

IC Grupos

Iniciação Científica em Teoria de Grupos

Marco Vieira Busetti

Professor: Francismar Ferreira Lima

Universidade Tecnológica Federal do Paraná

Curitiba, Novembro de 2024

Conteúdo

1 Generalidades sobre Grupos	3
1.1 Operações Binárias	3
1.2 Grupos	4
1.3 Subgrupos	7
1.4 Teorema de Lagrange	15
1.5 Grupos Quocientes	19
1.6 Homomorfismos de Grupos	29
1.7 Produto Direto de Grupos	43
1.8 Produto Semidireto de Grupos	47
2 Grupo Simétrico	48
2.1 Generalidades sobre o grupo simétrico	48
2.2 Ciclos e transposições	52
2.3 Assinatura	58

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:

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

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 :

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

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 satisfazem 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:

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

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 $n \in \mathbb{N}^*$,

$$SL_n(\mathbb{K}) \stackrel{\text{def}}{=} \{A \in GL_n(\mathbb{K}), \det(A) = 1\}$$

Temos que $(SL_n(\mathbb{K}), \cdot) \leq (GL_n(\mathbb{K}), \cdot)$, onde \cdot denota o produto usual de matrizes.

Chamamos $SL_n(\mathbb{K})$ de **grupo linear especial**.

Demonstração:

Mostremos que temos de fato $SL_n(\mathbb{K}) \leq GL_n(\mathbb{K})$.

Primeiramente, note que é evidente que $SL_n(\mathbb{K})$ é não vazio, pois $\text{Id}_n \in SL_n(\mathbb{K})$.

Mostremos que $\forall A, B \in SL_n(\mathbb{K})$, $AB^{-1} \in SL_n(\mathbb{K})$.

Sabemos que se $A, B \in SL_n(\mathbb{K})$ então $\det(A) = \det(B) = 1$.

Ora, sabemos que:

$$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)\det(B)^{-1} = 1 \cdot 1 = 1.$$

Logo, mostramos que $SL_n(\mathbb{K}) \leq GL_n(\mathbb{K})$. □

Exemplo 1.3.4

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 $H = n\mathbb{Z}$. \square

Exemplo 1.3.5

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:

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

Portanto:

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

Temos também que:

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

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

Deduzimos de (I):

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

Substituindo em (II):

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

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

Logo, deduzimos que:

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

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:

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

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

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

Realizemos, primeiramente, algumas convenções de notação:

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

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

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 1.3.6

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 1.3.7

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

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:

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

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. □

Definição 1.3.5

Definimos $G' \stackrel{\text{def}}{=} \langle \{xyx^{-1}y^{-1} | (x, y) \in G \times G\} \rangle$ como o subgrupo dos comutadores do grupo G .

Podemos também denotar $G' \stackrel{\text{def}}{=} [G, G]$, onde, para $x, y \in G$, temos:

$$[x, y] \stackrel{\text{def}}{=} xyx^{-1}y^{-1}.$$

Observações:

- Note que G' é de fato um subgrupo de G , uma vez que ele é, por definição, um subgrupo gerado;
- Note que, para um dado grupo G e $x, y \in G$, **não** necessariamente temos $[x, y] = [y, x]$.

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

Exemplo 1.3.8

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

Proposição 1.3.5

Seja G um grupo finito e α 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 α , onde $n \in \mathbb{Z}$.

Ora, a partir da geração de infinitos valores distintos de potências de α , 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 $\mathcal{O}(\alpha) < \infty$.

□

Proposição 1.3.6

Seja G um grupo e α 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 $t = \min \{k \in G : k > 0\}$.

Note que, caso a proposição seja satisfeita, então temos $\mathcal{O}(\alpha) = t$.

Demonstração:

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

Comecemos 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) :

Seja $\alpha \in G$ tal que $\langle \alpha \rangle = \{\alpha^n : n \in \mathbb{Z}\}$, sabemos via o Algoritmo de Euclides que:

$$n = qt + r, \quad q, t \in \mathbb{Z} \quad \text{e} \quad r \in \llbracket 0, t-1 \rrbracket$$

Temos, portanto:

$$\alpha^n = \alpha^{qt+r} = \alpha^{qt}\alpha^r = (\alpha^t)^q\alpha^r = e^q\alpha^r = \alpha^r$$

Portanto $\alpha^n = \alpha^r$, $\forall n \in \mathbb{Z}$ e $r \in \llbracket 0, t-1 \rrbracket$.

Logo, deduzimos que:

$$\langle \alpha \rangle = \{\alpha^0, \dots, \alpha^{t-1}\} \implies \mathcal{O}(\alpha) < \infty$$

Para mostrar que de fato temos $\mathcal{O}(\alpha) = t$, mostremos que $\alpha^{r_1} \neq \alpha^{r_2}$, $\forall r_1, r_2 \in \llbracket 0, t-1 \rrbracket$.

Suponha, por absurdo, que $\exists r_1, r_2 \in \llbracket 0, t-1 \rrbracket$ tal que $\alpha^{r_1} = \alpha^{r_2}$.

Temos, portanto:

$$\alpha^{r_1} = \alpha^{r_2} \iff \alpha^{r_1-r_2} = e$$

Absurdo, pois $r_1 - r_2 < t$, porém t é minimal.

Logo, como todos elementos de $\langle \alpha \rangle$ são distintos, deduzimos que $\mathcal{O}(\alpha) = t$. □

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:

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

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 ζ a função definida abaixo:

$$\begin{aligned} \zeta : & H \rightarrow xH \\ & h \mapsto xh \end{aligned}$$

A função ζ é claramente sobrejetiva por definição.

ζ 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 β 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: $|G| = |H|[G : H]$.

Corolário 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 o corolário acima possa ser justificado 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 $\text{Card}(I) = [G : H]$:

$$\bigsqcup_{i \in I} x_iH = G.$$

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:

$$G = \bigsqcup_{i_1 \leq i \leq n} x_iH.$$

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 1.4.1

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 1.4.2

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:

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

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:

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

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

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

Comecemos 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 "•" definida na **Definição 1.5.2** só estará bem definida se, e somente se:

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

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. \square

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.

Exemplo 1.5.3

Seja G um grupo e G' o subgrupo dos comutadores de G . Logo $G' \trianglelefteq G$.

Demonstração:

Sabemos, a partir da **Definição 1.3.5** que $G' \leq G$.

Seja $g \in G$ e tomemos $q = xyx^{-1}y^{-1} = [x, y]$, para $x, y \in G$.

Temos, portanto:

$$gqg^{-1} = g(xyx^{-1}y^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1})$$

Tomando $k = gxg^{-1}$ e $l = gyg^{-1}$, deduzimos que:

$$gqg^{-1} = klk^{-1}l^{-1} = [k, l] \in G'$$

Temos, portanto, recursivamente para um elemento genérico $g' \in G'$:

$$gg'g^{-1} = \underbrace{\prod_{i=1}^{n \in \mathbb{N}} \underbrace{(g[x_i, y_i]g^{-1})}_{\in G'}}_{\in G'}$$

Concluímos que $gg'g^{-1} \in G'$.

Logo, $G' \trianglelefteq G$.

□

Exemplo 1.5.4

Seja $n \in \mathbb{N}^*$.

Temos que $SL_n(\mathbb{K}) \trianglelefteq GL_n(\mathbb{K})$

Demonstração:

Sabemos que $SL_n(\mathbb{K}) \leq GL_n(\mathbb{K})$, mostremos portanto que:

$$GSG^{-1} \in SL_n(\mathbb{K}), \forall (G, S) \in GL_n(\mathbb{K}) \times SL_n(\mathbb{K})$$

Ora, sabemos que $\det(G) \neq 0$ e que $\det(G^{-1}) = \det(G)^{-1}, \forall G \in GL_n(\mathbb{K})$.

Portanto:

$$\begin{aligned}\det(GSG^{-1}) &= \det(G)\det(S)\det(G^{-1}) = \det(G)\det(S)\det(G)^{-1} = \\ &= \det(G)\det(G)^{-1}\det(S) = \det(S) = 1 \implies GSG^{-1} \in SL_n(\mathbb{K})\end{aligned}$$

Isto é,

$$SL_n(\mathbb{K}) \trianglelefteq GL_n(\mathbb{K})$$

□

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:

$$G = H \sqcup gH = H \sqcup Hg$$

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:**

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

Observação:

Note que o conjunto AB não necessariamente é um grupo mesmo que A e B o sejam.

Note, por exemplo, o caso do grupo S_3 :

$$A, B \leq S_3, \quad A = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}, \quad B = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

Note que A e B são de fato subgrupos de S_3 , pois:

$$A = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}, \quad e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma^2 = e,$$

$$e, \sigma, \sigma^{-1} = \sigma \in A \implies A \leq S_3.$$

$$B = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \tau^2 = e,$$

$$e, \tau, \tau^{-1} = \tau \in B \implies B \leq S_3.$$

Temos que o conjunto AB é dado por:

$$AB = \left\{ \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}_e, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

Ora, mas temos que:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \notin AB$$

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 (\iff):

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:

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

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:

Note que $H \cap K \leq H$ e $H \cap K \leq K$, então podemos escrever:

$$\begin{aligned} H &= \bigcup_{1 \leq i \leq r}^{\bullet} a_i(H \cap K), \quad \text{com } r = [H : H \cap K], \\ K &= \bigcup_{1 \leq j \leq s}^{\bullet} (H \cap K)b_j, \quad \text{com } s = [K : H \cap K]. \end{aligned}$$

Assim, o conjunto $HK = \{hk \mid h \in H, k \in K\}$ pode ser escrito como:

$$HK = \bigcup_{i=1}^r \bigcup_{j=1}^s a_i(H \cap K)b_j.$$

Cada conjunto $a_i(H \cap K)b_j$ possui $|H \cap K|$ elementos. A união acima é disjunta: se

$$a_i(H \cap K)b_j = a_{i'}(H \cap K)b_{j'},$$

então, por multiplicações à esquerda e direita, deduz-se que $i = i'$ e $j = j'$, dado que os a_i e b_j representam classes distintas.

Logo, temos rs conjuntos disjuntos de tamanho $|H \cap K|$, e portanto:

$$\text{Card}(HK) = rs \cdot |H \cap K| = [H : H \cap K][K : H \cap K] \cdot |H \cap K|.$$

Mas

$$|H| = [H : H \cap K] \cdot |H \cap K|, \quad |K| = [K : H \cap K] \cdot |H \cap K|,$$

e portanto:

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

□

Proposição 1.5.7

Seja G um grupo e $H, K \leq G$ tal que $HK \leq G$. Então:

$$[HK : K] = [H : H \cap K]$$

Demonstração:

Note, primeiramente, que $K \leq HK$, uma vez que $K \subseteq HK$, $K \leq G$ e $HK \leq G$. Logo, pelo **Teorema de Lagrange**, temos:

$$|HK| = |K| \cdot [HK : K] \iff \frac{|HK|}{|K|} = [HK : K]$$

Sabemos também que $H \cap K \leq H$, logo, analogamente:

$$|H| = |H \cap K| \cdot [H : H \cap K] \iff \frac{|H|}{|H \cap K|} = [H : H \cap K]$$

Pela **Proposição 1.5.6**, temos diretamente:

$$|HK| = \frac{|H||K|}{|H \cap K|} \iff \frac{|HK|}{|K|} = \frac{|H|}{|H \cap K|}$$

Logo, deduzimos que:

$$[HK : K] = [H : H \cap K]$$

□

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. □

Observação: muitas vezes iremos denotar $\bar{x} \stackrel{\text{def}}{=} xH$ para elementos de G/H por uma questão de simplificação de escrita.

Exemplo 1.5.5

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 1.5.8

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 $\langle x \rangle = G$.

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

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

Podemos reescrever a expressão acima como:

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

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

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

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

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, $G = Z(G)$. □

Proposição 1.5.9

Seja G um grupo e G' o seu subgrupo de comutadores.

O grupo quociente G/G' é abeliano.

Este grupo é denominado como *abelianização* de G e é denotado como G^{ab} .

Note que G' é o menor subgrupo normal de G com essa propriedade e G^{ab} representa o maior quociente abeliano de G .

Demonstração:

Note, primeiramente, que G^{ab} é de fato um grupo, uma vez que $G' \trianglelefteq G$.

Sejam $\bar{x} = xG'$, $\bar{y} = yG'$ elementos de G^{ab} , com $x, y \in G$, sabemos que:

$$xyx^{-1}y^{-1} \in G' \iff xy(yx)^{-1} \in G' \iff xyG' = yxG' \iff \bar{x}\bar{y} = \bar{y}\bar{x}$$

Concluímos, portanto, que G^{ab} é um grupo abeliano.

Para mostrar que G' é o menor subgrupo normal de G tal que G/G' é abeliano, basta mostrar que para quaisquer $H \trianglelefteq G$, se G/H for abeliano, então $G' \subseteq H$.

Suponha, por absurdo, que G/H é um grupo abeliano e $G' \not\subseteq H$.

Ora, então temos, para $x, y \in G$:

$$xyH = yxH \iff xy(yx)^{-1} \in H \iff xyx^{-1}y^{-1} \in H$$

Sabemos que $xyx^{-1}y^{-1} \in G'$, mas $G' \not\subseteq H$, portanto induzimos um absurdo.

Concluímos que $G' \subseteq H$. □

1.6 Homomorfismos de Grupos

Definição 1.6.1

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

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

Observações:

Note que, se $\varphi : G \rightarrow \mathcal{G}$ for um homomorfismo de grupos, então:

1. $\varphi(e_G) = e_{\mathcal{G}}$;
2. $\varphi(x^{-1}) = \varphi(x)^{-1}$.

De fato, note que, para o item 1., temos que:

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) * \varphi(e_G) \implies \varphi(e_G) = e_{\mathcal{G}}$$

E para o item 2., temos:

$$e_{\mathcal{G}} = \varphi(e_G) = \varphi(x \cdot x^{-1}) = \varphi(x) * \varphi(x^{-1}) \implies \varphi(x^{-1}) = \varphi(x)^{-1}$$

* Note também que muitas vezes as operações de G e de \mathcal{G} serão confundidas para fins de simplificação, isto é: $\varphi(ab) = \varphi(a)\varphi(b)$.

Definição 1.6.2

Sejam G e \mathcal{G} dois grupos. Definimos $\text{Hom}(G, \mathcal{G})$ como o **conjunto de todos os homomorfismos de G em \mathcal{G}** .

Exemplo 1.6.1

$\text{Id} : (G, \cdot) \rightarrow (G, \cdot)$, $\text{Id}(g) = g$ é um homomorfismo chamado *identidade*.

Exemplo 1.6.2

$\theta : G \rightarrow \mathcal{G}$, $\theta(g) = e_{\mathcal{G}}$, $\forall g \in G$, é um homomorfismo chamado *homomorfismo trivial*.

Exemplo 1.6.3

A função:

$$\det : \begin{cases} GL_n(\mathbb{K}) \rightarrow \mathbb{K}^* \\ A \mapsto \det(A) \end{cases}$$

é um homomorfismo de grupos, pois sabemos que $\forall A, B \in GL_n(\mathbb{K})$ temos:

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

Exemplo 1.6.4

Seja G um grupo e $N \trianglelefteq G$, logo a função:

$$\pi : \begin{cases} G \rightarrow G/N \\ x \mapsto xN \end{cases}$$

é um homomorfismo chamado de *projeção canônica*.

Demonstração:

Sejam $x, y \in G$, ora:

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

□

Exemplo 1.6.5

Seja $G = \mathbb{R}_+^* \times \mathbb{R}$ munido da operação \heartsuit definida por:

$$\begin{aligned} (a, b) \heartsuit (a', b') &= (aa', b + b'), \\ (a, b), (a', b') &\in G \end{aligned}$$

A função:

$$\spadesuit: \begin{cases} (G, \heartsuit) \rightarrow (\mathbb{C}^*, \cdot) \\ (r, \theta) \mapsto r e^{i\theta} \end{cases}$$

é um homomorfismo de grupos, onde e é o número de Euler, $i^2 = -1$ e:

$$e^{i\theta} \stackrel{\text{def}}{=} \cos \theta + i \sin \theta, \forall \theta \in \mathbb{R}$$

Demonstração:

Mostremos primeiramente que (G, \heartsuit) é de fato um grupo.

Por construção temos diretamente que \heartsuit é uma lei de composição interna em G .

Também sabemos que, pelo fato de \mathbb{R}_+^* ser um grupo com o produto usual e \mathbb{R} ser um grupo com a adição usual, temos diretamente que a dupla formada pela operação \heartsuit é um grupo.

Portanto, mostramos que (G, \heartsuit) é de fato um grupo.

Mostremos que \spadesuit é um homomorfismo de grupos.

Note, primeiramente, que \spadesuit é claramente uma função de G em \mathbb{C}^* .

Sejam $(r, \theta), (r', \theta') \in G$, temos que:

$$\spadesuit((r, \theta) \heartsuit (r', \theta')) = \spadesuit(rr', \theta + \theta') = rr' e^{i(\theta+\theta')} = \spadesuit(r, \theta) \cdot \spadesuit(r', \theta')$$

Logo, \spadesuit é de fato um homomorfismo de grupos. □

Definição 1.6.3

Definimos o **núcleo de um homomorfismo** φ o **subconjunto** $\ker \varphi \subseteq G$, tal que:

$$\ker \varphi \stackrel{\text{def}}{=} \{x \in G, \varphi(x) = e_G\}.$$

Proposição 1.6.1

O núcleo de um homomorfismo φ é um subgrupo normal de G .

Demonstração:

Note, primeiramente, que $\ker \varphi$ é não-vazio, uma vez que sempre teremos $\varphi(e_G) = e_G$.

Mostremos, portanto, que $\ker \varphi \leq G$.

Para isso, mostremos que $x, y \in \ker \varphi \implies xy^{-1} \in \ker \varphi$.

Sejam $x, y \in \ker \varphi$, temos:

$$\varphi(x \cdot y^{-1}) = \varphi(x) * \varphi(y^{-1}) = \varphi(x) * \varphi(y)^{-1} = e_G * e_G = e_G;$$

Deduzimos que $\ker \varphi \leq G$, mostremos, por fim, que $\ker \varphi \trianglelefteq G$:

Sejam $g, x \in G \times \ker \varphi$, mostremos que $gxg^{-1} \in \ker \varphi$.

$$\varphi(gxg^{-1}) = \varphi(g) * \varphi(x) * \varphi(g^{-1}) = \varphi(g) * e_G * \varphi(g^{-1}) = \varphi(g) * \varphi(g^{-1}) = \varphi(g) * \varphi(g)^{-1} = e_G.$$

Portanto, deduzimos que:

$$\ker \varphi \trianglelefteq G$$

□

Exemplo 1.6.6

Seja $n \in \mathbb{N}^*$. O núcleo do homomorfismo

$$\det : GL_n(\mathbb{K}) \rightarrow \mathbb{K}^*, \quad A \mapsto \det(A)$$

é dado por

$$\ker(\det) = \{A \in GL_n(\mathbb{K}), \det(A) = 1\} = SL_n(\mathbb{K}).$$

Definição 1.6.4

Definimos a **imagem de um homomorfismo** φ o **subconjunto** $\text{Im } \varphi \subseteq \mathcal{G}$ tal que:

$$\text{Im } \varphi \stackrel{\text{def}}{=} \{y \in \mathcal{G} \mid \exists x \in G, y = \varphi(x)\}$$

Proposição 1.6.2

A imagem de um homomorfismo φ é um subgrupo de \mathcal{G} .

Demonstração:

Note, primeiramente, que $\text{Im } \varphi$ é não vazio uma vez que $e_{\mathcal{G}} \in \text{Im } \varphi$.

Mostremos agora que $\forall x, y \in \text{Im } \varphi, xy^{-1} \in \text{Im } \varphi$:

Temos que:

$$x, y \in \text{Im } \varphi \implies \exists a, b \in G, x = \varphi(a) \text{ e } y = \varphi(b)$$

Ora, mas então temos:

$$\exists b^{-1} \in G \implies y^{-1} = \varphi(b^{-1}) = \varphi(b)^{-1}$$

Também temos que:

$$ab^{-1} \in G, \text{ logo, } \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = xy^{-1}$$

Portanto, via a definição de imagem de um homomorfismo de grupos deduzimos que:

$$xy^{-1} \in \text{Im } \varphi$$

Logo, mostramos que $\text{Im } \varphi \leq \mathcal{G}$.

□

Proposição 1.6.3

Sejam G e \mathcal{G} grupos tais que a função $\varphi : G \rightarrow \mathcal{G}$ define um homomorfismo de grupos. Logo:

$$\ker \varphi = \{e_G\} \iff \varphi \text{ injetiva.}$$

Demonstração:

Mostremos a implicação (\Rightarrow):

Para mostrar que φ é injetiva, é necessário mostrar a seguinte implicação:

$$\varphi(x) = \varphi(y) \implies x = y, \forall x, y \in G$$

Suponhamos que $\varphi(x) = \varphi(y)$, logo:

$$\varphi(x) = \varphi(y) \implies \varphi(x)\varphi(y)^{-1} = e_{\mathcal{G}} \implies \varphi(x)\varphi(y^{-1}) = e_{\mathcal{G}} \implies \varphi(xy^{-1}) = e_{\mathcal{G}}$$

Deduzimos, portanto, que $xy^{-1} \in \ker \varphi$.

Ora, por hipótese, temos que $\ker \varphi = \{e_{\mathcal{G}}\}$, logo deduzimos que:

$$x = y$$

Portanto, concluímos que φ é injetiva.

Mostremos a implicação (\Leftarrow):

Agora, supondo que φ é injetiva, mostremos que $\ker \varphi = \{e_{\mathcal{G}}\}$.

Para mostrar que $\ker \varphi = \{e_{\mathcal{G}}\}$ é necessário mostrar:

$$\text{Se } \varphi(x) = e_{\mathcal{G}} \implies x = e_{\mathcal{G}}, \forall x \in G$$

Sabemos que $\varphi(e_{\mathcal{G}}) = e_{\mathcal{G}}$.

Suponha que $\varphi(x) = e_{\mathcal{G}}$, para $x \in G$.

Porém, sabemos que φ é injetiva, logo:

$$\varphi(x) = \varphi(e_{\mathcal{G}}) \implies x = e_{\mathcal{G}}$$

Logo, concluímos que:

$$\ker \varphi = \{e_{\mathcal{G}}\}$$

□

Proposição 1.6.4

Sejam $\varphi : G \rightarrow \mathcal{G}$ e $\xi : \mathcal{G} \rightarrow \mathfrak{G}$ homomorfismos de grupos.

Logo, $(\xi \circ \varphi) : G \rightarrow \mathfrak{G}$ é um homomorfismo de grupos.

Demonstração:

Sejam $a, b \in G$.

Queremos mostrar que:

$$(\xi \circ \varphi)(ab) = (\xi \circ \varphi)(a)(\xi \circ \varphi)(b)$$

Sabemos que φ e ξ são homomorfismos de grupos, portanto:

$$(\xi \circ \varphi)(ab) = \xi(\varphi(ab)) = \xi(\varphi(a)\varphi(b)) = \xi(\varphi(a))\xi(\varphi(b)) = (\xi \circ \varphi)(a)(\xi \circ \varphi)(b)$$

Portanto, mostramos que $(\xi \circ \varphi)$ é de fato um homomorfismo de grupos.

□

Definição 1.6.5

Sejam G e \mathcal{G} grupos. Um homomorfismo $\varphi : G \rightarrow \mathcal{G}$ é chamado de **isomorfismo de grupos se φ é bijetivo**.

Caso φ seja um isomorfismo, dizemos que G e \mathcal{G} são **isomorfos** e denotamos-os como:

$$G \cong \mathcal{G}$$

Observação: note que para que dois grupos sejam isomorfos basta mostrar que existe um isomorfismo entre eles.

Exemplo 1.6.7

$(\mathbb{R}_+^*, \cdot) \cong (\mathbb{R}, +)$, onde $+$ e \cdot denotam as operações usuais de soma e produto, respectivamente, no conjunto \mathbb{R} .

Demonstração:

Seja $\varphi : \mathbb{R}_+^* \rightarrow \mathbb{R}$, $x \mapsto \log(x)$.

Mostremos que φ é um homomorfismo de grupos bijetivo.

Primeiramente, note que (\mathbb{R}_+^*, \cdot) e $(\mathbb{R}, +)$ são de fato grupos.

Sabemos também que a função:

$$\varphi(x) = \log(x), \quad x \in]0, \infty[= \mathbb{R}_+^*$$

é uma bijeção com imagem igual à \mathbb{R} .

Mostremos que φ é um homomorfismo de grupos.

Sejam $x, y \in \mathbb{R}_+^*$

$$\varphi(xy) = \log(xy) = \log(x) + \log(y) = \varphi(x) + \varphi(y)$$

Logo, deduzimos que φ é um isomorfismo de grupos e, portanto, temos:

$$(\mathbb{R}_+^*, \cdot) \cong (\mathbb{R}, +)$$

□

Proposição 1.6.5

Seja G um grupo finito e $g \in G$ tal que $O(g) = k \in \mathbb{Z}_+^*$. Então $\mathbb{Z}/k\mathbb{Z} \cong \langle g \rangle$.

Demonstração:

Nesta demonstração, a notação aditiva será utilizada para denotar a operação de soma usual em $\mathbb{Z}/k\mathbb{Z}$ e a operação do grupo G . Também serão considerados como elementos de $\mathbb{Z}/k\mathbb{Z}$, sem perda de generalidade, apenas os representantes de cada classe lateral do conjunto.

Seja a função φ definida a seguir:

$$\begin{aligned} \varphi : \mathbb{Z}/k\mathbb{Z} &\rightarrow \langle g \rangle \\ &x \mapsto xg \end{aligned}$$

Note que φ é de fato uma função e é injetiva. Sejam $x, y \in \mathbb{Z}/k\mathbb{Z}$.

$$\varphi(x) = \varphi(y) \iff xg = yg \iff xg - yg = 0 \iff g(x - y) = 0$$

Como $x, y \in \mathbb{Z}/k\mathbb{Z}$, então $x, y \in [0, k-1]$. Temos também que $\mathcal{O}(g) = k$. Portanto, temos:

$$g(x - y) = 0 \iff x - y = 0 \iff x = y$$

Logo, φ é de fato função e é injetora.

Note também que φ é trivialmente sobrejetora, uma vez que φ é injetora e $|\mathbb{Z}/k\mathbb{Z}| = \mathcal{O}(g) = k$.

Mostremos, por fim, que φ é um homomorfismo de grupos. Sejam $x, y \in \mathbb{Z}/k\mathbb{Z}$.

$$\varphi(x + y) = (x + y)g = xg + yg = \varphi(x) + \varphi(y)$$

Concluímos que φ é de fato um isomorfismo de grupos e portanto:

$$\mathbb{Z}/k\mathbb{Z} \cong \langle g \rangle$$

□

Proposição 1.6.6

Sejam G e \mathcal{G} grupos tal que $\varphi : G \rightarrow \mathcal{G}$ é um isomorfismo de grupos.

Logo, $\varphi^{-1} : \mathcal{G} \rightarrow G$ é um isomorfismo de grupos.

Demonstração:

Seja $\varphi : G \rightarrow \mathcal{G}$ um isomorfismo de grupos.

Logo:

$$\forall y \in \mathcal{G}, \exists! x \in G : \varphi(x) = y$$

Portanto, temos que:

$$\varphi^{-1}(\varphi(x)) = \varphi^{-1}(y) \iff x = \varphi^{-1}(y)$$

Dada a bijetividade de φ temos diretamente que φ^{-1} é também uma função bijetiva.

Mostremos que φ^{-1} é de fato um homomorfismo de grupos.

Sejam $x, y \in \mathcal{G}$, mostremos que:

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

Dada a bijetividade de φ , sabemos que existem $a, b \in G$ tais que $\varphi(a) = x$ e $\varphi(b) = y$.

Logo:

$$\varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(x)\varphi^{-1}(y)$$

Portanto, $\varphi^{-1} : \mathcal{G} \rightarrow G$ é isomorfismo de grupos.

□

Teorema 1.6.1**Primeiro Teorema dos Isomorfismos**

Sejam G e \mathcal{G} grupos tais que $\varphi : G \rightarrow \mathcal{G}$ é um homomorfismo de grupos. Então, a função ψ tal que:

$$\begin{aligned}\psi : \quad & G / \ker \varphi \rightarrow \text{Im } \varphi \\ & g \ker \varphi \mapsto \varphi(g)\end{aligned}$$

é um isomorfismo de grupos.

Isto é:

$$\frac{G}{\ker \varphi} \cong \text{Im } \varphi$$

Demonstração:

Mostremos que ψ é uma função bem definida e que se trata de uma função injetiva:

Sejam $\bar{x}, \bar{y} \in G / \ker \varphi$, temos:

$$\begin{aligned}\bar{x} = \bar{y} &\iff xy^{-1} \in \ker \varphi \iff \varphi(xy^{-1}) = e_{\mathcal{G}} \iff \\ &\iff \varphi(x)\varphi(y)^{-1} = e_{\mathcal{G}} \iff \varphi(x) = \varphi(y) \iff \psi(\bar{x}) = \psi(\bar{y})\end{aligned}$$

Logo, a função ψ está de fato bem definida e é injetiva.

Mostremos que ψ é uma função sobrejetora.

Seja $y \in \text{Im } \varphi$, então:

$$\exists x \in G; \varphi(x) = y$$

Temos, portanto:

$$\psi(\bar{x}) = \varphi(x) = y$$

Logo, ψ é sobrejetora.

Mostremos que ψ é um homomorfismo de grupos.

Primeiramente, note que $G / \ker \varphi$ e $\text{Im } \varphi$ são de fato grupos (já demonstrado).

Sejam $\bar{x}, \bar{y} \in G / \ker \varphi$, logo:

$$\psi(\bar{x}\bar{y}) = \psi(\bar{x}\bar{y}) = \varphi(xy) = \varphi(x)\varphi(y) = \psi(\bar{x})\psi(\bar{y})$$

Com isso, mostramos que ψ se trata de um isomorfismo de grupos e deduzimos que:

$$\frac{G}{\ker \varphi} \cong \text{Im } \varphi$$

□

Teorema 1.6.2**Segundo Teorema dos Isomorfismos**

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

$$H \trianglelefteq HK$$

e,

$$\frac{K}{H \cap K} \cong \frac{HK}{H}$$

Demonstração:

Note que HK é de fato um grupo, pois $H \trianglelefteq G$ e $K \leq G$.

Tal fato foi mostrado na **Proposição 1.5.4**.

Mostremos, primeiramente, que $H \trianglelefteq HK$:

Seja $x \in HK$, logo, é suficiente mostrar que $xHx^{-1} \subseteq H$.

Como $H \trianglelefteq G$, temos que:

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

Portanto:

$$xHx^{-1} = Hxx^{-1} = H$$

Logo, deduzimos que $H \trianglelefteq HK$.

Seja φ o homomorfismo de grupos definido a seguir:

$$\begin{aligned} \varphi : \quad & K \rightarrow \frac{HK}{H} \\ & x \mapsto xH \end{aligned}$$

Note que $\frac{HK}{H}$ é de fato um grupo, uma vez que $H \trianglelefteq HK$.

Note também que φ se trata mesmo de um homomorfismo (restrição da projeção canônica).

Mostremos que φ é um homomorfismo sobrejetivo.

Tome $x \in \frac{HK}{H}$, logo:

$$x = \underbrace{hk}_{\in HK} H = Hhk = Hk = kH = \varphi(k), \quad k \in K$$

Logo, mostramos que φ é sobrejetiva, isto é:

$$\text{Im}(\varphi) = \frac{HK}{H}$$

Mostremos agora que $\ker \varphi = H \cap K$.

Sabemos que, por definição:

$$\ker \varphi = \{k \in K : \varphi(k) = H\}$$

Deduzimos portanto que $k \in \ker \varphi \iff k \in H \cap K$.

Logo, deduzimos que $\ker \varphi = H \cap K$.

Aplicando o **Primeiro Teorema do Isomorfismo** deduzimos diretamente que:

$$\frac{K}{H \cap K} \cong \frac{HK}{H}$$

□

Teorema 1.6.3**Terceiro Teorema dos Isomorfismos**

Seja G um grupo e $H, K \trianglelefteq G$ tal que $K \subseteq H$.

Logo,

$$\frac{H}{K} \trianglelefteq \frac{G}{K}$$

e,

$$\frac{G/K}{H/K} \cong \frac{G}{H}$$

Demonstração:

Mostremos, primeiramente, que $H/K \trianglelefteq G/K$:

Seja $gK \in G/K$ e $hK \in H/K$, mostremos que $(gK)(hK)(gK)^{-1} \subseteq H/K$:

$$(gK)(hK)(gK)^{-1} = gKhKKg^{-1} = gKhKg^{-1} = ghKKg^{-1} =$$

$$= ghKg^{-1} = \underbrace{ghg^{-1}}_{\in H} K \in H/K$$

Logo, concluímos que:

$$\frac{H}{K} \trianglelefteq \frac{G}{K}$$

Seja a função φ definida a seguir:

$$\begin{aligned} \varphi : \quad & \frac{G}{K} \rightarrow \frac{G}{H} \\ & gK \mapsto gH \end{aligned}$$

Note que, como $K \subseteq H$, todo elemento de G/K é evidentemente elemento de G/H e a função é bem definida, sobrejetora e um homomorfismo de grupos.

Logo, deduzimos que:

$$\text{Im } \varphi = \frac{G}{H}$$

Mostremos que $\ker \varphi = H/K$:

Por definição, sabemos que:

$$\ker \varphi = \{gK \in G/K : \varphi(gK) = H\}$$

Logo:

$$gK \in \ker \varphi \iff \varphi(gK) = H \iff gH = H \iff g \in H \iff gK \subseteq H/K$$

Concluímos que $\ker \varphi = H/K$.

Portanto, aplicando o **Primeiro Teorema dos Isomorfismos** deduzimos diretamente que:

$$\frac{G/K}{H/K} \cong \frac{G}{H}$$

□

Definição 1.6.6

Sejam G e \mathcal{G} grupos.

Um epimorfismo de G em \mathcal{G} é um homomorfismo φ tal que φ é sobrejetivo.

Denotamos o conjunto de todos os epimorfismos de G em \mathcal{G} por $\text{Epi}(G, \mathcal{G})$.

Definição 1.6.7

Sejam G e \mathcal{G} grupos.

Um monomorfismo de G em \mathcal{G} é um homomorfismo φ tal que φ é injetivo.

Denotamos o conjunto de todos os monomorfismos de G em \mathcal{G} por $\text{Mon}(G, \mathcal{G})$.

Definição 1.6.8

Seja G um grupo.

Um automorfismo de G é um isomorfismo φ tal que:

$$\varphi : G \rightarrow G$$

Denotamos o conjunto de todos os automorfismos de G por $\text{Aut}(G)$.

Proposição 1.6.7

Seja G um grupo, então $(\text{Aut}(G), \circ)$ é um grupo, onde \circ denota a composição usual de funções.

Demonstração:

Note que $\text{Aut}(G)$ não é vazio, uma vez que o isomorfismo $\text{id} : G \rightarrow G$, $\text{id}(g) = g$ está em $\text{Aut}(G)$.

Evidentemente a função id é o elemento neutro de $\text{Aut}(G)$.

Também sabemos que a operação \circ é associativa via associatividade de composição usual de funções.

Pela **Proposição 1.6.6**, sabemos que o homomorfismo inverso, φ^{-1} , existe e é um isomorfismo. Logo, concluímos que $\varphi^{-1} \in \text{Aut}(G)$.

Por fim, sabemos que a composição de funções bijetivas resulta em uma função bijetiva e pela **Proposição 1.6.4** sabemos que a composição de homomorfismo de G em G é um homomorfismo de G em G .

Portanto, concluímos que \circ é uma lei de composição interna em $\text{Aut}(G)$.

Logo, deduzimos que $(\text{Aut}(G), \circ)$ é um grupo.

□

Exemplo 1.6.8

A função:

$$\mathcal{I}_g : \begin{matrix} G \rightarrow G \\ x \mapsto gxg^{-1} \end{matrix}$$

é um automorfismo de G denominado **automorfismo interno de G associado a $g \in G$** .

O automorfismo \mathcal{I}_g é também chamado de **conjugação por g** .

Demonstração:

Mostremos que \mathcal{I}_g é de fato um automorfismo de G , dado $g \in G$.

Mostremos, primeiramente, que \mathcal{I}_g é um homomorfismo de grupos.

Sabemos, trivialmente, que \mathcal{I}_g é de fato uma função.

Sejam $x, y \in G$, temos, por definição:

$$\mathcal{I}_g(xy) = gxyg^{-1} = gx(g^{-1}g)yg^{-1} = (gxg^{-1})(gyg^{-1}) = \mathcal{I}_g(x)\mathcal{I}_g(y)$$

Portanto, concluímos que \mathcal{I}_g é um homomorfismo de grupos.

Mostremos que \mathcal{I}_g é uma função bijetiva.

Sejam $x, y \in G$:

$$\mathcal{I}_g(x) = \mathcal{I}_g(y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow g^{-1}gxg^{-1}g = g^{-1}gyg^{-1}g \Rightarrow x = y$$

Logo, \mathcal{I}_g é injetiva.

Tomemos, ainda, $y \in G$ e $x = g^{-1}yg$. Temos, portanto:

$$\mathcal{I}_g(x) = g(g^{-1}yg)g^{-1} = y$$

Logo, \mathcal{I}_g é sobrejetiva.

Concluímos, portanto, que \mathcal{I}_g é um automorfismo de G .

□

Definição 1.6.9

Seja G um grupo, definimos:

$$\text{Inn}(G) = \{\mathcal{I}_g \in \text{Aut}(G) : g \in G\}$$

o conjunto de todos os automorfismos internos de G associados à $g \in G$.

Proposição 1.6.8

Seja G um grupo, temos:

$$\text{Inn}(G) \trianglelefteq \text{Aut}(G).$$

Demonstração:

Sabemos que $\text{Inn}(G) \subseteq \text{Aut}(G)$, por construção.

Mostremos primeiramente que para $\varphi_1, \varphi_2 \in \text{Inn}(G)$, $\varphi_1 \circ \varphi_2^{-1} \in \text{Inn}(G)$, onde \circ é a composição usual de funções.

Como o domínio e contradomínio das funções em $\text{Inn}(G)$ são iguais para as funções em $\text{Aut}(G)$, mostremos apenas a igualdade de suas leis de correspondência.

Ora, como $\varphi_1, \varphi_2 \in \text{Inn}(G)$, podemos escrevê-los, sem perda de generalidade, para um dado $x \in G$, como:

$$\varphi_1(x) = g_1 x g_1^{-1}, \quad g_1 \in G$$

$$\varphi_2(x) = g_2 x g_2^{-1}, \quad g_2 \in G$$

Temos:

$$\varphi_1 \circ \varphi_2^{-1}(x) = \varphi_1(\varphi_2^{-1}(x)) = g_1(g_2^{-1} x g_2)g_1^{-1} = (g_1 g_2^{-1})x(g_2 g_1^{-1}) =$$

$$= (g_1 g_2^{-1})x(g_1 g_2^{-1})^{-1} \in \text{Inn}(G)$$

Logo, concluímos que $\text{Inn}(G) \leq \text{Aut}(G)$.

Provemos agora que para $(\varphi, \phi) \in \text{Inn}(G) \times \text{Aut}(G)$, $\phi \circ \varphi \circ \phi^{-1} \in \text{Inn}(G)$. Seja $x \in G$ tal que:

$$\varphi(x) = g x g^{-1}, \quad g \in G$$

Temos:

$$(\phi \circ \varphi \circ \phi^{-1})(x) = \phi(\varphi(\phi^{-1}(x))) = \phi(g\phi^{-1}(x)g^{-1}) = \phi(g)x\phi(g)^{-1} \in \text{Inn}(G)$$

Logo, concluímos que:

$$\text{Inn}(G) \trianglelefteq \text{Aut}(G)$$

□

Definição 1.6.10

Seja G um grupo e $\varphi : G \rightarrow G$ um homomorfismo de grupos.

Dizemos que $X \subseteq G$ é **invariante por** φ se $\varphi(X) \subseteq X$.

Ou ainda, se $\forall x \in X \implies \varphi(x) \in X$.

Definição 1.6.11

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

H é dito **subgrupo característico de** G se H é invariante para todo $\varphi \in \text{Aut}(G)$ e o denotamos como:

$$H \trianglelefteq \triangleleft G$$

Observações:

- A partir da definição acima temos que, se $H < G$ e H é subgrupo característico de G , denotamos $H \triangleleft G$;

- A definição de subgrupo característico é considerada mais forte que a definição de subgrupo normal, uma vez que enquanto um subgrupo normal é invariante apenas para automorfismos internos, um subgrupo característico é invariante para todo automorfismo de G :

$$\begin{array}{ccc}
 H \leq G & \text{operação bem definida} \\
 \uparrow & & \\
 H \trianglelefteq G & \text{invariante por conjugação} \\
 \uparrow & & \\
 H \triangleleft G & \text{invariante por automorfismos}
 \end{array}$$

- Temos, portanto, diretamente que $H \triangleleft G \implies H \trianglelefteq G$.

Exemplo 1.6.9

Os subgrupos triviais de G são subgrupos característicos de G .

Exemplo 1.6.10

Seja G um grupo e $Z(G)$ seu centro, logo:

$$Z(G) \triangleleft G$$

Demonstração:

Seja $z \in Z(G)$, temos por definição que:

$$zg = gz, \forall g \in G$$

Seja $\varphi \in \text{Aut}(G)$, temos:

$$\varphi(zg) = \varphi(gz) \iff \varphi(z)\varphi(g) = \varphi(g)\varphi(z)$$

Como φ é um automorfismo, então sabemos que se trata de uma função bijetora. Logo, $\varphi(G) = G$ e podemos escrever $\varphi(g) = h$, $h \in G$.

Temos, portanto:

$$\varphi(z)h = h\varphi(z), \forall h \in G$$

Concluímos que $\varphi(z) \in Z(G)$.

Logo:

$$Z(G) \triangleleft G$$

□

Proposição 1.6.9

Seja $K \trianglelefteq H \trianglelefteq G$, então $K \trianglelefteq G$.

Demonstração:

Seja $\varphi \in \text{Aut}(H)$ tal que:

$$\varphi(K) \stackrel{\text{def}}{=} gKg^{-1}$$

Note que a função acima é bem definida uma vez que $K \subseteq H$ e $gHg^{-1} \in H$.

Como $K \trianglelefteq H$, então $\varphi(K) \subseteq K$.

Concluímos que:

$$gKg^{-1} \in K \implies K \trianglelefteq G.$$

□

Observações: note que $K \trianglelefteq H \trianglelefteq G \not\Rightarrow K \trianglelefteq G$.

Tomemos como contraexemplo a seguinte cadeia de normalidade:

$$\underbrace{\{e, s\}}_{\stackrel{\text{def}}{=} K} \trianglelefteq \underbrace{\{e, r^2, s, r^2s\}}_{\stackrel{\text{def}}{=} H} \trianglelefteq \underbrace{D_4}_{\stackrel{\text{def}}{=} G}.$$

Onde D_4 é o Grupo Diedral D_4 , s representa uma reflexão/espelhamento, r representa uma rotação de 90° no sentido antihorário e e representa o elemento neutro.

Note que de fato a cadeia de normalidade é verificada, uma vez que:

1. Temos que $K \leq H \leq G$;
2. K é evidentemente abeliano e portanto $K \trianglelefteq H$;
3. $\frac{|G|}{|H|} = 2$ e, pela **Proposição 1.5.2** temos diretamente que $H \trianglelefteq G$.

Mostremos que o item 1. é de fato verdadeiro, validando os itens 2. e 3..

Note que $H \subseteq D_4$ e é evidentemente não vazio. Além disso, cada elemento de H é seu próprio elemento inverso.

Temos também para os resultados não triviais gerados a partir das operações entre os elementos de H :

$$r^2r^2s = r^4s = s, \quad sr^2 = r^2s, \quad sr^2s = r^2, \quad r^2sr^2 = s, \quad r^2s^2 = r^2$$

Note que todos os resultados pertencem ao conjunto H .

Portanto, $H \leq G$. Note que $K \leq H$, trivialmente.

Concluímos que $K \leq H \leq G$ e, pelos itens 2. e 3., $K \trianglelefteq H \trianglelefteq G$.

Note, porém, que K não é normal a G , uma vez que:

$$\underbrace{r}_{\in G} \cdot \underbrace{s}_{\in K} \cdot \underbrace{r^{-1}}_{\in G} = r^2s \notin K$$

Concluímos, portanto, via contraexemplo, que a normalidade não é transitiva.

1.7 Produto Direto de Grupos

Nesta seção inteira a variável n representa um número inteiro positivo.

Definição 1.7.1

Seja $\mathfrak{G} = \{G_1, \dots, G_n\}$ uma família de grupos.

Definimos **produto direto externo** de \mathfrak{G} como sendo o conjunto $G_1 \times \dots \times G_n$ munido da operação:

$$(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) \stackrel{\text{def}}{=} (x_1 y_1, \dots, x_n y_n).$$

Denotamos, comumente:

$$\prod_{i=1}^n G_i \stackrel{\text{def}}{=} G_1 \times \dots \times G_n.$$

Observação: por uma questão de convenção, a operação “.” será omitida.

Proposição 1.7.1

A partir da **Definição 1.7.1**, temos que o produto direto externo de \mathfrak{G} é um grupo.

Demonstração:

Via a **Definição 1.7.1** temos que a operação “.” é uma lei de composição interna por construção.

Temos também, de forma evidente, que o elemento neutro e o elemento inverso de $x \stackrel{\text{def}}{=} (x_1, \dots, x_n) \in \prod_{i=1}^n G_i$ são dados por, respectivamente:

$$e \stackrel{\text{def}}{=} (e_1, \dots, e_n) \in \prod_{i=1}^n G_i$$

Onde e_n representa o elemento neutro do n -ésimo grupo do produto direto externo.

$$x^{-1} \stackrel{\text{def}}{=} (x_1^{-1}, \dots, x_n^{-1}) \in \prod_{i=1}^n G_i$$

Onde x_n^{-1} representa o elemento inverso para x_n no n -ésimo grupo do produto direto externo.

Temos também que o produto direto externo de \mathfrak{G} é evidentemente associativo, uma vez que G_1, \dots, G_n são grupos.

Concluímos, portanto, que $(\prod_{i=1}^n G_i, \cdot)$ é um grupo. □

Definição 1.7.2

Sejam G um grupo e $H_1, \dots, H_n \leq G$.

Dizemos que G é um **produto direto interno** de H_1, \dots, H_n se, e somente se, as seguintes condições são satisfeitas:

- $G = H_1 \dots H_n$;
- $H_i \trianglelefteq G$, $\forall i \in [\![1, n]\!]$;

- $H_i \cap H_1 \dots H_{i-1} H_{i+1} \dots H_n = \{e\}$, $\forall i \in \llbracket 2, n-1 \rrbracket$.

Caso G e H_1, \dots, H_n satisfaçam as condições acima, denotamos:

$$G \stackrel{\text{def}}{=} \bigodot_{i=1}^n H_i$$

Proposição 1.7.2

Sejam G um grupo e $H_1, \dots, H_n \leq G$.

Se G for um produto direto interno de H_1, \dots, H_n , então quaisquer elementos de H_1, \dots, H_n distintos comutam entre si.

Demonstração:

Sejam $(h_i, h_j) \in H_i \times H_j$, onde $i, j \in \llbracket 1, n \rrbracket$ e $i \neq j$.

Tomemos o elemento $g \stackrel{\text{def}}{=} [h_i, h_j] = h_i h_j h_i^{-1} h_j^{-1} \in G$.

Note que:

$$h_i h_j h_i^{-1} h_j^{-1} = (h_i h_j h_i^{-1}) h_j^{-1} \in H_j, \text{ pois } H_j \trianglelefteq G$$

$$h_i h_j h_i^{-1} h_j^{-1} = h_i (h_j h_i^{-1} h_j^{-1}) \in H_i, \text{ pois } H_i \trianglelefteq G$$

Temos, portanto, que $[h_i, h_j] \in H_i \cap H_j = \{e\}$.

Logo:

$$h_i h_j h_i^{-1} h_j^{-1} = e \iff h_i h_j = h_j h_i$$

Logo, quaisquer fatores de H_1, \dots, H_n distintos comutam entre si. □

Teorema 1.7.1

Sejam G um grupo e $H_1, \dots, H_n \leq G$.

Temos, a partir das notações nas definições 1.7.1 e 1.7.2, que:

$$G = \bigodot_{i=1}^n H_i \implies G \cong \prod_{i=1}^n H_i$$

Demonstração:

Suponha que $G = \bigodot_{i=1}^n H_i$.

Tomemos a função μ tal que:

$$\begin{aligned} \mu : \quad G &\rightarrow \prod_{i=1}^n H_i \\ h_1 \dots h_n &\mapsto (h_1, \dots, h_n) \end{aligned}$$

Note que a função está de fato bem definida e é trivialmente bijetiva por construção (a representação dos elementos $h_1 \dots h_n$ é considerada por definição única).

Mostremos, por fim, que μ é um homomorfismo de grupos.

Sejam $g \stackrel{\text{def}}{=} h_1 \dots h_n$ e $g' \stackrel{\text{def}}{=} h'_1 \dots h'_n$.

Temos:

$$\begin{aligned}\mu(gg') &= \mu((h_1 \dots h_n)(h'_1 \dots h'_n)) \\ &= \mu(h_1 h'_1 \dots h_n h'_n) \quad (\text{Proposição 1.7.2}) \\ &= (h_1 h'_1, \dots, h_n h'_n) \\ &= (h_1, \dots, h_n)(h'_1, \dots, h'_n) \\ &= \mu(g)\mu(g')\end{aligned}$$

Logo, μ é um isomorfismo de grupos e temos que:

$$G \cong \prod_{i=1}^n H_i$$

□

Observação: note que pela Proposição 1.6.4 temos também diretamente que:

$$G \cong \bigodot_{i=1}^n H_i \implies G \cong \prod_{i=1}^n H_i$$

Teorema 1.7.2

Teorema Chinês do Resto

Seja $M \stackrel{\text{def}}{=} m_1 \dots m_n \in \mathbb{Z}_+^*$ tal que $\text{mdc}(m_i, m_j) = 1$, $\forall i, j \in \llbracket 1, n \rrbracket$ e $i \neq j$.

Então:

$$\mathbb{Z}/M\mathbb{Z} \cong \prod_{i=1}^n \mathbb{Z}/m_i\mathbb{Z}$$

Demonstração:

Seja $M_i \stackrel{\text{def}}{=} \frac{M}{m_i}$, $\forall i \in \llbracket 1, n \rrbracket$. Note que $\overline{M_i} \in \mathbb{Z}/M\mathbb{Z}$, uma vez que $M_i \in \llbracket 1, M-1 \rrbracket$.

Note também que, evidentemente, temos $\mathcal{O}(M_i) = m_i$, uma vez que $m_i M_i = M$.

A partir da Proposição 1.6.5 temos portanto $\mathbb{Z}/m_i\mathbb{Z} \cong \langle M_i \rangle \cong \langle \overline{M_i} \rangle$.

Mostremos que $\mathbb{Z}/M\mathbb{Z} = \bigodot_{i=1}^n \langle \overline{M_i} \rangle$.

É evidente que $\langle \overline{M_i} \rangle \leq \mathbb{Z}/M\mathbb{Z}$, uma vez que, por definição, ele é um subgrupo gerado. Além disso, por estar munido da soma usual dos inteiros, também é um grupo abeliano. Temos diretamente que $\langle \overline{M_i} \rangle \trianglelefteq \mathbb{Z}/M\mathbb{Z}$.

Portanto, devido a operação de soma usual de inteiros, denotemos:

$$\langle \overline{M_1} \rangle \dots \langle \overline{M_n} \rangle \stackrel{\text{def}}{=} \sum_{i=1}^n \langle \overline{M_i} \rangle$$

Mostremos que:

$$\mathfrak{M} \stackrel{\text{def}}{=} \langle \overline{M_i} \rangle \cap \sum_{\substack{j \neq i \\ j \in \llbracket 1, n \rrbracket}} \langle \overline{M_j} \rangle = \{0\}, \quad \forall i \in \llbracket 1, n \rrbracket$$

Tomemos $\bar{x} \in \mathfrak{M}$.

Seja $\bar{x} \in \langle \overline{M_i} \rangle \setminus \{0\}$, temos por definição (e pela coprimalidade entre m_1, \dots, m_n) que $m_i \nmid x$, onde x é qualquer representante da classe lateral \bar{x} .

Seja $\bar{x} \in \langle \overline{M_i} \rangle \cup \mathfrak{M}$, logo x é expresso como combinação linear de elementos de $\langle \overline{M_1} \rangle, \dots, \langle \overline{M_{i-1}} \rangle, \langle \overline{M_{i+1}} \rangle, \dots, \langle \overline{M_n} \rangle$. Perceba que, por definição, todos os representantes de classe dos elementos de tais conjuntos são divisíveis por m_i , portanto $m_i \mid x$.

Como para $\bar{x} \in \mathfrak{M}$ temos $m_i \mid x$ e $m_i \nmid x$, concluímos que $\bar{x} = \bar{0}$.

Mostremos, por fim, que:

$$\sum_{i=1}^n \langle \overline{M_i} \rangle = \mathbb{Z}/M\mathbb{Z}$$

Note que pela **Proposição 1.5.6** temos que:

$$\left| \sum_{i=1}^n \langle \overline{M_i} \rangle \right| = \left| \langle \overline{M_1} \rangle + \sum_{i=2}^n \langle \overline{M_i} \rangle \right| = \frac{|\langle \overline{M_1} \rangle| \left| \sum_{i=2}^n \langle \overline{M_i} \rangle \right|}{\underbrace{\left| \langle \overline{M_1} \rangle \cap \sum_{i=2}^n \langle \overline{M_i} \rangle \right|}_{=1}} = m_1 \left| \sum_{i=2}^n \langle \overline{M_i} \rangle \right|$$

Aplicando a fórmula indutivamente em i , temos que:

$$\left| \sum_{i=1}^n \langle \overline{M_i} \rangle \right| = m_1 \left| \sum_{i=2}^n \langle \overline{M_i} \rangle \right| = \dots = m_1 \dots m_n = M$$

Como $\sum_{i=1}^n \langle \overline{M_i} \rangle \subseteq \mathbb{Z}/M\mathbb{Z}$, deduzimos diretamente que:

$$\sum_{i=1}^n \langle \overline{M_i} \rangle = \mathbb{Z}/M\mathbb{Z}$$

Concluímos, finalmente, que:

$$\mathbb{Z}/M\mathbb{Z} = \bigoplus_{i=1}^n \langle \overline{M_i} \rangle \implies \mathbb{Z}/M\mathbb{Z} \cong \prod_{i=1}^n \mathbb{Z}/m_i\mathbb{Z}$$

□

Exemplo 1.7.1

Seja $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Como $6 = 3 \cdot 2$ e $\text{mdc}(2, 3) = 1$, temos que:

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

Onde $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$, $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$ e:

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{(\bar{a}, \bar{b}); \bar{a} \in \mathbb{Z}/2\mathbb{Z}, \bar{b} \in \mathbb{Z}/3\mathbb{Z}\}.$$

1.8 Produto Semidireto de Grupos

Capítulo 2

Grupo Simétrico

2.1 Generalidades sobre o grupo simétrico

Retomemos com mais detalhes a construção do *grupo simétrico*, introduzido de forma breve no **Exemplo 1.2.3**.

Definição 2.1.1

Seja X um conjunto finito e não vazio. A função bijetiva $\sigma : X \rightarrow X$ é chamada de **permutação de X** .

Denotamos o conjunto de todas as permutações de X como \mathfrak{S}_X . Se $X = \{1, \dots, n\}$ então também podemos denotar \mathfrak{S}_X como \mathfrak{S}_n , onde $n \in \mathbb{Z}_+^*$.

Observação: por convenção o símbolo para composição usual de funções será omitido, isto é, para $\sigma, \tau \in \mathfrak{S}_X$:

$$\sigma\tau \stackrel{\text{def}}{=} \sigma \circ \tau$$

Definição 2.1.2

O conjunto \mathfrak{S}_X munido da operação usual de composição de funções é chamado de **grupo de permutações de X** , ou **grupo simétrico de X** .

Observações:

- Note que o conjunto \mathfrak{S}_X com a composição usual de funções forma de fato um grupo, uma vez que a composição de funções bijetivas retorna de fato uma função bijetiva, a composição é associativa, toda função bijetiva admite uma função inversa e o elemento neutro é a função identidade, qual denotaremos $e \stackrel{\text{def}}{=} id_X$.
- Seja $X = \{1, \dots, n\}$ e $\sigma \in \mathfrak{S}_n$, utilizamos comumente a notação a seguir para descrever a permutação σ :

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

Exemplo 2.1.1

Sejam $\sigma, \tau \in \mathfrak{S}_3$, tal que:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Temos:

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

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

Note que $\sigma\tau \neq \tau\sigma$, logo \mathfrak{S}_3 não é grupo abeliano.

Evidentemente, \mathfrak{S}_X não é abeliano para $\text{Card}(X) \geq 3$.

Proposição 2.1.1

Seja X um conjunto não vazio tal que $\text{Card}(X) = n \in \mathbb{Z}_+^*$.

Então $|\mathfrak{S}_X| = n!$.

Demonstração:

Seja $\sigma \in \mathfrak{S}_X$ e $X \stackrel{\text{def}}{=} \{a_1, \dots, a_n\}$.

Como σ é uma função bijetiva, então para um elemento $a_i \in X$ é possível realizar n escolhas de imagem de a_i para $a_j \in X$, com $i, j \in \llbracket 1, n \rrbracket$.

Uma vez tomada essa relação entre os dois elementos de X tomamos novamente um $a_k \in X \setminus \{a_i\}$ e escolhemos uma imagem no conjunto $X \setminus \{a_j\}$. Como $X \setminus \{a_j\}$ possui $\text{Card}(X) - 1$ elementos, possuímos $n - 1$ escolhas de bijeção.

Realizamos esse passo a passo recursivamente até bijetarmos todo os elementos do domínio X .

Como todos as escolhas de bijeção em cada passo formam escolhas independentes, podemos utilizar o princípio multiplicativo para mostrar diretamente que existem no total $n \cdot (n - 1) \cdot \dots \cdot 1 = n!$ possibilidades de funções bijetoras em \mathfrak{S}_X .

Portanto, $|\mathfrak{S}_X| = n!$.

□

Teorema 2.1.1**Teorema de Cayley**

Sejam G um grupo finito tal que $|G| = n \in \mathbb{Z}_+^*$ e G_0 seu conjunto subjacente (isto é, o conjunto G sem a estrutura de grupo).

A função Υ :

$$\begin{aligned} \Upsilon : G &\longrightarrow \mathfrak{S}_{G_0} \\ g &\longmapsto \Upsilon_g : G_0 &\longrightarrow G_0 \\ &&x &\longmapsto gx \end{aligned}$$

é um homomorfismo injetivo.

Demonstração:

Mostremos que Υ é de fato função e é injetiva.

Sejam $g_1, g_2 \in G$ tais que $g_1 = g_2$, temos que:

$$g_1 = g_2 \iff g_1x = g_2x \iff \Upsilon_{g_1} = \Upsilon_{g_2} \iff \Upsilon(g_1) = \Upsilon(g_2)$$

Portanto, Υ é função injetiva.

Mostremos que Υ é um homomorfismo de grupos.

Sejam $g_1, g_2 \in G$, temos que:

$$\Upsilon(g_1g_2) = \Upsilon_{g_1g_2}(x) = g_1g_2x = g_1(g_2x) = \Upsilon_{g_1}\Upsilon_{g_2} = \Upsilon(g_1)\Upsilon(g_2)$$

Portanto, Υ é um homomorfismo injetivo. □

Observações:

- Note que G não é isomorfo a \mathfrak{S}_{G_0} , uma vez que $|G| = n \neq |\mathfrak{S}_{G_0}| = n!$, como mostrado na **Proposição 2.1.1**;
- Como mostramos que se trata de um homomorfismo de grupos injetivo, então a estrutura de grupo é preservada e é possível mapear cada elemento de G para algum elemento de \mathfrak{S}_{G_0} , em outras palavras:
 ”**Todo grupo finito é isomorfo a um subgrupo de um grupo simétrico**”.

Exemplo 2.1.2

Colocar algum exemplo do Teorema de Cayley...

Definição 2.1.3

Seja X um conjunto finito e não vazio. Chamamos de **suporte de uma permutação σ de X** o conjunto de elementos em X cuja imagem é diferente do elemento no domínio. Isto é:

$$\text{supp}(\sigma) \stackrel{\text{def}}{=} \{x \in X, \sigma(x) \neq x\}.$$

Exemplo 2.1.3

Seja $\sigma \in \mathfrak{S}_5$ tal que:

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

Temos que $\text{supp}(\sigma) = \{1, 2, 3\}$.

Proposição 2.1.2

Sejam X um conjunto finito não vazio e $\sigma \in \mathfrak{S}_X$.

Se $x \in \text{supp}(\sigma)$, então $\sigma^n(x) \in \text{supp}(\sigma)$, $\forall n \in \mathbb{Z}$.

Demonstração:

Suponha que $x \in \text{supp}(\sigma)$, por definição temos que $\sigma(x) \neq x$.

Pela bijetividade, temos que $\sigma(\sigma(x)) = \sigma^2(x) \neq \sigma(x)$ e, portanto, $\sigma(x) \in \text{supp}(\sigma)$.

Realizando recursivamente este procedimento temos evidentemente que $\sigma^n(x) \in \text{supp}(\sigma)$, $\forall n \in \mathbb{Z}_+$.

Como X é um conjunto finito, observamos que quaisquer potências negativas de σ equivalem à potências positivas, pois a ordem de σ é finita. Portanto, o resultado vale para qualquer $n \in \mathbb{Z}$. □

Observação: deduzimos, portanto, que o suporte de uma permutação σ de X é invariante sob σ .

Proposição 2.1.3

Sejam X um conjunto finito e não vazio tal que $\text{Card}(X) = n \in \mathbb{Z}_+^*$ e $\tau_1, \dots, \tau_k \in \mathfrak{S}_X$ de suporte dois a dois disjuntos, onde $k \in [\![1, n]\!]$.

Seja $\sigma \in \mathfrak{S}_X$ tal que $\sigma = \tau_1 \dots \tau_k$, então para $x \in X$ temos:

$$\sigma(x) = \begin{cases} \tau_i(x) & \text{se } x \in \text{supp}(\tau_i) \text{ para } i \in [\![1, k]\!], \\ x & \text{se } x \notin \text{supp}(\tau_i) \text{ para } i \in [\![1, k]\!]. \end{cases}$$

Temos também que os elementos τ_1, \dots, τ_k comutam entre si e:

$$\text{supp}(\sigma) = \bigsqcup_{i=1}^k \text{supp}(\tau_i).$$

Demonstração:

Seja $x \in \text{supp}(\tau_i)$, para algum $i \in [\![1, k]\!]$. Pela **Proposição 2.1.2** temos que $\tau_i(x) \in \text{supp}(\tau_i)$.

Como $\forall j \in [\![1, k]\!]$ tal que $i \neq j$ temos que $\text{supp}(\tau_j) \cap \text{supp}(\tau_i) = \emptyset$, então $\sigma(x) = \tau_i(x)$.

Caso $x \notin \text{supp}(\tau_i)$, para algum $i \in [\![1, k]\!]$, temos evidentemente que $\sigma(x) = x$, uma vez que $\sigma = \tau_1 \dots \tau_k$.

Note que a composição entre os elementos τ_1, \dots, τ_k também comuta.

Sejam $i, j \in [\![1, k]\!]$ tais que $i \neq j$. Suponha que $x \in \text{supp}(\tau_i)$. Como $\text{supp}(\tau_i) \cap \text{supp}(\tau_j) = \emptyset$, temos que:

$$\tau_i(\tau_j(x)) = \underbrace{\tau_i(x)}_{\in \text{supp}(\tau_i)} = \tau_j(\tau_i(x))$$

Simetricamente o mesmo é válido para $x \in \text{supp}(\tau_j)$. Suponha, agora, que $x \notin \text{supp}(\tau_i) \sqcup \text{supp}(\tau_j)$, temos trivialmente que:

$$\tau_i(\tau_j(x)) = \tau_i(x) = x = \tau_j(\tau_i(x)) = \tau_j(x)$$

Portanto temos que $\tau_i \tau_j = \tau_j \tau_i$, $\forall i, j \in [\![1, k]\!]$ tais que $i \neq j$.

A partir das observações feitas acima temos diretamente que:

$$\text{supp}(\sigma) = \bigsqcup_{i=1}^k \text{supp}(\tau_i).$$

□

2.2 Ciclos e transposições

Definição 2.2.1

Seja $X = \{x_1, \dots, x_n\}$ tal que $\text{Card}(X) \geq 2$. Uma permutação $\sigma \in \mathfrak{S}_X$ é chamada de **k -ciclo** (onde $k \in \llbracket 2, n \rrbracket$) se:

$$\begin{aligned}\sigma(x_1) &= x_2 \\ \sigma(x_2) &= x_3 \\ &\dots \\ \sigma(x_{k-1}) &= x_k \\ \sigma(x_k) &= x_1 \\ \sigma(y) &= y, y \in X \setminus \{x_1, \dots, x_k\}\end{aligned}$$

Denotamos tal k -ciclo como:

$$\sigma \stackrel{\text{def}}{=} (x_1 \dots x_k).$$

Observações:

- A notação x_1, \dots, x_k utilizada não implica que o ciclo deve atuar necessariamente nos primeiros k elementos indexados do conjunto X . De maneira rigorosa, um k -ciclo é determinado por uma escolha ordenada de k elementos distintos $a_1, \dots, a_k \in X$. A definição aplica-se fazendo a correspondência $\sigma(a_i) = a_{i+1}$ (com $a_{k+1} = a_1$ e fixando todos os elementos em $X \setminus \{a_1, \dots, a_k\}$);
- Note que, por definição, se $\sigma = (x_1 x_2 \dots x_k)$, então $\text{supp}(\sigma) = \{x_1 x_2 \dots x_k\}$;
- Perceba que a escolha de x_1 como ponto de partida para o k -ciclo σ é arbitrária, é possível começar com qualquer outro $x_i \in \text{supp}(\sigma)$:

$$(x_1 x_2 \dots x_k) = (x_i x_{i+1} \dots x_k x_1 \dots x_{i-1});$$

- Chamamos também um k -ciclo de **ciclo de largura k** ;
- Caso σ, τ sejam ciclos com suportes dois a dois disjuntos, temos diretamente via a **Proposição 2.1.3** que $\sigma\tau = \tau\sigma$;
- Note que nem toda permutação é um ciclo. Tomemos $\sigma \in \mathfrak{S}_4$ tal que:

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

Evidentemente σ não é um ciclo, porém σ pode ser escrito como produto de 2 ciclos de suportes disjuntos.

Definição 2.2.2

Uma **transposição** é um 2-ciclo.

Proposição 2.2.1

Sejam $X = \{x_1, \dots, x_n\}$ para $n \geq 2$. Logo, todo k -ciclo de \mathfrak{S}_X é igual a um produto de $k - 1$ transposições.

Demonstração:

Seja $\sigma \in \mathfrak{S}_X$ tal que $\sigma = \underbrace{(x_1 \ x_k)(x_1 \ x_{k-1}) \dots (x_1 \ x_2)}_{k-1 \text{ transposições}}$.

Sabemos também que se $x \notin \{x_1, \dots, x_k\}$ então $\sigma(x) = x$.

Perceba pela definição de σ que $\sigma(x_1) = x_2$, $\sigma(x_2) = x_3$, \dots , $\sigma(x_k) = x_1$.

Logo temos diretamente que $\sigma = (x_1 \ \dots \ x_k)$.

□

Exemplo 2.2.1

Tomemos alguns exemplos de permutações em \mathfrak{S}_3 :

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

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

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \ 2 \ 3) = (2 \ 3 \ 1) = (3 \ 1 \ 2) = (1 \ 2)(2 \ 3).$$

Proposição 2.2.2

Sejam $X = \{x_1, \dots, x_n\}$ para $n \geq 2$ e $\sigma \in \mathfrak{S}_X$ um k -ciclo, onde $k \in \llbracket 2, n \rrbracket$.
Então $\mathcal{O}(\sigma) = k$.

Demonstração:

Note primeiramente que $\mathcal{O}(\sigma) \geq k$, pois $\forall i \in \llbracket 1, k-1 \rrbracket$ temos $\sigma^i(x_1) \neq x_1$.

Perceba que $\sigma^{k-1}(x_1) = x_k \implies \sigma^k(x_1) = x_1$.

Analogamente, realizamos o mesmo procedimento $\forall i \in \llbracket 2, k \rrbracket$.

Deduzimos que $\sigma^k = \text{id}_X \implies \mathcal{O}(\sigma) = k$.

□

Proposição 2.2.3

Seja $X = \{x_1, \dots, x_n\}$ para $n \geq 2$. Tomemos $\sigma \in \mathfrak{S}_X$ tal que:

$$\sigma = \gamma_1 \dots \gamma_t, \quad t \in \llbracket 1, n \rrbracket$$

Onde γ_i é um k_i -ciclo, $\forall i \in \llbracket 1, t \rrbracket$ e γ_i, γ_j tem suportes disjuntos $\forall i, j \in \llbracket 1, t \rrbracket$, $i \neq j$.

Então, $\mathcal{O}(\sigma) = \text{mmc}(k_1, \dots, k_t)$.

Demonstração:

Seja $h \in \mathbb{Z}_+^*$ tal que $\sigma^h = \text{id}_X$.

Note que, como $\gamma_i \gamma_j = \gamma_j \gamma_i$, $\forall i, j \in \llbracket 1, t \rrbracket$ tal que $i \neq j$, pela **Proposição 2.1.3** temos:

$$\sigma^h = (\gamma_1 \dots \gamma_t)^h = \gamma_1^h \dots \gamma_t^h = \text{id}_X$$

Como os suportes de cada fator γ de σ são dois a dois disjuntos, é necessário que h seja um múltiplo de cada ordem k_i para cada γ_i , $\forall i \in \llbracket 1, t \rrbracket$ simultaneamente.

Por definição, temos que $\min(h) = \text{mmc}(k_1, \dots, k_t)$.

Como $\mathcal{O}(\sigma) = \min(h)$, deduzimos que $\mathcal{O}(\sigma) = \text{mmc}(k_1, \dots, k_t)$. □

Teorema 2.2.1

Seja $X = \{x_1, \dots, x_n\}$ para $n \geq 2$. Então toda permutação $\sigma \in \mathfrak{S}_X \setminus \{\text{id}_X\}$ pode ser decomposta em um produto de ciclos de suportes dois a dois disjuntos. Tal decomposição é única, exceto pela ordem em que os ciclos são escritos.

Demonstração:

Seja $\sigma \in \mathfrak{S}_X \setminus \{\text{id}_X\}$.

Tomemos de forma arbitrária um elemento x_j , com $j \in \llbracket 1, n \rrbracket$ tal que $\sigma(x_j) \neq x_j$. Note que é garantido que tal elemento exista, uma vez que $\sigma \neq \text{id}_X$.

Definimos o seguinte conjunto:

$$\mathfrak{O}(x) \stackrel{\text{def}}{=} \{\sigma^k(x) ; k \in \mathbb{Z}\}$$

Note que a restrição $\sigma|_{\mathfrak{O}(x)}$ forma um k -ciclo e $\text{supp}(\sigma|_{\mathfrak{O}(x)}) = \mathfrak{O}(x)$, pela **Proposição 2.1.2**.

Realizamos o mesmo procedimento para todo $x \in X \setminus \mathfrak{O}(x_j)$ tal que $\sigma(x) \neq x$ e assim sucessivamente. Como X é um conjunto finito, realizamos tal procedimento em um número finito de passos.

Pela **Proposição 2.1.3** temos que a família $\{\mathfrak{O}(x)\}_{x \in X}$ forma uma partição de $X \setminus I$, onde $I \stackrel{\text{def}}{=} \{x \in X ; \sigma(x) = x\}$.

Sendo \mathfrak{R} o conjunto dos representantes de cada k_x -ciclo $\sigma|_{\mathfrak{O}(x)}$, $\forall x \in X \setminus I$, temos:

$$\text{supp}(\sigma) = \bigsqcup_{r \in \mathfrak{R}} \text{supp}(\sigma|_{\mathfrak{O}(r)})$$

deduzimos que σ é igual a composição de todo k_x -ciclo $\sigma|_{\mathfrak{O}(r)}$, onde $r \in \mathfrak{R}$.

Mostremos que tal decomposição é única.

Sejam $\sigma_1 = \rho_1 \dots \rho_h$ e $\sigma_2 = \eta_1 \dots \eta_m$ duas decomposições em ciclos de suportes dois a dois disjuntos de σ , onde $h, m \in \llbracket 1, \lfloor \frac{n}{2} \rfloor \rrbracket$.

Perceba que, como os suportes de cada ciclo são dois a dois disjuntos, necessariamente $\rho_i(x) = \eta_j(x)$, para todo $x \in X$ e $i, j \in \llbracket 1, \lfloor \frac{n}{2} \rfloor \rrbracket$.

Utilizando a mesma lógica de forma induutiva em todos os elementos de X , concluímos que para todo $x \in X$ iremos obter as mesmas partições $\mathfrak{O}(x)$ nas quais podemos escrever $\text{supp}(\sigma)$.

Como o produto entre quaisquer ciclos de σ é comutativo, deduzimos diretamente que $\sigma_1 = \sigma_2$. □

Observação: note que para calcular a ordem de uma permutação $\sigma \in \mathfrak{S}_X$ basta decompor σ em ciclos de suportes dois a dois disjuntos e calcular sua ordem via a regra vista na **Proposição 2.2.3**.

Exemplo 2.2.2

Exercício 5.41 da referência [GL22].

(a) Seja $\sigma_{(a)} \in \mathfrak{S}_9$ tal que:

$$\sigma_{(a)} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix} = \underbrace{(1\ 2\ 3\ 4\ 5)}_{\text{ordem }=5} \underbrace{(8\ 9)}_{\text{ordem }=2}$$

$$\implies \mathcal{O}(\sigma_{(a)}) = \text{mmc}(5, 2) = 10$$

(b) Seja $\sigma_{(b)} \in \mathfrak{S}_7$ tal que:

$$\sigma_{(b)} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 4 & 3 & 1 & 2 & 7 \end{pmatrix} = \underbrace{(1\ 6\ 2\ 5)}_{\text{ordem }=4} \underbrace{(3\ 4)}_{\text{ordem }=2}$$

$$\implies \mathcal{O}(\sigma_{(b)}) = \text{mmc}(4, 2) = 4$$

(c) Seja $\sigma_{(c)} \in \mathfrak{S}_9$ tal que:

$$\sigma_{(c)} = (1\ 2\ 3)(4\ 5)(1\ 6\ 8\ 7\ 9)(1\ 5) = (1\ 4\ 5\ 6\ 8\ 7\ 9\ 2\ 3)$$

$$\implies \mathcal{O}(\sigma_{(c)}) = 9$$

(d) Seja $\sigma_{(d)} \in \mathfrak{S}_3$ tal que:

$$\sigma_{(d)} = (1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2)$$

$$\implies \mathcal{O}(\sigma_{(d)}) = 3.$$

Corolário 2.2.1

Seja X um conjunto finito e não vazio tal que $\text{Card}(X) = n \in \mathbb{Z}_{\geq 2}$.

Então, todo elemento de \mathfrak{S}_X é igual a um produto de no máximo $n - 1$ transposições.

Demonstração:

Seja $\sigma \in \mathfrak{S}_X$ uma permutação tal que:

$$\sigma = \gamma_1 \dots \gamma_m, \quad m \in [\![1, \left\lfloor \frac{n}{2} \right\rfloor]\!]$$

Definimos $\mathcal{O}(\gamma_i) = k_i$, $\forall i \in [\![1, m]\!]$ (de tal forma que γ_i é um k_i -ciclo).

Sabemos a partir da **Proposição 2.2.1** que cada k -ciclo pode ser escrito como $k - 1$ transposições (de suportes não necessariamente disjuntos).

Como possuímos m ciclos dois a dois disjuntos, temos:

$$\sum_{i=1}^m k_i - 1 = \sum_{i=1}^m k_i - \sum_{i=1}^m 1 = \sum_{i=1}^m k_i - m$$

Como $\sum_{i=1}^m k_i \leq n$ e $m \in \llbracket 1, \lfloor \frac{n}{2} \rfloor \rrbracket$, σ pode se fatorar em no máximo $n - 1$ transposições (de suportes não necessariamente disjuntos). \square

Observação: diferentemente do **Teorema 2.2.1**, a decomposição de uma permutação $\sigma \in \mathfrak{S}_X$ em transposições não é necessariamente única. Será mostrado na **Proposição 2.2.4** que uma permutação pode também ser decomposta em transposições elementares.

Exemplo 2.2.3

Seja $\sigma \in \mathfrak{S}_8$ tal que:

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

Note que, seguindo a mesma estratégia de prova da **Proposição 2.2.1**, podemos ainda reescrever σ como:

$$\sigma = (1\ 7\ 8)(2\ 5\ 3\ 6) = (1\ 8)(1\ 7)(2\ 6)(2\ 3)(2\ 5)$$

Definição 2.2.3

Seja $X = \{x_1, \dots, x_n\}$.

Uma **transposição elementar** é uma transposição $\tau \in \mathfrak{S}_X$ da forma:

$$\tau = (x_i\ x_{i+1}), \quad i \in \{1, \dots, n-1\}$$

Isto é, uma transposição cujas imagens são elementos consecutivos de X .

Proposição 2.2.4

Toda transposição de um conjunto finito e não vazio X pode ser decomposta em transposições elementares de X .

Demonstração:

Seja $(x_i\ x_j)$ uma transposição de $X = \{x_1, \dots, x_n\}$, onde $i < j$.

Note que podemos escrever $(x_i\ x_j)$ como:

$$(x_i\ x_j) = (x_i\ x_{i+1})(x_{i+1}\ x_{i+2}) \dots (x_{j-2}\ x_{j-1})(x_{j-1}\ x_j)(x_{j-2}\ x_{j-1}) \dots (x_{i+1}\ x_{i+2})(x_i\ x_{i+1})$$

Note que de fato, ao realizar o produto das transposições elementares acima, temos que:

$$x_i \rightarrow x_{i+1} \rightarrow \dots \rightarrow x_{j-1} \rightarrow x_j$$

e,

$$x_j \rightarrow x_{j-1} \rightarrow \dots \rightarrow x_{i+1} \rightarrow x_i.$$

Além disso, temos também diretamente que:

$$x_k \rightarrow x_k, \quad \forall k \in \llbracket i, j \rrbracket$$

Isto conclui a prova e mostra que de fato podemos escrever quaisquer transposições de um conjunto finito e não vazio X em transposições elementares de X . \square

Observação: note que a decomposição de uma dada transposição em transposições elementares não é única. Temos, por exemplo, em \mathfrak{S}_3 :

$$(1\ 3) = (1\ 2)(2\ 3)(1\ 2) = (2\ 3)(1\ 2)(2\ 3)$$

Exemplo 2.2.4

Seja $\sigma \in \mathfrak{S}_5$ tal que:

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

Temos que:

$$\begin{aligned} \sigma &= (1\ 3\ 5\ 4) = (1\ 4)(1\ 5)(1\ 3) = (1\ 2)(2\ 3)(3\ 4)(2\ 3)(1\ 2) \\ &\quad (1\ 2)(2\ 3)(3\ 4)(4\ 5)(3\ 4)(2\ 3)(1\ 2) \\ &\quad (1\ 2)(2\ 3)(1\ 2) \\ &= (1\ 2)(2\ 3)(4\ 5)(3\ 4)(1\ 2) \end{aligned}$$

Corolário 2.2.2

Seja X um conjunto finito e não vazio tal que $\text{Card}(X) = n \in \mathbb{Z}_{\geq 2}$.

Então, todo elemento de \mathfrak{S}_X é igual a um produto de transposições elementares.

Demonstração:

O resultado é consequência imediata da combinação do **Corolário 2.2.1** e da **Proposição 2.2.4**. \square

Proposição 2.2.5

Sejam $X = \{x_1, \dots, x_n\}$ tal que $n \geq 2$ e $(x_i\ x_j)$ uma transposição arbitrária de X .

Então, $\forall \sigma \in \mathfrak{S}_X$, temos:

$$\sigma(x_i\ x_j)\sigma^{-1} = (\sigma(x_i)\ \sigma(x_j)).$$

Demonstração:

Seja $x \in X \setminus \{\sigma(x_i), \sigma(x_j)\}$. Temos diretamente que:

$$\sigma^{-1}(x) = \underbrace{x'}_{x' \in X \setminus \{x_i, x_j\}} \implies ((x_i\ x_j)\sigma^{-1})(x) = x' \implies (\sigma(x_i\ x_j)\sigma^{-1})(x) = \sigma(x') = x$$

Tomemos agora $x = \sigma(x_i)$, temos que:

$$\sigma^{-1}(\sigma(x_i)) = x_i \implies ((x_i \ x_j)\sigma^{-1})(\sigma(x_i)) = x_j \implies (\sigma(x_i \ x_j)\sigma^{-1})(\sigma(x_i)) = \sigma(x_j)$$

Analogamente temos que $x = \sigma(x_j) \implies (\sigma(x_i \ x_j)\sigma^{-1})(\sigma(x_j)) = \sigma(x_i)$.

Concluímos que $\sigma(x_i \ x_j)\sigma^{-1} = (\sigma(x_i) \ \sigma(x_j))$.

□

Teorema 2.2.2

Seja $X = \{x_1, x_2, \dots, x_n\}$ tal que $n \geq 3$.

Então, o grupo \mathfrak{S}_X é gerado por $\tau = (x_1 \ x_2)$ e $\gamma = (x_1 \ x_2 \ \dots \ x_n)$.

Isto é, $\forall \sigma \in \mathfrak{S}_X, \exists a_1, \dots, a_p, b_1, \dots, b_p \in \mathbb{Z}$ tal que:

$$\sigma = \prod_{i=1}^p \tau^{a_i} \gamma^{b_i}$$

Demonstração:

A partir do **Corolário 2.2.2**, basta mostrar que o produto de τ e γ formam uma transposição elementar.

Ora, pela **Proposição 2.2.5** temos diretamente que:

$$\gamma^k \tau \gamma^{-k} = (x_{k+1} \ x_{k+2}), \quad \forall k \in \llbracket 0, n-2 \rrbracket$$

Portanto, concluímos que \mathfrak{S}_X pode ser gerado a partir de apenas τ e γ .

□

Observação: a partir do resultado acima deduzimos que \mathfrak{S}_X é um grupo dicíclico.

2.3 Assinatura

Definição 2.3.1

Sejam X um conjunto ordenado, finito e não vazio e uma permutação $\sigma \in \mathfrak{S}_X$.

Chamamos de **inversão em** σ o par ordenado $(x, y) \in X^2$ tq. $x < y$ e $\sigma(x) > \sigma(y)$.

Denotamos o número de inversões de uma dada permutação σ como $\mathcal{I}(\sigma)$.

Exemplo 2.3.1

Seja $\sigma \in \mathfrak{S}_9$ tal que:

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

Contando cada par de inversões partindo do primeiro elemento temos que:

$$\mathcal{I}(\sigma) = 2 + 7 + 4 + 2 + 1 + 0 + 1 + 0 + 0 = 17.$$

Definição 2.3.2

Sejam X um conjunto ordenado, finito e não vazio e uma permutação $\sigma \in \mathfrak{S}_X$. Definimos a **assinatura de σ** como o resultado da função $\varepsilon(\sigma) \stackrel{\text{def}}{=} (-1)^{\mathcal{I}(\sigma)}$.

Observação: note que, embora a definição de inversão dependa de uma relação de ordem em X , a assinatura $\varepsilon(\sigma)$ é uma propriedade intrínseca da permutação. Se X for um conjunto finito qualquer, podemos sempre munir X de uma ordem total arbitrária para calcular $\varepsilon(\sigma)$; o valor obtido será independente da ordem escolhida.

Definição 2.3.3

A partir das notações da **Definição 2.3.2**, uma permutação $\sigma \in \mathfrak{S}_X$ é dita **par** se $\varepsilon(\sigma) = 1$.

Simetricamente, uma permutação $\sigma \in \mathfrak{S}_X$ é dita **ímpar** se $\varepsilon(\sigma) = -1$.

Exemplo 2.3.2

Retomando o **Exemplo 2.3.1** temos diretamente que σ é uma permutação de assinatura igual à -1 e é, portanto, ímpar:

$$\varepsilon(\sigma) = (-1)^{\mathcal{I}(\sigma)} = (-1)^{17} = -1.$$

Proposição 2.3.1

Seja X um conjunto finito, não vazio e munido de uma ordem total. Logo, toda transposição de \mathfrak{S}_X é uma permutação ímpar.

Demonstração:

Seja $\tau = (x\ y) \in \mathfrak{S}_X$ uma transposição tal que, pela ordem total de X , $x < y$ e $\tau(x) > \tau(y)$.

Note que, como $x < y$ e $\tau(x) > \tau(y)$, então temos diretamente que $\forall z_x \in X_{<x}, \tau(x) > z$.

Simetricamente, temos que $\forall z_y \in X_{>y}, \tau(y) < z$.

Portanto, resta contar o número de inversões para $z \in \llbracket x, y \rrbracket$.

Ora, para todo $z \in \llbracket x, y \rrbracket$ temos diretamente que $\tau(y) > z, \forall z \in \llbracket x, y \rrbracket$.

Seja M o número de inversões $(\tau(y), z)$ calculado acima.

Note que, de forma análoga, temos que $\tau(x) < z, \forall z \in \llbracket x, y \rrbracket$.

Portanto, o número de inversões dos pares $(\tau(x), z)$ é também M .

Entretanto, como contabilizamos duas vezes a inversão $(\tau(x), \tau(y))$, temos que $\mathcal{I}(\tau) = 2M - 1$.

Portanto, $\varepsilon(\tau) = -1$ e τ é ímpar. □

Teorema 2.3.1

Sejam X um conjunto finito tal que $\text{Card}(X) \geq 2$ e munido de uma ordem total e uma permutação $\sigma \in \mathfrak{S}_X$.

Portanto, ao decompor $\sigma = \tau_1 \dots \tau_m$, onde τ_i é uma transposição, temos que:

$$\varepsilon(\sigma) = (-1)^m$$

Demonstração



Bibliografia

- [GL22] Arnaldo Garcia and Yves Lequin. *Elementos de Álgebra*. Projeto Euclides.
IMPA, Rio de Janeiro, 7 edition, 2022.