

# IC Grupos

Iniciação Científica em Teoria de Grupos

Marco Vieira Buseti

Professor: Francismar Ferreira Lima

Universidade Tecnológica Federal do Paraná

Curitiba, Novembro de 2024

# Capítulo 1

## Generalidades sobre Grupos

### 1.1 Operações Binárias

#### Definição 1.1.1

Sejam  $G$  e  $E$  conjuntos não-vazios e  $\oplus$  uma função tal que:

$$\oplus : \begin{array}{c} G \times G \rightarrow E \\ (a, b) \mapsto \oplus(a, b) \end{array}$$

Definimos a função acima como a **operação binária de dois elementos de  $G$  em  $E$**  e a escrevemos comumente como:  $a \oplus b$ .

#### Exemplo 1.1.1

A adição usual  $+$  é uma operação binária de dois elementos de  $\mathbb{I}$  em  $\mathbb{R}$ . Onde  $\mathbb{I}$  denota o conjunto dos números irracionais.

#### Exemplo 1.1.2

Sejam  $(a, b) \in \mathbb{R}^2$ , a função que define a distância cartesiana entre dois pontos  $a$  e  $b$ :

$$\text{dist}(a, b) : \begin{array}{c} \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}^+ \\ (a, b) \mapsto \sqrt{a^2 + b^2} \end{array}$$

representa uma operação binária de dois elementos de  $\mathbb{R}$  em  $\mathbb{R}^+$ .

#### Definição 1.1.2

A partir das notações acima, definimos **lei de composição interna de  $G \times G \rightarrow G$  se  $E = G$** .

*Observação: caso não haja ambiguidade, denotaremos simplesmente **lei de composição interna em  $G$**  para representar a lei de composição interna de  $G \times G \rightarrow G$ .*

#### Exemplo 1.1.3

A operação usual  $+$  em  $\mathbb{N}$  é uma lei de composição interna em  $\mathbb{N}$ , ao contrário da operação usual  $-$  de  $\mathbb{N}$  em  $\mathbb{Z}$ .

## 1.2 Grupos

### Definição 1.2.1

Seja  $G$  um conjunto não-vazio. **Dizemos que  $(G, \cdot)$  é um grupo** se, e somente se,  $\cdot$  é uma lei de composição interna em  $G$  tal que:

1.  $\exists e \in G, \forall x \in G : x \cdot e = e \cdot x = x$ ;
2.  $\forall x \in G, \exists \hat{x} \in G : x \cdot \hat{x} = \hat{x} \cdot x = e$ ;
3.  $\forall x, y, z \in G : (x \cdot y) \cdot z = x \cdot (y \cdot z)$ .

*Observações:*

*Levando em consideração as notações acima, temos:*

1. *Primeiramente, notamos que  $e$  e  $\hat{x}$  são únicos, uma vez que:*

*Supondo que existam  $e$  e  $e'$  pertencentes à  $G$  que satisfazem o item 1, temos:*

$$x \cdot e = x = x \cdot e' \implies \hat{x} \cdot x \cdot e = \hat{x} \cdot x \cdot e' \implies e = e' \quad \square$$

*Supondo agora que existam  $\hat{x}$  e  $\hat{x}'$  que satisfaçam o item 2, temos:*

$$\hat{x} \cdot x = e = \hat{x}' \cdot x \implies \hat{x} \cdot x \cdot \hat{x} = \hat{x}' \cdot x \cdot \hat{x} \implies \hat{x} \cdot e = \hat{x}' \cdot e \implies \hat{x} = \hat{x}' \quad \square$$

2. *Notamos por convenção  $x^{-1}$  no lugar de  $\hat{x}$  no **item 2** (dada sua unicidade).*
3. *Caso  $\forall (x, y) \in G \times G : x \cdot y = y \cdot x$ , dizemos que  $G$  é um grupo abeliano (ou comutativo).*
4. *Caso  $G$  seja um grupo abeliano, então*

$$(x \cdot y)^n = x^n \cdot y^n, \quad \forall n \in \mathbb{Z}.$$

### Exemplo 1.2.1

$(\mathbb{Z}, +)$ ,  $(\mathbb{Z}/n\mathbb{Z}, +)$ ,  $(\mathbb{R}^*, \cdot)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$ ,  $(\mathbb{C}^*, \cdot)$ ,  $(\mathbb{Q}^*, \cdot)$  são grupos abelianos (onde  $+$  e  $\cdot$  denotam as operações usuais de adição e produto em  $\mathbb{C}$ ).

### Exemplo 1.2.2

$(GL_n(\mathbb{K}), \times)$  define uma estrutura de grupo, onde  $\mathbb{K} = \mathbb{C}$  ou  $\mathbb{R}$  e  $GL_n(\mathbb{K})$  define o conjunto das matrizes  $n \times n$  invertíveis com entradas em  $\mathbb{K}$ .

### Exemplo 1.2.3

Seja  $A$  um conjunto não-vazio. Seja

$$\mathcal{P}(f) = \{f : A \rightarrow A \mid f \text{ bijetiva}\}$$

O conjunto das funções  $f$  bijetivas de  $A$  em  $A$ .

$(\mathcal{P}(f), \circ)$  define uma estrutura de grupo, onde  $\circ$  representa composição entre funções.

Caso  $A$  seja um conjunto finito e  $n \in \mathbb{N}$  tal que  $\text{Card}(A) = n$ ,  $\mathcal{P}(f)$  será representado por  $S_n$  e será chamado de **grupo simétrico ou grupo das permutações**.

#### Exemplo 1.2.4

Seja, neste exemplo, para fins de simplificação,  $\mathbb{Z}/n\mathbb{Z} \stackrel{\text{def}}{=} \mathbb{Z}_n$ , para  $n \in \mathbb{Z}$ .  
Seja a operação  $\odot$  em  $\mathbb{Z}_n$  definida da seguinte forma:

$$\odot : \begin{array}{c} \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n \\ (\bar{a}, \bar{b}) \mapsto \bar{a} \odot \bar{b} = \overline{a \cdot b} \end{array}$$

onde  $\cdot$  é a operação usual de produto nos inteiros.

Temos que  $(\mathbb{Z}_p^*, \odot)$ , onde  $p$  é um número primo, é um grupo abeliano.

#### Demonstração:

Por construção, temos que  $\bar{a} \odot \bar{b} \in \mathbb{Z}_p^*$ .

Para mostrar a associatividade, sejam  $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_p^*$ .

Temos que:

$$\begin{aligned} \bar{a} \odot (\bar{b} \odot \bar{c}) &= \bar{a} \odot (\overline{b \cdot c}) = \\ &= \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = (\bar{a} \odot \bar{b}) \odot \bar{c}. \end{aligned}$$

O elemento neutro é evidentemente o elemento  $\bar{1} \in \mathbb{Z}_p^*$ , pois:

$$\bar{a} \odot \bar{1} = \overline{a \cdot 1} = \bar{a}, \quad \forall \bar{a} \in \mathbb{Z}_p^*.$$

Também temos que para todo elemento de  $\mathbb{Z}_p^*$ , existe elemento inverso, pois, sabemos que:

$$\forall \bar{a} \in \mathbb{Z}_p^* \implies \text{mdc}(a, p) = 1.$$

Logo, pelo Teorema de Bézout, temos que existem  $x$  e  $y$  inteiros tais que:

$$ax - py = 1$$

Ora mas isso é a mesma coisa que afirmar que existe uma solução para a equação:

$$a \cdot x \equiv 1 \pmod{p} \iff \bar{a} \odot \bar{x} = \bar{1}.$$

Logo, deduzimos que  $\forall \bar{a} \in \mathbb{Z}_p^*, \exists \bar{a}^{-1} \in \mathbb{Z}_p^*$ .

Além disso, é evidente que a operação  $\odot$  é comutativa.

Portanto, provamos que  $(\mathbb{Z}_p^*, \odot)$  é um grupo abeliano.

□

**Exemplo 1.2.5**

Seja  $G = ]-1, 1[$ ,  $(G, \star)$  tal que

$$\forall x, y \in G : x \star y = \frac{x + y}{1 + xy}$$

define um grupo abeliano.

**Demonstração:**

Provemos primeiramente que  $\forall x, y \in G, x \star y \in G$ .

Fixando  $y \in G$  temos a seguinte função de  $x \in G$ :

$$f(x) = \frac{x + y}{1 + xy}$$

A função é derivável em  $G$ . Tomando sua derivada temos:

$$f'(x) = \frac{1 - y^2}{(1 + xy)^2}$$

Temos evidentemente  $\forall (x, y) \in G \times G, f'(x) > 0$ .

(De forma simétrica podemos mostrar o mesmo escrevendo  $f$  como uma função de  $y$ ).

Logo, deduzimos que a função  $f$  é estritamente crescente.

Portanto:

$$f(-1) < x \star y < f(1) \iff \frac{y - 1}{1 - y} < x \star y < \frac{1 + y}{1 + y} \iff -1 < x \star y < 1$$

Logo, provamos que  $x \star y \in G$ .

Provemos os outros axiomas:

*Existência do neutro:*

Tomando  $y = 0$  temos:

$$x \star 0 = \frac{x + 0}{1 + 0 \cdot x} = x$$

Portanto, deduzimos que o elemento neutro do grupo  $G$  é dado por  $e = 0$ .

*Existência do inverso:*

Tomando  $y = -x$  temos:

$$x \star -x = \frac{x - x}{1 - (-x)x} = 0$$

Portanto, deduzimos que o elemento inverso do grupo  $G$  existe e é dado por  $x^{-1} = -x$ .

*Associatividade:*

Sejam  $x, y, z \in G$ , mostremos que  $(x \star y) \star z = x \star (y \star z)$

Temos:

$$\begin{aligned}
(x \star y) \star z &= \frac{(x \star y) + z}{1 + (x \star y)z} = \frac{\frac{x+y}{1+xy} + z}{1 + z\frac{x+y}{1+xy}} = \frac{x + y + z + xyz}{1 + xy + xz + yz} = \\
&= \frac{x(1 + yz) + (y + z)}{(1 + yz) + x(y + z)} = \frac{x + \frac{y+z}{1+yz}}{1 + x\frac{y+z}{1+yz}} = x \star (y \star z)
\end{aligned}$$

Mostrando, assim, a associatividade.

Ainda, temos que o grupo é evidentemente abeliano.  $\square$

### 1.3 Subgrupos

#### Definição 1.3.1

Seja  $(G, \cdot)$  um grupo. Um subconjunto  $H \subseteq G$  é chamado de subgrupo de  $G$  (denotamos  $H \leq G$ ) se, e somente se,  $(H, \cdot)$  é um grupo.

*Observação:* temos ainda que se  $H \subset G$ , temos então  $H$  é chamado de subgrupo próprio de  $G$  e denotamos como  $H < G$ .

#### Proposição 1.3.1

Seja  $H \subseteq G$  tal que  $H \neq \emptyset$  e  $(G, \cdot)$  é um grupo.  $H \leq G$  é equivalente à satisfazer as seguintes condições:

1.  $h_1 \cdot h_2 \in H, \forall (h_1, h_2) \in H \times H;$
2.  $h^{-1} \in H, \forall h \in H.$

#### Demonstração:

É necessário mostrarmos as duas implicações da equivalência:

$$H \leq G \implies (1.) \text{ e } (2.) \tag{1.1}$$

$$(1.) \text{ e } (2.) \implies H \leq G \tag{1.2}$$

A implicação (1.1) é trivial. Ora, se  $H \leq G$ , então pela definição de subgrupo temos que  $h_1 \cdot h_2 \in H$  e  $h^{-1} \in H$ , isto é  $\exists h^{-1} \in H : h \cdot h^{-1} = h^{-1} \cdot h = h$ .

Para a implicação (1.2):

Sabemos que  $H \subseteq G$ , logo, se  $h_1 \cdot h_2 \in H \implies h_1 \cdot h_2 \in G$ . Ora, sabemos que  $(G, \cdot)$  é um grupo. Logo, a associatividade é satisfeita. Para demonstrar que  $e \in H$ , basta tomarmos  $h_2 = h^{-1}$  a partir de (2.). Logo, temos  $h \cdot h^{-1} = e \in H$ . Com isso mostramos todos os axiomas necessários e deduzimos que  $H \leq G$ .  $\square$

**Exemplo 1.3.1**

$(\mathbb{U}^*, \cdot)$ ,  $(\mathbb{R}^*, \cdot)$ ,  $(\mathbb{R}_+^*, \cdot)$ ,  $(\mathbb{Q}^*, \cdot)$ ,  $(\mathbb{Q}_+^*, \cdot)$  são subgrupos de  $(\mathbb{C}^*, \cdot)$ , onde  $\cdot$  denota a multiplicação usual em  $\mathbb{C}$ .

**Exemplo 1.3.2**

$G$  e  $\{e\}$  são subgrupos *triviais* de  $G$ .

**Exemplo 1.3.3**

Seja  $n \in \mathbb{Z}$ ,  $(n\mathbb{Z}, +)$  são subgrupos de  $(\mathbb{Z}, +)$ , e, em particular, são os únicos.

**Demonstração:**

É evidente que  $(n\mathbb{Z}, +)$  são subgrupos de  $(\mathbb{Z}, +)$ . Mostremos que são os únicos!

Seja  $(H, +)$  um subgrupo qualquer de  $(\mathbb{Z}, +)$ . Se  $H = \{0\}$ , então  $H = 0\mathbb{Z}$ .

Suponhamos agora  $H \neq \{0\}$ . Seja  $n = \min\{a \in H, a > 0\}$ .

Logo, como  $n \in H$  e  $H \leq \mathbb{Z}$ , temos que  $n\mathbb{Z} \subseteq H$ .

De maneira inversa, seja  $h \in H$ . Logo, pelo Algoritmo de Euclides, existem  $q, r \in \mathbb{Z}$  tais que:

$$h = qn + r \quad (0 \leq r < n)$$

Porém, note que, como  $h \in H$ , temos:

$$r = h - qn \in H$$

Porém, sabemos que  $0 \leq r < n$ .

Ora, como  $n$  é o elemento mínimo de  $H$  estritamente maior que 0, deduzimos que apenas podemos ter  $r = 0$ .

Logo:

$$h = qn \implies h \in n\mathbb{Z} \implies H \subseteq n\mathbb{Z}.$$

Portanto deduzimos que  $H = n\mathbb{Z}$ . □

**Exemplo 1.3.4**

Seja  $G$  um grupo e  $I$  um conjunto não-vazio de índices. Se  $\{H_i\}_{i \in I}$  é uma família de subgrupos de  $G$ , então  $\bigcap_{i \in I} H_i$  é um subgrupo de  $G$ .

**Demonstração:**

Como visto na **Proposição 1.3.1**, mostremos que:

1.  $\forall x_1, x_2 \in \bigcap_{i \in I} H_i \implies x_1 \cdot x_2 \in \bigcap_{i \in I} H_i$ ;
2.  $\forall x \in \bigcap_{i \in I} H_i \implies \exists x^{-1} \in \bigcap_{i \in I} H_i$ .

Provemos o **item 1**:

Sejam,

$$x_1, x_2 \in \bigcap_{i \in I} H_i$$

Logo:

$$\forall i \in I, x_1, x_2 \in H_i$$

Sabemos também que:

$$\forall i \in I, H_i \leq G$$

Portanto, deduzimos que:

$$\forall i \in I, x_1 \cdot x_2 \in H_i$$

Mas isso é a mesma coisa que dizer:

$$\forall x_1, x_2 \in \bigcap_{i \in I} H_i \implies x_1 \cdot x_2 \in \bigcap_{i \in I} H_i$$

Provemos o **item 2**:

Analogamente ao **item 1**, sabemos que:

$$x_0 \in \bigcap_{i \in I} H_i \iff \forall i \in I, x_0 \in H_i$$

Porém, sabemos que:

$$\forall i \in I, H_i \leq G$$

Logo, deduzimos que:

$$\forall i \in I, x_0 \in H_i, \exists x_0^{-1} \in H_i$$

Mas isso é a mesma coisa que:

$$\forall x \in \bigcap_{i \in I} H_i \implies \exists x^{-1} \in \bigcap_{i \in I} H_i$$

Portanto, provamos que:

$$\bigcap_{i \in I} H_i \leq G$$

□

### Definição 1.3.2

Seja  $G$  um grupo. O subconjunto  $Z(G)$  tal que:

$$Z(G) = \{x \in G : xg = gx, \forall g \in G\}$$

define um subgrupo de  $G$  chamado *centro* de  $G$ .

### Demonstração:

Como visto na **Proposição 1.3.1**, para mostrar que  $Z(G) \leq G$  é necessário mostrar que  $x \cdot x^{-1} \in Z(G)$ ,  $\forall x \in Z(G)$ .

Nota:  $Z(G)$  é claramente não vazio uma vez que o elemento neutro comuta com todos elementos de  $G$  e, portanto, está em  $Z(G)$ .



Temos que:

Se:

$$x \in Z(G) \Rightarrow x \cdot g = g \cdot x, \forall g \in G.$$

Logo, teremos:

$$xgx^{-1} = g \Rightarrow x^{-1}xgx^{-1} = x^{-1}g \Rightarrow gx^{-1} = x^{-1}g, \forall g \in G$$

Portanto:

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

Temos também que:

$$x_1 \in Z(G) \Rightarrow x_1g = gx_1, \forall g \in G \quad (\text{I})$$

$$x_2 \in Z(G) \Rightarrow x_2g = gx_2, \forall g \in G \quad (\text{II})$$

Deduzimos de (I):

$$x_1g = gx_1 \Rightarrow g = x_1^{-1}gx_1$$

Substituindo em (II):

$$x_2x_1^{-1}gx_1 = x_1^{-1}gx_1x_2 \Rightarrow x_2x_1^{-1}x_1g = x_1^{-1}gx_1x_2 \Rightarrow$$

$$\Rightarrow x_2g = x_1^{-1}gx_1x_2 \Rightarrow (x_1x_2)g = g(x_1x_2)$$

Logo, deduzimos que:

$$(x_1, x_2) \in Z(G) \times Z(G) \Rightarrow x_1 \cdot x_2 \in Z(G)$$

Portanto,  $Z(G) \leq G$ . □

*Observação:* O subgrupo centro serve o propósito de "medir a comutatividade" de um dado grupo. Por exemplo, observamos que  $Z(\mathbb{Z}) = \mathbb{Z}$ ,  $Z(GL_2(\mathbb{R})) = \{\lambda I : \lambda \in \mathbb{R}^*\}$  e  $Z(S_n) = \{e\}$ ,  $n \geq 3$ .

### Definição 1.3.3

Seja  $(G, \cdot)$  um grupo e  $X$  um conjunto não-vazio tal que  $X \subseteq G$ . **Chamamos de subgrupo gerado por um subconjunto a interseção de todos os subgrupos de  $G$  que contém  $X$ .** Denotamos-o como  $\langle X \rangle$ .

Matematicamente temos:

$$\langle X \rangle = \bigcap \{H : H \leq G \text{ e } X \subseteq H\}$$

### Proposição 1.3.2

A partir das notações da **Definição 1.3.3**, temos que  $\langle X \rangle$  é o menor subgrupo de  $G$  que contém  $X$ .

**Demonstração:**

Suponha que  $J \leq G$  seja o menor subgrupo de  $G$  tal que  $X \subseteq J$ .

Ora, como  $J \leq G$  e  $X \subseteq J$ , então:  $\langle X \rangle \subseteq J$ .

Entretanto, também sabemos que  $J$  é o menor subgrupo de  $G$  tal que  $X \subseteq J$ .

Portanto, deduzimos que  $J \subseteq H$ ,  $\forall H : H \leq G$  e  $X \subseteq H$ .

Porém, para todo  $H$  subgrupo de  $G$  temos que  $X \subseteq H$ , logo, deduzimos que  $J \subseteq \langle X \rangle$ .

Portanto,  $J = \langle X \rangle$ .

□

### Proposição 1.3.3

A partir das notações da **Definição 1.3.3**, temos que:

$$\langle X \rangle = \{x_1 x_2 \dots x_n : x_i \in X \cup X^{-1}, n \geq 1\}$$

**Demonstração:**

Sejam:

$$\dot{X} \stackrel{def}{=} \bigcap \{H : H \leq G \text{ e } X \subseteq H\}$$

$$\bar{X} \stackrel{def}{=} \{x_1 x_2 \dots x_n : x_i \in X \cup X^{-1}, n \geq 1\}$$

Queremos mostrar que:  $\dot{X} = \bar{X}$ .

Realizemos, primeiramente, algumas convenções de notação:

$$\bar{x}_p \stackrel{def}{=} x_1 x_2 \dots x_p, p \in \mathbb{Z}_+^*$$

$$\bar{x}_p^{-1} \stackrel{def}{=} x_1^{-1} x_2^{-1} \dots x_p^{-1}, p \in \mathbb{Z}_+^*$$

É evidente que  $\bar{x}_p, \bar{x}_p^{-1} \in \bar{X}$ . Assim como  $\bar{x}_p \bar{x}_p^{-1} \in \bar{X}$ , o que nos mostra que  $\bar{X} \leq G$ .

Mostremos que  $\dot{X} \subseteq \bar{X}$ :

Sabemos que:

$$\bar{X} = \{\bar{x}_p : x_i \in X \cup X^{-1}, p \in \mathbb{Z}_+^* \text{ e } 1 \leq i \leq p\}$$

Evidentemente temos que:

$$\forall x \in X \implies x \in \bar{X}$$

Uma vez que  $\bar{X} \leq G$ , temos diretamente que  $\dot{X} \subseteq \bar{X}$ .

Isso se dá pelo fato de que  $\dot{X}$  é o menor subgrupo de  $G$  contendo  $X$ , e, como  $\bar{X}$  é um subgrupo de  $G$  contendo  $X$ , realizamos tal dedução.

Mostremos agora que  $\bar{X} \subseteq \dot{X}$ :

Seja  $H \leq G$  tal que:

$$H \leq G \text{ e } X \subseteq H.$$

Ora, temos evidentemente que:

$$\forall \bar{x}_p \in \bar{X} \implies \bar{x}_p \in H.$$

Logo:

$$\bar{x}_p \in H \implies \bar{x}_p \in \bigcap_{i \in I} H_i$$

Onde  $I$  é um conjunto não-vazio de índices.

Evidentemente temos então que  $\bar{x}_p \in \dot{X}$ .

Logo,  $\bar{X} \subseteq \dot{X}$ .

Portanto, mostramos que:  $\bar{X} = \dot{X}$ .

□

#### Exemplo 1.3.5

Seja o grupo  $(\mathbb{R}^*, \cdot)$  e o subconjunto  $E \subset \mathbb{R}^*$  tal que  $E = \{2\}$ . O subgrupo gerado por  $E$  é, portanto,  $H = \{2^n, n \in \mathbb{Z}\}$ .

De forma genérica, para um grupo  $G$  e um elemento  $a \in G$ , temos:  $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$ .

De forma geral, dado um grupo  $G$ , para determinarmos um subgrupo  $H$  gerado por um subconjunto  $X$  devemos provar os seguintes pontos:

1.  $H$  é um subgrupo de  $G$
2.  $X \subset H$
3. Se  $H'$  é um outro subgrupo tal que  $X \subset H'$ , então  $H \subset H'$

#### Definição 1.3.4

Seja  $G$  um grupo.  $G$  é **chamado de grupo cíclico** quando ele pode ser gerado por um único elemento  $x \in G$ .

#### Exemplo 1.3.6

$$\mathbb{Z} = \langle 1 \rangle, \mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle, \mathbb{U} = \langle e^{\frac{2\pi i}{n}} \rangle.$$

#### Proposição 1.3.4

Se  $G$  é um grupo cíclico, então  $G$  é um grupo abeliano.

#### Demonstração:

Seja  $a \in G$  tal que  $G = \langle a \rangle$ . Podemos representar  $G$  como:

$$G = \{..., (a^{-1})^r, ..., (a^{-1})^2, a^{-1}, e, a, a^2, ..., a^r, ...\}$$

Onde  $r \in \mathbb{Z}$ .

Sejam  $(x, y) \in G \times G$ , queremos mostrar que  $x \cdot y = y \cdot x$ .

Sabemos que:

$$x = a^{r_1}, r_1 \in \mathbb{Z}$$

$$y = a^{r_2}, r_2 \in \mathbb{Z}$$

Logo:

$$x \cdot y = a^{r_1} \cdot a^{r_2} = a^{r_1+r_2} \stackrel{(*)}{=} a^{r_2+r_1} = a^{r_2} \cdot a^{r_1} = y \cdot x$$

(\*) : deduz-se que  $r_1 + r_2 = r_2 + r_1$  pois estamos trabalhando dentro do grupo abeliano  $(\mathbb{Z}, +)$ .

Portanto,  $G$  é um grupo abeliano.  $\square$

### Definição 1.3.5

Definimos  $\langle \{xyx^{-1}y^{-1} \mid (x, y) \in G \times G\} \rangle$  como o subgrupo dos comutadores do grupo  $G$ . Denotaremos-o por  $G'$ .

### Definição 1.3.6

Seja  $(G, \cdot)$  um grupo. Definimos **ordem do grupo**  $(G, \cdot)$  a **quantidade de elementos no conjunto**  $G$  e a denotamos por  $|G|$ .

Se  $\alpha \in G$ , a **ordem de  $\alpha$**  é a **ordem do subgrupo gerado por  $\alpha$** , denotada por  $\mathcal{O}(\alpha)$ , isto é,  $\mathcal{O}(\alpha) = |\langle \alpha \rangle|$ .

### Exemplo 1.3.7

$$|\mathbb{Z}| = \infty, |\mathbb{Z}/n\mathbb{Z}| = n, |(\mathbb{Z}/p\mathbb{Z})^*| = p - 1, |S_n| = n!$$

### Proposição 1.3.5

Seja  $G$  um grupo finito e  $\alpha$  um elemento de  $G$ .

Logo,  $\mathcal{O}(\alpha) < \infty$ .

#### Demonstração:

Provemos a **Proposição 1.3.5** via absurdo.

Suponha que  $\mathcal{O}(\alpha)$  seja não finito, logo podemos gerar  $n$  valores distintos a partir de potências de  $\alpha$ , onde  $n \in \mathbb{Z}$ .

Ora, a partir da geração de infinitos valores distintos de potências de  $\alpha$ , sabemos que, para dado valor inteiro  $k$ , teremos  $\alpha^k \notin G$ . Ora, mas  $\langle \alpha \rangle$  é um subgrupo de  $G$ . Absurdo.

Portanto, temos que  $\mathcal{O}(\alpha) < \infty$ .  $\square$

### Proposição 1.3.6

Seja  $G$  um grupo e  $\alpha$  um elemento de  $G$ . Então, as seguintes proposições são equivalentes:

- (i) A ordem  $\mathcal{O}(\alpha)$  é finita. Isto é,  $\mathcal{O}(\alpha) < \infty$ ;
- (ii)  $\exists t \in \mathbb{Z}_+^* : \alpha^t = e$ , onde  $t = \min \{k \in G : k > 0\}$ .

#### Demonstração:

Queremos provar que:  $(i) \iff (ii)$ .

Começamos provando a implicação  $(i) \implies (ii)$  :

Temos, por definição, que  $\langle \alpha \rangle = \{\alpha^m \mid m \in \mathbb{Z}\}$ .

Como  $\mathcal{O}(\alpha) < \infty$ , temos que  $\exists p, q \in \mathbb{Z} : p > q$  e  $\alpha^p = \alpha^q$ .

Deduzimos diretamente que:  $\alpha^{p-q} = e$ . Como  $p-q \in \mathbb{Z}_+^*$ , mostramos  $(i) \implies (ii)$ .

Note que a escolha do valor  $p-q$  ocorre sem perda de generalidade, uma vez que o conjunto  $\mathbb{Z}_+^*$  é enumerável e sempre podemos garantir a minimalidade de  $p-q$ .

Provemos  $(ii) \implies (i)$ :

Ora, a partir de  $(ii)$  sabemos que  $\langle \alpha \rangle$  é finito e, pela minimalidade de  $t$ , sua ordem é igual à  $t$ .

Portanto, a partir da **Proposição 1.3.5** temos diretamente que  $\mathcal{O}(\alpha) < \infty$ .

Portanto, com isso, mostramos que  $(ii) \implies (i)$  e, conseqüentemente, mostramos  $(i) \iff (ii)$ .

□

## 1.4 Teorema de Lagrange

### Definição 1.4.1

Seja  $G$  um grupo e  $H$  um subgrupo de  $G$ . Definimos **classe lateral à esquerda de  $H$  em  $G$  que contém  $x$**  o subconjunto  $xH$  de  $G$  tal que  $\forall x \in G$ :

$$xH = \{xh \mid h \in H\}$$

Analogamente definimos **classe lateral à direita de  $H$  em  $G$  que contém  $x$**  o subconjunto  $Hx$  de  $G$  tal que  $\forall x \in G$ :

$$Hx = \{hx \mid h \in H\}$$

*Observações:*

- As classes laterais de  $G$  não são necessariamente subgrupos de  $G$ ;
- Quando não houver confusão possível, podemos denominar as classes laterais à esquerda/direita de  $H$  em  $G$  que contém  $x$  como simplesmente: classe lateral à esquerda/direita de  $H$ .

### Definição 1.4.2

A cardinalidade do conjunto das classes laterais à esquerda ou à direita é definida como o **índice de  $H$  em  $G$** , e será denotada por  $[G : H]$ .

*Observação:* note que o número de classes laterais à direita de  $H$  é igual ao número de classes laterais à esquerda de  $H$  (por mais que as classes laterais sejam diferentes).

Isto se dá pelo fato de que a função:

$$\phi : \begin{aligned} &\{\text{classes lat. à esquerda}\} \rightarrow \{\text{classes lat. à direita}\} \\ &xH \mapsto Hx^{-1} \end{aligned}$$

é claramente uma bijeção.

**Teorema 1.4.1****Teorema de Lagrange (Grupos)**

Seja  $G$  um grupo finito e  $H$  um subgrupo de  $G$ .

Logo,  $|H|$  divide  $|G|$ .

**Demonstração:**

Seja  $x \in G \setminus H$ , consideremos o conjunto das classes laterais à esquerda de  $H$ :

$$xH = \{xh \mid h \in H\}$$

Mostremos que  $H \cap xH = \emptyset$ :

Supondo  $\alpha \in H \cap xH$ :

$$\alpha \in H \cap xH \iff \alpha = xh \in H.$$

Como  $\alpha = xh \in H$ , logo  $\exists h^{-1} \in H$  tal que  $hh^{-1} \in H$

Portanto:

$$\alpha h^{-1} = xhh^{-1} \in H \iff x \in H \implies \text{Absurdo, pois } x \in G \setminus H.$$

Logo,  $H \cap xH = \emptyset$ .

Agora mostremos que  $\text{Card}(xH) = |H|$ :

Seja  $\zeta$  a função definida abaixo:

$$\zeta : \begin{array}{l} H \rightarrow xH \\ h \mapsto xh \end{array}$$

A função  $\zeta$  é claramente sobrejetiva por definição.

$\zeta$  também é injetiva pois se  $(xh_1, xh_2) \in (xH)^2$ :

$$xh_1 = xh_2 \implies x^{-1}xh_1 = x^{-1}xh_2 \implies h_1 = h_2.$$

Portanto, deduzimos que  $\text{Card}(xH) = |H|$ .

Consideremos agora o conjunto  $yH$  das classes laterais à esquerda de  $H$  em  $G$  que contém  $y$  tal que  $y \notin H \cup xH$ .

Já mostramos anteriormente que  $y \notin H$ .

Mostremos que  $yH \cap xH = \emptyset$

Supondo  $\beta \in yH \cap xH$ :

Então  $\beta$  pode ser escrito de duas formas:

$$\beta = yh_1$$

$$\beta = xh_2$$

Logo, temos:

$$yh_1 = xh_2 \implies y = xh_2h_1^{-1} \in xH \implies \text{Absurdo, pois } y \notin H \cup xH.$$

Analogamente ao passo anterior podemos provar que  $\text{Card}(yH) = \text{Card}(xH) = |H|$ .

Portanto, realizando os passos acima sucessivamente, criamos partições de  $G$ .

Como  $G$  é finito, o processo terá finalizado após  $n$  etapas.

Portanto, temos:  $|G| = n|H|$ . □

*Observações:*

1. *Segue como consequência direta do **Teorema de Lagrange** que caso  $G$  seja um grupo finito e  $\alpha \in G$ , então  $\mathcal{O}(\alpha)$  divide  $|G|$ .*
2. *Temos diretamente pela **Definição 1.4.2** que:  $|G| = |H|[G : H]$ .*

### Proposição 1.4.1

Seja  $G$  um grupo não finito e  $H \leq G$ .  
Então vale o **Teorema de Lagrange**.

#### Demonstração:

Demonstraremos novamente o **Teorema de Lagrange** de forma que a proposição acima possa ser justificada de forma clara.

Seja  $G$  um grupo e  $H \leq G$ .

Ora, sabemos que:

$$\text{Ou } xH = yH \text{ ou } xH \cap yH = \emptyset, \forall (x, y) \in G \times G.$$

Sabemos também que, sendo  $I$  um conjunto não vazio de índices tal que  $\text{Card}(I) = [G : H]$ :

$$\dot{\bigcup}_{i \in I} x_i H = G.$$

Como  $|G|$  é não finito, então se  $|H|$  ou  $[G : H]$  são não finitos, vale que  $|G| = |H|[G : H]$ .

Suponhamos, agora, que  $|H| < \infty$  e  $[G : H] < \infty$ .

Como  $[G : H] < \infty$ , então  $|I| < \infty$ .

Logo, podemos escrever  $I$  como:

$$I = \{i_1, i_2, \dots, i_n, n \in \mathbb{N}\}.$$

Logo:

$$G = \dot{\bigcup}_{i_1 \leq i \leq n} x_i H.$$

Portanto, podemos escrever:

$$|G| = \sum_{k=1}^n |x_{i_k} H|.$$

Ora, deduzimos na demonstração do **Teorema de Lagrange** que  $|xH| = |H|$ ,  $\forall x \in G$ .

Portanto temos que:

$$|G| = n|H|.$$

Ora, mas  $|G|$  é não finito e  $|H| < \infty$ . Absurdo !

Portanto, deduzimos que  $|H|$  ou  $[G : H]$  são não finitos.

Assim, provamos que o **Teorema de Lagrange** vale também para  $|G|$  não finito. Isto é:

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

□

### Proposição 1.4.2

Seja  $G$  um grupo finito de ordem  $p \in \mathbb{N}^*$ .  
Se  $p$  for primo, então  $G$  é um grupo cíclico.

#### Demonstração:

Pelo Teorema de Lagrange sabemos que se  $H$  é subgrupo de um grupo finito  $G$ , então  $|H|$  divide  $|G|$ .

Como  $|G| = p$  primo, então os únicos subgrupos possíveis de  $G$  são seus subgrupos triviais.

Seja  $x \in G$  tal que  $x \neq e$ , onde  $e$  é o elemento neutro de  $G$ .

Logo, o único subgrupo gerado por  $x$  é o próprio  $G$ ,  $\langle x \rangle = G$

*Observação: como visto na **Proposição 1.3.2**,  $G$  também é abeliano!*

□

### Teorema 1.4.2

#### Teorema de Euler (Grupos)

Seja  $(G, \cdot)$  um grupo finito tal que  $|G| = n$ ,  $n \in \mathbb{Z}$ . Então:

$$\forall g \in G, g^n = 1.$$

#### Demonstração:

Seja  $g$  um elemento do grupo finito  $G$ . Sabemos que  $\langle g \rangle \leq G$ . Sabemos também, pelo **Teorema de Lagrange** que  $\mathcal{O}(g)$  divide a ordem de  $G$ .

Ora, podemos então escrever:

$$|G| = k\mathcal{O}(g), k \in \mathbb{Z}$$

Porém, pela **Proposição 1.3.6**, deduzimos:

$$g^n = g^{|G|} = g^{k\mathcal{O}(g)} = (g^{\mathcal{O}(g)})^k = e^k = e$$

Ora, demonstramos, com o argumento acima, sem perda de generalidade, tal fato para qualquer elemento de  $G$ .

□

### Teorema 1.4.3

#### Pequeno Teorema de Fermat

Seja  $p$  um número primo e  $a \in \mathbb{Z} \setminus p\mathbb{Z}$ , então:

$$a^{p-1} \equiv 1 \pmod{p}.$$

#### Demonstração:



O **Pequeno Teorema de Fermat** é evidentemente o caso específico do **Teorema de Euler** em que  $(G, \cdot) = ((\mathbb{Z}/p\mathbb{Z})^*, \odot)$ . □

### Proposição 1.4.3

Seja  $G$  um grupo e sejam  $K < H < G$ .  
Logo  $[G : K] = [G : H][H : K]$ .

#### Demonstração:

Basta aplicar sucessivamente o **Teorema de Lagrange**:

$$\begin{aligned} H < G &\Rightarrow |G| = |H| \cdot [G : H] \quad (\text{I}) \\ K < H &\Rightarrow |H| = |K| \cdot [H : K] \quad (\text{II}) \\ K < G &\Rightarrow |G| = |K| \cdot [G : K] \quad (\text{III}) \end{aligned}$$

Combinando as expressões (I) e (II), obtemos:

$$|G| = |K| \cdot [H : K] \cdot [G : H] = |K| \cdot [G : K]$$

Portanto:

$$[G : K] = [G : H] \cdot [H : K]$$
□

## 1.5 Grupos Quocientes

### Definição 1.5.1

Seja  $G$  um grupo e  $H \leq G$ .  
Chamamos de **conjunto quociente** o conjunto  $G/H$  (ou  $\frac{G}{H}$ ) **cujos elementos são as classes laterais à esquerda (ou à direita) de  $H$  em  $G$ .**

*Observação:* decorre da definição acima que  $|G/H| = [G : H]$ .

### Definição 1.5.2

Seja  $G$  um grupo e  $H \leq G$ .  
**Definimos a seguinte operação entre as classes laterais à esquerda de  $H$  em  $G$ :**

$$\bullet : \begin{aligned} G/H \times G/H &\rightarrow G/H \\ (xH, yH) &\mapsto xyH \end{aligned}$$

*Observações:*

- Note que, por convenção, estamos tratando das classes laterais à esquerda de  $H$  em  $G$ . Entretanto, a definição é válida para classes laterais à direita também.
- A operação definida é uma **lei de composição interna** por construção.

- Não mostramos ainda que a operação está de fato bem definida, isto é:

$$\begin{cases} (x_1H, y_1H) \in G/H \times G/H \\ (x_2H, y_2H) \in G/H \times G/H \end{cases}$$

$$\text{Se } (x_1H, y_1H) = (x_2H, y_2H) \implies x_1y_1H = x_2y_2H.$$

Tal fato será destacado na **Proposição 1.5.1**.

### Proposição 1.5.1

Seja  $G$  um grupo e  $H \leq G$ .

As afirmações a seguir são equivalentes:

- (i) A operação definida na **Definição 1.5.2** está bem definida;
- (ii)  $gHg^{-1} \subseteq H$ ,  $\forall g \in G$ ;
- (iii)  $gHg^{-1} = H$ ,  $\forall g \in G$ ;
- (iv)  $gH = Hg$ ,  $\forall g \in G$ .

### Demonstração:

Mostremos as equivalências:

$$(i) \iff (ii) \quad (\text{I})$$

$$(ii) \iff (iii) \quad (\text{II})$$

$$(iii) \iff (iv) \quad (\text{III})$$

Começemos mostrando a equivalência (I):

Ora, perceba que para  $(x, y) \in G \times G$  e  $(h, h') \in H \times H$ , temos que:

$x$  e  $xh$  são representantes distintos para a mesma classe lateral  $xH$ .

$y$  e  $yh'$  são representantes distintos para a mesma classe lateral  $yH$ .

Portanto, podemos deduzir que a operação " $\bullet$ " definida na **Definição 1.5.2** só estará bem definida se, e somente se:

$$xyH = xhyh'H, \forall (x, y) \in G \times G \text{ e } \forall (h, h') \in H \times H.$$

Logo:

$$xyH = xhyh'H \iff y^{-1}x^{-1}xyH = y^{-1}x^{-1}xhyh'H \iff H = y^{-1}hyh'H.$$

Ora, mas isso é equivalente à dizer que a operação só estará bem definida se, e somente se:

$$ghg^{-1} \in H, \forall g \in G, \forall h \in H.$$

Com isso mostramos a equivalência (I).

Mostremos a equivalência (II):

Para a implicação  $(ii) \implies (iii)$  mostremos que:

$$gHg^{-1} \subseteq H \implies H \subseteq gHg^{-1}, \forall g \in G.$$

Ora, temos diretamente da hipótese:

$$\begin{aligned} gHg^{-1} \subseteq H &\implies g^{-1}Hg \subseteq H \implies g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1} \\ &\implies H \subseteq gHg^{-1} \end{aligned}$$

Logo, podemos concluir que:

$$gHg^{-1} \subseteq H \implies H = gHg^{-1}.$$

A implicação (iii)  $\implies$  (ii) é evidente.

Com isso mostramos a equivalência (II).

Mostremos a equivalência (III):

$$gHg^{-1} = H \iff gHg^{-1}g = Hg \iff gH = Hg.$$

Assim mostramos a equivalência (III).

Tendo mostrado as equivalências (I), (II) e (III), mostramos que todas as afirmações são duas a duas equivalentes. □

### Definição 1.5.3

Um subgrupo  $H$  é um **subgrupo normal** de  $G$  caso ele satisfaça as afirmações equivalentes da **Proposição 1.5.1**.

Neste caso, denotamos:

$$H \trianglelefteq G$$

*Observações:*

- Note que caso  $H \trianglelefteq G$  então as classes laterais à esquerda e à direita de  $H$  são iguais;
- Denotamos  $H \triangleleft G$  se  $H$  é um **subgrupo normal próprio** de  $G$ .
- De forma geral quando queremos mostrar que um subgrupo  $H$  é subgrupo normal de um grupo  $G$ , mostramos que  $ghg^{-1} \in H$ .

### Exemplo 1.5.1

$G$  e  $\{e\}$  (subgrupos triviais de  $G$ ) são claramente subgrupos normais de  $G$ .

### Exemplo 1.5.2

Seja  $G$  um grupo e  $Z(G)$  o centro de  $G$ . Logo,  $Z(G) \trianglelefteq G$ .

**Demonstração:**

Já mostramos anteriormente que  $Z(G) \leq G$ .

Para mostrar que  $Z(G) \trianglelefteq G$  basta mostrar que:

$$\forall (g, z) \in G \times Z(G) \implies gzg^{-1} \in Z(G)$$

Ora, mas pela própria definição de centro (todos elementos de  $G$  que comutam entre si), sabemos que:

$$\text{Se } z \in Z(G) \implies zg = gz, \forall g \in G.$$

Logo:

$$gzg^{-1} = zgg^{-1} = z \in Z(G).$$

□

*Observações:*

- De forma geral, é evidente que se  $H \leq Z(G)$ , então  $H \trianglelefteq G$ ;
- Isso equivale ainda a dizer que se  $G$  é um grupo abeliano, então todos seus subgrupos são normais.

#### Definição 1.5.4

Seja  $G$  um grupo não-trivial.

**Chamamos  $G$  de grupo simples caso seus únicos subgrupos normais sejam  $\{e\}$  e  $G$ .**

Isto é, caso seus únicos subgrupos normais sejam os subgrupos triviais.

#### Proposição 1.5.2

Seja  $G$  um grupo e  $H \leq G$ .

Se  $[G : H] = 2$ , então  $H \trianglelefteq G$ .

**Demonstração:**

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

Demonstremos por disjunção de casos:

Caso  $g \in H$ . Logo:

$$gH = H = Hg$$

Caso  $g \notin H$ . Logo:

Como  $[G : H] = 2$ , temos de imediato:

$$G/H = \{H, gH\}$$

Logo:

$$G = H \dot{\cup} gH = H \dot{\cup} Hg$$

Portanto, deduzimos de imediato que:

$$gH = Hg$$

Logo:  $H \trianglelefteq G$ .

□

**Definição 1.5.5**

Sejam  $G$  um grupo e  $A, B \leq G$ . Definimos o conjunto  $AB$  da seguinte forma:

$$AB = \{ab, a \in A, b \in B\}.$$

**Proposição 1.5.3**

Seja  $G$  um grupo e  $H, K \leq G$ . Logo:

$$HK \text{ é um subgrupo de } G \iff HK = KH.$$

**Demonstração:**

Mostremos a implicação ( $\implies$ ):

Seja  $HK$  um subgrupo de  $G$ .

Logo, temos que:

$$HK = (HK)^{-1} = K^{-1}H^{-1} = KH$$

Mostremos, agora, a implicação ( $\impliedby$ ):

Seja  $HK = KH$ , mostremos que  $HK \leq G$ .

Para mostrar que  $HK \leq G$  é suficiente mostrar que:

$$(HK)(HK) = HK$$

$$(HK)^{-1} = HK$$

Note que essa é uma forma diferente, porém equivalente, de enunciar a **Proposição 1.3.1**.

Ora, temos diretamente que:

$$(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$$

$$(HK)^{-1} = K^{-1}H^{-1} = KH = HK$$

Com isso mostramos a proposição. □

**Proposição 1.5.4**

Seja  $G$  um grupo e  $H, K \leq G$ . Se  $H \trianglelefteq G$  ou  $K \trianglelefteq G$ , então  $HK \leq G$ .

**Demonstração:**

Sejam  $H, K \leq G$ . Tomemos  $H$  como subgrupo normal de  $G$  e mostremos, sem perda de generalidade, que  $HK \leq G$ .

Para mostrarmos que  $HK \leq G$  é suficiente mostrar que a operação de  $HK$  é uma lei de composição interna em  $HK$  e que para todo elemento de  $HK$ , existe elemento inverso.

Note, primeiramente, que  $HK$  é não vazio, uma vez que  $H, K \leq G$ .

Sejam  $a, b \in HK$ , mostremos que  $ab \in HK$ .

Ora, se  $a, b \in HK$ , então:

$$a = hk, \quad h \in H, \quad k \in K$$

$$b = h'k', \quad h' \in H, \quad k' \in K$$

Portanto, temos que:

$$ab = hkh'k' = hkh'k^{-1}kk' = \underbrace{(hkh'k^{-1})}_{\in H}(kk') \in HK$$

Mostremos, agora, que para  $a \in HK$ ,  $\exists a^{-1} \in HK$ .

Ora, como  $a \in HK$ , então analogamente ao passo anterior temos que:

$$a = hk, \quad h \in H, \quad k \in K$$

Portanto:

$$a^{-1} = k^{-1}h^{-1} = k^{-1}h^{-1}kk^{-1} = \underbrace{(k^{-1}h^{-1}k)}_{\in H}(k^{-1}) \in HK$$

Portanto, mostramos que  $HK \leq G$ . □

### Proposição 1.5.5

Seja  $G$  um grupo e  $H, K \trianglelefteq G$ . Então  $HK \trianglelefteq G$ .

#### Demonstração:

Sabemos a partir do **Proposição 1.5.4** que se  $H \trianglelefteq G$  ou  $K \trianglelefteq G$ , temos que  $HK \leq G$ .

Mostremos que se  $H \trianglelefteq G$  e  $K \trianglelefteq G$ , temos  $HK \trianglelefteq G$ .

Para isso, é suficiente mostrarmos que  $gHKg^{-1} \in HK$ .

Ora, como  $H, K \trianglelefteq G$ , temos:

$$gHKg^{-1} = gHg^{-1}gKg^{-1} = \underbrace{(gHg^{-1})}_{\in H}\underbrace{(gKg^{-1})}_{\in K} \in HK$$

□

### Proposição 1.5.6

Seja  $G$  um grupo finito e  $H, K \leq G$ . Então:

$$\text{Card}(HK) = \frac{|H||K|}{|H \cap K|}$$

#### Demonstração:

□

**Definição 1.5.6**

Seja  $G$  um grupo e  $H \trianglelefteq G$ .

**Então  $(G/H, \bullet)$  é um grupo chamado de grupo quociente.**

**Demonstração:**

Mostremos que  $(G/H, \bullet)$  é de fato um grupo.

Ora, pela **Definição 1.5.2** sabemos que a operação " $\bullet$ " é uma lei de composição interna por construção. Sabemos também, pela **Proposição 1.5.1** que caso  $H \trianglelefteq G$ , então " $\bullet$ " está bem definida.

Nos resta mostrar que  $(G/H, \bullet)$  satisfaz os axiomas de grupo.

De fato,  $G/H$  é associativo em relação à operação " $\bullet$ " pois:

Sejam  $xH, yH, zH \in G/H$ , temos:

$$(xH \bullet yH) \bullet zH = (xy)H \bullet zH = (xy)zH \stackrel{(*)}{=} x(yz)H = xH \bullet (yH \bullet zH).$$

Também temos evidentemente que o elemento neutro é dado por  $H \in G/H$ .

Ora, seja  $xH \in G/H$ , temos evidentemente:

$$xH \bullet H = xH = H \bullet xH.$$

Por fim, temos que para dado  $xH \in G/H$ , seu elemento inverso é dado por  $x^{-1}H \in G/H$ .

De fato:

$$xH \bullet x^{-1}H = xx^{-1}H = H = x^{-1}xH = x^{-1}H \bullet xH.$$

Portanto,  $(G/H, \bullet)$  é de fato um grupo. □

**Exemplo 1.5.3**

O grupo  $\mathbb{Z}/n\mathbb{Z}$  é um grupo quociente formado pelo quociente entre  $\mathbb{Z}$  e  $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ .

**Proposição 1.5.7**

Seja  $G$  um grupo e  $Z(G)$  seu centro.

Se o grupo  $G/Z(G)$  for cíclico, então  $G = Z(G)$ .

**Demonstração:**

Seja  $G/Z(G)$  um grupo cíclico.

Mostremos que  $G = Z(G)$ , isto é, que  $G$  é um grupo abeliano.

Como  $G/Z(G)$  é cíclico, então existe  $x \in G/Z(G)$  tal que  $\langle x \rangle = G/Z(G)$ .

Portanto, sabemos que, para determinado inteiro  $k \in \mathbb{Z}$ , temos:

$$gz' = x^k, (g, z') \in G \times Z(G)$$

Podemos reescrever a expressão acima como:

$$g = x^k z, (g, z) \in G \times Z(G)$$

Tomemos  $g_1, g_2 \in G$  tal que:

$$g_1 \stackrel{def}{=} x^{k_1} z_1, \quad (k_1, z_1) \in \mathbb{Z} \times Z(G)$$

$$g_2 \stackrel{def}{=} x^{k_2} z_2, \quad (k_2, z_2) \in \mathbb{Z} \times Z(G)$$

Portanto temos:

$$g_1 g_2 = x^{k_1} z_1 x^{k_2} z_2 = x^{k_1+k_2} z_1 z_2 = x^{k_2} x^{k_1} z_1 z_2 = x^{k_2} z_2 x^{k_1} z_1 = g_2 g_1.$$

Isso se dá pelo fato de qualquer elemento de  $z \in Z(G)$  comutar com elementos de  $G$  e, portanto, elementos de  $G/Z(G)$ .

Com isso, mostramos que  $G$  é um grupo abeliano e, portanto,  $G = Z(G)$ . □

## 1.6 Homomorfismos de Grupos

### Definição 1.6.1

Sejam  $(G, \cdot)$  e  $(\mathcal{G}, *)$  dois grupos. Uma função  $\phi : G \rightarrow \mathcal{G}$  é chamada de homomorfismo de grupos se:

$$\phi(a \cdot b) = \phi(a) * \phi(b), \quad \forall a, b \in G$$