

# Notas sobre Teoria dos Grupos para Programa de Iniciação Científica e Mestrado - PICME

Rodrigo Yuske Yamauchi

1 de novembro de 2024

# Sumário

1	Introdução a grupos	3
2	Subgrupos	7
3	Classes Laterais	10
4	Subgrupos Normais e Grupos Quocientes	14
5	Homomorfismos de Grupos	18
6	Produto Direto de Grupos	31
7	Grupos de Permutações	39

# Capítulo 1

## Introdução a grupos

**Definição 1.0.1.** Seja um conjunto  $A$  e uma operação binária  $A \cdot A \rightarrow A$ , diz-se que  $(A, \cdot)$  é um grupo quando são satisfeitas as condições necessárias a seguir:

- I)  $\forall a, b, c \in A, \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$  (associatividade);
- II)  $\exists e \in A$  tal que  $a \cdot e = a$  (elemento neutro);
- III)  $\forall a \in A, \exists b \in A$ , tal que  $a \cdot b = e$  (elemento inverso).

A partir deste momento, uma operação  $a \cdot b$ , tais que  $a, b \in A$  e  $(A, \cdot)$  é um grupo, também será denotada simplesmente por  $ab$  e o grupo poderá ser denotado pelo seu conjunto, e.g.,  $A$  é um grupo.

**(Generalização da Associatividade)** Seja  $A$  um grupo, mostraremos que para  $a_0 \dots a_n \in A$ ,

$$(a_0 \dots a_s)(a_{s+1} \dots a_n) = (a_0 \dots a_r)(a_{r+1} \dots a_n),$$

tal que  $r, s \in \mathbb{N}$  e  $0 < r < s < n$ .

Para  $n = 2$ , é evidente que o que queremos mostrar é verdadeiro, uma vez que

$$(a_0 a_1) a_2 = a_0 (a_1 a_2)$$

é a própria condição de  $A$  ser um grupo.

Para  $n > 2$  e por indução em  $n$ , suponhamos que  $\forall n'$ , tal que  $n' < n$ , seja verdade que

$$(a_0 \dots a_{s'}) (a_{s'+1} \dots a_{n'}) = (a_0 \dots a_{r'}) (a_{r'+1} \dots a_{n'}),$$

onde  $0 < r' < s' < n'$ .

Como  $r < s < n$ , temos pela hipótese da indução que, sendo  $r' = r$ ,  $s' = s - 1$  e  $n' = s$ ,

$$\begin{aligned} (a_0 \dots a_s)(a_{s+1} \dots a_n) &= ((a_0 \dots a_{s-1})(a_s)) (a_{s+1} \dots a_n) \\ &= ((a_0 \dots a_r)(a_{r+1} \dots a_s)) (a_{s+1} \dots a_n) \\ &= (a_0 \dots a_r) ((a_{r+1} \dots a_s)(a_{s+1} \dots a_n)) \\ &= (a_0 \dots a_r)(a_{r+1} \dots a_n), \end{aligned}$$

como queríamos provar.  $\square$

Enunciaremos o seguinte lema que nos será útil posteriormente:

**Lema 1.0.2.** Sejam  $a, b, c \in A$ , se

$$b \cdot a = c \cdot a \quad \Rightarrow \quad b = c.$$

*Demonstração.* Seja  $a'$  o elemento inverso de  $a$ ,

$$\begin{aligned} b \cdot a \cdot a' &= c \cdot a \cdot a' \\ b \cdot e &= c \cdot e \\ \therefore b &= c. \end{aligned}$$

$\square$

**Proposição 1.0.3.** Sendo  $(A, \cdot)$  um grupo, mostraremos agora a comutatividade e unicidade de  $e \in A$ , tal que  $a \cdot e = a$ , e de  $a' \in A$ , tal que  $a \cdot a' = e$ .

Para a comutatividade do elemento inverso, temos que

$$\begin{aligned}
 aa' &= e \\
 &= a'(a')' \\
 &= (a'e)(a')' \\
 &= a'(e(a')') \\
 &= a'((aa')(a')') \\
 &= a'(a(a'(a')')) \\
 &= a'(ae) = a'a,
 \end{aligned}$$

como queríamos mostrar.  $\square$

Quanto a comutatividade do elemento neutro,

$$ae = a(a'a) = (aa')a = ea,$$

como queríamos.  $\square$

Provaremos a unicidade do elemento neutro por contradição, seja  $e' \neq e$  um elemento neutro do grupo, tem-se então que

$$\begin{aligned}
 e'a &= a \\
 &= ea,
 \end{aligned}$$

então, pelo Lema 1.0.2,  $e' = e$  e entramos em contradição, como queríamos mostrar.  $\square$

A fim de provar a unicidade do elemento inverso, consideremos  $b, b' \in A$ , tais que ambos sejam elementos inversos de  $a$ . Assim,

$$\begin{aligned}
 b \cdot a &= e = b' \cdot a \\
 \therefore b &= b',
 \end{aligned}$$

pelo lema acima novamente, como queríamos mostrar.  $\square$

A partir de agora, denotaremos por  $a^{-1}$  o único elemento inverso de  $a \in A$ .

Note que agora é possível **redefinir** o conceito de grupo já com a unicidade e comutatividade dos elementos neutro e inverso e com a generalidade da associatividade, visto que estes todos são consequências diretas da definição mais abstrata.

Alguns **exemplos** notáveis de grupos são descritos a seguir.

Exemplo 1) O conjunto dos inteiros com a operação usual de soma é um grupo infinito, i.e., com um número infinito de elementos. Tal conjunto é denotado por  $(\mathbb{Z}, +)$ .

Exemplo 2) O conjunto das classes de equivalência módulo  $n$ , i.e.,  $\{\bar{0}, \dots, \overline{n-1}\}$  e a soma dessas classes denotada por  $\bigoplus_n$  formam um grupo  $(\mathbb{Z}/n\mathbb{Z}, \bigoplus_n)$  finito de  $n$  elementos. Esse exemplo de grupo será melhor definido e mais explorado posteriormente.

Exemplo 3) O conjunto das permutações<sup>1</sup> de  $n$  elementos com a operação de composição de funções  $\circ$  é um grupo e é denotado por  $S_n$ .

Assim, se  $n = 3$ ,

$$S_3 = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\},$$

onde a notação  $\begin{pmatrix} 123 \\ abc \end{pmatrix}$  representa a função tal que  $f(1) = a$ ,  $f(2) = b$  e  $f(3) = c$ .

Por fim, definimos ainda o que é um grupo abeliano, um exemplo importante de grupo a ser estudado mais a frente.

**Definição 1.0.4.** Um grupo  $A$  *abeliano* ou *comutativo* é um grupo em que a seguinte propriedade é satisfeita:

$$ab = ba, \quad \forall a, b \in A.$$

---

<sup>1</sup>Relação de bijeção entre um dado conjunto  $A$  e  $\{0, \dots, |A| - 1\}$ .

## Capítulo 2

# Subgrupos

**Definição 2.0.1.** Seja  $A$  um grupo e  $H \subseteq A$  não vazio, então se  $H$  com a mesma operação de  $A$ , tal que  $H \cdot H \rightarrow H$ , também é um grupo, o chamaremos de subgrupo de  $A$  e denotaremos por  $H \leq A$ . Ou seja, para que  $H$  seja um subgrupo de  $A$  as seguintes condições devem ser satisfeitas:

- I)  $\forall a, b, c \in H, a \cdot (b \cdot c) = (a \cdot b) \cdot c$  (associatividade);
- II)  $\exists e \in H$  tal que  $a \cdot e = a$  (elemento neutro);
- III)  $\forall a \in H, \exists b \in A$ , tal que  $a \cdot b = e$  (elemento inverso);
- IV)  $\forall a, b \in H, a \cdot b \in H$  (operação binária fechada).

**Proposição 2.0.2.** Seja  $H \subseteq A$  não vazio. Então,  $H \leq A$  se, e somente se, as seguintes condições são satisfeitas:

1.  $\forall a, b \in H, a \cdot b \in H$ ;
2.  $\forall a \in H, a^{-1} \in H$ .

*Demonstração.* Sendo  $H \leq A$ , então a primeira condição é imediatamente satisfeita. E, como  $a \in A$  tem um único elemento inverso  $a^{-1} \in A$ , se  $a \in H$ , então  $a^{-1} \in H$  pela condição da existência de elemento inverso para que  $H$  seja subgrupo. Reciprocamente, se  $H$  satisfaz a primeira condição da proposição, claramente é satisfeita a condição de operação binária fechada de subgrupo. Ademais, como vale a associatividade para elementos de  $A$  e  $H \subseteq A$ , então consequentemente vale a associatividade para elementos de  $H$ . Ora, e se existe elemento inverso para todo elemento de  $h \in H$ ,  $hh^{-1} = e$ , tal que  $e \in A$ , e pela condição de operação binária fechada,  $e \in H$ . Assim, é garantido a existência de elemento

neutro e inverso  $\forall h$ . □

Alguns exemplos de subgrupos são descritos a seguir:

Exemplo 1) O subconjunto  $\{e\}$  forma um subgrupo para todo grupo, onde  $e$  é o elemento neutro do grupo.

Exemplo 2) O subconjunto  $H \subseteq A$ , tal que  $A \subseteq H$ , i.e., o próprio conjunto  $A$  é subgrupo de  $A$ .

**Definição 2.0.3.** Seja  $S \subseteq A$  um subconjunto não vazio, onde  $A$  é um grupo. Definimos

$$\langle S \rangle = \{s_0 s_1 s_2 \dots s_n \mid n \in \mathbb{N}, s_i \in S \text{ ou } s_i^{-1} \in S\}.$$

Ademais, se  $a \in A$ , notaremos  $\langle \{a\} \rangle$  diretamente como  $\langle a \rangle$ .

**Proposição 2.0.4.** Sejam  $S \subseteq A$  um subconjunto não vazio e  $A$  um grupo, então  $\langle S \rangle$  é um subgrupo de  $A$ .

*Demonstração.* Basta provar a proposição 2.0.2. Seja  $x, y \in \langle S \rangle$ ,

$$x = a_0 a_1 \dots a_n, \text{ com } a_i \in S \text{ ou } a_i^{-1} \in S.$$

$$y = b_0 b_1 \dots b_m, \text{ com } b_i \in S \text{ ou } b_i^{-1} \in S.$$

Ora,  $xy = a_0 a_1 \dots a_n b_0 b_1 \dots b_m$ , tal que todos os fatores são elementos de  $S$  ou são o inverso de um elemento de  $S$ . Ademais,  $x^{-1} = a_0^{-1} a_1^{-1} \dots a_n^{-1}$ , tal que todos os fatores são elementos de  $S$  ou inverso de um elemento de  $S$ . Assim,  $xy, x^{-1} \in \langle S \rangle$ , como queríamos. □

Dessa forma, a partir de agora chamaremos  $\langle S \rangle$  por **subgrupo gerado pelo subconjunto  $S$** , onde  $S$  é o **conjunto gerador**.

**Definição 2.0.5.** Um grupo é dito **cíclico** quando ele pode ser gerado por um elemento, i.e.,  $\exists a \in A$  tal que  $A = \langle a \rangle$ . Note que  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ .

**Definição 2.0.6.** Chamaremos de **ordem** de um grupo  $A$ , o número de elementos de  $A$ , e será denotada por  $|A|$ . Além disso, se um grupo é gerado por um elemento  $a$ , a ordem de  $a$  será a ordem do subgrupo gerado por  $a$ , i.e.,  $|a| = |\langle a \rangle|$ .



**Teorema 2.0.7.** Sejam  $A$  um grupo e  $a \in A$ , tal que a ordem de  $a$ ,  $|a| = m$ , é finita. Então  $m$  é o menor inteiro positivo tal que  $a^m = e$ , onde  $e$  é o elemento neutro de  $A$ .

*Demonstração.* Primeiro mostraremos que, sendo  $|a|$  finita, existe um inteiro positivo  $k$  tal que  $a^k = e$ . Temos a seguinte generalização para  $\langle a \rangle$ :

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\},$$

tal que  $|a| = m$ . Assim, devem existir, sem perda de generalidade,  $p, q \in \mathbb{Z}$ , tal que  $p > q$  e  $a^p = a^q$ . Ora,

$$\begin{aligned} a^p \cdot a^{-q} &= a^q \cdot a^{-q} \\ a^{p-q} &= e, \end{aligned}$$

portanto, como  $p - q > 0$ ,  $\exists k > 0$ , tal que  $a^k = e$ .

Agora, considere a sequência de potências de  $a$ :

$$e, a^1, a^2, \dots, a^{k'-1},$$

onde  $k'$  é o menor inteiro  $k$ , tal que  $a^k = e$ . Mostraremos que todos os elementos dessa sequência são distintos. Para  $k' = 1$ , há apenas um elemento, e é imediata a validade da afirmação. Para  $k' > 1$ , suponhamos, sem perda de generalidade,  $p, q \in \mathbb{Z}_{\geq 0}$ , tal que  $q < p < k'$ . Ora,

$$\begin{aligned} a^p \cdot a^{-q} &= a^q \cdot a^{-q} \\ a^{p-q} &= e, \end{aligned}$$

porém, como  $0 < p - q < k'$ , entramos em contradição, já que  $k'$  é o menor inteiro tal que essa relação é verdadeira. Portanto, a sequência de potências de  $a$ :

$$e, a^1, a^2, \dots, a^{k'-1}$$

possui todos elementos distintos.

Por fim, basta mostrar que  $k' = m$ . Para isso, consideremos  $n \in \mathbb{Z}$ . Pelo algoritmo de Euclides, pode-se escrever  $n = qk' + r$ , tal que  $0 \leq r < k'$ . Assim,

$$a^n = a^{qk'+r} = a^{qk'} \cdot a^r = e \cdot a^r = a^r.$$

Isso significa que para qualquer  $n$ ,  $a^n$  encontra-se na sequência de elementos distintos enunciada acima. Portanto,

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{e, a^1, a^2, \dots, a^{k'-1}\},$$

e ainda, como  $|a| = m$ ,  $m = k'$ , como queríamos mostrar. □

## Capítulo 3

# Classes Laterais

**Definição 3.0.1.** Sejam  $S \leq A$ ,  $A$  um grupo e  $a \in A$ , define-se como **classe lateral à esquerda de  $S$  em  $A$**  o subconjunto de  $A$

$$aS = \{as \mid s \in S\}.$$

(uma **classe lateral à direita** é definida por  $Sa = \{sa \mid s \in S\}$ ).

Analogamente, pode-se definir a seguinte relação

$$y \sim_E a \Leftrightarrow \exists s \in S \text{ tal que } y = as.$$

Assim, a **classe lateral à esquerda de  $S$**  pode também ser escrita como

$$aS = \{y \in A \mid y \sim_E a\}$$

**Proposição 3.0.2.** A relação

$$y \sim_E a \Leftrightarrow \exists s \in S \text{ tal que } y = as$$

é uma relação de equivalência<sup>a</sup>.

---

<sup>a</sup>Uma relação de equivalência é uma relação que seja reflexiva, simétrica e transitiva

*Demonstração.* Primeiramente, provaremos que a relação é reflexiva, i.e.,  $a \sim_E a$ . Ora,  $\forall a \in A$ ,

$$ae \in A,$$

onde  $e$  é o elemento identidade do subgrupo  $S$ .

Mostraremos agora que a relação é simétrica, i.e., se  $y \sim_E a$ , então  $a \sim_E y$ . Ora, se  $\exists s \in S$  tal que  $y = as$ , então

$$\begin{aligned} y &= as \\ ys^{-1} &= ass^{-1} \\ ys^{-1} &= a, \end{aligned}$$

onde  $s^{-1} \in S$ , uma vez que  $S$  é um subgrupo.

Finalmente, mostraremos que a relação é transitiva, i.e., se  $y \sim_E a$  e  $a \sim_E b$ , onde  $a, b \in A$ , então  $y \sim_E b$ . Ora, se  $\exists s \in S$  tal que  $y = as$  e  $\exists t \in S$  tal que  $a = bt$ , então

$$\begin{aligned} y &= as \\ &= bts \\ &= bu, \end{aligned}$$

onde  $u = ts \in S$ , uma vez que  $S$  é um subgrupo. Assim, a relação apresentada é uma relação de equivalência, como queríamos mostrar.  $\square$

**Lema 3.0.3.** Se  $\sim$  é uma relação de equivalência em  $A$ , então o conjunto de todas as classes de equivalência definidas por  $\sim$ , forma uma partição de  $A$ .

*Demonstração.* Consideraremos a seguinte notação para uma classe de equivalência:  $[a] = \{b \in A \mid a \sim b\}$ . Precisamos, então, mostrar que

- a) cada elemento do conjunto é não vazio;
- b) os elementos são disjuntos entre si;
- c) a união de todos os elementos (classes de equivalência) formam  $A$ .

Ora,  $\forall a \in A$ ,  $a \sim a$  é garantido pela definição de relação de equivalência. Assim,  $a \in [a]$ , ou seja,  $[a] \neq \emptyset$ .

Por contraposição mostraremos que os elementos do conjunto são disjuntos entre si, i.e., se  $[a] \cap [b] \neq \emptyset$ , então  $[a] = [b]$ . Ora, se a intersecção entre  $[a]$  e  $[b]$  não é o conjunto vazio,

$$\exists c \mid a \sim c \text{ e } b \sim c,$$

e consequentemente  $c \sim a$  e  $c \sim b$ . Assim, pelas propriedades de simetria e transitividade,

$$\forall x \in [a] \mid x \sim a \Rightarrow x \sim c \Rightarrow x \sim b,$$

ou seja,  $x \in [b]$ , ou ainda,  $[a] \subseteq [b]$ . A mesma lógica pode ser aplicada para provar  $[b] \subseteq [a]$ . Portanto,  $[a] = [b]$ , como queríamos.

Por fim, mostraremos que a união de todos os elementos formam  $A$ . Ora,  $\forall a \in A$ , todo elemento da classe de equivalência  $[a]$  pertence à  $A$ , assim, a união de todas as classes de equivalência é subconjunto de  $A$ . Para o caminho inverso, tem-se que  $\forall a \in A$ ,  $a \in [a]$ . Como  $[a]$  pertence a união de todas as classes de equivalência, então  $A$  é subconjunto da união de todas as classes de equivalência. Portanto,  $A = \bigcup_{a \in A} [a]$ , como queríamos, concluindo a prova.  $\square$

**Definição 3.0.4.** A cardinalidade do conjunto de classes laterais à esquerda de  $S$  em  $A$  é o **índice** de  $S$  em  $A$ , denotado por  $(A : S)$ .

**Proposição 3.0.5.** Todas as classes laterais de  $S$  em  $A$  têm a mesma cardinalidade, que é igual a  $|S|$ .

*Demonstração.* Ora,  $S \rightarrow aS$  é claramente uma bijeção de cada classe lateral com  $S$ . O mesmo pode ser afirmado sobre as classes laterais à direita.  $\square$

**Teorema 3.0.6. (Teorema de Lagrange)** Sejam  $A$  um grupo finito e  $S \leq A$ . Então  $|S| \cdot (A : S) = |A|$ .

*Demonstração.* Como mostrado pelo lema 3.0.3, o conjunto das classes laterais à esquerda de  $S$  em  $A$  formam uma partição de  $A$ . Ademais, pela proposição 3.0.5, a cardinalidade de cada classe lateral é igual à cardinalidade de  $S$ . Assim,

$$|A| = |S| \cdot (A : S),$$

como queríamos mostrar.  $\square$

**Teorema 3.0.7. (Pequeno Teorema de Fermat)** Seja  $p$  um número primo, então para  $a$  não múltiplo de  $p$

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

*Demonstração.* Denotando o módulo  $p$  de um número  $k$  por  $\bar{k}$ , tem-se que

$$\bar{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}.$$

Ora,  $\mathbb{Z}/p\mathbb{Z}$  é um grupo com a operação de multiplicação  $\odot$ , tal que  $\bar{1}$  é o elemento neutro e para  $a, b \in \mathbb{Z}/p\mathbb{Z}$ ,  $\bar{a} \odot \bar{b} = \overline{ab}$ . A cardinalidade desse grupo é  $p - 1$ .

Assim, pelo teorema 3.0.6,  $|\langle \bar{a} \rangle|$  divide a cardinalidade de  $\mathbb{Z}/p\mathbb{Z}$ . E, pelo teorema 2.0.7,

$$\begin{aligned}\bar{a}^{(p-1)} &= \bar{a}^{(k \cdot |\langle a \rangle|)} = \bar{1}^{(k)} \\ &= \bar{1},\end{aligned}$$

ou seja,

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

como queríamos. □

## Capítulo 4

# Subgrupos Normais e Grupos Quocientes

Um caso importante no estudo da teoria de grupos, que nos será útil mais a frente, para um grupo  $A$  e um subgrupo  $H \leq A$ , é quando a função com operação herdada de  $A$

$$(xH, yH) \mapsto xyH, \quad (4.1)$$

para  $x, y \in A$ , está bem definida, isto é, quando o conjunto de subconjuntos de  $A$  forma um grupo.

**Proposição 4.0.1.**  $(xH, yH) \mapsto xyH$  estar bem definida é equivalente a  $aha^{-1} \in H, \forall h \in H$ , tal que  $a \in A$ .

*Demonstração.* Para que a operação seja bem definida, duas entradas iguais na função devem resultar na mesma saída. Isto é, sejam  $(x_1H, y_1H)$  e  $(x_2H, y_2H)$  iguais, então  $x_1y_1H = x_2y_2H$ .

Assim, sejam duas entradas iguais

$$x_1h_1 = x_2h_2$$

$$y_1j_1 = y_2j_2,$$

tais que  $\exists h_2, \forall h_1 \in H$  e  $\exists j_2, \forall j_1 \in H$ .

$$\Rightarrow x_1 = x_2h_2h_1^{-1}$$

$$y_1 = y_2j_2j_1^{-1}$$

Disso, é verdade então que

$$\begin{aligned}(y_2^{-1}x_2^{-1})x_1y_1 &= (y_2^{-1}x_2^{-1})x_2h_2h_1^{-1}y_2j_2j_1^{-1} \\ &= y_2^{-1}h_2h_1^{-1}y_2j_2j_1^{-1}.\end{aligned}$$

Ora, como apontado acima que a operação estar bem definida acontece quando  $x_1y_1H = x_2y_2H$ , i.e.,  $(y_2^{-1}x_2^{-1})x_1y_1 \in H$ , tem-se que

$$\begin{aligned}(y_2^{-1}x_2^{-1})x_1y_1 \in H &\Leftrightarrow (y_2^{-1}x_2^{-1})x_2h_2h_1^{-1}y_2j_2j_1^{-1} \in H \\ &\Leftrightarrow y_2^{-1}h_2h_1^{-1}y_2j_2j_1^{-1} \in H \\ &\Leftrightarrow y_2^{-1}h_2h_1^{-1}y_2 \in H,\end{aligned}$$

pois  $j_2j_1^{-1} \in H$ .

Tomando  $h = h_2h_1^{-1}$ , relembremos que  $h_2$  é um elemento não arbitrário e  $h_1$  é um elemento arbitrário, assim,  $h$  também é um elemento arbitrário e pode-se concluir que

$$x_1y_1H = x_2y_2H \Leftrightarrow (y_2^{-1}x_2^{-1})x_1y_1 \in H \Leftrightarrow y_2^{-1}hy_2 \in H, \quad (4.2)$$

$\forall h \in H$ , tal que  $y_2 \in A$ , como queríamos mostrar.  $\square$

**Proposição 4.0.2.** Seja  $H \leq A$ , onde  $A$  é um grupo. Então as afirmações seguintes são todas equivalentes:

0.  $(xH, yH) \mapsto xyH$  estar bem definida;
1.  $aHa^{-1} \subseteq H, \forall a \in A$ ;
2.  $aHa^{-1} = H, \forall a \in A$ ;
3.  $aH = Ha, \forall a \in A$ .

*Demonstração.* Que o item 0  $\Leftrightarrow$  item 1 já foi provado pela proposição 4.0.1. Para mostrar que 1  $\Rightarrow$  2, consideremos  $h \in H$  e  $a \in A$ ,

$$h = a^{-1}(aha^{-1})a \in a^{-1}(aHa^{-1})a \subseteq a^{-1}Ha = bHb^{-1},$$

$\forall b \in A$ .

Ademais, é imediato que 2  $\Rightarrow$  1. Por fim, que 2  $\Leftrightarrow$  3 é óbvio uma vez que

$$aHa^{-1} = H \Leftrightarrow aHa^{-1}a = aH = Ha.$$

$\square$

**Definição 4.0.3.** Chama-se de *subgrupo normal* de um grupo  $A$  (denotado por  $H \trianglelefteq A$ ) um subgrupo  $H \leq A$  tal que  $H$  satisfaça uma (e, portanto, todas) das afirmações da proposição anterior. Nota-se ainda que como nesse caso as classes laterais à direita de  $H$  e à esquerda de  $H$  são iguais, elas serão chamadas simplesmente por *classes laterais*.

Alguns exemplos de subgrupos normais estão descritos a seguir:

Exemplo 1) O subgrupo  $\{e\}$  e o próprio grupo  $A$  são subgrupos normais de  $A$ ;

Exemplo 2) O subgrupo (chamado de centro de  $A$ )

$$Z(A) = \{x \in A \mid xa = ax, \forall a \in A\} \triangleleft A.$$

Ou ainda, mais geralmente, se  $H < Z(A)$ , então  $H \triangleleft A$ . A prova disso vem diretamente da afirmação 3 da proposição 4.0.2;

Exemplo 3) Se um grupo  $A$  é abeliano (rever definição 1.0.4), então todo subgrupo de  $A$  é normal em  $A$ . A prova disso vem diretamente do item anterior, uma vez que o centro de um grupo abeliano é o próprio grupo.

**Teorema 4.0.4.** Considere um subgrupo normal  $H$  de um grupo  $A$ . Então, o conjunto das classes laterais, com operação induzida de  $A$ , é também um grupo. Note que esse grupo não é subgrupo de  $A$ .

*Demonstração.* O conjunto das classes laterais é dado por

$$\{aH \mid a \in A\}.$$

Assim, sejam  $a, b \in A$ ,

$$\begin{aligned} aH \cdot bH &= aH \cdot Hb \\ &= aHb \\ &= abH, \end{aligned}$$

como  $ab \in A$ , mostramos que a operação induzida de  $A$  para o conjunto das classes laterais é fechada. Ademais, uma vez que a operação é induzida, temos garantida a associatividade, pois, sejam  $a, b, c \in A$ ,

$$(aH \cdot bH) \cdot cH = (abc)H = aH \cdot (bH \cdot cH).$$

Agora, consideremos  $e$  o elemento identidade de  $A$  e  $a \in A$ , então

$$eH \cdot aH = (ea)H = aH,$$



i.e.,  $eH = H$  é o elemento identidade do grupo das classes laterais. Por fim, sejam  $a \in A$  e  $a^{-1} \in A$  o elemento inverso de  $a$ . Então,

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

i.e.  $a^{-1}H$  é o elemento inverso da classe  $aH$ . □

**Definição 4.0.5.** Sejam  $A$  um grupo e  $H \leq A$  um subgrupo, então o grupo de todas suas classes laterais (denotado por  $A/H$ ) com a operação induzida de  $A$  é chamado de *grupo quociente* de  $A$  por  $H$ .

**Proposição 4.0.6.** Sejam  $A$  um grupo e  $A'$  seu subgrupo dos comutadores, i.e.,  $\langle \{xyx^{-1}y^{-1} | x, y \in A\} \rangle$ . Então,

1.  $A/A'$  é abeliano;
2.  $A'$  é o menor subgrupo normal de  $A$  com a propriedade do item anterior. Ou seja, se  $H \triangleleft A$  é tal que  $A/H$  é abeliano, então  $A' \subseteq H$ .

*Demonstração.* Para o item 1, consideremos  $a, b \in A$ , então, como  $(b^{-1}a^{-1}ba) \in A'$ ,

$$aA' \cdot bA' = abA' = ab(b^{-1}a^{-1}ba)A' = baA' = bA' \cdot aA'. \quad \square$$

Para o item 2, suponhamos um grupo  $A$  e um subgrupo  $H \leq A$ , tal que  $A/H$  seja abeliano. Então, para  $a, b \in A$ ,

$$abH = aH \cdot bH = bH \cdot aH = baH.$$

Ora, multiplicando ambas as extremidades da equação pela esquerda por  $(ba)^{-1}$ , tem-se

$$a^{-1}b^{-1}abH = H,$$

ou seja,  $A' \subseteq H$ . □

## Capítulo 5

# Homomorfismos de Grupos

**Definição 5.0.1.** Sejam  $(A, \cdot)$  e  $(\mathcal{A}, \times)$  dois grupos. A função  $f : A \rightarrow \mathcal{A}$  é dita um *homomorfismo* se

$$f(a \cdot b) = f(a) \times f(b), \quad \forall a, b \in A.$$

Alguns exemplos de homomorfismos de grupos estão descritos a seguir:

Exemplo 1) Identidade:  $Id : (A, \cdot) \rightarrow (A, \cdot)$ ,  $Id(a) = a$ ,  $a \in A$ .

Exemplo 2) Trivial:  $e : A \rightarrow \mathcal{A}$ ,  $e(a) = e_{\mathcal{A}}, \forall a \in A$ .

Exemplo 3) Projeção Canônica: Sendo  $H \triangleleft A$ , então  $\phi : A \rightarrow A/H$ ,  $\phi(a) = aH = Ha$ .

Exemplo 4) Sejam  $A$  é um grupo abeliano e  $n \in \mathbb{Z}$  fixo, então  $\phi_n : A \rightarrow A$ ,  $\phi_n(a) = a^n$  é um homomorfismo.

Exemplo 5) Seja  $a \in A$  fixo, então  $\mathcal{I}_a : A \rightarrow A$ ,  $\mathcal{I}_a(x) = axa^{-1}$ ,  $x \in A$ , é um homomorfismo bijetivo.

*Demonstração.* Primeiramente, mostraremos que  $\mathcal{I}_a$  é um homomorfismo. Ora,

$$\begin{aligned} \mathcal{I}_a(xy) &= axya^{-1} \\ &= ax(a^{-1}a)ya^{-1} \\ &= (axa^{-1})(aya^{-1}) \\ &= \mathcal{I}_a(x)\mathcal{I}_a(y). \end{aligned}$$

Ademais, mostraremos que  $\mathcal{I}_a$  é bijetiva. Uma função é bijetiva se, e somente se, a função admite inversa (a demonstração disso é encontrada facilmente na internet).

Assim, mostraremos que  $\mathcal{I}_a^{-1}(x) = a^{-1}xa$  é a inversa de  $\mathcal{I}_a$ . Ora,  $\forall x \in A$ ,

$$\begin{aligned}\mathcal{I}_a^{-1}(\mathcal{I}_a(x)) &= a^{-1}(axa^{-1})a \\ &= (a^{-1}a)x(a^{-1}a) \\ &= x,\end{aligned}$$

e, logo, a função é bijetora. □

Algumas propriedades importantes de homomorfismo de grupos está listada a seguir. Seja  $f : (A, \cdot) \rightarrow (\mathcal{A}, \times)$ , então:

1.  $f(e_A) = e_{\mathcal{A}}$ .

A demonstração disso vem de que

$$f(e_A) = f(e_A \cdot e_A) = f(e_A) \times f(e_A) \Rightarrow f(e_A) = e_{\mathcal{A}}.$$

2.  $f(a^{-1}) = f(a)^{-1}$ .

A demonstração disso vem de que  $e_{\mathcal{A}} = f(a \cdot a^{-1}) = f(a) \times f(a^{-1})$

$$\Rightarrow f(a)^{-1} = f(a)^{-1} \times e_{\mathcal{A}} = f(a)^{-1} = f(a^{-1}).$$

3. chama-se por *núcleo* do homomorfismo  $f$  o subgrupo normal de  $A$

$$\ker f := \{a \in A \mid f(a) = e_{\mathcal{A}}\}.$$

A prova de que  $\ker f < A$  vem de que, sejam  $x, y \in \ker f$ , então

$$f(x \cdot y) = f(x) \times f(y) = e_{\mathcal{A}}.$$

$$f(x^{-1}) = f(x)^{-1} = e_{\mathcal{A}}.$$

Ademais, tem-se que  $\ker f \triangleleft A$  pois, para qualquer  $a \in A$ ,

$$\begin{aligned}f(axa^{-1}) &= f(a) \times f(x) \times f(a)^{-1} = f(a) \times f(a)^{-1} = e_{\mathcal{A}} \\ &\Rightarrow axa^{-1} \in \ker f. \quad \square\end{aligned}$$

4. chama-se por *imagem* de  $f$  o subgrupo de  $\mathcal{A}$

$$\text{Im}(f) = \{y \in \mathcal{A} \mid y = f(a) \text{ para algum } a \in A\}.$$

A prova que  $\text{Im}(f) < \mathcal{A}$  vem de que, sejam  $x, y \in \text{Im}(f)$ , então  $\exists a, b \in A$  tais que

$$x \times y = f(a) \times f(b) = f(a \cdot b) \in \text{Im}(f).$$

$$\begin{aligned}e_{\mathcal{A}} &= f(e_A) = f(a \cdot a^{-1}) = f(a) \times f(a^{-1}) = x \times x^{-1} \\ &\Rightarrow x^{-1} = f(a^{-1}) \in \text{Im}(f).\end{aligned}$$

5. se  $H \leq A$ , então  $f(H) \leq \mathcal{A}$  e  $f^{-1}(f(H)) = H \ker f$ .

A prova que  $f(H) \leq \mathcal{A}$  vem de que, sendo  $x, y \in f(H)$ , então  $\exists a, b \in H$  tais que

$$x \times y = f(a) \times f(b) = f(a \cdot b) \in f(H).$$

$$\begin{aligned} e_{\mathcal{A}} &= f(e_A) = f(a \cdot a^{-1}) = f(a) \times f(a^{-1}) = x \times x^{-1} \\ &\Rightarrow x^{-1} = f(a^{-1}) \in f(H). \end{aligned}$$

Ademais, provaremos que  $f^{-1}(f(H)) = H \ker f$ . Sejam  $h \in H$  e  $k \in \ker f$ , então

$$\begin{aligned} f(h \cdot k) &= f(h) \times f(k) = f(h) \times e_{\mathcal{A}} = f(h) \in f(H) \\ &\Rightarrow H \ker f \subseteq f^{-1}(f(H)). \end{aligned}$$

A inclusão contrária vem de que seja  $x \in f^{-1}(f(H))$ , então

$$f(x) \in f(H),$$

assim,  $\exists h \in H$ , tal que  $f(x) = f(h)$ . Dessa forma,

$$f(h)^{-1}f(x) = e_{\mathcal{A}} \Rightarrow h^{-1}x \in \ker f.$$

Então,

$$x = h(h^{-1}x) \in H \ker f. \quad \square$$

6.  $\ker f = \{e_A\} \Leftrightarrow f$  é injetiva.

Para a função ser injetiva, para quaisquer  $a, b \in A$ , se  $f(a) = f(b)$ , então  $a = b$ . Ora, sejam  $a, b \in \ker f$ , então

$$f(a) = f(b) = e_{\mathcal{A}}.$$

Sabemos que  $f(e_A) = e_{\mathcal{A}}$  para qualquer homomorfismo. Assim,

$$a = b \Leftrightarrow \ker f = \{e_A\}. \quad \square$$

7. se  $\mathcal{O}(x)$  é finita, então  $\mathcal{O}(f(x))$  divide  $\mathcal{O}(x)$ .

A prova disso vem de que

$$x^{\mathcal{O}(x)} = e_A.$$

Assim,

$$e_{\mathcal{A}} = f(e_A) = f(x^{\mathcal{O}(x)}) = f(x)^{\mathcal{O}(x)},$$

i.e.,  $\mathcal{O}(f(x))$  divide  $\mathcal{O}(x)$ .

8. seja  $g : (\mathcal{A}, \times) \rightarrow (\mathcal{H}, \odot)$  um outro homomorfismo, então a composição

$$g \circ f : (A, \cdot) \rightarrow (\mathcal{H}, \odot)$$

também é um homomorfismo.

A prova disso vem de que

$$g \circ f(x \cdot y) = g(f(x \cdot y)) = g(f(x) \times f(y)) = g(f(x)) \odot g(f(y)) = (g \circ f(x)) \odot (g \circ f(y)). \quad \square$$

**Definição 5.0.2.** Seja  $f : A \rightarrow \mathcal{A}$  um homomorfismo.  $f$  é chamado de *isomorfismo* se existe um homomorfismo  $g : \mathcal{A} \rightarrow A$  tal que  $f \circ g = id_{\mathcal{A}}$  e  $g \circ f = id_A$ . Utilizaremos a notação  $A \simeq \mathcal{A}$  para denotar a relação de isomorfismo entre os grupos.

**Proposição 5.0.3.** Seja  $f : (A, \cdot) \rightarrow (\mathcal{A}, \times)$  um homomorfismo, então  $f$  é um isomorfismo se, e somente se,  $f$  é bijetora.

Prova: Pelo Teorema de Cantor-Bernstein-Schroeder<sup>a</sup>, tem-se que  $(\Rightarrow)$  é imediato. Ademais, suponhamos que  $f$  é bijetiva, então  $\forall x, y \in \mathcal{A}$ ,

$$\begin{aligned} f^{-1}(x \times y) &= f^{-1}(f(a) \times f(b)) \\ &= f^{-1}(f(a \cdot b)) \\ &= a \cdot b \\ &= f^{-1}(x) \cdot f^{-1}(y), \end{aligned}$$

tais que  $a = f^{-1}(x), b = f^{-1}(y) \in A$ . Assim, mostramos que  $(\Leftarrow)$  também é verdadeira.  $\square$

<sup>a</sup>O qual diz que se existe injeção de  $A \rightarrow B$  e de  $B \rightarrow A$ , então existe uma bijeção  $A \rightarrow B$ .

**Proposição 5.0.4.** Seja  $f : A \rightarrow \mathcal{A}$  um homomorfismo injetivo de grupos. Então

$$\mathcal{O}(f(x)) = \mathcal{O}(x), \quad \forall x \in A.$$

*Demonstração.* A ordem de  $f(x)$  é dada pela cardinalidade do subgrupo gerado por  $f(x)$ , i.e.,  $|\langle f(x) \rangle|$ . Como já apontado ao analisar subgrupos gerados por um único elemento, podemos escrever isso também como

$$|\{f(x)^n \mid n \in \mathbb{Z}\}|.$$

Como já mostrado,

$$\langle x \rangle = \{e, x, x^2, x^3, \dots, x^{\mathcal{O}(x)-1}\},$$

onde todos os elementos são distintos.

Uma vez que a função  $f$  é um homomorfismo injetivo, tem-se

$$f(x^n) = f(\underbrace{x \cdot x \cdot (\dots) \cdot x}_{n \text{ elementos}}) = \underbrace{f(x) \times f(x) \times (\dots) \times f(x)}_{n \text{ elementos}},$$

tal que para cada entrada  $a \neq b$ , com  $a, b \in A$ ,  $f(a) \neq f(b)$ . Assim,  $\mathcal{O}(x) = \mathcal{O}(f(x))$ .  $\square$

**Teorema 5.0.5.** (Primeiro Teorema do Isomorfismo). Seja  $f : A \rightarrow \mathcal{A}$  um homomorfismo de grupos. Então,

$$Im(f) \simeq A/ker(f).$$

*Demonstração.* Provaremos primeiramente que o isomorfismo dado por

$$\phi : A/ker(f) \rightarrow Im(f)$$

$$f(x) = \phi(x \cdot ker(f))$$

é bem definido, i.e., se

$$\forall x, y \in A, xker(f) = yker(f) \Rightarrow \phi(xker(f)) = \phi(yker(f)).$$

Ora,

$$\begin{aligned} & xker(f) = yker(f) \\ \Leftrightarrow & y^{-1}x \in ker(f) \\ \Leftrightarrow & f(y^{-1}x) = e_{\mathcal{A}} \\ \Leftrightarrow & f(y)^{-1} \times f(x) = e_{\mathcal{A}} \\ \Leftrightarrow & f(x) = f(y). \end{aligned}$$

Portanto,  $\phi$  é bem definida.

$\phi$  também é um homomorfismo uma vez que

$$\phi(xker(f) \cdot yker(f)).$$

Como  $ker(f) < A$ ,

$$\begin{aligned} \phi(xker(f) \cdot yker(f)) &= \phi(xyker(f)) \\ &= f(xy) \\ &= f(x)f(y) \\ &= \phi(xker(f))\phi(yker(f)). \end{aligned}$$

Ademais, mostraremos que  $\phi$  é injetiva. Ora, mostramos que

$$f(x) = f(y) \Leftrightarrow x\ker(f) = y\ker(f).$$

Assim, pela definição de  $\phi$ ,

$$\phi(x\ker(f)) = \phi(y\ker(f)) \Leftrightarrow x\ker(f) = y\ker(f),$$

que é a definição de injetividade.

Mostraremos por fim a subjetividade de  $\phi$ . Ora, tem-se que

$$Im(\phi) = \phi(A\ker(f)) = f(A) = Im(f),$$

i.e., a imagem de  $\phi$  é equivalente ao seu contra-domínio ( $Im(f)$ ), como queríamos.

O diagrama comutativo abaixo ilustra essa prova.

$$\begin{array}{ccc} & A & \\ \swarrow & \circlearrowleft & \searrow f \\ A/\ker(f) & \xrightarrow{\phi} & Im(f) \subseteq \mathcal{A} \end{array}$$

□

Neste momento, enunciaremos um lema que será útil para o próximo teorema.

**Lema 5.0.6.** Sejam  $H \leq A$  um subgrupo e  $N \triangleleft A$  um subgrupo normal. Então,

$$H \cap N \triangleleft H.$$

*Demonstração.* Uma vez que sendo ambos  $H$  e  $N$  subgrupos de  $A$ , a associatividade, o elemento identidade e inversa de cada elemento nos subgrupos são herdados de  $A$ . Assim, sejam  $x, y \in H \cap N$ , então  $x, y \in H$  e  $x, y \in N$ . Como  $xy^{-1} \in H$  e  $xy^{-1} \in N$ ,  $xy^{-1} \in H \cap N$ , i.e., a operação é fechada e para todo elemento existe elemento inverso correspondente. Assim,  $H \cap N$  é um subgrupo de  $H$ . Ademais, seja  $h \in H$  e  $x \in H \cap N$ , então

$$h x h^{-1} \in H,$$

pois  $x \in H$  e a operação é fechada. Além disso,

$$h x h^{-1} \in N,$$

pois  $x \in N$  e  $N$  é um subgrupo normal. Portanto,

$$h x h^{-1} \in H \cap N,$$

i.e.,  $H \cap N$  é subgrupo normal de  $H$ .

□

**Teorema 5.0.7.** (Segundo Teorema do Isomorfismo). Sejam  $H \leq A$  um subgrupo e  $N \triangleleft A$  um subgrupo normal. Então,

$$\frac{H}{H \cap N} \simeq \frac{HN}{N}.$$

*Demonstração.* Temos pelo Lema 5.0.6 que

$$H \cap N \triangleleft H.$$

Agora, seja  $f : H \rightarrow HN/N$ ,  $f(h) = hN$ . Mostraremos que  $f$  é um homomorfismo já que

$$\begin{aligned} f(h_1 h_2) &= (h_1 h_2)N \\ &= (h_1 N)(h_2 N) \\ &= f(h_1) f(h_2). \end{aligned}$$

Notemos agora que

$$\begin{aligned} \ker(f) &= \{h \in H \mid hN = e_{HN/N} = N\} \\ &= \{h \in H \mid h \in N, \} \end{aligned}$$

i.e.,  $\ker(f) = H \cap N$ .

Por fim, mostraremos que  $f$  é sobrejetora. Ora, pela definição,

$$f(h) \in HN/N \Rightarrow f(H) \subseteq HN/N.$$

E, por sua vez, qualquer elemento de  $HN/N$ ,

$$\begin{aligned} hnN = hN = f(h) \in f(H) &\Rightarrow HN/N \subseteq f(H) \\ &\Rightarrow f(H) = HN/N, \end{aligned}$$

i.e.,  $f$  é sobrejetora.

Dessa forma, pelo Teorema 5.0.5, tem-se que

$$f(H) \simeq H/\ker f(f) \Rightarrow \frac{HN}{N} \simeq \frac{H}{H \cap N}.$$

□

**Teorema 5.0.8.** (Terceiro Teorema do Isomorfismo). Sejam  $H$  e  $N$  subgrupos normais de  $A$ , tais que  $N \subseteq H \subseteq A$ . Então,

$$\frac{A/N}{H/N} \simeq A/H.$$



*Demonstração.* Primeiramente, mostraremos que  $N \triangleleft H$ , o que é imediato uma vez que  $H \subseteq A$  e  $N \triangleleft A$ .

Agora, seja a função  $f : A/N \rightarrow A/H$ , tal que  $f(aN) = aH$ . Mostraremos que ela é bem definida. Ora, sejam

$$xN = yN.$$

Então,

$$y^{-1}x \in N \subseteq H,$$

ou seja,

$$y^{-1}x \in H \Rightarrow xH = yH,$$

e a função é bem definida.

A prova que  $f$  é um homomorfismo vem de que

$$\begin{aligned} f(xN)f(yN) &= (xH)(yH) \\ &= xyH \\ &= f(xyN) \\ &= f((xN)(yN)). \end{aligned}$$

Ademais, tem-se que

$$\begin{aligned} \ker(f) &= \{xN \in A/N \mid f(xN) = e_{A/H}\} \\ &= \{xN \in A/N \mid xH = H\} \\ &= \{xN \in A/N \mid x \in H\} \\ &= H/N. \end{aligned}$$

Além disso, das propriedades do homomorfismo, sabe-se que o  $\ker(f) = H/N$  é subgrupo normal do domínio de  $f$ , isto é,  $A/N$ .

Por fim,  $f$  é sobrejetiva já que, sendo  $aH \in A/H$ , claramente,

$$aH = f(aN) \in f(A/N).$$

Assim,

$$f(A/N) = A/H.$$

Dessa forma, pelo Teorema 5.0.5, tem-se que

$$f(A/N) \simeq (A/N)/\ker f(f) \Rightarrow A/H \simeq \frac{A/N}{H/N}.$$

□

Enunciaremos agora alguns lemas sobre funções e sobre homomorfismos de grupos que nos serão úteis para o próximo teorema.

**Definição 5.0.9.** Seja uma função  $f : X \rightarrow Y$ , então, sendo  $A \subseteq X$  e  $B \subseteq Y$ , definimos

$$f(A) = \{y \in Y \mid y = f(a), \text{ para algum } a \in A\},$$

e definimos como sendo a *pré-imagem* de  $f$

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

**Lema 5.0.10.** Sejam uma função  $f : X \rightarrow Y$  e  $A \subseteq X$  e  $B \subseteq Y$ , é verdade que:

1.  $f(f^{-1}(B)) \subseteq B$ ; ou ainda  $f(f^{-1}(B)) = B$ , sse  $f$  é sobrejetora;
2.  $f^{-1}(f(A)) \supseteq A$ ; ou ainda  $f^{-1}(f(A)) = A$ , sse  $f$  é injetora.

*Demonstração.* Para a primeira afirmação, tem-se que

$$\begin{aligned} f(f^{-1}(B)) &= f(\{x \in X \mid f(x) \in B\}) \\ &\subseteq B. \end{aligned}$$

Ademais, se  $f$  é sobrejetora, seja  $b \in B$ ,

$$\exists x \in X \mid f(x) = b.$$

Ora, então  $x \in f^{-1}(B)$  pela definição de pré-imagem, e

$$b = f(x) \in f(f^{-1}(B)).$$

Já para a segunda afirmação, tem-se

$$\begin{aligned} f^{-1}(f(A)) &= f^{-1}(\{y \in Y \mid y = f(a), \text{ para algum } a \in A\}) \\ &= \{x \in X \mid f(x) \in \{y \in Y \mid y = f(a), \text{ para algum } a \in A\}\} \\ &= \{x \in X \mid f(x) = f(a), \text{ para algum } a \in A\} \\ &\supseteq A. \end{aligned}$$

Além disso, se  $f$  é injetora, seja  $z \in f^{-1}(f(A))$ . Então, pela definição de pré-imagem,

$$f(z) = f(a) \in f(A),$$

para algum  $a \in A$ . Ora, como  $f$  é injetora,

$$z = a \in A.$$

□

Note que se uma função  $f^{-1}$  satisfaz  $f(f^{-1}(B)) = B$  e  $f^{-1}(f(A)) = A$ , ela é também é a função inversa de  $f$ .

**Lema 5.0.11.** Seja um homomorfismo de grupos  $\phi : A \rightarrow H$ , então, sendo  $X \leq A$  e  $Y \leq H$  subgrupos, é verdade que:

1.  $\phi(\phi^{-1}(Y)) = Y \cap \text{Im}(\phi)$ ;
2.  $\phi^{-1}(\phi(X)) = X \ker(\phi)$ .

*Demonstração.* Para a primeira afirmação, tem-se que  $\phi(\phi^{-1}(Y)) \subseteq Y$  pelo lema anterior (5.0.10) e ainda, por definição,  $\phi(\phi^{-1}(Y)) \subseteq \text{Im}(\phi)$ . Assim,

$$\phi(\phi^{-1}(Y)) \subseteq Y \cap \text{Im}(\phi).$$

Ademais, sendo  $z \in Y \cap \text{Im}(\phi)$ ,  $\exists a \in A$ , tal que

$$\phi(a) = z \in Y.$$

Ora, então, pela definição de pré-imagem,

$$\begin{aligned} a &\in \phi^{-1}(Y) \\ \Rightarrow z &= \phi(a) \in \phi(\phi^{-1}(Y)). \end{aligned}$$

Já para a segunda afirmação, tem-se que  $\phi^{-1}(\phi(X)) = X \ker(\phi)$  pela propriedade do isomorfismo já provada (ver propriedade 5).

E ainda, caso  $\phi$  seja injetora,  $\ker(\phi) = \{e_A\}$  e  $X \ker(\phi) = X$ , e assim

$$\phi^{-1}(\phi(X)) = X.$$

□

**Lema 5.0.12.** O homomorfismo (projeção canônica)

$$\phi : A \rightarrow A/H,$$

onde  $H \triangleleft A$ , é sobrejetiva. E, ainda,

$$\ker(\phi) = H.$$

*Demonstração.* Seja  $z \in A/H$ , então como  $z = aH$  e  $a \in A$ ,

$$z = aH = \phi(a) \in \phi(A),$$

ou seja,  $\phi$  é sobrejetiva.

Além disso, provaremos que o  $\ker(f) = H$ . Ora,

$$\begin{aligned}\ker(f) &= \{a \in A \mid f(a) = H\} \\ &= \{a \in A \mid aH = H\} \\ &= \{a \in A \mid a \in H\} \\ &= H.\end{aligned}$$

□

**Teorema 5.0.13.** (Teorema da Correspondência). Seja  $N \triangleleft A$  um subgrupo normal. Então, o homomorfismo  $f : A \rightarrow A/N$  (projeção canônica) induz uma correspondência bijetiva entre o conjunto  $\mathcal{L}_N$  dos subgrupos de  $A$  que contêm  $N$  e o conjunto  $\mathcal{L}$  dos subgrupos de  $A/N$ , dada por:

$$\hat{f} : V \in \mathcal{L}_N \mapsto f(V) = V/N \in \mathcal{L}.$$

Ademais,  $\hat{f}^{-1} : \mathcal{L} \rightarrow \mathcal{L}_N$ , tal que  $H \mapsto f^{-1}(H)$ , é função inversa de  $\hat{f}$ . Além disso, sejam  $X \in \mathcal{L}_N$  e  $Y \in \mathcal{L}$ ,

- i.  $X \triangleleft A \Rightarrow f(X) \triangleleft \text{Im}(f)$ ;
- ii.  $Y \triangleleft \text{Im}(f) \Rightarrow f^{-1}(Y) \triangleleft A$ .

*Demonstração.* Mostraremos inicialmente que  $V/N \leq A/N$ . Sendo  $x, y \in V/N$ ,  $\exists a, b \in V$  tais que

$$xy = (aN)(bN),$$

e como  $N \triangleleft A$  e  $N \subseteq V \leq A$ ,

$$xy = abN \in V/N,$$

já que  $ab \in V$ . Ademais,

$$x^{-1} = (aN)^{-1} = a^{-1}N \in V/N,$$

já que  $a^{-1} \in V$ . Assim, mostramos que

$$V/N \leq A/N,$$

i.e.,  $V/N$  é subgrupo de  $A/N$  e  $V/N \in \mathcal{L}$ .

Mostraremos agora que  $\hat{f}$  é bijetora ao mostrar que a função pré-imagem

$$\hat{f}^{-1} : H \mapsto f^{-1}(H) \in \mathcal{L}_N$$

é função inversa de  $\hat{f}$ .

Ora, pelo lema 5.0.12,  $f$  é sobrejetora. Seja  $H \in \mathcal{L}$ , vamos provar agora que  $\exists K \leq A$ , tal que

$$H = K/N.$$

Mostraremos inicialmente que essa afirmação é equivalente a

$$H \leq A/N \Rightarrow H = f^{-1}(H)/N.$$

Seja  $K := f^{-1}(H)$ . Então, devemos mostrar que  $K \leq A$  e  $N \subseteq K$ . Suponhamos  $x, y \in K = f^{-1}(H)$ . É verdade, portanto, que

$$f(x), f(y) \in H.$$

Como  $H$  é um grupo,

$$\begin{aligned} & f(x)f(y) \in H \\ \Rightarrow & f(xy) \in H \\ \Rightarrow & xy \in f^{-1}(H) = K. \end{aligned}$$

Ademais, como  $f(x) \in H$ ,

$$\begin{aligned} & f(x)^{-1} \in H \\ \Rightarrow & f(x^{-1}) \in H \\ \Rightarrow & x^{-1} \in f^{-1}(H) = K. \end{aligned}$$

E, portanto,  $K \leq A$ .

Mostraremos agora que sendo  $n \in N$ ,  $n \in K$ . Ora,

$$\begin{aligned} \Rightarrow & f(n) = nN \in H \\ \Rightarrow & n \in f^{-1}(H) = K \\ \Rightarrow & N \subseteq K. \end{aligned}$$

Provaremos agora que  $H = f^{-1}(H)/N$ .

( $\supseteq$ ) Seja  $x \in f^{-1}(H)/N$ . Então  $\exists y \in f^{-1}(H)$ , tal que

$$x = yN.$$

Uma vez que  $f$  é sobrejetora e  $f^{-1}(H) \subseteq A$ ,

$$x = yN = f(y) \in H.$$

( $\subseteq$ ) Seja  $h \in H \leq A/N$ . Podemos escrever  $h$  como

$$h = aN = f(a),$$

onde  $a \in A$ . Assim,

$$f(a) \in H \Rightarrow a \in f^{-1}(H).$$

Ora, então,

$$h = aN \in f^{-1}(H)/N.$$

Demonstrado que  $f(K) = K/N$  para algum  $K \leq A$  e  $N \triangleleft K$ ,

$$H = f(K) \in f(\mathcal{L}_N)$$

$$\Rightarrow \mathcal{L} \subseteq f(\mathcal{L}_N),$$

e  $\hat{f}$  é sobrejetora. Assim, pelo lema 5.0.10,

$$\hat{f}(\hat{f}^{-1}(\mathcal{L})) = \mathcal{L}.$$

Além disso, já mostramos que  $\ker(f) = N$ . Assim, sendo  $V \in \mathcal{L}_N$ ,

$$\hat{f}^{-1}(\hat{f}(V)) = f^{-1}(f(V)) = V\ker(f) = VN = V$$

$$\Rightarrow \hat{f}^{-1}(\hat{f}(\mathcal{L}_N)) = \mathcal{L}_N,$$

i.e.,  $\hat{f}$  é injetora. Assim, mostramos que  $\hat{f}^{-1}$  é inversa de  $\hat{f}$  e  $\hat{f}$  é bijetora.

Por fim,

(i.) Seja  $b \in f(A) = \text{Im}(f)$ . Como  $f$  é sobrejetiva,  $b = f(a)$ , para algum  $a \in A$ . Então, uma vez que  $X \triangleleft A$ ,  $Xa = aX$ , e

$$bf(X) = f(a)f(X) = f(aX) = f(Xa) = f(X)f(a) = f(X)b.$$

Portanto, pela definição de normalidade de grupos,

$$f(X) \triangleleft \text{Im}(f).$$

(ii.) Sendo  $Y \triangleleft \text{Im}(f)$ , queremos mostrar que  $f^{-1}(Y) \triangleleft A$ . Isso é equivalente a mostrar que,  $\forall a \in A$ ,

$$af^{-1}(Y)a^{-1} \subseteq f^{-1}(Y) \Leftrightarrow f(af^{-1}(Y)a^{-1}) \subseteq Y \Leftrightarrow f(a)Yf(a)^{-1} \subseteq Y.$$

Ora, como  $Y \triangleleft \text{Im}(f)$ ,

$$f(a)Yf(a)^{-1} \subseteq Y, \quad \forall a \in A,$$

como queríamos. □

## Capítulo 6

# Produto Direto de Grupos

Veremos agora uma maneira de se obter um grupo a partir de dois grupos quaisquer.

**Definição 6.0.1.** Sejam dois grupos  $A$  e  $B$ , o produto direto  $A \times B$  é definido em termo de **componentes** (pares ordenados  $(a, b)$ , tais que  $a \in A$  e  $b \in B$ ) e pelo produto cartesiano desses pares ordenados, i.e.,

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2),$$

onde  $(a_1 a_2, b_1 b_2)$  também é um elemento de  $A \times B$  e, logo, a operação é fechada.

**Proposição 6.0.2.** O produto direto  $A \times B$  satisfaz os axiomas de grupo e, logo, é um grupo.

*Demonstração.* Primeiramente, mostraremos que a operação é associativa. Ora,

$$\begin{aligned} ((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, b_3) &= (a_1 a_2, b_1 b_2) \cdot (a_3, b_3) \\ &= ((a_1 a_2) a_3, (b_1 b_2) b_3) \\ &= (a_1 (a_2 a_3), b_1 (b_2 b_3)) \\ &= (a_1, b_1) \cdot (a_2 a_3, b_2 b_3) \\ &= (a_1, b_1) \cdot ((a_2, b_2) \cdot (a_3, b_3)). \end{aligned}$$

Mostraremos agora que a operação tem elemento inverso e identidade. Seja  $a \in A$  e  $b \in B$ , então,

$$(a, b) \cdot (a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (id_A, id_B),$$

onde  $(id_A, id_B)$  é claramente a identidade da operação. □

Buscaremos agora descobrir as condições para que um grupo seja isomorfo a algum produto direto de grupos.

Enunciaremos para isso, um lema que nos será útil para provar essas condições.

**Lema 6.0.3.** Sejam  $A_1, A_2, \dots, A_n$  subgrupos de um grupo  $A$ , então, dadas as seguintes suposições:

1.  $A = A_1 A_2 \dots A_n$ ;
2.  $A_i \triangleleft A, \forall i = 1, \dots, n$ ;
3.  $A_i \cap (A_1 \dots A_{i-1} A_{i+1} \dots A_n) = \{e\}, \forall i = 1, \dots, n$ ;
4.  $\forall a \in A$ , existem únicos  $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$ , tais que  $a = a_1 a_2 \dots a_n$ ;
5.  $\forall i, j$ , tais que  $1 \leq i, j \leq n$ , sendo  $a_i \in A_i$  e  $a_j \in A_j$ ,  $a_i a_j = a_j a_i$ ;

é verdade que 1., 2., 3.  $\Leftrightarrow$  4., 5..

*Demonstração.* Começaremos mostrando que  $(1., 2., 3. \Rightarrow 4.)$ . Seja  $a = a_1 a_2 \dots a_n \in A$ , sendo  $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$ . Suponhamos  $b_1 \in A_1, b_2 \in A_2, \dots, b_n \in A_n$ , tais que  $a = b_1 b_2 \dots b_n$ . Assim,

$$a_1 a_2 \dots a_n = b_1 b_2 \dots b_n$$

$$\begin{aligned} \Rightarrow a_1 &= b_1 b_2 \dots b_n (a_2 \dots a_n)^{-1} \\ \Rightarrow a_1 &= b_1 b_2 \dots b_n a_n^{-1} \dots a_2^{-1} \\ \Rightarrow b_1^{-1} a_1 &= b_2 \dots b_n a_n^{-1} \dots a_2^{-1} \\ \Rightarrow b_1^{-1} a_1 &\in A_2 \dots A_n A_n \dots A_2. \end{aligned}$$

Ora, como  $A_i \triangleleft A, \forall i = 1, \dots, n$ , por comutatividade, i.e.,  $A_i A_j = A_j A_i$  para  $1 \leq j \leq n$ , tem-se

$$\begin{aligned} b_1^{-1} a_1 &\in A_2 A_2 A_3 A_3 \dots A_{n-1} A_{n-1} A_n A_n \\ &\in A_2 A_3 \dots A_{n-1} A_n. \end{aligned}$$

Assim, pela propriedade (3.),

$$b_1^{-1} a_1 = e \Rightarrow a_1 = b_1.$$

Analogamente, fazemos o mesmo procedimento em tal igualdade a fim de chegar que  $a_2 = b_2, a_3 = b_3, \dots, a_n = b_n$ . Dessa forma, mostramos indutivamente a propriedade (4.).



Agora, mostraremos que  $(1., 2., 3. \Rightarrow 5.)$ . Sejam  $a_i \in A_i$  e  $a_j \in A_j$ . Então, um elemento da forma

$$a_i a_j a_i^{-1} a_j^{-1}$$

é tal que

$$(a_i a_j a_i^{-1}) a_j^{-1} \in A_j,$$

uma vez que  $A_j \triangleleft A$ .

Ainda, como  $A_i \triangleleft A$ ,

$$a_i (a_j a_i^{-1} a_j^{-1}) \in A_i.$$

Ora, então pela propriedade (3.),

$$a_i a_j a_i^{-1} a_j^{-1} \in A_i \cap A_j = \{e\}.$$

Assim,

$$a_i a_j = a_j a_i,$$

como queríamos mostrar.

Finalmente, mostraremos que  $(4., 5. \Rightarrow 1., 2., 3.)$ . A propriedade (1.) é claramente satisfeita a partir da propriedade (4.)

Para mostrar que a propriedade (2.) é satisfeita, queremos mostrar que

$$a A_i a^{-1} \subseteq A_i, \forall a \in A \text{ e } \forall i = 1, \dots, n.$$

Pela propriedade (4.) ou (1.), temos que  $a$  pode ser escrito da forma

$$a = a_1 a_2 \dots a_n.$$

Então, fixado  $i \in \{1, \dots, n\}$ , seja  $x \in A_i$ . Pela comutatividade da propriedade (5.) e por  $a_i x a_i^{-1} \in A_i$ ,

$$\begin{aligned} a x a^{-1} &= a_1 \dots a_i \dots a_n x (a_1 \dots a_i \dots a_n)^{-1} \\ &= a_1 \dots a_i \dots a_n x a_n^{-1} \dots a_i^{-1} \dots a_1^{-1} \\ &= a_1 \dots a_i x \dots a_n a_n^{-1} \dots a_i^{-1} \dots a_1^{-1} \\ &= a_1 \dots (a_i x a_i^{-1}) \dots a_1^{-1} \\ &= a_1 a_1^{-1} a_2 a_2^{-1} \dots (a_i x a_i^{-1}) \\ &= a_i x a_i^{-1} \\ &\in A_i, \end{aligned}$$

como queríamos.

Por fim, mostraremos que a propriedade (3.) é satisfeita. Para isso, seja um elemento  $x \in A_i \cap A_1 \dots A_{i-1} A_{i+1} \dots A_n$ . Como  $x \in A_i$ , então pela propriedade (4.),

$$x = a_1 a_2 \dots a_n, \text{ com } a_j = e \in A_j \text{ para } j \neq i \text{ e } a_i = x.$$

Ora, como  $x \in A_1 \dots A_{i-1} A_{i+1} \dots A_n$ ,

$$x = b_1 \dots b_{i-1} b_i b_{i+1} \dots b_n, \text{ com } b_j \in A_j \text{ e } b_i = e.$$

Utilizando ainda a propriedade (4.), existem únicos  $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$ . Assim,  $a_1 = b_1, a_2 = b_2, \dots, a_n = b_n$ , i.e.,

$$a_i = b_i \Rightarrow x = e,$$

e portanto,

$$A_i \cap (A_1 \dots A_{i-1} A_{i+1} \dots A_n) = \{e\},$$

como queríamos mostrar. □

**Teorema 6.0.4.** Sejam  $A, H_1, \dots, H_n$  grupos. O grupo  $A$  é isomorfo ao grupo  $H_1 \times \dots \times H_n$  se, e somente se,  $A$  possui os subgrupos  $A_1 \simeq H_1, \dots, A_n \simeq H_n$  tais que:

1.  $A = A_1 A_2 \dots A_n$ .
2.  $A_i \triangleleft A, \forall i = 1, \dots, n$ .
3.  $A_i \cap (A_1 \dots A_{i-1} A_{i+1} \dots A_n) = \{e\}, \forall i = 1, \dots, n$ .

*Demonstração.* ( $\Leftarrow$ ) Seja  $f : A \rightarrow A_1 \times \dots \times A_n$  uma relação, tal que

$$f(a) = (a_1, \dots, a_n),$$

onde  $a = a_1 a_2 \dots a_n$  com  $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$ .

Mostraremos agora que  $f$  é uma função bem definida. Sejam  $a = b \in A$ , então,

$$a = a_1 a_2 \dots a_n, \text{ tais que } a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$$

$$b = b_1 b_2 \dots b_n, \text{ tais que } b_1 \in A_1, b_2 \in A_2, \dots, b_n \in A_n.$$

Ora, pela propriedade (4.) do Lema 6.0.3,

$$a_1 = b_1, a_2 = b_2, \dots, a_n = b_n.$$

Assim,

$$f(a) = f(b),$$

como queríamos.

Ademais, mostraremos que  $f$  é um homomorfismo, aplicando a propriedade (5.) do Lema 6.0.3.

$$\begin{aligned}
 f(ab) &= f(a_1 \dots a_n b_1 \dots b_n) \\
 &= f(a_1 b_1 \dots a_n b_n) \\
 &= (a_1 b_1, \dots, a_n b_n) \\
 &= (a_1, \dots, a_n) \times (b_1, \dots, b_n) \\
 &= f(a) \times f(b).
 \end{aligned}$$

Finalmente, mostraremos que  $f$  é uma bijeção. Ora, sejam  $f(a) = f(b)$  para  $a, b \in A$ ,

$$\begin{aligned}
 f(a) &= f(b) \\
 \Rightarrow (a_1, \dots, a_n) &= (b_1, \dots, b_n) \\
 \therefore a_1 &= b_1, \dots, a_n = b_n,
 \end{aligned}$$

i.e.,  $a = b$  ( $f$  é injetora).

Para a sobrejetividade, consideremos um elemento  $y \in A_1 \times \dots \times A_n$ . Então, pela definição de produto direto,

$$y = (a_1, \dots, a_n),$$

tais que  $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$ . Uma vez que, pela propriedade (1.),  $A = A_1 A_2 \dots A_n$ ,

$$y \in f(a),$$

como queríamos.

Finalmente, mostraremos que a função  $F : A_1 \times \dots \times A_n \rightarrow H_1 \times \dots \times H_n$ , tal que  $F : (a_1, \dots, a_n) \mapsto (f_1(a_1), \dots, f_n(a_n))$ , é uma bijeção. Seja  $f_i$  a relação de isomorfismo entre  $A_i$  e  $H_i$ ,  $f_i : A_i \rightarrow H_i$ . A função  $F$  está bem definida uma vez que, sendo  $(a_1, \dots, a_n), (b_1, \dots, b_n) \in A_1 \times \dots \times A_n$ , tais que  $(a_1, \dots, a_n) = (b_1, \dots, b_n)$ , é verdade que  $a_i = b_i, \forall i = 1, \dots, n$ . Assim, como  $f_i$  é um isomorfismo,

$$f_i(a_i) = f_i(b_i).$$

Portanto, tem-se que

$$F((a_1, \dots, a_n)) = (f_1(a_1), \dots, f_n(a_n)) = (f_1(b_1), \dots, f_n(b_n)) = F((b_1, \dots, b_n)).$$

Mostraremos agora a injetividade de  $F$ . Sejam  $(a_1, \dots, a_n), (b_1, \dots, b_n) \in A_1 \times \dots \times A_n$ , tais que  $F((a_1, \dots, a_n)) = F((b_1, \dots, b_n))$ . Então, é verdade que

$$(f_1(a_1), \dots, f_n(a_n)) = (f_1(b_1), \dots, f_n(b_n)).$$

Temos, assim, que  $f_i(a_i) = f_i(b_i)$ . Ora, como  $f_i$  é um isomorfismo,  $a_i = b_i$  e, então,

$$(a_1, \dots, a_n) = (b_1, \dots, b_n).$$

Resta-nos agora mostrar a sobrejetividade de  $F$ . Para isso, consideremos  $(h_1, \dots, h_n) \in H_1 \times \dots \times H_n$ . Ora, como já assumimos que existe  $f_i$  tal que  $A_i \simeq H_i$ , temos que

$$\exists a_i, \text{ tal que } f_i(a_i) = h_i, \text{ para } i = \{1, \dots, n\}.$$

Assim, podemos escrever que

$$(h_1, \dots, h_n) = (f_1(a_1), \dots, f_n(a_n)) \in F(A_1 \times \dots \times A_n).$$

( $\Rightarrow$ ) Suponhamos  $\phi : A \rightarrow H_1 \times \dots \times H_n$  um isomorfismo de grupos. Mostraremos que  $A$  contém os subgrupos  $A_1 \simeq H_1, \dots, A_n \simeq H_n$  (com as condições citadas no teorema). Sendo  $X_i = Y_1 \times Y_2 \times \dots \times Y_n$ , tal que  $Y_j = \{e\}$  se  $j \neq i$  e  $Y_j = H_j$  se  $j = i$  com  $i = 1, \dots, n$ , definimos

$$A_i := \phi^{-1}(X_i) \subseteq A.$$

É verdade que  $X_i$  é subgrupo de  $H_1 \times \dots \times H_n$  uma vez que sendo  $a, b \in X_i$ ,  $a = (x_1, \dots, x_n)$  e  $b = (y_1, \dots, y_n)$ , tais que  $x_j = y_j = e$  se  $j \neq i$ . Então,

$$\begin{aligned} ab^{-1} &= (x_1, \dots, x_n)(y_1, \dots, y_n)^{-1} \\ &= (x_1, \dots, x_n)(y_1^{-1}, \dots, y_n^{-1}) \\ &= (x_1y_1^{-1}, \dots, x_iy_i^{-1}, \dots, x_ny_n^{-1}) \\ &= (e, \dots, e, x_iy_i^{-1}, e, \dots, e) \\ &\in X_i. \end{aligned}$$

Ademais, precisamos mostrar que  $A_i$  é subgrupo de  $A$ . Dados  $a, b \in A_i$ , tem-se, por  $\phi$  ser um isomorfismo, que  $\phi(a), \phi(b) \in X_i$ . Ora,

$$\phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in X_i.$$

Então,

$$ab^{-1} \in \phi^{-1}(X_i) = A_i.$$

Queremos mostrar ainda que  $A_i \simeq H_i$ . Seja, então, a função

$$\begin{aligned} \phi_i : X_i &\rightarrow H_i \\ (h_1, \dots, h_n) &\mapsto h_i. \end{aligned}$$

$\phi_i$  é um homomorfismo já que, dados  $a, b \in X_i$ ,  $a = (x_1, \dots, x_n)$  e  $b = (y_1, \dots, y_n)$ , tais que  $x_j = y_j = e$  se  $j \neq i$ ,

$$\begin{aligned}\phi_i(ab) &= \phi_i((x_1, \dots, x_n)(y_1, \dots, y_n)) \\ &= \phi_i((x_1y_1, \dots, x_iy_i, \dots, x_ny_n)) \\ &= x_iy_i \\ &= \phi_i(a)\phi_i(b).\end{aligned}$$

$\phi_i$  também é sobrejetiva, pois sendo  $h_i \in H_i$  e

$$x_i := (h_1, \dots, h_i, \dots, h_n) \in X_i,$$

com  $h_j = e$ , se  $j \neq i$ , tem-se que

$$h_i = \phi_i(x_i).$$

Além disso,  $\phi_i$  é injetiva uma vez que para  $(a_1, \dots, a_n), (b_1, \dots, b_n) \in X_i$ , tais que

$$\phi_i((a_1, \dots, a_n)) = \phi_i((b_1, \dots, b_n)),$$

é verdade que  $a_i = b_i$ . Então,

$$(a_1, \dots, a_n) = (b_1, \dots, b_n),$$

uma vez que  $a_j = b_j = e$  se  $j \neq i$ . Mostrado que  $\phi_i$  é um isomorfismo, então,

$$\phi_i \circ \phi(A_i) = \phi_i(\phi(A_i)) = \phi_i(\phi(\phi^{-1}(X_i))) = \phi_i(X_i) = H_i$$

Portanto, podemos afirmar que

$$A_i \simeq_{\phi_i \circ \phi} H_i,$$

como queríamos.

Quanto à propriedade (1.), seja  $a \in A$ , como  $\phi$  é uma bijeção,  $\phi^{-1}(H_1 \times \dots \times H_n) = A$ . Ora, pela definição de produto direto de grupos,

$$H_1 \times \dots \times H_n = X_1 X_2 \dots X_n.$$

Assim,

$$\begin{aligned}\phi^{-1}(X_1 X_2 \dots X_n) &= A \\ \phi^{-1}(X_1) \phi^{-1}(X_2) \dots \phi^{-1}(X_n) &= A \\ A_1 A_2 \dots A_n &= A,\end{aligned}$$

como queríamos.

A propriedade (3.) vem de que

$$\begin{aligned}
 Y &= A_i \cap (A_1 \dots A_{i-1} A_{i+1} \dots A_n) \\
 &= \phi^{-1}(X_i) \cap \phi^{-1}(X_1 \dots X_{i-1} X_{i+1} \dots X_n) \\
 &= \phi^{-1}(\{e\} \times \dots \times \{e\} \times H_i \times \{e\} \times \dots \times \{e\}) \cap \phi^{-1}(H_1 \times \dots \times H_{i-1} \times \{e\} \times H_{i+1} \times \dots \times H_n) \\
 &= \{e\}.
 \end{aligned}$$

Quanto à propriedade (2.), queremos mostrar que  $aA_ia^{-1} \subseteq A_i, \forall i = 1, 2, \dots, n, \forall a \in A$ .

Ora,

$$\begin{aligned}
 \phi(aA_ia^{-1}) &= \phi(a)\phi(A_i)\phi(a^{-1}) \\
 &= (h_1, h_2, \dots, h_n)(\{e\} \times \dots \times \{e\} \times H_i \times \{e\} \times \dots \times \{e\})(h_1^{-1}, h_2^{-1}, \dots, h_n^{-1}) \\
 &= (h_1h_1^{-1}, \dots, h_{i-1}h_{i-1}^{-1}, h_iH_ih_i^{-1}, h_{i+1}h_{i+1}^{-1}, \dots, h_nh_n^{-1}) \\
 &= \{e\} \times \dots \times \{e\} \times H_i \times \{e\} \times \dots \times \{e\} \\
 &= \phi(A_i).
 \end{aligned}$$

Como  $\phi$  é bijetora,

$$aA_ia^{-1} = A_i,$$

como queríamos mostrar. □

## Capítulo 7

# Grupos de Permutações

Antes de propriamente discorrer sobre grupos de permutações, enunciaremos algumas definições e proposições que serão úteis para isso.

**Definição 7.0.1.** Chama-se de **conjunto subjacente** de um grupo  $A$  o conjunto de  $A$  sem a estrutura de grupo.

**Proposição 7.0.2.** Seja  $C$  um conjunto. Então,  $(Bij(C), \circ)$  é um grupo, onde

$$Bij(C) = \{f : C \rightarrow C \mid f \text{ é uma bijeção}\}$$

e  $\circ$  é a operação de composição de funções.

Esse grupo é designado por  $\mathcal{P}(C)$ .

*Demonstração.* A fim de provar que  $\mathcal{P}(C)$  é de fato um grupo começamos mostrando que, sendo  $f, g \in \mathcal{P}(C)$ , então  $f \circ g \in \mathcal{P}(C)$ , i.e., que a operação é fechada. Como  $f$  e  $g$  são bijetoras pela definição do conjunto  $Bij(C)$ , tem-se que

$$f \circ g : C \rightarrow C.$$

Sendo  $c, d \in C$ , se  $f \circ g(c) = f \circ g(d)$ , então,

$$f(g(c)) = f(g(d)) \Leftrightarrow f^{-1}(f(g(c))) = f^{-1}(f(g(d))) \Leftrightarrow g(c) = g(d) \Leftrightarrow g^{-1}(g(c)) = g^{-1}(g(d)) \Leftrightarrow c = d,$$

ou seja,  $f \circ g$  é injetiva. Além disso, seja  $c \in C$ . Ora, como  $f$  é sobrejetora,  $\exists x \in C$  tal que  $f(x) = c$ . E, como  $g$  é sobrejetora,  $\exists y \in C$  tal que  $g(y) = x$ . Assim,

$$f(g(y)) = c,$$

isto é,  $f \circ g$  é sobrejetora. Logo,  $f \circ g$  é bijetora e é elemento de  $\mathcal{P}(C)$ .

Sejam  $f, g, h \in \mathcal{P}(C)$ , mostraremos que a operação de composição é associativa. Assim,

$$f \circ (g \circ h)(C) = f \circ (g(h(C))) = f(g(h(C))) = (f \circ g)(h(C)) = (f \circ g) \circ h(C).$$

Por fim, resta mostrar que o grupo admite elemento identidade e inversa. Ora, para  $f \in \mathcal{P}(C)$ , como  $f$  é bijetora,  $\exists g \in \mathcal{P}(C)$  tal que  $g = f^{-1}$ . Assim,

$$f \circ g(C) = Id_{\mathcal{P}(C)},$$

onde

$$Id_{\mathcal{P}(C)} : c \mapsto c.$$

□

Um conjunto de grupos bastante útil no estudo de grupos finitos é dos grupos de permutações. Assim, a proposição 7.0.3 a seguir mostra que qualquer grupo finito é isomorfo a um subgrupo de um grupo de permutações.

**Teorema 7.0.3.** (Cayley) Seja  $A$  um grupo finito, tal que  $n = |A|$ , e  $A_0$  o conjunto subjacente a  $A$ . Então,

$$\begin{aligned} T : A &\rightarrow \mathcal{P}(A_0) && \simeq S_n \\ a &\mapsto T_a : A_0 && \xrightarrow{\sim} A_0 \\ x &\mapsto ax, \end{aligned}$$

é um homomorfismo injetivo.

*Demonstração.* Mostraremos inicialmente que  $T$  está bem definida. Sejam  $a_1, a_2 \in A$  e  $a_1 = a_2$ , então  $T_{a_1}(x_i) = a_1 x_i = a_2 x_i = T_{a_2}(x_i), \forall x_i \in A_0$ . Assim,  $T_{a_1} = T_{a_2}$ .

Agora, mostraremos que  $T$  é um homomorfismo. Sejam  $a_1, a_2 \in A$ , então  $T_{a_1 a_2}(x_i) = (a_1 a_2)x_i = a_1(a_2 x_i) = T_{a_1}(T_{a_2}(x_i))$ . Assim,  $T_{a_1 a_2} = T_{a_1} T_{a_2}$ .

Por fim, mostraremos que  $T$  é injetivo. Tem-se que se  $a \in \ker(T)$ , então  $T_a = Id_{A_0}$ . Ora, se  $T_a = Id_{A_0}$ , então  $ax = x, \forall x \in A_0$ . Assim,  $a = e$ , e portanto  $\ker(T) = \{e\}$ , o que implica que  $T$  é injetivo, pelas propriedades do homomorfismo. □

**Definição 7.0.4.** Uma permutação  $\alpha \in S_n$  é um  $r$ -ciclo se existem  $a_1, a_2, \dots, a_r \in \{1, \dots, n\}$  distintos tais que  $\alpha(a_1) = a_2, \alpha(a_2) = a_3, \dots, \alpha(a_{r-1}) = a_r, \alpha(a_r) = a_1$ , e os demais elementos de  $\{1, \dots, n\}$  são mapeados a eles mesmos. Esse  $r$ -ciclo é denotado por  $(a_1 \dots a_r)$ , onde  $r$  é o comprimento do ciclo.

É interessante apontar que 2-ciclos são chamados de *transposições*.

Alguns **exemplos** interessantes de  $r$ -ciclos em  $S_5$  são listados a seguir.



Exemplo 1)  $\begin{pmatrix} 12345 \\ 23451 \end{pmatrix}$  é um 5-ciclo com uma possível representação (12345).

Exemplo 2)  $\begin{pmatrix} 12345 \\ 32145 \end{pmatrix}$  é uma transposição com possível representação (13).

Exemplo 3) O único 1-ciclo é a identidade  $\begin{pmatrix} 12345 \\ 12345 \end{pmatrix}$  com possível representação (1).

**Definição 7.0.5.** Sejam  $\alpha, \beta \in S_n$  um  $r_1$ -ciclo e um  $r_2$ -ciclo.  $\alpha$  e  $\beta$  são ditas disjuntas se  $\forall a \in \{1, 2, \dots, n\}$ , tem-se  $\alpha(a) = a$  **ou**  $\beta(a) = a$ .

**Proposição 7.0.6.** Dados  $\alpha, \beta \in S_n$  dois ciclos disjuntos, então  $\alpha\beta = \beta\alpha$ .

*Demonstração.* Ora, por definição,  $\forall a \in \{1, 2, \dots, n\}$ ,  $\alpha(a) = a$  **ou**  $\beta(a) = a$ . Assim, para o caso em que  $\alpha(a) = a$ ,

$$\alpha(\beta(a)) = \beta(a) = \beta(\alpha(a)).$$

Já para o caso em que  $\beta(a) = a$ ,

$$\alpha(\beta(a)) = \alpha(a) = \beta(\alpha(a)).$$

Portanto,  $\alpha\beta = \beta\alpha$ . □

**Proposição 7.0.7.** Seja  $\alpha \in S_n$  um  $r$ -ciclo. Mostre que a ordem de  $\alpha$  é igual a  $r$ .

*Demonstração.* Para mostrarmos que a ordem de  $\alpha$  é igual a  $r$ , mostraremos que  $\alpha^r = Id$  (1) e que  $r$  é o menor inteiro positivo com essa propriedade.

Primeiro, vamos mostrar que  $\alpha^r = Id$ . Isso significa que  $\alpha^r(a_i) = a_i$  para todo  $i = 1, \dots, r$ . Mas isso é verdade por definição de  $r$ -ciclo, pois  $\alpha(a_i) = a_{i+1}$  para  $i = 1, \dots, r-1$  e  $\alpha(a_r) = a_1$ . Então, aplicando  $\alpha$  repetidamente  $r$  vezes, temos que  $\alpha^r(a_i) = a_{i+r} = a_i$ , onde usamos a aritmética modular para simplificar o índice, tal que  $\alpha(a_i) = a_{i+1}$ ,  $\alpha(a_{i+1}) = a_{i+2}$ ,  $\dots$ ,  $\alpha(a_{i+(r-i-1)}) = a_r$  e  $\alpha(a_r) = a_1$ ,  $\dots$ ,  $\alpha(a_{i-1}) = a_i$ . Como existem  $i$  elementos entre  $a_{i-1}$  e  $a_r$  e existem  $r-i$  elementos entre  $a_{i+(r-i-1)}$  e  $a_i$ , então  $\alpha^r(a_i) = a_i$ .

Para mostrar que  $r$  é o menor inteiro positivo que satisfaz essa propriedade, suponhamos que exista um inteiro positivo  $s < r$ , tal que  $\alpha^s = Id$ . Ora, isso contradiz a definição de  $r$ -ciclo, pois teríamos que  $\alpha^s(a_i) = a_{i+s} = a_i$ , o que significa que  $s = 0$  ou  $s = r$ . Mas  $s$  não pode ser zero, pois é um inteiro positivo. E  $s \neq r$ , pois assumimos que  $s < r$ . Portanto,  $r$  é o menor inteiro positivo com essa propriedade. □

**Proposição 7.0.8.** Sejam  $\alpha_1, \dots, \alpha_t \in S_n$  ciclos disjuntos de comprimentos  $r_1, \dots, r_t$ , respectivamente, Mostre que o produto  $\alpha_t \dots \alpha_1$  tem ordem igual a  $MMC\{r_1, \dots, r_t\}$ .

*Demonstração.* Mostraremos primeiramente, utilizando a proposição 7.0.6, que, sendo  $\alpha, \beta \in S_n$  dois ciclos disjuntos, então  $(\alpha\beta)^k = \alpha^k\beta^k$ ,  $\forall k \in \mathbb{N}$ . Ora,

$$(\alpha\beta)^k = \underbrace{\alpha\beta}_{k \text{ vezes}} = \underbrace{\alpha}_{k \text{ vezes}} \underbrace{\beta}_{k \text{ vezes}} = \alpha^k\beta^k.$$

Ademais, com a proposição 7.0.7, tem-se que

$$(\alpha_t \dots \alpha_1)^{MMC\{r_1, \dots, r_t\}} = \alpha_t^{MMC\{r_1, \dots, r_t\}} \dots \alpha_1^{MMC\{r_1, \dots, r_t\}} = Id,$$

pois  $MMC\{r_1, \dots, r_t\}$  é múltiplo de cada  $r_i$ .

Por fim, mostraremos que  $MMC\{r_1, \dots, r_t\}$  é o menor inteiro positivo que satisfaz a propriedade, e logo é a ordem do produto. Ora, seja  $s < MMC\{r_1, \dots, r_t\}$  um inteiro positivo, tal que  $(\alpha_t \dots \alpha_1)^s = Id$ . Então,  $\alpha_t^s \dots \alpha_1^s = Id$ . Isso implica que  $\alpha_i^s = Id$ ,  $\forall i = 1, \dots, t$ . Todavia, isso contradiz com o fato de que a ordem de cada  $\alpha_i$  ser igual a  $r_i$ . Logo,  $MMC\{r_1, \dots, r_t\}$  é igual a ordem do produto  $\alpha_t \dots \alpha_1$ .  $\square$

**Proposição 7.0.9.** Seja  $\alpha \in S_n$  e  $\alpha \neq Id$ . Então,  $\alpha$  é igual a um produto de ciclos disjuntos de comprimentos  $\geq 2$ , tal que a fatoração é única a menos da ordem dos fatores.

*Demonstração.* Vamos provar a existência da fatoração por indução no número de elementos  $n$  do conjunto  $\{1, 2, \dots, n\}$  sobre o qual  $S_n$  age.

Para  $n = 2$ , a única permutação diferente da identidade é a transposição  $(1 \ 2)$ , que é um ciclo de comprimento 2.  $\square$