leq i, j < n$ tal que

$$g^i = g^j \Rightarrow g^{i-j} = e$$

$\Rightarrow n \mid i-j$ ↯ Pois $i, j < n$.

Logo, $|\langle g \rangle| = n = o(g)$ #

Exemplos:

① Em K_4 temos $\langle a \rangle = \{e, a\}$, pois $a^2 = e$.

② Em Q_8 temos $\langle i \rangle = \{1, i, i^2 = -1, i^3 = -i\}$

③ $\langle e \rangle = \{e\}$

④ Qual a ordem de 2 em $\mathbb{Z}$.

$o(2) = \infty$, pois $\langle 2 \rangle = 2\mathbb{Z}$ é infinito.

Obs.: Se $|\langle g \rangle| = \infty$, então definimos:

$$o(g) = \infty$$

Vamos ver exemplos de grupos gerados por 2 elementos:

⑤ Considere $G = \langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle$

Veja que

$(ab)^2 = abab = e \Rightarrow a^2 bab^2 = ab \Rightarrow ba = ab$

Logo, G é abeliano.

Portanto, $G = K_4$:

$$K_4 = \langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle = \{e, a, b, ab\}.$$

⑥ Considere $G = \langle a, b \mid a^4 = e,\ a^2 = b^2,\ ab = ba^{-1} \rangle$

Como $a^4 = e$, temos $a^{-1} = a^3$.

Escrevemos

$$G = \{e, a, b, a^2, a^3, b^3, ab, ba\} = Q_8$$

$$a^2 = b^2$$

Temos a seguinte identificação:

$e \leftrightarrow 1$, $a \leftrightarrow i$, $b \leftrightarrow j$, $ab \leftrightarrow k$, $a^2 \leftrightarrow -1$, $a^3 \leftrightarrow -i$,

$b^3 \leftrightarrow -j$ e $ba \leftrightarrow -k$

Veja que

- $abab = ba^{-1}ab = b^2 = a^2$ //
  $abab = (ab)^2$
- $(ba)^2 = baba = bba^{-1}a = b^2 = a^2$ //
- $a^2b = b^2b = b^3$ //
- $a^3b = a^2ab = a^2ba^{-1} = aaba^{-1} = ba^{-1}a^{-1}a^{-1} = ba^3a^3a^3 = ba^8a$
  $= b(a^4)^2a = be^2a = ba$ //
- $ba^3 = ba^{-1} = ab$ //
- $aba = ba^{-1}a = b$ //
- $bab = bba^{-1} = b^2a^3 = a^2a^3 = a^4a = a$ // e
- $a^3b^3 = a^3bb^2 = a^3ba^2 = baa^2 = ba^3 = ab$
- $aba^2 = ba^3a^2 = ba^4a = ba$

Proposição 11: Seja $g \in G$ tal que $|\langle g \rangle| = o(g) = \infty$.

Daí, valem

1) $g^n = e \iff n = 0$

2) $g^n = g^m \Rightarrow n = m$

Prova:

1) ($\Rightarrow$) Suponha que $n \neq 0$.

- Se $n > 0$, então $\langle g \rangle = \{e, g, \dots, g^{n-1}\}$ é finito ↯
- Se $n < 0$, então $g^{-n} = (g^n)^{-1} = e^{-1} = e$

  $\Rightarrow \langle g \rangle$ é finito ↯

Logo, $n = 0$

($\Leftarrow$) $g^0 = e$.

2) $g^n = g^m \Rightarrow g^{n-m} = e \overset{1)}{\Rightarrow} n - m = 0 \Rightarrow n = m$. #

Definição 12: Um grupo G é dito ser <u>cíclico</u> se existe $g \in G$ tal que $G = \langle g \rangle$.

Dizemos que

- G é gerado por g.
- g é <u>gerador</u> de G.

Proposição 13: Se G é cíclico, então G é abeliano.

Prova: Sejam $g^n, g^m \in G = \langle g \rangle$.

Lembre que potências comutam: $g^n g^m = g^{n+m} = g^m g^n$.

Logo, G é abeliano. #

Contrapositiva: G não abeliano $\Rightarrow$ G não é cíclico.

Exemplos:

1) Q_8 e $GL_n(\mathbb{R})$ não são cíclicos, pois não são abelianos.

2) Em K_4 temos:

- $\langle e \rangle = \{e\}$ · $\langle a \rangle = \{e, a\}$ · $\langle b \rangle = \{e, b\}$ · $\langle c \rangle = \{e, c\}$

Como nenhum desses gerados é K_4, temos que o grupo de Klein não é cíclico.

3) $\mathbb{Z}$ é cíclico pois $\mathbb{Z} = \langle 1 \rangle$.

4) $\mathbb{Q}$ é cíclico?

Suponha que $\mathbb{Q} = \left\langle \frac{a}{b} \right\rangle$ com $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$, $\frac{a}{b}$ irredutível.

Considere $\frac{a}{2b}$. Daí, esse número pode ser escrito:

$$\frac{a}{2b} = k\frac{a}{b},\ k \in \mathbb{Z} \Rightarrow k = \frac{1}{2} \lightning$$

Portanto, $\mathbb{Q}$ não é cíclico.

Proposição 14: Seja $g \in G$ tal que $o(g) = n$. Daí, para $k > 0$ vale

$$\langle g^k \rangle = \langle g^{mdc(k,n)} \rangle$$

Prova: Seja $d = mdc(k,n)$.

($\subseteq$) Como $d \mid k$, temos $k = md$, $m \in \mathbb{Z}$. Daí,

$$g^k = g^{md} = (g^d)^m$$

$$\Rightarrow g^k \in \langle g^d \rangle \Rightarrow \langle g^k \rangle \subseteq \langle g^d \rangle.$$

↳ fechamento

(2) Pelo Lema de Bézout temos $d = rk + sn$, para certos $r, s \in \mathbb{Z}$. Daí,

$$g^d = g^{rk+ns} = (g^k)^r (g^n)^s = (g^k)^r e^s = (g^k)^r$$

$$\Rightarrow g^d \in \langle g^k \rangle \Rightarrow \langle g^d \rangle \subseteq \langle g^k \rangle.$$

↳ fechamento

Portanto, $\langle g^k \rangle = \langle g^d \rangle$. #

Proposição 15: Seja G é cíclico de ordem n.

Se $mdc(n,m)=1$, então $G=\langle g^m\rangle$.

Prova: Se $d=mdc(n,m)=1$, então pela proposição anterior temos

$$\langle g^m\rangle = \langle g^d\rangle = \langle g\rangle = G. \quad \#$$

Exemplo 1: Seja G um grupo cíclico de ordem 12, digamos que $G=\langle g\rangle$. Daí,

G é gerado também por g^5, g^7, g^{11}.

Exemplo 2: Considere $G=\langle i\rangle=\{1,-1,i,-i\}$ em Q_8.

↳ ordem 4

Pela proposição anterior temos

$$G=\langle i^3\rangle=\langle -i\rangle.$$

→ Os grupos $\mathbb{Z}_n$.

Considere $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ com as operações:

- adição: $\bar{a} + \bar{b} = \overline{a+b}$.
- multiplicação: $\bar{a} \cdot \bar{b} = \overline{ab}$.

Proposição 16: $(\mathbb{Z}_n, +)$ é um grupo abeliano.

Prova:

(1) é associativo

(2) o neutro é $\bar{0}$

(3) o simétrico de $\bar{a}$ é $\overline{n-a}$.

(4) $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$. #

Obs.: $\mathbb{Z}_n$ não é grupo com $\cdot$, pois $\bar{0}$ não possui inverso.

Seguer podemos afirmar que $(\mathbb{Z}_n^*, \cdot)$ é grupo para n qualquer.

Proposição 17: $(\mathbb{Z}_n^*, \cdot)$ é grupo $\Leftrightarrow$ n é primo.

Prova:

($\Rightarrow$) Suponha que n é composto, isto é,

$$n = ab, \quad 1 < a, b < n \quad (\bar{a}, \bar{b} \in \mathbb{Z}_n^*)$$

Daí,

$$\bar{n} = \overline{ab} = \bar{a}\,\bar{b} \Rightarrow \bar{a}\,\bar{b} = \bar{0} \; \lightning$$

Pois $\bar{0} \notin \mathbb{Z}_n^*$. Logo, n é primo

↳ fechamento

($\Leftarrow$)

(1) é associativo

(2) o neutro é $\bar{1}$

(3) Como n é primo, então $\bar{a} \in \mathbb{Z}_n^*$ é inversível: $(\bar{a})^{-1} = \bar{r}$, r tal que $ar + ns = 1$.

(4) é comutativo: $\bar{a}\,\bar{b} = \overline{ab} = \overline{ba} = \bar{b}\,\bar{a}$. #

Obs.: Se $\mathbb{Z}_n^*$ não é grupo, pelo menos

$$U(\mathbb{Z}_n) = \{\bar{a} \in \mathbb{Z}_n^* \text{ inversível}\}$$

$$= \{\bar{a} \in \mathbb{Z}_n \mid mdc(a, n) = 1\} \text{ é grupo.}$$

Exemplos:

1) $\langle \overline{0} \rangle = \{\overline{0}\}$

2) A ordem de $\mathbb{Z}_n$ é n e a ordem de $\mathbb{Z}_n^*$ é $n-1$

3) $U(\mathbb{Z}_{12}) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ é grupo

4) $\langle \overline{2} \rangle = \langle \overline{0}, \overline{2}, \overline{4}, \overline{6} \rangle$ em $\mathbb{Z}_8$

5) $\mathbb{Z}_n$ é cíclico, pois $\mathbb{Z}_n = \langle \overline{1} \rangle$.

6) $\mathbb{Z}_{12}$ é gerado por $\overline{1}, \overline{5}, \overline{7}, \overline{11}$.

7) $\mathbb{Z}_n = \langle \overline{a} \rangle = \langle \overline{mdc(a,n)} \rangle$

8) Vamos obter $\langle \overline{2} \rangle$ em $\mathbb{Z}_{11}^*$:

- $\overline{2}^0 = \overline{1}$
- $\overline{2}^1 = \overline{2}$
- $\overline{2}^2 = \overline{4}$
- $\overline{2}^3 = \overline{8}$
- $\overline{2}^4 = \overline{16} = \overline{5}$
- $\overline{2}^5 = \overline{32} = \overline{10}$
- $\overline{2}^6 = \overline{64} = \overline{9}$
- $\overline{2}^7 = \overline{128} = \overline{7}$
- $\overline{2}^8 = \overline{256} = \overline{3}$
- $\overline{2}^9 = \overline{512} = \overline{6}$
- $\overline{2}^{10} = \ldots$

Portanto, $\mathbb{Z}_{11}^* = \langle \overline{2} \rangle$ e portanto é cíclico.

→ O grupo simétrico

Podemos formar um grupo com funções?
Vamos escolher a operação de composição: $\circ$.
Para termos o fechamento, precisamos escolher

$$f : X \to X$$

C1) Associatividade

$$((f_1 \circ f_2) \circ f_3)(x) = (f_1 \circ f_2)(f_3(x))$$

$$= f_1(f_2(f_3(x))) = f_1((f_2 \circ f_3)(x))$$

$$= (f_1 \circ (f_2 \circ f_3))(x) \quad \checkmark$$

C2) O elemento neutro é a função identidade:

$$I : X \to X$$
$$x \mapsto x$$

pois • $(f \circ I)(x) = f(I(x)) = f(x)$
• $(I \circ f)(x) = I(f(x)) = f(x)$ ✓

C3) Para existir f^{-1}, f deve ser <u>bijetora</u>.

Dessa forma

$$S_X = \{ f : X \longrightarrow X \mid f \text{ é bijeção} \}$$

é um grupo com a composição, chamado de grupo simétrico de X.

Se X tem n elementos, costuma-se denotar

$$X = \{1, 2, \ldots, n\},$$

assim escreveremos o grupo simétrico de n elementos:

$$\boxed{S_n = \{ \sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\} \mid \sigma \text{ é bijeção} \}}$$

Exemplos:

① $S_1 = \{ I \}$, $I : 1 \longmapsto 1$

② $S_2 = \{ I, f \}$, onde

$I : \{1,2\} \longrightarrow \{1,2\}$

$1 \longmapsto 1$

$2 \longmapsto 2$

$f : \{1,2\} \longrightarrow \{1,2\}$

$1 \longmapsto 2$

$2 \longmapsto 1$

Veja que $\sigma \in S_n$ é uma permutação dos elementos de $\{1, 2, \ldots, n\}$, por isso S_n também é chamado de grupo das permutações de n elementos.

Logo, temos $\boxed{|S_n| = n!}$

③

$I : \{1,2,3\} \longrightarrow \{1,2,3\}$

$1 \longmapsto 1$

$2 \longmapsto 2$

$3 \longmapsto 3$

$f_{12} : \{1,2,3\} \longrightarrow \{1,2,3\}$

$1 \longmapsto 2$

$2 \longmapsto 1$

$3 \longmapsto 3$

$f_{13} : \{1,2,3\} \longrightarrow \{1,2,3\}$

$1 \longmapsto 3$

$2 \longmapsto 2$

$3 \longmapsto 1$

$f_{23} : \{1,2,3\} \longrightarrow \{1,2,3\}$

$1 \longmapsto 1$

$2 \longmapsto 3$

$3 \longmapsto 2$

$f_{123} : \{1,2,3\} \longrightarrow \{1,2,3\}$

$1 \longmapsto 2$

$2 \longmapsto 3$

$3 \longmapsto 1$

$f_{132} : \{1,2,3\} \longrightarrow \{1,2,3\}$

$1 \longmapsto 3$

$2 \longmapsto$

$3 \longmapsto$

Portanto,

$$S_3 = \{I, f_{12}, f_{13}, f_{23}, f_{123}, f_{132}\}$$

$$|S_3| = 3! = 6.$$

④ Em S_3 temos $\langle f_{12} \rangle = \{I, f_{12}\}$, pois

- $(f_{12} \circ f_{12})(1) = f_{12}(f_{12}(1)) = f_{12}(2) = 1$
- $(f_{12} \circ f_{12})(2) = f_{12}(f_{12}(2)) = f_{12}(1) = 2$
- $(f_{12} \circ f_{12})(3) = f_{12}(f_{12}(2)) = f_{12}(3) = 3$

$\Big\} f_{12}^2(x) = x.$

$\Rightarrow (f_{12})^2 = I \Rightarrow o(f_{12}) = 2.$

Proposição 18: S_n não é abeliano se $n \geq 3$.

Prova: Basta considerar:

$f_{12} : \{1, \dots, n\} \longrightarrow \{1, \dots, n\}$ e $f_{23} : \{1, \dots, n\} \longrightarrow \{1, \dots, n\}$

$$\begin{array}{ccc} 1 & \longmapsto & 2 \\ 2 & \longmapsto & 1 \\ 3 & \longmapsto & 3 \\ \vdots & & \vdots \\ n & \longmapsto & n \end{array} \qquad \begin{array}{ccc} 1 & \longmapsto & 1 \\ 2 & \longmapsto & 3 \\ 3 & \longmapsto & 2 \\ 4 & \longmapsto & 4 \\ \vdots & & \vdots \\ n & \longmapsto & n \end{array}$$

Daí, temos

- $(f_{12} \circ f_{23})(1) = f_{12}(f_{23}(1)) = f_{12}(1) = 2$
- $(f_{23} \circ f_{12})(1) = f_{23}(f_{12}(1)) = f_{23}(2) = 3$

$\Big\} \neq$

Logo, S_n não é abeliano para $n \geq 3$. #

- Notação Matricial em S_n

Seja $\sigma \in S_n$, costuma-se denotar:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Por exemplo, $f_{123} : \{1,2,3\} \longrightarrow \{1,2,3\}$ em S_3

$$\begin{aligned} 1 &\longmapsto 2 \\ 2 &\longmapsto 3 \\ 3 &\longmapsto 1 \end{aligned}$$

fica

$$f_{123} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Nessa notação temos

- $I = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$

- O inverso de $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ é

obtido trocando as linhas:

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

Exemplo 1: Obter o inverso de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$

Basta trocar as linhas:

$$\sigma^{-1} = \begin{pmatrix} 4 & 5 & 1 & 3 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

Exemplo 2: Considere

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \quad \text{e} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Vamos compor

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \quad \checkmark$$

Sempre compomos da direita para a esquerda.

• Notação por ciclos

A notação por ciclos consiste em escrever uma permutação considerando "voltas" completas.

Por exemplo:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 3 & 2 & 7 & 1 & 4 & 9 & 6 & 8 \end{pmatrix}$$

Podemos começar por qualquer elemento, tradicionalmente se começa por 1:

- $1 \longrightarrow 5 \longrightarrow 1$ ✓
- $2 \longrightarrow 3 \longrightarrow 2$ ✓
- $4 \longrightarrow 7 \longrightarrow 9 \longrightarrow 8 \longrightarrow 6 \longrightarrow 4$ ✓

Dessa forma, escrevemos

$$\sigma = (15)(23)(47986)$$

Se algum elemento não permuta, não escrevemos:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix} = (13)(25)$$

O elemento neutro costuma ser denotado por

$$I = (1),$$

mas poderia ser $I = (2), \ldots, (n)$.

Exemplo: Na notação de ciclos:

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}$$

- Produto de Ciclos

Sempre realizado da direita para a esquerda.

Exemplos:

- $(13)(132) = (1)(23) = (23)$
- $(123)(132) = (1)(2)(3) = (1) \Rightarrow (123)^{-1} = (132)$
- $(13)(12)(14) = (1423)$
- $(13)(426)(53)(71)(5138)(92) = (15738)(2964)$
- $(123)^2 = (123)(123) = (132)$
- $(123)^3 = (123)(123)^2 = (123)(132) = (1)$ $\Rightarrow o((123)) = 3$

Obs.: Ciclos disjuntos comutam, pois não permutam elementos em comum, por exemplo:

$$(132)(54) = (54)(132).$$

Exemplo: Obter a ordem de $(12)(34)$ em S_4:

$$\begin{aligned}((12)(34))^2 &= (12)(34)(12)(34)\\ &= (12)(12)(34)(34)\\ &= (12)^2(34)^2\\ &= (1)(1) = (1)\end{aligned}$$

Daí, concluímos que

$$o((12)(34)) = 2 \quad \text{e} \quad ((12)(34))^{-1} = (12)(34).$$

Definição 19: Um ciclo que permuta r elementos é dito ser um r-ciclo:

$$\sigma = (a_1\ a_2 \cdots a_r).$$

Proposição 20: A ordem de um r-ciclo é r.

Prova: Considere o r-ciclo $\sigma = (a_1\ a_2 \dots a_i\ a_{i+1} \dots a_r)$

Veja que

$$\sigma(a_i) = a_{i+1}$$
$$\sigma^2(a_i) = \sigma(\sigma(a_i)) = \sigma(a_{i+1}) = a_{i+2}$$
$$\sigma^3(a_i) = a_{i+3}$$
$$\vdots$$
$$\sigma^{r-i}(a_i) = a_{i+r-i} = a_r$$
$$\sigma^{r-i+1}(a_i) = a_1$$
$$\sigma^{r-i+2}(a_i) = a_2$$
$$\vdots$$
$$\sigma^r(a_i) = \sigma^{r-i+i}(a_i) = a_i$$

$\Rightarrow \sigma^r = I \Rightarrow o(\sigma) = r.$ #

Exemplo: • $(1354)^4 = I$

• A ordem de $\underbrace{(24)(316)}_{\text{disjuntos}}$ é $6 = mmc(2,3)$, pois

$$((24)(316))^6 = (24)^6(316)^6 = ((24)^2)^3((316)^3)^2 = I^3 I^2 = I$$

Proposição 21: $(a_1\, a_2\, a_3 \cdots a_{r-1}\, a_r)^{-1} = (a_1\, a_r\, a_{r-1} \cdots a_3\, a_2)$

Prova: Como $\theta(\sigma) = r$, então

$$\sigma^{-1} = \sigma^{r-1}.$$

Veja que σ^{r-1} leva a_i em uma posição anterior. Daí,

$$\sigma^{r-1}(a_1) = a_r,\ \sigma^{r-1}(a_2) = a_1, \cdots,\ \sigma^{r-1}(a_{r-1}) = a_{r-2}$$

$$\sigma^{r-1}(a_r) = a_{r-1}$$

Daí,

$$\sigma^{r-1} = (a_1\, a_r\, a_{r-1}\, a_{r-2} \cdots a_3\, a_2) \quad \#$$

Exemplos:

- $(124)^{-1} = (142)$
- $(315)^{-1} = (351)$
- $\big((23)(154)\big)^{-1} = (23)^{-1}(154)^{-1} = (23)(145)$
  (↳ disjuntos)
- $\big((124)(132)\big)^{-1} = (134)^{-1} = (143)$

→ Grupos Diedrais

Considere P_n um polígono regular de n lados. Defina

$$D_n = \{ \sigma : P \to P \mid \sigma \text{ é bijeção e } \sigma(P_n) = P_n \}$$

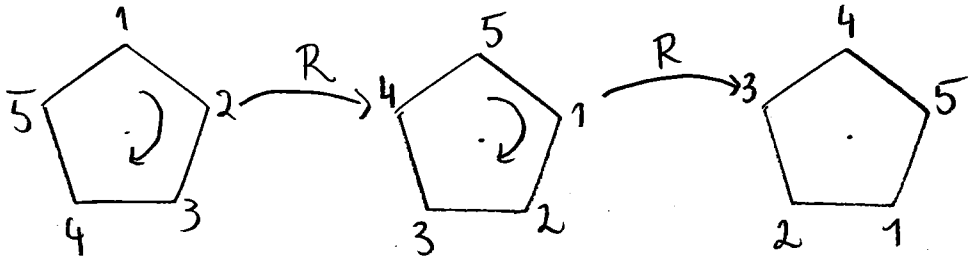
ou seja, σ não altera o polígono, é uma <u>simetria</u>.

Como $D_n \subseteq S_n$, temos que C1, C2, C3 estão satisfeitas. Ademais, D_n é fechado:

$$\sigma(\tau(P_n)) = \sigma(P_n) = P_n, \quad \forall\, \sigma, \tau \in D_n$$

Existem 2 tipos de bijeções que são invariantes em um polígono regular

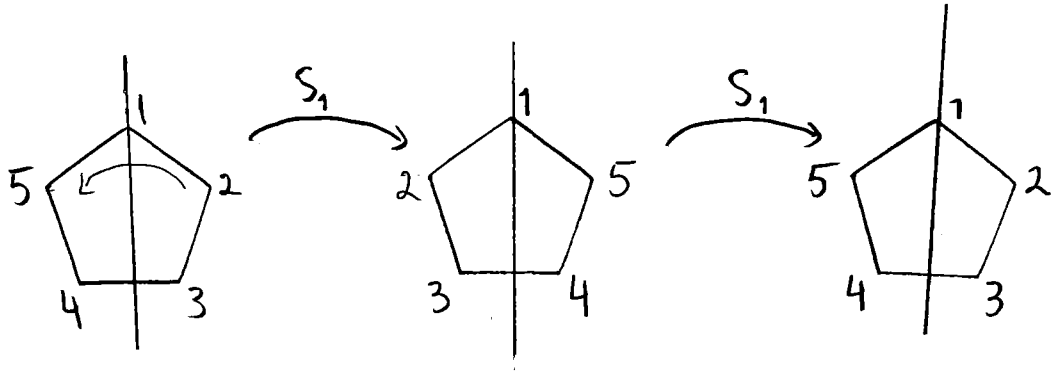
1) <u>Rotação</u>: plana no sentido horário de $\frac{2\pi}{n}$ em torno do eixo que passa pelo centro da circunferência que circunscreve P_n. Veja



Para retornar à posição original devemos fazer

$$\boxed{R^n = I}$$

2) Reflexão: rotação espacial de 180° em torno de um eixo de simetria do polígono. Veja:



Para retornar à posição original basta fazer S^2 (360°), ou seja:

$$\boxed{S^2 = I}$$

S é a operação de refletir

Em D_n temos

- n rotações: $R, R^2, \ldots, R^n = I$.
- n reflexões (uma para cada vértice)

Por esse motivo, mudamos a notação para

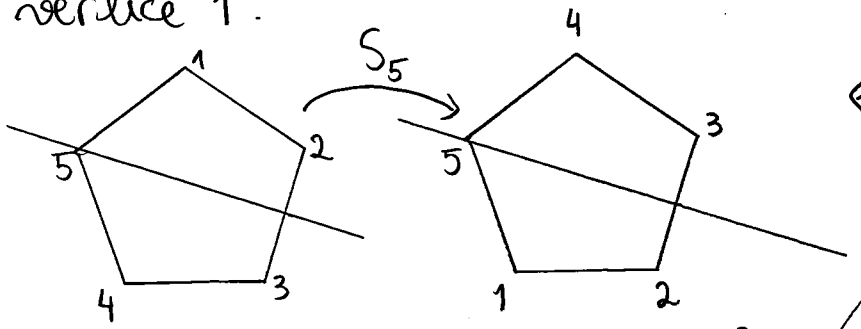
$$D_{2n},$$

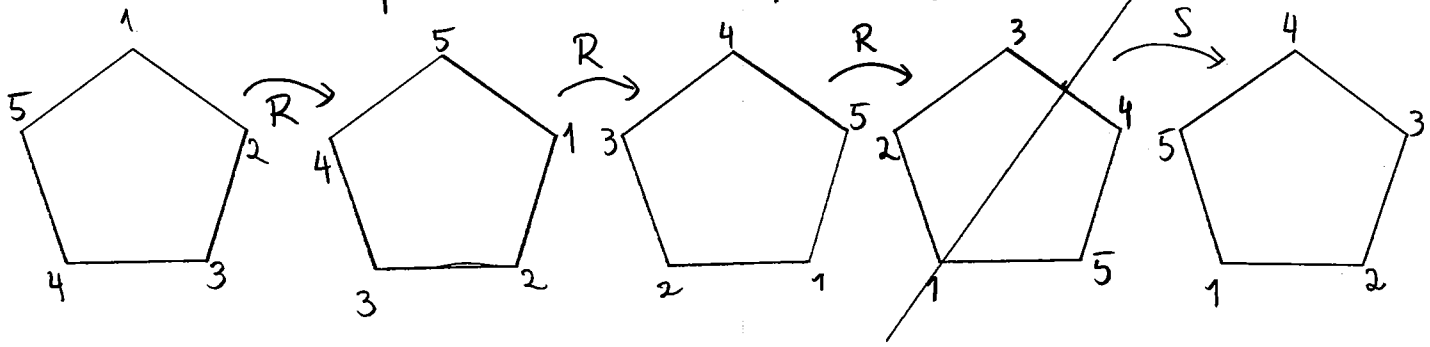
que é o <u>grupo diedral</u> de um polígono de n lados.

Podemos obter qualquer reflexão aplicando R algumas vezes e por último aplicamos S.

Vamos fixar S como a reflexão pelo eixo que passa pelo vértice 1.

Exemplo:





Observe que $S \circ R^i = SR^i$ não pode ser uma rotação, pois

$$SR^i = R^j \Rightarrow S = R^{j-i},$$

um absurdo, uma vez que reflexão e rotação são simetrias distintas.

Assim,

$$S, SR, SR^2, \cdots, SR^{n-1}$$

são as n reflexões em D_{2n}.

Portanto, escrevemos:

$$D_{2n} = \{\underbrace{I, R, R^2, \cdots, R^{n-1}}_{\text{rotações}}, \underbrace{S, SR, SR^2, \cdots, SR^{n-1}}_{\text{reflexões}}\}$$

Agora, de forma algébrica, vamos considerar:

$$R = (1\ 2\ 3\ \cdots\ n) \quad \text{e} \quad S = (2n)(3\ n-1)(4\ n-2)\cdots(i\ n+2-i)$$

Proposição: $SR = R^{-1}S = R^{n-1}S$

Prova:

- $SR = (2n)(3\ n-1)(4\ n-2)(1\ 2\ 3\ 4\ \cdots\ n-2\ \ n-1\ \ n)$

  $= (1n)(2\ n-1)(3\ n-2)\cdots$

- $R^{n-1}S = R^{-1}S$

  $= (1\ n\ n-1\ n-2\ \cdots\ 4\ 3\ 2)(2n)(3\ n-1)(4\ n-2)\cdots$

  $= (1n)(2\ n-1)(3\ n-2)\cdots$

#

Podemos escrever

$$\boxed{SR = R^{-1}S} \quad \text{ou} \quad \boxed{RS = SR^{-1}} \quad \text{ou} \quad \boxed{SRS = R^{-1}}$$

Isso implica que D_{2n} não é abeliano. Também,

$$RS = SR^{-1} \Rightarrow R^{k-1}RS = R^{k-1}SR^{-1}$$

$$\Rightarrow R^kS = S(R^{-1})^{k-1}R^{-1}$$

$$= S(R^{-1})^k$$

$$\Rightarrow \boxed{R^kS = S(R^{-1})^k} \text{ ou } \boxed{R^kS = SR^{k(n-1)}}, n \geq 3.$$

Exemplo: Conside um pentágono regular.

Temos $D_{10} = \{I, R, R^2, R^3, R^4, S, SR, SR^2, SR^3, SR^4\}$.

Vamos operar

- $R^3S = SR^{3(5-1)} = SR^{3.4} = SR^{12} = SR^2$.
- $SSR^4 = S^2R^4 = R^4$
- $SR^2R^4 = SR^6 = SR$

- $RSR = RR^{-1}S = S$
- $RSR^2 = SR^{-1}R^2 = SR$

De forma abstrata, podemos escrever:

$$D_{2n} = \langle a, b \mid a^2 = e = b^n,\ ba = ab^{-1} \rangle$$

Exemplo: De forma abstrata, se $n = 2$ temos

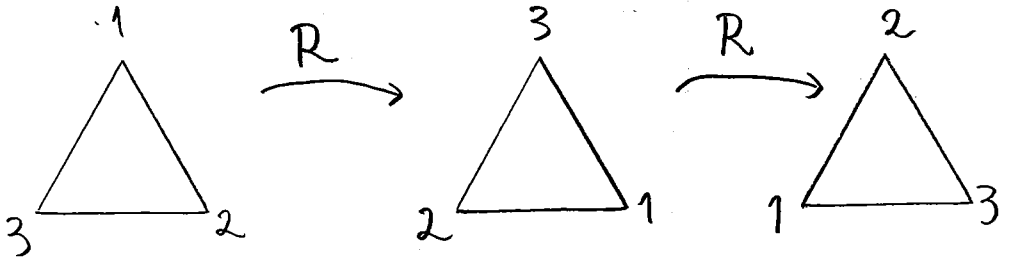
$$D_4 = \langle a, b \mid a^2 = e = b^2,\ ba = ab^{-1} = ab \rangle$$
$$= \{e, a, b, ab\}$$

Veja que D_4 é abeliano. Ademais,

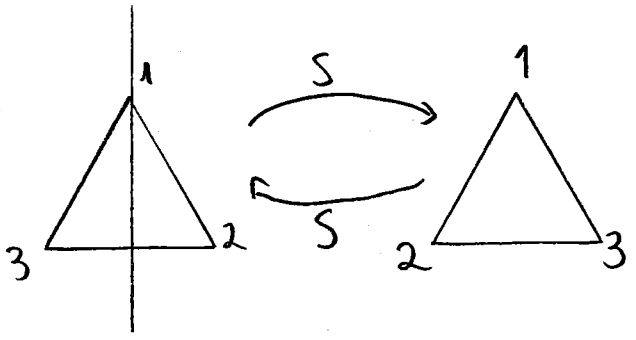
$$(ab)^2 = a^2 b^2 = ee = e$$

Portanto, $D_4 = K_4$.

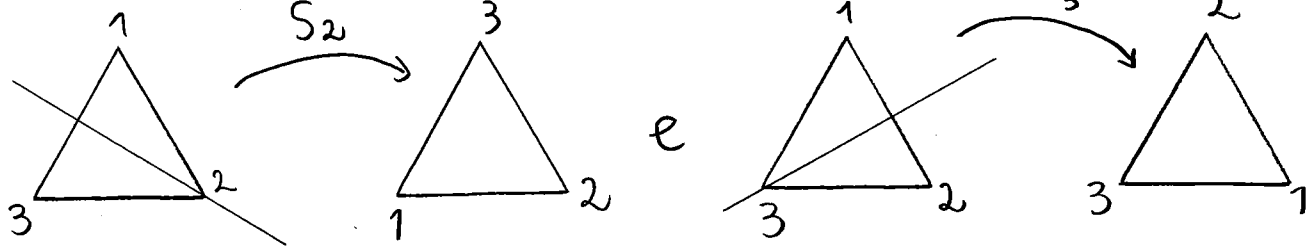
→ Grupo Diedral do triângulo equilátero

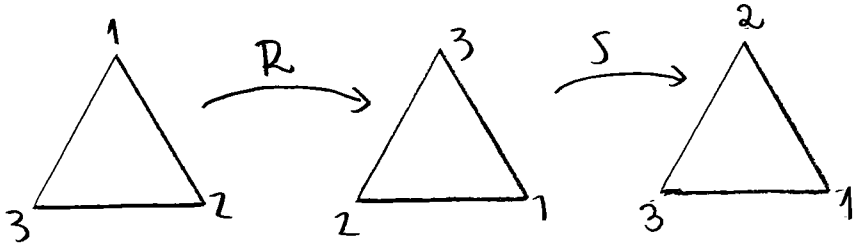


$R^3 = I$

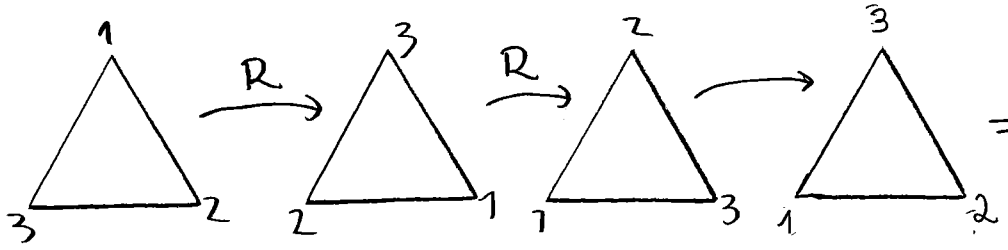


Consideremos S_2 e S_3





$\Rightarrow SR = S_3$



$\Rightarrow SR^2 = S_2$

Por fim, escrevemos

$$D_6 = \langle a, b \mid a^2 = e = b^3,\ ba = ab^{-1} = ab^2 \rangle$$
$$= \{e, a, b, b^2, ab, ab^2\}$$

Já o grupo diedral do quadrado é:

$$D_8 = \langle a, b \mid a^2 = e = b^4,\ ba = ab^3 \rangle$$
$$= \{e, a, b, b^2, b^3, ab, ab^2, ab^3\}.$$

Subgrupos

Definição 23: Um subconjunto H de G é um subgrupo se for um grupo.

Exemplo: O conjunto dos ímpares não é subgrupo de $\mathbb{Z}$, pois não possui o zero e não é fechado:

$$3+5=8 \text{ não é ímpar}$$

Notação: $H \leq G$.

Proposição 24: Seja G um grupo e $\emptyset \neq H \subseteq G$.
Se $xy^{-1} \in H$, $\forall x, y \in H$, então $H \leq G$.

Prova:

(1) Como G é associativo, temos que $H \subseteq G$ é.
(2) Para $x \in H$, vale que $xx^{-1} = e \in H$.
(3) Como $e \in H$, temos que $ex^{-1} \in H \Rightarrow x^{-1} \in H$.

Fechamento: Sejam $x, y \in H$. Daí, $y^{-1} \in H$ e

$$x(y^{-1})^{-1} = xy \in H \Rightarrow H \text{ é fechado}$$

Logo, H é grupo e portanto $H \leq G$. #

Exemplos: ⓪ $\{e\}$ e G são os subgrupos triviais de G.

① $\mathbb{Z}_+$ não é subgrupo de $\mathbb{Z}$, pois não há simétrico.

② $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$

③ $\mathbb{R}_+^* < \mathbb{R}$

④ $\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$

⑤ $\langle g \rangle < G$ é o subgrupo gerado por g.

⑥ $n\mathbb{Z} < \mathbb{Z}$

⑦ $D_{2n} < S_n$

⑧ $SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A = 1\} < GL_n(\mathbb{R})$, pois se $\det A = 1 = \det B$, então

$$\det(AB^{-1}) = \det A \det(B^{-1}) = 1 \cdot \frac{1}{\det B} = 1 \cdot \frac{1}{1} = 1 \Rightarrow AB^{-1} \in SL_n(\mathbb{R}).$$

⑨ $D_n(\mathbb{R}) < M_n(\mathbb{R})$, pois

$$\operatorname{diag}(a_1, \ldots, a_n) - \operatorname{diag}(b_1, \ldots, b_n) = \operatorname{diag}(a_1 - b_1, \ldots, a_n - b_n)$$

⑩ Sejam $g \in G$ e $H \leq G$, $gHg^{-1} := \{ghg^{-1} \mid h \in H\} \leq G$.
De fato, sejam $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$. Daí,

$$(gh_1g^{-1})(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = g(h_1h_2^{-1})g^{-1} \in gHg^{-1},$$

uma vez que $h_1h_2^{-1} \in H$, pois $H \leq G$.

Proposição 25: Todos os subgrupos de $\mathbb{Z}$ são da forma $n\mathbb{Z}$, $n \in \mathbb{Z}_+$.

Prova: Seja $H \leq G$.

Se $H = \{0\}$, então $H = 0\mathbb{Z}$

Se $H \neq \{0\}$, então existe $m \in H$, $m \neq 0$, e também temos $-m \in H$. Dessa forma, existe

$$n = \min(H \cap \mathbb{Z}_+^*)$$

Como H é subgrupo e $n \in H$ temos que $n\mathbb{Z} \subseteq H$.

Por outro lado, pelo TADE:

$$x = nq + r, \quad 0 \leq r < n, \quad x \in H$$

$\Rightarrow r = x - nq$

$\Rightarrow r \in H$, pois $x \in H$ e $n\mathbb{Z} \subseteq H$.

Como $n = \min(H \cap \mathbb{Z}_+^*)$ e $0 \leq r < n$, segue que $r = 0$.

Daí, $x = nq \Rightarrow x \in n\mathbb{Z} \Rightarrow H \subseteq n\mathbb{Z}$.

Portanto, $H = n\mathbb{Z}$. #

Obs.: Mesmo G não sendo abeliano, podemos ter $H \leq G$ abeliano. Por exemplo

$\langle i \rangle = \{1, -1, i, -i\}$ é abeliano, mesmo Q_8 não sendo.

Proposição 26: Seja G cíclico e $H \leq G$.
Então H é cíclico

Prova: Se $H = \{e\}$, então $H = \langle e \rangle$.

Se $H \neq \{e\}$, então existe $e \neq x \in H \subseteq G$.
Como G é cíclico, temos $G = \langle g \rangle$, daí podemos escrever $x = g^k$, $k \in \mathbb{Z}$. Como H é subgrupo, temos que $x^{-1} = g^{-k} \in H$. Logo, H tem potência com expoente +.

Considere $d = \min\{k \in \mathbb{Z}_+^* \mid g^k \in H\}$ e $y = g^d$.
Observe que $y \in H$. Vamos mostrar que $H = \langle y \rangle$.
Como $y \in H$, temos que $\langle y \rangle \subseteq H$.
Seja $h \in H$, Como $G = \langle g \rangle$, escrevemos $h = g^n$, pelo TADE:

$$n = dq + r, \quad 0 \leq r < d.$$

Logo,

$$g^n = g^{dq+r} = (g^d)^q g^r = y^q g^r$$

$$\Rightarrow g^r = g^n y^{-q} = h y^{-q} \in H, \text{ pois } h \in H \text{ e } \langle y \rangle \subseteq H.$$

Como $0 \leq r < d$ e $g^r \in H$, pela minimalidade de d segue que $r = 0$. Portanto, $h = g^n = (g^d)^q = y^q$.
$\Rightarrow h \in \langle y \rangle \Rightarrow H \subseteq \langle y \rangle \Rightarrow H = \langle y \rangle$. #

Classes Laterais, Subgrupos Normais e Grupo Quociente

Definição 27: Sejam G um grupo, $H \leq G$ e $g \in G$.

Definimos

- Classe lateral à esquerda de H determinada por g:

$$gH := \{gx \mid x \in H\}$$

- Classe lateral à direita de H determinada por g:

$$Hg := \{xg \mid x \in H\}$$

Obs.:

1) $eH = H = He$
2) $g \in gH, Hg$, pois $g = ge = eg$.
3) Se $x \in H$, então $xH = H = Hx$, pois H é subgrupo.
4) Se G é aditivo, denotamos $g + H$ e $H + g$.
5) gH e Hg nem sempre são subgrupos de G.
6) Se G é abeliano, então

$$gH = \{gx \mid x \in H\} = \{xg \mid x \in H\} = Hg.$$

Exemplos:

① $3+2\mathbb{Z} = \{\dots, -3, -1, 1, 3, 5, 7, \dots\}$ (não é grupo)

$= 2\mathbb{Z}+3$

② Em D_6, temos $\langle a\rangle = \{e, a\}$. Daí,

- $b\langle a\rangle = \{b, ba\} = \{b, ab^2\}$
- $\langle a\rangle b = \{b, ab\}$

$\Rightarrow b\langle a\rangle \neq \langle a\rangle b$

③ Em $\mathbb{Z}_{10}$, considere $H = \langle \overline{2}\rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$

- $\overline{4} + H = \{\overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}\} = \{\overline{4}, \overline{6}, \overline{8}, \overline{0}, \overline{2}\} = H$
- $\overline{7} + H = \{\overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{15}\} = \{\overline{7}, \overline{9}, \overline{1}, \overline{3}, \overline{5}\}$

Proposição 28: Seja $H \leq G$ finito, então

$$\#(xH) = \#(yH), \ \forall x, y \in G.$$

Prova: Provemos que $f: xH \longrightarrow yH$ é bijecção.
$xh \longmapsto yh$

- **Injetiva:**

Se $f(xh) = f(xh')$, então

$$yh = yh' \Rightarrow h = h' \Rightarrow xh = xh'.$$

• Sobrejetiva: Seja $yh \in yH$. Daí,

$$yh = f(xh) \Rightarrow f \text{ é sobrejetivo.}$$

Como $\#$ é finito, xH e yH são finitos. Logo,

$$\#(xH) = \#(yH). \quad \#$$

Obs:

1) Seja $g \in G$ e $H \leq G$. Daí,

$$\#(gH) = \#(eH) = \#(H) = |H|,$$

isto é,

$$\boxed{\#(gH) = |H|}$$

2) A proposição anterior também vale para classes laterais à direita.

Definição 29: Considere a seguinte relação em G:

$$xRy \Leftrightarrow x^{-1}y \in H$$

Vamos provar que R é de equivalência:

- Reflexiva: $x^{-1}x = e \in H \Rightarrow xRx$
- Simétrica:

$$xRy \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} \in H$$
$$\Rightarrow y^{-1}x \in H \Rightarrow yRx$$

- Transitiva:

$$xRyRz \Rightarrow x^{-1}y, y^{-1}z \in H$$
$$\Rightarrow x^{-1}yy^{-1}z = x^{-1}z \in H \Rightarrow xRz.$$

Dessa forma, podemos obter a classe de equivalência de $g \in G$:

$$\overline{g} = \{x \in G \mid gRx\}$$
$$= \{x \in G \mid g^{-1}x \in H\}$$
$$= \{x \in G \mid g^{-1}x = h \in H\}$$
$$= \{x \in G \mid x = gh,\ h \in H\}$$
$$= \{gh \mid h \in H\}$$
$$= gH$$

Logo, as classes de equivalência são classes laterais.

Obs.: 1) As classes laterais são disjuntas, pois são classes de equivalência, ou seja,

$$xH = yH \iff xRy \iff x^{-1}y \in H.$$

2) Veja que

$$gH = H \iff e^{-1}g \in H \iff g \in H.$$

3) Vale que

$$xH = yH \quad \text{ou} \quad xH \cap yH = \emptyset.$$

Podemos definir o conjunto quociente:

$$G/R = \{\bar{g} \mid g \in G\}$$
$$= \{gH \mid g \in G\} := G/H$$

Definição 30: Seja G finito e $H \leq G$.

O <u>índice de H em G</u> é

$$[G : H] = \#(G/H).$$

Exemplos: ① Observe que

$$\{\overline{4} + \langle \overline{2} \rangle\} \cup \{\overline{7} + \langle \overline{2} \rangle\} = \mathbb{Z}_{10}$$

Dessa forma, $[\mathbb{Z}_{10} : \langle \overline{2} \rangle] = 2$.

② Considere $H = \langle a \rangle = \{e, a\}$ em D_6.

Temos:

- $e\,H = (H)$
- $a\,H = \{a, a^2\} = \{e, a\} = (H)$
- $b\,H = \{b, ba\} = \boxed{\{b, ab^2\}}$
- $b^2 H = \{b^2, b^2 a\} = \{b^2, ab\}$
- $ab\,H = \{ab, aba\} = \{b^2, ab\}$
- $ab^2 H = \{ab^2, ab^2 a\} = \boxed{\{b, ab^2\}}$

$\to b^2 a = bba$
$= b\,ab^2$
$= ab^2 b^2$
$= a\,b^3 b$
$= ab$ //

$\to aba = a\,ab^2$
$= a^2 b^2 = b^2$ //

$\to ab^2 a = a\,ab$
$= a^2 b = b$

Portanto,

$$G/_H = \{H, bH, b^2 H\}.$$

E assim,

$$[D_6 : \langle a \rangle] = 3.$$

Definição 31: Um subgrupo H de G é dito ser normal se

$$gH = Hg, \ \forall g \in G.$$

Notação: $H \trianglelefteq G$.

Obs.: Escrever $gH = Hg$ é uma igualdade de conjuntos, não significa que $gx = xg$, $x \in H$.

$$gH = Hg \iff \forall x \in H \ \exists y \in H \mid gx = yg.$$

Exemplos:

① Os subgrupos triviais $\{e\}$ e G são normais.
De fato,

- $g\{e\} = \{g\} = \{e\}g$
- $gG = G = Gg$

② $H = \langle (12) \rangle = \{(1), (12)\}$ não é normal em S_3.
De fato, $\#((23)H) = \#(H(23)) = |H| = 2$.
Daí,

- $(23)H = \{(23), (23)(12) = (132)\}$ $\Big\}$ $\neq$
- $H(23) = \{(23), (12)(23) = (123)\}$ $\Big\}$

Proposição 32: Todo subgrupo de um grupo abeliano é normal.

Prova: $gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg$.

Obs.: Isso não significa que um subgrupo abeliano é normal.

Exemplos

1) $n\mathbb{Z} \triangleleft \mathbb{Z}$

2) $\mathbb{Q}^* \triangleleft \mathbb{R}^* \triangleleft \mathbb{C}^*$

3) $\langle \bar{a} \rangle \triangleleft \mathbb{Z}_n$

Caracterização de subgrupo normal

Lembre que

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\} \leq G.$$

Observe que

$$|gHg^{-1}| = \#((gHg^{-1})g)$$
$$= \#(gH) = |H|$$

Proposição 33 $H \trianglelefteq G \iff gHg^{-1} = H$, $\forall g \in G$.

Prova:

($\Leftarrow$) Vamos mostrar que $gH \subseteq Hg$ e $gH \supseteq Hg$:

($\subseteq$) Considere $gh_1 \in gH$. Temos que $gh_1g^{-1} \in gHg^{-1} = H$. Daí,

$$gh_1g^{-1} = h_2 \in H \Rightarrow gh_1 = h_2g \in Hg \Rightarrow gH \subseteq Hg.$$

($\supseteq$) Seja $h_3g \in Hg$. Temos

$$g^{-1}h_3(g^{-1})^{-1} \in g^{-1}H(g^{-1})^{-1} = H$$

$$\Rightarrow g^{-1}h_3g \in H \Rightarrow g^{-1}h_3g = h_4 \in H$$

$$\Rightarrow h_3g = gh_4 \Rightarrow Hg \subseteq gH.$$

($\Rightarrow$) Seja $H \trianglelefteq G$, provemos que $H \subseteq gHg^{-1}$ e $H \supseteq gHg^{-1}$.

($\subseteq$) Se $h \in H$, escreveremos

$$h = g(g^{-1}hg)g^{-1} \underset{\text{normal}}{=} g(g^{-1}gh')g^{-1} = gh'g^{-1} \in gHg^{-1}.$$

($\supseteq$) Se $ghg^{-1} \in gHg^{-1}$, então

$$ghg^{-1} = h''gg^{-1} = h'' \in H \Rightarrow gHg^{-1} \subseteq H. \quad \#$$

Obs. importante:

Basta provarmos que $\boxed{gHg^{-1} \subseteq H.}$
De fato,

$ghg^{-1} \in H, \forall g \in G \Rightarrow g^{-1}hg \in H$

Daí, considerando $gHg^{-1} \subseteq H$, temos

$$h = g(\underbrace{g^{-1}hg}_{\in H})g^{-1} \in gHg^{-1} \Rightarrow H \subseteq gHg^{-1}.$$

Moral da história: $H \trianglelefteq G \Leftrightarrow gHg^{-1} \subseteq H$

Exemplos:

① $D_2^*(\mathbb{R})$ não é normal a $GL_2(\mathbb{R})$.

Tome $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$ e $X = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in D_2^*(\mathbb{R})$.

Veja que

$$AXA^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \notin D_2^*(\mathbb{R}).$$

(2) $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$, pois

$A \in GL_n(\mathbb{R})$ e $X \in SL_n(\mathbb{R})$

$\Rightarrow \det(AXA^{-1}) = \det A \det X \det A^{-1}$

$= \det A \cdot 1 \cdot \frac{1}{\det A} = 1$

$\Rightarrow AXA^{-1} \in SL_n(\mathbb{R})$.

Grupo Quociente

Defina o conjunto:

$$(aH)(bH) = \{ah_1bh_2 \mid h_1, h_2 \in H\}$$

Proposição 34: $H \trianglelefteq G \Leftrightarrow (aH)(bH) = (ab)H$, $\forall a, b \in G$.

Prova:

($\Rightarrow$) Vamos provar que $(aH)(bH) \overset{\subseteq}{\supseteq} (ab)H$.

($\subseteq$) Considere $ah_1bh_2 \in (aH)(bH)$, $h_1, h_2 \in H$.

Como $H \trianglelefteq G$, temos $h_1b = bh_3$, para certo $h_3 \in H$.

Daí, $ah_1bh_2 = ab\underbrace{h_3h_2}_{\in H} \in (ab)H \Rightarrow (aH)(bH) \subseteq (ab)H$.

($\supseteq$) Seja $(ab)h \in H$. Daí,

$abh = aebh \in (aH)(bH)$

$\Rightarrow (ab)H \subseteq (aH)(bH)$.

($\Leftarrow$) Se $(aH)(bH) = (ab)H$, $\forall\, a, b \in G$, então dado $g \in G$ temos

$$(gH)(g^{-1}H) = (gg^{-1})H$$
$$= eH = H$$

$$\Rightarrow ghg^{-1}h_1 = h_2, \quad h, h_1, h_2 \in H$$

$$\Rightarrow ghg^{-1} = h_2 h_1^{-1} \in H, \ \forall\, h \in H.$$

$$\Rightarrow gHg^{-1} \subseteq H \Rightarrow H \trianglelefteq G.$$

#

Moral da história: Se $H \trianglelefteq G$, então definimos o seguinte produto em G/H:

$$(aH)(bH) = (ab)H.$$

Proposição 35: G/H é grupo $\Leftrightarrow H \trianglelefteq G$.

Prova: ($\Rightarrow$) Se G/H é grupo, temos

$$(aH)(bH) = (ab)H$$

$$\Rightarrow H \trianglelefteq G.$$

($\Leftarrow$) Se $H \trianglelefteq G$, então $(aH)(bH) = (ab)H$.

Daí,

C1) $aH(bHcH) = a((bc)H)$

$= (a(bc))H$

$= ((ab)c)H$

$= ((ab)H)(cH$

$= (aHbH)cH$

C2) o elemento neutro é $eH = H$:

$(eH)(aH) = (ea)H = aH = (aH)(eH)$.

C3) O inverso de aH é $a^{-1}H$:

$(aH)(a^{-1}H) = (aa^{-1})H = eH = H$

Logo, G/H é grupo. #

Definição 36: Se $H \trianglelefteq G$, G/H é o grupo quociente de G por H.

A ordem de G/H é:

$$|G/H| = [G:H].$$

Obs.:

1) $G/\{e\} = \{\{g\} \mid g \in G\} \Rightarrow |G/\{e\}| = |G|$

2) $G/G = \{G\} \Rightarrow |G/G| = 1.$

3) Se G é abeliano, então

$$(aH)(bH) = (ab)H = (ba)H = (bH)(aH)$$

$$\Rightarrow G/H \text{ é abeliano}$$

4) Se $G = \langle g \rangle$ é cíclico, então para $a \in G$ temos:

$$aH = g^k H = \underbrace{(gH)\cdots(gH)}_{k \text{ vezes}}$$

$$= (gH)^k$$

$$\Rightarrow G/H = \langle gH \rangle \Rightarrow G/H \text{ é cíclico.}$$

5) Se $N \trianglelefteq G$ e $N \subseteq H \leq G$, então $N \trianglelefteq H$ e podemos definir também H/N.

Exemplo

Como $\mathbb{Z}$ é abeliano, $n\mathbb{Z} < \mathbb{Z}$, temos que $\mathbb{Z}/n\mathbb{Z}$ é grupo.

Observe que

$$\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} \mid x \in \mathbb{Z}\}$$

Mas $x + n\mathbb{Z}$ é a classe de equivalência de x considerando a congruência módulo n. Daí,

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} &= \{x + n\mathbb{Z} \mid x \in \mathbb{Z}\} \\ &= \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\} \\ &= \mathbb{Z}_n.\end{aligned}$$

Portanto, podemos interpretar o grupo $\mathbb{Z}_n$ como sendo o grupo quociente $\mathbb{Z}/n\mathbb{Z}$.

Teorema de Lagrange

Seja G finito e $H \leq G$, então $|H|$ divide $|G|$.

Prova: Considere $[G : H] = r$.

Daí, temos $g_1H, g_2H, \dots, g_rH$ classes laterais.

Temos

$$G = \bigcup_{i=1}^{r} g_iH$$

$$\Rightarrow |G| = \#(g_1H) + \cdots + \#(g_rH)$$

$$= \underbrace{|H| + \cdots + |H|}_{r \times} = r|H| \Rightarrow |H| \,|\, |G| \quad \#$$

O Teorema de Lagrange resignifica o índice:

$$\boxed{[G : H] = \frac{|G|}{|H|}}$$

Se $H \trianglelefteq G$, temos

$$\boxed{|G/H| = \frac{|G|}{|H|}}$$

Exemplo: Um grupo de ordem 12 só pode ter subgrupos de ordem $1, 2, 3, 4, 6, 12$.

Obs.: Se G é finito, então pelo Teorema de Lagrange:

$$o(g) = |\langle g \rangle| \text{ divide } |G|.$$

Proposição 37: Se $|G| = n$, então $g^n = e$, $\forall g \in G$.

Prova: Se $o(g) = m$, então $m \mid |G| = n$. Daí,

$$n = mK \Rightarrow g^n = g^{mK} = (g^m)^K = e^K = e. \quad \#$$

Exemplo: Em S_3 não há elemento de ordem 4.

Exemplo: G é dito ser um p-grupo se $|G| = p^k$, onde p é primo.

Seja $H \leq G$, onde G é um p-grupo.

Pelo Teorema de Lagrange,

$$|H| \mid |G| = p^k \Rightarrow |H| = p^m, \quad m \leq K$$

logo, um subgrupo de um p-grupo é também um p-grupo.

Proposição 38: Se $|G| = p$, p primo, então G é cíclico.

Prova: Considere $g \in G$, $g \neq e$. Temos que

$$|\langle g \rangle| \;|\; |G| = p \Rightarrow |\langle g \rangle| = 1 \text{ ou } p.$$

Como $g \neq e$, segue que $|\langle g \rangle| = p$.
Daí, $\langle g \rangle = G$. Portanto, G é cíclico. #

Exemplo: Subgrupos de S_3.

Pelo Teorema de Lagrange, S_3 só pode ter subgrupos de ordem:

- 1 : $\{e\}$
- 6 : S_3
- 2 e 3, que serão cíclicos pela proposição anterior:

→ ordem 2 : $\langle (12) \rangle$, $\langle (13) \rangle$ e $\langle (23) \rangle$

→ ordem 3 : $\langle (123) \rangle = \langle (132) \rangle$

São somente 4 subgrupos não triviais.

Homomorfismos

Definição 39: Sejam $(G_1, *)$ e $(G_2, \cdot)$ grupos.

Uma aplicação $f: G_1 \to G_2$ é um homomorfismo se satisfaz:

$$f(\underbrace{x * y}_{\text{em } G_1}) = \underbrace{f(x) \cdot f(y)}_{\text{em } G_2}$$

Por praticidade, usaremos a notação por justaposição:

$$f(xy) = f(x)f(y)$$

Exemplos:

① $f: G_1 \longrightarrow G_2$ é homomorfismo
$x \longmapsto e_2$

Veja que

$$f(xy) = e_2 = e_2 e_2 = f(x)f(y).$$

② $I: G \to G$ é homomorfismo, pois
$x \longmapsto x$

$$f(xy) = xy = f(x)f(y).$$

③ $f : \mathbb{Z} \longrightarrow n\mathbb{Z}$ é homom., pois
$x \longmapsto nx$

$$f(x+y) = n(x+y) = nx + ny = f(x) + f(y)$$

④ $f : \mathbb{R} \longrightarrow \mathbb{R}^*$ é homom., pois
$x \longmapsto e^x$

$$f(x+y) = e^{x+y} = \underbrace{e^x}_{>0}\ \underbrace{e^y}_{>0} = f(x)\,f(y).$$

⑤ Considere $f : \mathbb{C} \longrightarrow M_2(\mathbb{R})$ dada por

$$f(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Temos

$$\begin{aligned} f(z+w) &= f(a+bi+c+di) \\ &= f(a+c+i(b+d)) \\ &= \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\ &= f(a+bi) + f(c+di) = f(z) + f(w). \end{aligned}$$

é homom.

⑥ $f: \mathbb{C} \longrightarrow \mathbb{R}^2$ é homom., pois
$a+bi \longmapsto (a,b)$

$$\begin{aligned} f(a+bi+c+di) &= f(a+c+i(b+d)) \\ &= (a+c, b+d) \\ &= (a,b)+(c,d) \\ &= f(a+bi)+f(c+di). \end{aligned}$$

⑦ $f: GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$ é homom., pois
$A \longmapsto \det A$

$$f(AB) = \det(AB) = \det A \det B = f(A) f(B).$$

⑧ $f: \mathbb{Z} \longrightarrow \mathbb{Z}_n$ é homom., pois
$x \longmapsto \overline{x}$

$$f(x+y) = \overline{x+y} = \overline{x} + \overline{y} = f(x) + f(y).$$

⑨ $f: K_4 \subset S_4 \longrightarrow D_4$ é homomorfismo.

$$\begin{aligned} (1) &\longmapsto e \\ (12)(34) &\longmapsto a \\ (13)(24) &\longmapsto b \\ (14)(23) &\longmapsto ab \end{aligned}$$

(10) $\pi : G \longrightarrow G/N$ é homom., pois

$g \longmapsto gN$

$$\pi(xy) = xyN = (xN)(yN) = \pi(x)\,\pi(y).$$

Proposição 40 (Propriedades) Seja $f: G_1 \to G_2$ um homom.

1) $f(e_1) = e_2$

2) $f(x^{-1}) = (f(x))^{-1}$

3) $f(x^n) = (f(x))^n$

Prova: Seja $x \in G_1$.

1) $f(x)\,f(e_1) = f(x\,e_1) = f(x)$
$f(e_1)\,f(x) = f(e_1 x) = f(x)$ $\Rightarrow f(e_1) = e_2$.

2) $f(x^{-1})\,f(x) = f(x^{-1}x) = f(e_1) = e_2$
$f(x)\,f(x^{-1}) = f(xx^{-1}) = f(e_1) = e_2$ $\Rightarrow (f(x))^{-1} = f(x^{-1})$.

3) $f(x^n) = f(\underbrace{x \cdot x \cdots x}_{n\times})$

$= \underbrace{f(x) \cdots f(x)}_{n\times} = (f(x))^n$. #

Alguns nomes:

1) $f: G \to G$ homom. é um endomorfismo.

2) $f: G_1 \to G_2$ homom. injetivo é um monomorfismo.

3) $f: G_1 \to G_2$ homom. sobrejetivo é um epimorfismo.

4) $f: G_1 \to G_2$ homom. bijetor é um isomorfismo.

Notação: $G_1 \cong G_2$

5) $f: G \to G$ isomorfismo é um automorfismo.

Exemplo: Vamos caracterizar os endomorfismos em $\mathbb{Z}$. Veja que

- $f(0) = 0 = 0 f(1)$
- Se $n \in \mathbb{Z}_+^*$, $f(n) = f(\overbrace{1 + \cdots + 1}^{n\times}) = \underbrace{f(1) + \cdots + f(1)}_{n\times} = n f(1)$
- Se $n \in \mathbb{Z}_-^*$, então $f(n) = -f(-n) = -(-n) f(1) = n f(1)$ (↳ $+$)

Portanto, os endomorfismos em $\mathbb{Z}$ são da forma:

$$f(n) = n f(1)$$

Lembrando:

i) f é injetivo $\Leftrightarrow$ $f(x) = f(y) \Rightarrow x = y$

ii) $f: G_1 \to G_2$ é sobrejetivo $\Leftrightarrow$ $\forall\, y \in G_2 \; \exists\, x \in G_1 \mid y = f(x)$.

Exemplos: o) $f(x) = \bar{x}$ não é injetivo, pois $\bar{n} = \bar{0}$, $n \neq 0$.

① $f: \mathbb{Z} \longrightarrow n\mathbb{Z}$, $f(x) = nx$

i) $f(x) = f(y) \Rightarrow nx = ny \Rightarrow x = y \Rightarrow f$ é injetivo.

ii) $n\mathbb{Z} \ni nx = f(x)$, $x \in \mathbb{Z} \Rightarrow f$ é sobrejetivo.

② $f: \mathbb{R} \longrightarrow \mathbb{R}^*$, $f(x) = e^x$.

i) $f(x) = f(y) \Rightarrow e^x = e^y \Rightarrow x = y \Rightarrow f$ é injetivo

ii) Como $e^x > 0$, $\forall\, x \in \mathbb{R}$, $y \in \mathbb{R}_-$ não pode ser escrito como e^x para algum $x \in \mathbb{R}$. Logo, f não é sobrejetivo.

③ $\pi: G \to G/N$, $\pi(g) = gN$.

i) $\pi(x) = \pi(y) \Rightarrow xN = yN \Rightarrow xy^{-1} \in N \Rightarrow f$ não é injetivo.

ii) Seja $gN \in G/N$, temos

$$gN = \pi(g) \Rightarrow \pi \text{ é sobrejetivo}$$

Definição 41: A imagem do homom. $f: G_1 \to G_2$ é o conjunto

$$Im(f) = f(G_1) = \{f(x) \mid x \in G_1\}.$$

Exemplo: $f: \mathbb{R} \to \mathbb{R}^*$, $f(x) = e^x$.

$Im(f) = f(\mathbb{R}) = \mathbb{R}_+^*$, pois $e^x > 0$.

Proposição 42: Seja $f: G_1 \to G_2$ um epimorfismo. Daí,

1) G_1 abeliano $\Rightarrow$ G_2 abeliano

2) $G_1 = \langle a \rangle \Rightarrow G_2 = \langle f(a) \rangle$.

3) $N \trianglelefteq G_1 \Rightarrow f(N) \trianglelefteq G_2$

Prova:

1) Sejam $x, y \in G_2$. Como f é sobrejetivo, existem $a, b \in G_1$ tais que $x = f(a)$ e $y = f(b)$. Daí,

$$xy = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = yx$$

(G_1 é abeliano)

Logo, G_2 é abeliano.

2) Se $y \in G_2$, existe $x \in G_1$ tal que $y = f(x)$.
Como $x \in G_1 = \langle a \rangle$ temos $x = a^n$. Daí,

$$y = f(x) = f(a^n) = (f(a))^n$$

$\Rightarrow G_2 = \langle f(a) \rangle \Rightarrow G_2$ é cíclico

3) $y \in G_2 \Rightarrow y = f(x)$, $x \in G_1$. Seja $a \in f(N)$.
Daí, $a = f(n)$, $n \in N$. Logo,

$$\begin{aligned} y a y^{-1} &= f(x) f(n) (f(x))^{-1} \\ &= f(x) f(n) f(x^{-1}) \\ &= f(x n x^{-1}) \in f(N), \end{aligned}$$

pois $N \trianglelefteq G_1 \Rightarrow x n x^{-1} \in N$. Portanto, $f(N) \trianglelefteq G_2$. #

Proposição 43: Se $f: G_1 \to G_2$ é isomorfismo, então

$$o(g) = o(f(g)), \ \forall g \in G_1.$$

Prova: Sejam $o(g) = n$ e $o(f(g)) = m$. Daí,

$$[f(g)]^n = f(g^n) = f(e_1) = e_2 \Rightarrow \boxed{m \mid n}.$$

Ademais,

$$f(e_1) = e_2 = [f(g)]^m = f(g^m) \overset{\text{injetivo}}{\Rightarrow} g^m = e_1 \Rightarrow \boxed{n \mid m}.$$

Portanto, $n = m$. #

Exemplos:

① $S_3 \not\cong \mathbb{Z}_6$, pois S_3 não é abeliano e $\mathbb{Z}_6$ é.

② $K_4 \not\cong \mathbb{Z}_4$, pois $\mathbb{Z}_4$ é cíclico e K_4 não é.

③ $K_4 \not\cong \mathbb{Z}_4$, pois $o(\bar{1}) = o(\bar{3}) = 4$ em K_4 temos $o(a) = o(b) = o(ab) = 2$.

④ Seja $f: \mathbb{Z} \to \mathbb{Z}$ um automorfismo, como $\mathbb{Z} = \langle 1 \rangle$ temos que $\mathbb{Z} = \langle f(1) \rangle \Rightarrow f(1) = \pm 1 \Rightarrow \begin{cases} f(x) = x \cdot 1 = x \\ f(x) = x(-1) = -x \end{cases}$

Definição 44: Seja $f: G_1 \to G_2$ um homom.

O <u>núcleo</u> de f é o conjunto:

$$\operatorname{Ker} f = \{ x \in G_1 \mid f(x) = e_2 \}$$

Exemplos:

1) Seja $f: \mathbb{R} \to \mathbb{R}^*$ dada por $f(x) = e^x$.

Temos

$$\operatorname{Ker} f = \{ x \in \mathbb{R} \mid f(x) = e^x = 1 \}$$
$$= \{0\}.$$

2) $f: \mathbb{Z} \to \mathbb{Z}_n$.

Temos que

$$\begin{aligned} \operatorname{Ker} f &= \{x \in \mathbb{Z} \mid f(x) = \overline{x} = \overline{0}\} \\ &= \{x \in \mathbb{Z} \mid x \in n\mathbb{Z}\} \\ &= n\mathbb{Z}. \end{aligned}$$

3) Seja $f(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Veja que

$$\operatorname{Ker} f = \left\{a+bi \in \mathbb{C} \mid f(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}$$

$$\begin{aligned} &= \{a+bi \in \mathbb{C} \mid a = 0 = b\} \\ &= \{0\} \end{aligned}$$

4) $f: GL_n(\mathbb{R}) \to \mathbb{R}^*$ dada por $f(A) = \det A$.

Temos

$$\begin{aligned} \operatorname{Ker} f &= \{A \in GL_n(\mathbb{R}) \mid f(A) = 1\} \\ &= \{A \in GL_n(\mathbb{R}) \mid \det A = 1\} \\ &= SL_n(\mathbb{R}) \end{aligned}$$

Proposição 45: Seja $f: G_1 \to G_2$ um homom. Daí,

1) $\mathrm{Im} f \leq G_2$

2) $\ker f \trianglelefteq G_1$

3) f é injetivo $\Leftrightarrow \ker f = \{e_1\}$.

Prova:

1) Considere $x, y \in \mathrm{Im} f$. Daí, $x = f(a)$ e $y = f(b)$, para $a, b \in G_1$. Daí,

$$xy^{-1} = f(a)[f(b)]^{-1} = f(a) f(b^{-1})$$
$$= f(ab^{-1}) \in \mathrm{Im} f$$

Logo, $xy^{-1} \in \mathrm{Im} f \Rightarrow \mathrm{Im} f \leq G_2$.

2) Sejam $a, b \in \ker f$. Daí, $f(a) = e_2 = f(b)$

$\Rightarrow f(ab^{-1}) = f(a) f(b^{-1}) = e_2 (f(b))^{-1} = e_2 \cdot e_2^{-1} = e_2$

$\Rightarrow ab^{-1} \in \ker f \Rightarrow \ker f \leq G_1$.

Agora, considere $g \in G_1$ e $h \in \ker f$. Daí,

$f(ghg^{-1}) = f(g) f(h) f(g^{-1}) = f(g) e_2 (f(g))^{-1} = e_2$

$\Rightarrow ghg^{-1} \in \ker f \Rightarrow \ker f \trianglelefteq G_1$.

3)

($\Rightarrow$) Seja $x \in \ker f$. Daí,

$$f(x) = e_2 = f(e_1) \xrightarrow[\text{injetivo}]{} x = e_1 \Rightarrow \ker f = \{e_1\}.$$

($\Leftarrow$) Sejam $x, y \in G_1$. Daí,

$$f(x) = f(y) \Rightarrow f(x)[f(y)]^{-1} = e_2$$

$$\Rightarrow f(x) f(y^{-1}) = e_2$$

$$\Rightarrow f(xy^{-1}) = e_2$$

$$\Rightarrow xy^{-1} \in \ker f$$

$$\Rightarrow xy^{-1} = e_2$$

$$\Rightarrow x = y$$

$\Rightarrow f$ é injetivo. $\#$

Exemplo:

- $f: \mathbb{R} \to \mathbb{R}^*$, $f(x) = e^x$, é injetivo, pois $\ker f = 0$.
- $f: GL_n(\mathbb{R}) \to \mathbb{R}^*$, $f(A) = \det A$, não é injetivo, pois $\ker f = SL_n(\mathbb{R}) \neq \{I_n\}$

- $f : \mathbb{C} \to M_2(\mathbb{R})$, $f(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, é injetivo.
- $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(x) = \bar{x}$, não é injetivo pois

$$\ker f = n\mathbb{Z} \neq \{0\}.$$

- Em $\pi : G \to G/N$ temos

$$g \longmapsto gN$$

$$\ker \pi = \{g \in G \mid \pi(g) = gN = N\}$$

$$= \{g \in G \mid g \in N\}$$

$$= N \neq \{e\}$$

logo, π não é injetivo.

Teorema do isomorfismo

Seja $f : G \to J$ homomorfismo, então

$$G/\ker f \cong \operatorname{Im} f$$

Prova: Considere a aplicação

$$\varphi : G/\ker f \longrightarrow \operatorname{Im} f$$
$$g\ker f \longmapsto f(g)$$

- φ está bem definida: não depende do representante

$$a\ker f = b\ker f \Rightarrow a^{-1}b \in \ker f$$
$$\Rightarrow f(a^{-1}b) = e_J$$
$$\Rightarrow f(a^{-1})\, f(b) = e_J$$
$$\Rightarrow [f(a)]^{-1} f(b) = e_J$$
$$\Rightarrow f(a) = f(b)$$
$$\Rightarrow \varphi(a\ker f) = \varphi(b\ker f) \quad \checkmark$$

- φ é homomorfismo:

$$\varphi(a\ker f \; b\ker f) = \varphi((ab)\ker f)$$
$$= f(ab)$$
$$= f(a)\, f(b)$$
$$= \varphi(a\ker f)\, \varphi(b\ker f). \quad \checkmark$$

- φ é injetivo:

$$\ker\varphi = \{a\ker f \mid \varphi(a\ker f) = e_J\}$$
$$= \{a\ker f \mid f(a) = e_J\}$$
$$= \{a\ker f \mid a \in \ker f\}$$
$$= \ker f = e_{G/\ker f} \Rightarrow \varphi \text{ é injetivo}$$

- φ é sobrejetivo:

Seja $y \in \operatorname{Im} f$. Daí,

$$y = f(x) = \varphi(x\ker f) \Rightarrow \varphi \text{ é sobrejetivo.}$$

Portanto, φ é um isomorfismo:

$$G/\ker f \simeq \operatorname{Im} f.$$

#

Exemplos:

① $f: \mathbb{Z} \to \mathbb{Z}_n$, $f(x) = \overline{x}$.

Veja que f é sobrejetivo.

Como $\operatorname{Ker} f = n\mathbb{Z}$, temos

$$\mathbb{Z}/n\mathbb{Z} \cong \operatorname{Im} f = \mathbb{Z}_n$$

② $f: GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$, $f(A) = \det A$.

Veja que

$$x \in \mathbb{R}^* \Rightarrow x = \det(\operatorname{diag}(\underbrace{x, 1, \ldots, 1}_{n}))$$

$$\Rightarrow \operatorname{Im} f = \mathbb{R}^*$$

Daí, pelo Teorema do Isomorfismo temos:

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$$

$SL_n(\mathbb{R})$ ↳ núcleo de f.

③ $f: \mathbb{Z} \to n\mathbb{Z}$, $f(x) = nx$, f é bijetivo.

Daí, pelo Teorema do isomorfismo:

$$\mathbb{Z}/\{0\} \cong n\mathbb{Z}$$

④ Sejam $n, m \in \mathbb{Z}_+^*$ coprimos e considere:

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$$
$$x \longmapsto (\overline{x}, \overline{x}) = (x + n\mathbb{Z}, x + m\mathbb{Z})$$

- f é homom:

$$f(x+y) = ((x+y)+n\mathbb{Z},\ (x+y)+m\mathbb{Z})$$
$$= ((x+n\mathbb{Z})+(y+n\mathbb{Z}),\ (x+m\mathbb{Z})+(y+m\mathbb{Z}))$$
$$= (x+n\mathbb{Z}, x+m\mathbb{Z}) + (y+n\mathbb{Z}, y+m\mathbb{Z})$$
$$= f(x) + f(y)$$

- f é sobrejetivo:

Seja $(x+n\mathbb{Z}, y+m\mathbb{Z}) \in \mathbb{Z}_n \times \mathbb{Z}_m$.
Como $mdc(n,m) = 1$, existem $r, s \in S$ tais que

$$rn + sm = 1$$

$$\Rightarrow \begin{cases} rn = 1 - sm \Rightarrow rn \equiv 1 \pmod m \Rightarrow yrn \equiv y \pmod m \\ sm = 1 - rn \Rightarrow sm \equiv 1 \pmod n \Rightarrow xsm \equiv x \pmod n \end{cases}$$

Daí, considere:

$$a = yrn + xsm$$

$$\Rightarrow \begin{cases} a + n\mathbb{Z} = xsm + n\mathbb{Z} = x + n\mathbb{Z} \\ a + m\mathbb{Z} = yrn + m\mathbb{Z} = y + m\mathbb{Z} \end{cases} \Rightarrow f(a) = (x+n\mathbb{Z}, y+m\mathbb{Z})$$

- **núcleo:**

$$\ker f = \{x \in \mathbb{Z} \mid f(x) = (x+n\mathbb{Z}, x+m\mathbb{Z}) = (\bar{0}, \bar{0})\}$$

$$= \{x \in \mathbb{Z} \mid (x+n\mathbb{Z}, y+m\mathbb{Z}) = (n\mathbb{Z}, m\mathbb{Z})\}$$

$$= \{x \in \mathbb{Z} \mid x \in n\mathbb{Z} \text{ e } x \in m\mathbb{Z}\}$$

$$= n\mathbb{Z} \cap m\mathbb{Z}$$

$$= nm\mathbb{Z}, \text{ pois}$$

i) $x \in n\mathbb{Z} \cap m\mathbb{Z} \Rightarrow x = na = mb \Rightarrow n \mid mb$

$\Rightarrow n \mid b$, pois $\text{mdc}(n,m) = 1$, daí $b = nk \Rightarrow x = mb = nmk$.

ii) $x \in nm\mathbb{Z} \Rightarrow x = nma = \begin{cases} (ma)n \Rightarrow x \in n\mathbb{Z} \\ (na)m \Rightarrow x \in m\mathbb{Z} \end{cases}$

$\Rightarrow x \in n\mathbb{Z} \cap m\mathbb{Z} \Rightarrow nm\mathbb{Z} \subseteq n\mathbb{Z} \cap m\mathbb{Z}$.

Portanto, pelo Teorema do Isomorfismo:

$$\mathbb{Z}_{nm} \cong \mathbb{Z}/_{nm\mathbb{Z}} \cong \mathbb{Z}_n \times \mathbb{Z}_m$$

$$\Rightarrow \mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}, \quad \text{mdc}(n,m) = 1$$

Teorema Chinês do resto!

Teorema de Caracterização de grupos cíclicos

Seja G um grupo cíclico, então

1) $|G| = n \Rightarrow G \cong \mathbb{Z}_n$.

2) $|G| = \infty \Rightarrow G \cong \mathbb{Z}$.

Prova: Considere $G = \langle a \rangle$ e

$$f : \mathbb{Z} \longrightarrow G$$
$$k \longmapsto a^k$$

- f é homom.:

$$f(k+j) = a^{k+j} = a^k a^j = f(k) f(j)$$

- f é sobrejetiva:

$g \in G \Rightarrow g = a^k = f(k)$.

- Núcleo:

$$\operatorname{Ker} f = \{ k \in \mathbb{Z} \mid f(k) = a^k = e \}$$

1) Se $|G| = n$, então $o(a) = |\langle a \rangle| = |G| = n$

$\Rightarrow n \mid k \Rightarrow \operatorname{Ker} f = \{ k \in \mathbb{Z} \mid k \in n\mathbb{Z} \} = n\mathbb{Z}$.

2) Se $|G| = \infty$, então $g^k = e \Rightarrow k = 0$. Daí,

$$\ker f = \{k \in \mathbb{Z} \mid k = 0\} = \{0\}$$

Portanto, pelo Teorema do Isomorfismo:

1) $|G| = n \Rightarrow \mathbb{Z}/n\mathbb{Z} \cong \operatorname{Im} f = G \Rightarrow \boxed{G \cong \mathbb{Z}_n}$

2) $|G| = \infty \Rightarrow \mathbb{Z}/\{0\} \cong \operatorname{Im} f = G \Rightarrow \boxed{G \cong \mathbb{Z}}$.

#