

# Teoria de Grupos: notas de estudo

Guilherme Philippi

29 de janeiro de 2021

# Sumário

<b>1</b>	<b>Grupos</b>	<b>2</b>
1.1	Lei de composição . . . . .	2
1.2	Grupos . . . . .	3
1.3	Subgrupos . . . . .	4
1.4	Homomorfismos . . . . .	5
1.5	Isomorfismos . . . . .	5
1.6	Grupos de Permutação . . . . .	6
1.7	Relações de Equivalência e Partições . . . . .	7
1.8	Orbitas, ciclos e grupos alternados . . . . .	9
1.9	Coclasses . . . . .	10
1.10	Restrição de um homomorfismo para um subgrupo . . . . .	11
1.11	Produto de Grupos . . . . .	12
1.12	Aritmética Modular . . . . .	13
1.13	Estrutura de grupos abelianos finitamente gerados . . . . .	14
1.14	Grupos de Quociente . . . . .	15
	<b>Referências Bibliográficas</b>	<b>15</b>

# Capítulo 1

## Grupos

### 1.1 Lei de composição

**Definição 1.1.1** (Lei de composição). Uma *lei de composição* sobre um conjunto  $S$  é uma função (ou, uma operação binária)  $*$  :  $S \times S \longrightarrow S$ .

**Observação 1.1.1** (Notação de operação). Usaremos a notação  $*(a, b) = a * b$ , para simplificar a escrita de propriedades. Também, quando não houver ambiguidade, suprimiremos o símbolo da lei, fazendo  $a * b = ab$ .

**Definição 1.1.2.** Para  $a, b, c \in S$ , uma lei de composição  $*$  é dita

- *Associativa*, se  $(a * b) * c = a * (b * c)$ ;
- *Comutativa*, se  $a * b = b * a$ .

**Proposição 1.1.1.** *Seja uma lei associativa dada sobre o conjunto  $S$ . Há uma única forma de definir, para todo inteiro  $n$ , um produto de  $n$  elementos  $a_1, \dots, a_n \in S$  (diremos  $[a_1 \cdots a_n]$ ) com as seguintes propriedades:*

1. *o produto  $[a_1]$  de um elemento é o próprio elemento;*
2. *o produto  $[a_1 a_2]$  de dois elementos é dado pela lei de composição;*
3. *para todo inteiro  $1 \leq i \leq n$ ,  $[a_1 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n]$ .*

*Demonstração.* A demonstração dessa proposição é feita por indução em  $n$ . □

**Definição 1.1.3.** Dizemos que  $e \in S$  é *identidade* para uma lei de composição se  $ea = ae = a$  para todo  $a \in S$ .

**Proposição 1.1.2.** *O elemento identidade é único.*

*Demonstração.* Se  $e, e'$  são identidades, já que  $e$  é identidade, então  $ee' = e'$  e, como  $e'$  é uma identidade,  $ee' = e$ . Logo  $e = e'$ , isto é, a identidade é única. □

**Observação 1.1.2.** Usaremos  $\bar{1}$  para representar a identidade multiplicativa e  $\bar{0}$  para denotar a aditiva.

**Definição 1.1.4** (Elemento inverso). Seja uma lei de composição que possua uma identidade. Um elemento  $a \in S$  é chamado *invertível* se há um outro elemento  $b \in S$  tal que  $ab = ba = 1$ . Desde que  $b$  exista, ela é única e a denotaremos por  $a^{-1}$  e a chamaremos *inversa de  $a$* .

**Proposição 1.1.3.** *Se  $a, b \in S$  possuem inversa, então a composição  $(ab)^{-1} = b^{-1}a^{-1}$ .*

**Observação 1.1.3** (Potências). Usaremos as seguintes notações:

- $a^n = a^{n-1}a$  é a composição de  $a \cdots a$   $n$  vezes;
- $a^{-n}$  é a inversa de  $a^n$ ;
- $a^0 = \vec{1}$ .

Com isso, tem-se que  $a^{r+s} = a^r a^s$  e  $(a^r)^s = a^{rs}$ . (Isso não induz uma notação de fração  $\frac{b}{a}$  a menos que seja uma lei comutativa, visto que  $ba^{-1}$  pode ser diferente de  $a^{-1}b$ ). Para falar de uma lei de composição aditiva, usaremos  $-a$  no lugar de  $a^{-1}$  e  $na$  no lugar de  $a^n$ .

## 1.2 Grupos

**Definição 1.2.1** (Grupo). Um *grupo*  $(G, *)$  é um conjunto  $G$  onde uma lei de composição  $*$  é dada sobre  $G$  tal que os seguintes axiomas são satisfeitos:

1. (*Associatividade*). Para todo  $a, b, c \in G$ , tem-se

$$(a * b) * c = a * (b * c);$$

2. (*Existência da identidade*). Existe um elemento  $\vec{1} \in G$  tal que, para todo  $a \in G$ ,

$$\vec{1} * a = a * \vec{1} = a;$$

3. (*Existência do inverso*). Para todo  $a \in G$  existe um elemento  $a' \in G$  tal que

$$a * a' = a' * a = \vec{1}.$$

**Observação 1.2.1.** É comum abusar da notação e chamar um grupo  $(G, *)$  e o conjunto de seus elementos  $G$  pelo mesmo símbolo, omitindo a lei de composição na falta de ambiguidade.

**Definição 1.2.2** (Grupo abeliano). Um *grupo abeliano* é um grupo com uma lei de composição comutativa. Costuma-se usar a notação aditiva para grupos abelianos.

**Proposição 1.2.1** (Lei do cancelamento). *Seja  $a, b, c$  elementos de um grupo  $G$ . Se  $ab = ac$ , então  $b = c$ .*

## 1.3 Subgrupos

**Definição 1.3.1** (Subgrupo). Um subconjunto  $H$  de um grupo  $G$  é chamado de *subgrupo* de  $G$  (e escreve-se  $H \leq G$ ) se possuir as seguintes propriedades:

1. (*Fechado*). Se  $a, b \in H$ , então  $ab \in H$ ;
2. (*Identidade*).  $1 \in H$ ;
3. (*Inversível*). Se  $a \in H$ , então  $a^{-1} \in H$ .

**Observação 1.3.1** (Lei de composição induzida). Veja que a propriedade 1 necessita de uma lei de composição. Usamos a lei de composição de  $G$  para definir uma lei de composição de  $H$ , chamada *lei de composição induzida*. Essas propriedades garantem que  $H$  é um grupo com respeito a sua lei induzida.

**Definição 1.3.2** (Subgrupo apropriado). Todo grupo  $G$  possui dois subgrupos triviais: O subgrupo formado por todos os elementos de  $G$  e o subgrupo  $\{1\}$ , formado pela identidade de  $G$ . Diz-se que um subgrupo é um *subgrupo apropriado* se for diferente desses dois.

**Definição 1.3.3** (Centro de um grupo). O *centro*  $Z(G)$  de um grupo  $G$  é o conjunto de elementos que comutam com todo elemento de  $G$ :

$$Z(G) = \{z \in G \mid zx = xz \text{ para todo } x \in G\}.$$

**Exemplo 1.3.1.** Utilizando da notação multiplicativa, define-se o *subgrupo cíclico*  $H$  gerados por um elemento arbitrário  $x$  de um grupo  $G$  como o conjunto de todas as potências de  $x$ :  $H = \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\}$ .

**Definição 1.3.4.** Chama-se *ordem* de um grupo  $G$  o número  $|G|$  de elementos de  $G$ .

Também pode-se definir um subgrupo de um grupo  $G$  *gerado por um subconjunto*  $U \subset G$ . Esse é o menor subgrupo de  $G$  que contém  $U$  e consiste de todos os elementos de  $G$  que podem ser expressos como um produto de uma cadeia de elementos de  $U$  e seus inversos.

**Exemplo 1.3.2.** O *grupo de quaternions*  $H$  é o menor subgrupo do conjunto de matrizes  $2 \times 2$  complexas invertíveis que não é cíclico. Isso consiste nas oito matrizes

$$H = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\},$$

onde

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Os dois elementos  $\mathbf{i}, \mathbf{j}$  geram  $H$ , e o cálculo leva as formulas

$$\mathbf{i}^4 = 1, \quad \mathbf{i}^2 = \mathbf{j}^2, \quad \mathbf{j}\mathbf{i} = \mathbf{i}^3\mathbf{j}.$$

## 1.4 Homomorfismos

**Definição 1.4.1** (Homomorfismo de grupo). Sejam  $(G, *)$  e  $(G', \cdot)$  dois grupos. Um *homomorfismo*  $\varphi : G \longrightarrow G'$  é um mapeamento tal que

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b), \quad \forall a, b \in G. \quad (\text{propriedade de homomorfismo})$$

**Exemplo 1.4.1** (Inclusão). Seja  $H$  o subgrupo de um grupo  $G$ . O homomorfismo  $i : H \longrightarrow G$  é dito *inclusão* de  $H$  em  $G$ , definido por  $i(x) = x$ .

**Proposição 1.4.1.** Um homomorfismo  $\varphi : G \longrightarrow G'$  mapeia a identidade de  $G$  à identidade de  $G'$  e transforma as inversas de  $G$  nas respectivas inversas em  $G'$ . Isto é,  $\varphi(\vec{1}) = \vec{1}$  e  $\varphi(a^{-1}) = \varphi(a)^{-1}$ .

**Observação 1.4.1.** Por conta da Proposição 1.4.1, dizemos que o mapeamento  $\varphi$  preserva a estrutura algébrica de grupo.

**Definição 1.4.2** (Imagem). A *imagem* de um homomorfismo  $\varphi : G \longrightarrow G'$  é o subconjunto de  $G'$

$$\text{im } \varphi = \{x \in G' \mid x = \varphi(a), \text{ para algum } a \in G\} = \varphi(G).$$

**Proposição 1.4.2.** A imagem de um homomorfismo  $\varphi : G \longrightarrow G'$  é um subgrupo de  $G'$ .

**Definição 1.4.3** (Núcleo). O *núcleo* do homomorfismo  $\varphi : G \longrightarrow G'$  é o subconjunto de  $G$  formado pelos elementos que são mapeados pela identidade em  $G'$ :

$$\text{nu } \varphi = \{a \in G \mid \varphi(a) = 1\} = \varphi^{-1}(1).$$

**Proposição 1.4.3.** O núcleo de um homomorfismo  $\varphi : G \longrightarrow G'$  é um subgrupo de  $G$ .

## 1.5 Isomorfismos

**Definição 1.5.1** (Isomorfismo de grupos). Dois grupos  $(G, *)$  e  $(G', \cdot)$  são ditos *isomorfos* se possuírem um homomorfismo bijetivo entre si, isto é, há um mapeamento *bijetivo*  $\varphi : G \longrightarrow G'$  (chamado *relação de isomorfismo*) que respeita a propriedade de homomorfismo:

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b), \text{ para todo } a, b \in G.$$

**Observação 1.5.1.** Usa-se a notação  $G \approx G'$  para dizer que  $G$  é isomorfo a  $G'$ .

**Definição 1.5.2** (Classe de isomorfismo). Diz-se que o conjunto de grupos isomórfos a um dado grupo  $G$  é a *classe de isomorfismo* de  $G$ .

**Proposição 1.5.1.** Qualquer dois grupos em uma mesma classe de isomorfismo também são isomorfos entre si.

**Definição 1.5.3** (Automorfismo). Quando uma relação de isomorfismo  $\varphi : G \longrightarrow G$  é definida de um grupo  $G$  para ele mesmo, chamamos esse tipo de isomorfismo de *automorfismo* de  $G$ .

**Exemplo 1.5.1** (Conjugação). Seja  $b \in G$  um elemento fixo. Então, a *conjugação de  $G$  por  $b$*  é o mapeamento  $\varphi$  de  $G$  para ele mesmo definido por

$$\varphi_b(x) = bxb^{-1}.$$

Esse é um automorfismo porque:

- é compatível com a propriedade de homomorfismo:

$$\varphi_b(xy) = bxyb^{-1} = bx\bar{1}yb^{-1} = bxb^{-1}byb^{-1} = \varphi_b(x)\varphi_b(y);$$

- é um mapa bijetivo visto que existe a função inversa  $\varphi_b^{-1}(x) = b^{-1}xb = \varphi_{b^{-1}}(x)$  (isto é, a conjugação por  $b^{-1}$ ) que, de forma análoga, também é compatível com a propriedade de homomorfismo.

**Observação 1.5.2** (Abelianos). Se o grupo é abeliano possui a conjugação trivial:  $bab^{-1} = abb^{-1} = a$  (mapa identidade). Porém, qualquer grupo não comutativo tem alguma conjugação não trivial, isto é, existe ao menos um  $b$  que não está no centro do grupo, portanto, ao menos o automorfismo não trivial dado pela conjugação do grupo por  $b$  existe.

**Definição 1.5.4** (Conjugado). O elemento  $bab^{-1}$  é chamado *conjugado de  $a$  por  $b$* . Dois elementos  $a, a' \in G$  são ditos *conjugados* se existe  $b \in G$  tal que  $a' = bab^{-1}$ .

**Observação 1.5.3.** O conjugado tem uma interpretação muito útil: Se escrevermos  $bab^{-1}$  como  $a'$ , então

$$ba = a'b.$$

Ou seja, pode-se pensar na conjugação como a mudança em  $a$  que resulta de mover  $b$  de um lado para o outro na equação.

**Proposição 1.5.2.** *Seja  $\varphi : G \rightarrow G'$  um homomorfismo. Se  $a \in \text{nu } \varphi$  e  $b$  é qualquer elemento do grupo  $G$ , então o conjugado  $bab^{-1} \in \text{nu } \varphi$ .*

**Definição 1.5.5** (Subgrupo normal). Um subgrupo  $N$  de um grupo  $G$  é chamado *subgrupo normal* (escreve-se  $N \trianglelefteq G$ ) se para cada  $a \in N$  e  $b \in G$ , o conjugado  $bab^{-1} \in N$ .

**Observação 1.5.4.** Fica claro que o núcleo de um homomorfismo é um subgrupo normal. Além disso, todo subgrupo de um grupo abeliano também é um subgrupo normal, porém, isso não é necessariamente verdade em subgrupos de grupos não abelianos (veja Observação 1.5.2).

**Proposição 1.5.3.** *O centro de todo grupo é um subgrupo normal do grupo.*

## 1.6 Grupos de Permutação

**Definição 1.6.1** (Permutação de um conjunto). Uma permutação de um conjunto  $A$  é uma função bijetiva  $\varphi : A \rightarrow A$  do conjunto para ele mesmo.

**Proposição 1.6.1** (Multiplicação de permutações). *Seja  $A$  um conjunto onde duas permutações  $\tau, \sigma$  são dadas. A composição de funções  $\tau \circ \sigma$  (chamada multiplicação de permutações) é uma lei de composição sobre  $A$ .*

**Proposição 1.6.2.** *Sejam  $A$  um conjunto não vazio,  $S_A$  o conjunto de todas as permutações de  $A$  e  $\circ$  uma multiplicação de permutações sobre  $A$ . Então,  $(S_A, \circ)$  é um grupo.*

**Definição 1.6.2** (Grupo simétrico sobre  $n$  símbolos). Seja  $A$  o conjunto finito  $\{1, 2, \dots, n\}$ . O grupo de todas as permutações de  $A$  é um *grupo simétrico sobre os  $n$  símbolos*  $1, 2, \dots, n$  e é representado por  $S_n$ .

**Observação 1.6.1.** É importante perceber que  $S_n$  possui  $n!$  elementos, isso é, a quantidade de toda combinação de  $n$  elementos.

**Exemplo 1.6.1** (Grupos diedrais). O grupo  $S_3$  de  $3! = 6$  elementos forma um grupo de simetrias de um triângulo equilátero com vértices 1, 2 e 3. As 6 permutações que formam esse grupo são as 3 rotações e os 3 espelhamentos possíveis sobre os vértices do triângulo. Também chamamos  $S_3$  de  $D_3$ , pois  $D_3$  forma o terceiro *grupo diedral*. O  $n$ -ésimo grupo diedral  $D_n$  é o grupo de simetrias de um polígono regular de  $n$  vértices.

**Definição 1.6.3** (Restrição da imagem de uma função). Sejam  $f : A \rightarrow B$  uma função e  $H$  um subconjunto de  $A$ . A *imagem de  $H$  por  $f$*  é  $\{f(h) \mid h \in H\}$  e é representada por  $f|_H$ .

**Lema 1.6.1.** *Sejam  $G$  e  $G'$  grupos e  $\varphi : G \rightarrow G'$  um homomorfismo injetivo. Então,  $\varphi|_G$  é um subgrupo de  $G'$  e  $\varphi$  provê um isomorfismo de  $G$  com  $\varphi|_G$ .*

**Teorema 1.6.1** (Teorema de Cayley). *Todo grupo é isomorfo a um grupo de permutações.*

## 1.7 Relações de Equivalência e Partições

**Definição 1.7.1** (Partições). Seja  $S$  um conjunto. Uma *partição*  $P$  de  $S$  é uma subdivisão de  $S$  em subconjuntos não vazios e não sobrepostos, isto é, uma união de conjuntos disjuntos.

**Exemplo 1.7.1.** Pode-se particionar o conjunto dos números inteiros  $\mathbb{Z}$  na união de disjuntos  $P \cup I$ , onde  $P = \{z \in \mathbb{Z} \mid z \text{ é par}\}$  e  $I = \{z \in \mathbb{Z} \mid z \text{ é ímpar}\}$ .

**Definição 1.7.2** (Relações de equivalência). Uma *relação de equivalência* sobre um conjunto  $S$  é uma relação que se mantém sobre um subconjunto de elementos de  $S$ . Escreve-se  $a \sim b$  para representar a equivalência de  $a, b \in S$ , que precisa respeitar os seguintes axiomas:

1. (*Transitiva*). Se  $a \sim b$  e  $b \sim c$ , então  $a \sim c$ ;
2. (*Simétrica*). Se  $a \sim b$ , então  $b \sim a$ ;
3. (*Reflexiva*).  $a \sim a$ .

**Observação 1.7.1.** A noção de partição em  $S$  e a relação de equivalência em  $S$  são logicamente equivalentes: Dada uma partição  $P$  sobre  $S$ , pode-se definir uma relação de equivalência  $R$  tal que, se  $a$  e  $b$  estão no mesmo subconjunto partição, então  $a \sim b$  e, dada uma relação de equivalência  $R$ , podemos definir uma partição



$P$  tal que o subconjunto que contém  $a$  é o conjunto de todos os elementos  $b$  onde  $a \sim b$ . Esse subconjunto é chamado de *classe de equivalência de  $a$*

$$C_a = \{b \in S \mid a \sim b\}$$

e  $S$  é particionado em classes de equivalência.

**Proposição 1.7.1.** *Sejam  $C_a$  e  $C_b$  duas classes de equivalência do conjunto  $S$ . Se existe  $d$  tal que  $d \in C_a$  e  $d \in C_b$ , então  $C_a = C_b$ .*

**Observação 1.7.2.** Seja um conjunto  $S$ . Suponha que exista uma relação de equivalência ou uma partição sobre  $S$ . Então, pode-se construir um novo conjunto  $\bar{S}$  formado pelas classes de equivalência ou os subconjuntos partições de  $S$ . Essa construção induz uma notação muito útil: para  $a \in S$ , a classe de equivalência de  $a$  ou o subconjunto partição que contém  $a$  serão denotados como o elemento  $\bar{a} \in \bar{S}$ . Desta forma, a notação  $\bar{a} = \bar{b}$  significa que  $a \sim b$  e chamamos  $a, b \in S$  de *representantes* das respectivas classes de equivalência  $\bar{a}, \bar{b} \in \bar{S}$ .

**Definição 1.7.3.** Seja um mapeamento  $\varphi : S \rightarrow T$ . Chama-se de *relação de equivalência determinada por  $\varphi$*  a relação dada por  $\varphi(a) = \varphi(b) \Rightarrow a \sim b$ . Além disso, para um elemento  $t \in T$ , o subconjunto de  $\varphi^{-1}(t) = \{s \in S \mid \varphi(s) = t\}$  é dito *imagem inversa de  $t$  por  $\varphi$* .

**Proposição 1.7.2.** *Seja um mapeamento  $\varphi : S \rightarrow T$  e  $t \in T$  um elemento qualquer de  $T$ . Se a imagem inversa  $\varphi^{-1}(t)$  é não vazia, então  $t \in \text{im } \varphi$  e  $\varphi^{-1}(t)$  forma uma classe de equivalência  $\bar{\varphi} \in \bar{S}$  através da relação determinada por  $\varphi$ .*

**Definição 1.7.4** (Congruência). Seja  $\varphi : G \rightarrow G'$  um homomorfismo. A relação de equivalência definida por  $\varphi$  é usualmente denotada por  $\equiv$  ao invés de  $\sim$  e a chamamos de *congruência*:

$$\varphi(a) = \varphi(b) \Rightarrow a \equiv b, \text{ para } a, b \in G.$$

**Proposição 1.7.3.** *Seja  $\varphi : G \rightarrow G'$  um homomorfismo e  $a, b \in G$ . Então as seguintes afirmações são equivalentes:*

- $\varphi(a) = \varphi(b)$
- $b = an$ , para algum  $n \in \text{nu } \varphi$
- $a^{-1}b \in \text{nu } \varphi$ .

**Definição 1.7.5** (classe lateral em relação ao núcleo). Seja  $\varphi : G \rightarrow G'$  um homomorfismo,  $a \in G$  e  $n \in \text{nu } \varphi$ . O conjunto

$$a \text{ nu } \varphi = \{g \in G \mid g = an, \text{ para algum } n \in \text{nu } \varphi\}$$

é dito *classe lateral de  $\text{nu } \varphi$  em  $G$* .

**Observação 1.7.3.** Pode-se particionar o grupo  $G$  em *classes de congruência*, formadas pelas classe laterais  $a \text{ nu } \varphi$ . Estas são imagens inversas do mapeamento  $\varphi$ .

**Proposição 1.7.4.** *O homomorfismo de grupo  $\varphi : G \rightarrow G'$  é injetivo se, e somente se, seu núcleo é o subgrupo trivial  $\{1\}$ .*

**Observação 1.7.4.** Esse resultado da uma forma de verificar se um homomorfismo  $\varphi$  é também um isomorfismo: Se  $\text{nu } \varphi = \{1\}$  e  $\text{im } \varphi = G'$ , então  $\varphi$  é, pelos respectivos motivos, injetiva e sobrejetiva. Então é um isomorfismo.

## 1.8 Órbitas, ciclos e grupos alternados

**Definição 1.8.1** (Órbita). Seja  $\sigma$  uma permutação de um conjunto  $A$ . Chamamos de *órbitas de  $\sigma$*  a classe de equivalência em  $A$  determinada pela relação de equivalência  $\sim$ :

$$\text{para } a, b \in A, \quad a \sim b \iff b = \sigma^n(a), \text{ para algum } n \in \mathbb{Z}.$$

**Observação 1.8.1.** A relação apresentada na Definição 1.8.1 é, de fato, uma relação de equivalência. Como segue:

- é reflexiva, já que  $a = \sigma^0(a) \implies a \sim a$ ;
- é simétrica pois, se  $a \sim b \implies \exists n \in \mathbb{Z}$  tal que  $b = \sigma^n(a)$ , então  $a = \sigma^{-n}(b)$ . Como  $-n \in \mathbb{Z}$ , então  $b \sim a$ ;
- é transitiva, visto que  $a \sim b \implies b = \sigma^n(a)$  e  $b \sim c \implies c = \sigma^m(b)$ , para algum  $n, m \in \mathbb{Z}$ , então  $c = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(a) \implies a \sim c$ .

**Exemplo 1.8.1** (Órbita trivial). Já que a permutação identidade  $i$  de  $A$  leva cada elemento de  $A$  para a mesma posição, as órbitas de  $i$  são os subconjuntos de apenas um elemento de  $A$ .

**Definição 1.8.2** (Ciclo). Uma permutação  $\sigma \in S_n$  é um *ciclo* se possuir no máximo uma órbita contendo mais que um elemento. O *comprimento* de um ciclo é o número de elementos de sua maior órbita.

**Exemplo 1.8.2.** Seja a permutação

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

Como a órbita  $(1, 3, 6)$  é a única que contém mais de um elemento, essa permutação sobre o conjunto  $\{1, 2, 3, 4, 5, 6, 7, 8\}$  é um ciclo de comprimento 3.

**Observação 1.8.2** (Notação de ciclos). Podemos representar um ciclo com a notação de uma única linha, da forma

$$\mu = (1, 3, 6),$$

indicando apenas os elementos da maior órbita do ciclo. Perceba que as demais órbitas não precisam ser representadas pois serão os índices fixos da permutação.

**Exemplo 1.8.3** (Produto de ciclos). Pode-se construir uma permutação como um multiplicação de ciclos (veja a definição 1.6.1). Por exemplo,

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

**Proposição 1.8.1.** Toda permutação  $\sigma$  de um conjunto finito é um produto de ciclos disjuntos.

**Definição 1.8.3** (Transposição). Um ciclo de comprimento 2 é uma transposição.

**Corolário 1.8.1.** *Qualquer permutação de um conjunto finito de pelo menos dois elementos é um produto de transposições.*

**Definição 1.8.4** (Permutações pares e ímpares). Uma permutação de um conjunto finito é *par* ou *ímpar* se pode ser expressa, respectivamente, por um número par ou ímpar de produtos de permutações.

**Proposição 1.8.2.** *Uma permutação em  $S_n$  pode ser expressa como um produto de um número ímpar de transposições se e somente se não puder ser expressa como um número par de transposições e vice-versa.*

**Proposição 1.8.3.** *Seja o grupo simétrico  $S_n$  com  $n \geq 2$ . Então, a coleção de todas as permutações ímpares de  $\{1, 2, \dots, n\}$  forma um subgrupo de  $S_n$  de ordem  $\frac{n!}{2}$ .*

**Definição 1.8.5** (Grupo alternado). O subgrupo de  $S_n$  formado pelas permutações ímpares de  $n$  símbolos é chamado *grupo alternado*  $A_n$ .

**Observação 1.8.3.** Os grupos  $S_n$  e  $A_n$  são muito importantes. O teorema de Cayley mostra que todo grupo finito  $G$  é estruturalmente idêntico a algum subgrupo de  $S_n$ , para  $n = |G|$ . Pode-se mostrar que não há formulas envolvendo apenas radicais para solucionar uma equação polinomial de grau  $n \geq 5$ . Por mais que isso não seja óbvio, esse fato se deve, na verdade, a estrutura de  $A_n$ .

## 1.9 Classe lateral

Definimos classe lateral somente em relação ao núcleo de um homomorfismo mas, na verdade, pode-se definir uma classe lateral para qualquer subgrupo  $H$  de um grupo  $G$ .

**Definição 1.9.1** (classe lateral a esquerda). Seja um subgrupo  $H$  de um grupo  $G$ . O subconjunto da forma

$$aH = \{ah \mid h \in H\}$$

é dito *classe lateral a esquerda de  $H$  em  $G$* .

**Proposição 1.9.1.** *A classe lateral é uma classe de equivalência para a relação de congruência*

$$b = ah \Rightarrow a \equiv b, \text{ para algum } h \in H.$$

**Observação 1.9.1.** Daí segue que, como classes de equivalência particionam um grupo, classe laterais a esquerda de um subgrupo particionam o grupo.

**Definição 1.9.2** (Índice de um subgrupo). O número de classe laterais a esquerda de um subgrupo  $H$  em um grupo  $G$  chama-se *índice de  $H$  em  $G$*  e é denotado como  $[G : H]$ .

**Observação 1.9.2.** Como há uma bijeção do subgrupo  $H$  para a classe lateral  $aH$ , a cardinalidade de  $aH$  tem de ser a mesma de  $H$ . Isto é, as classe laterais de  $H$  particionam  $G$  em partes de mesma ordem.

**Proposição 1.9.2.** *Seja  $aH$  a classe lateral do subgrupo  $H$  no grupo  $G$ . Então, a ordem  $|G|$  do grupo  $G$  é dada por*

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

**Proposição 1.9.3** (Teorema de Lagrange). *Seja  $G$  um grupo finito e  $H$  um subgrupo de  $G$ . A ordem de  $H$  divide a ordem de  $G$ .*

**Definição 1.9.3** (Ordem de um elemento). *Seja  $G$  um grupo. A ordem de um elemento  $a \in G$  é a ordem do grupo cíclico gerado por  $a$ .*

**Proposição 1.9.4.** *Seja um grupo  $G$  com  $p$  elementos tal que  $p$  é primo e  $a \in G$  diferente da identidade. Então  $G$  é o grupo cíclico  $\{1, a, \dots, a^{p-1}\}$  gerado por  $a$ .*

**Observação 1.9.3.** Também podemos obter uma expressão para calcular a ordem de um grupo de homomorfismo. Seja  $\varphi : G \rightarrow G'$  um homomorfismo. Como as classes laterais à esquerda do núcleo de  $\varphi$  são as imagens inversas  $\varphi^{-1}$ , elas estão em uma correspondência biunívoca com a imagem. Daí segue que

$$[G : \text{nu } \varphi] = |\text{im } \varphi|.$$

**Proposição 1.9.5.** *Seja  $\varphi : G \rightarrow G'$  um homomorfismo onde  $G$  e  $G'$  são finitos. Então*

$$|G| = |\text{nu } \varphi| \cdot |\text{im } \varphi|.$$

**Definição 1.9.4** (classe laterais à direita). Os conjuntos da forma

$$Ha = \{ha \mid h \in H\}$$

chamam-se *classe laterais à direita de um subgrupo  $H$* . Esses são classes de equivalência para a relação de congruência à direita

$$b = ha \Rightarrow a \equiv b, \text{ para algum } h \in H.$$

**Proposição 1.9.6.** *Seja um subgrupo  $H$  de um grupo  $G$ . As seguintes afirmações são equivalentes:*

- $H$  é subgrupo normal,
- $aH = Ha$  para todo  $a \in G$ .

## 1.10 Restrição de um homomorfismo para um subgrupo

**Observação 1.10.1.** O objetivo dessa seção é apresentar ferramentas para analisar um subgrupo  $H$  do grupo  $G$  a fim de garantir propriedades do grupo  $G$ . No geral, os subgrupos são mais específicos e menos complexos de se trabalhar.

**Proposição 1.10.1.** *Sejam  $K$  e  $H$  dois subgrupos do grupo  $G$  tal que a interseção  $K \cap H$  é um subgrupo de  $H$ . Se  $K$  é um subgrupo normal de  $G$ , então  $K \cap H$  é um subgrupo normal de  $H$ .*

**Exemplo 1.10.1.** Com esse resultado, se  $G$  é finito pode-se utilizar o Teorema de Lagrange para obter informações sobre a interseção dos dois subgrupos: a interseção divide  $|H|$  e  $|K|$ . Se  $|H|$  e  $|K|$  não tem o mesmo fator de divisão, então  $K \cap H = \{1\}$ .

**Definição 1.10.1** (Restrição de um homomorfismo para um subgrupo). Sejam o homomorfismo  $\varphi : G \rightarrow G'$  e  $H$  um subgrupo de  $G$ . Uma *restrição de  $\varphi$  para o subgrupo  $H$*  é o homomorfismo  $\varphi|_H : H \rightarrow G'$  definido como

$$\varphi|_H(h) = \varphi(h), \text{ para todo } h \in H.$$

**Proposição 1.10.2.** Sejam o homomorfismo  $\varphi : G \rightarrow G'$  e  $H$  um subgrupo de  $G$ . O núcleo de uma restrição  $\varphi|_H$  é a interseção do núcleo de  $\varphi$  e  $H$ .

**Proposição 1.10.3.** Sejam  $\varphi : G \rightarrow G'$  um homomorfismo,  $H'$  um subgrupo de  $G'$  e  $\varphi^{-1}(H') = \{x \in G \mid \varphi(x) \in H'\}$  a imagem inversa de  $H'$ . Então

- $\varphi^{-1}(H')$  é um subgrupo de  $G$ .
- Se  $H'$  é um subgrupo normal de  $G'$ , então  $\varphi^{-1}(H')$  é um subgrupo normal de  $G$ .
- $\varphi^{-1}(H')$  contém o núcleo de  $\varphi$
- A restrição de  $\varphi$  para  $\varphi^{-1}(H')$  define um homomorfismo  $\varphi^{-1}(H') \rightarrow H'$ , de forma que o núcleo desse homomorfismo é o núcleo de  $\varphi$ .

## 1.11 Produto de Grupos

**Definição 1.11.1** (Produto de grupos). Seja  $G, G'$  dois grupos. O *produto*  $G \times G'$  é um grupo formado pelo produto das componentes dos grupos  $G$  e  $G'$ , isso é, pela regra

$$(a, a'), (b, b') \rightsquigarrow (ab, a'b'),$$

onde  $a, b \in G$  e  $a', b' \in G'$ . O par  $(1, 1)$  é uma identidade e  $(a, a')^{-1} = (a^{-1}, a'^{-1})$ . A propriedade associativa é preservada em  $G \times G'$  pois também é em  $G$  e  $G'$ .

**Proposição 1.11.1.** A ordem de  $G \times G'$  é o produto das ordens de  $G$  e  $G'$ .

**Observação 1.11.1** (Projeções). O produto de grupos é composto pelos homomorfismos:

$$i : G \rightarrow G \times G', \quad i' : G' \rightarrow G \times G', \quad p : G \times G' \rightarrow G, \quad p' : G \times G' \rightarrow G',$$

definidos como

$$i(x) = (x, 1), \quad i'(x') = (1, x'), \quad p(x, x') = x, \quad p'(x, x') = x'.$$

Os mapeamentos  $i, i'$  são injetivos, já os mapeamentos  $p, p'$  são sobrejetivos, onde nu  $p = 1 \times G'$  e nu  $p' = G \times 1$ . Esses mapeamentos são chamados de *projeções*. Desde que são núcleos,  $G \times 1$  e  $1 \times G'$  são subgrupos normais de  $G \times G'$ .

**Proposição 1.11.2** (Propriedades de Mapeamento dos Produtos). *Seja  $H$  um grupo qualquer. O homomorfismo  $\Phi : H \longrightarrow G \times G'$  tem correspondência biunívoca com o par  $(\varphi, \varphi')$  de homomorfismos*

$$\varphi : H \longrightarrow G, \quad \varphi' : H \longrightarrow G'.$$

*O núcleo de  $\Phi$  é a interseção  $(\text{nu } \phi) \cap (\text{nu } \phi')$ .*

**Observação 1.11.2.** É extremamente desejável encontrar uma relação isomorfa entre um grupo  $G$  e um produto de outros dois grupos  $H \times H'$ . Quando isso acontece, e infelizmente não são muitas as vezes, trabalhar com os grupos  $H$  e  $H'$  costumam ser mais simples que  $G$ .

**Proposição 1.11.3.** *Sejam  $r, s \in \mathbb{Z}$  não divisíveis entre si. Um grupo cíclico de ordem  $rs$  é isomorfo ao produto dos grupos cíclicos de ordem  $r$  e  $s$ .*

**Observação 1.11.3.** Em contrapartida, um grupo cíclico de ordem par 4, por exemplo, não é isomorfo ao produto de dois grupos cíclicos de ordem 2. Também não podemos afirmar nada com base no resultado anterior sobre grupos não cíclicos.

**Definição 1.11.2** (Conjunto de produtos). Sejam dois subgrupos  $A, B$  de um grupo  $G$ . Chamamos o *conjunto de produtos de elementos de  $A$  e  $B$*  por

$$AB = \{x \in G \mid x = ab \text{ para algum } a \in A \text{ e } b \in B\}.$$

**Proposição 1.11.4.** *Sejam  $H$  e  $K$  os subgrupos de um grupo  $G$ .*

- *Se  $H \cap K = \{1\}$ , o mapeamento de produto  $p : H \times K \longrightarrow G$  definido por  $p(h, k) = hk$  é injetivo e sua imagem é o subconjunto  $HK$ ;*
- *Se um dos subgrupos  $H$  ou  $K$  é um subgrupo normal de  $G$ , então os conjuntos de produtos  $HK$  e  $KH$  são iguais e  $HK$  é subgrupo de  $G$ ;*
- *Se ambos  $H$  e  $K$  são subgrupos normais,  $H \cap K = \{1\}$  e  $HK = G$ , então  $G$  é isomorfo ao grupo de produto  $H \times K$ .*

## 1.12 Aritmética Modular

**Definição 1.12.1** (Congruente modulo  $n$ ). Seja  $n \in \mathbb{N}$ . Dizemos que dois inteiros  $a, b$  são *congruentes modulo  $n$* , e escrevemos

$$a \equiv b \pmod{n},$$

se  $n$  divide  $b - a$ , ou se  $b = a + nk$  para algum inteiro  $k$ . Chamamos as classes de equivalência definidas por essa relação de *classes de equivalência módulo  $n$* , ou *classes de resíduo módulo  $n$* .

**Exemplo 1.12.1.** A classe de congruência de 0 é o subgrupo  $\bar{0}$  de todos os múltiplos de  $n$

$$\bar{0} = n\mathbb{Z} = \{\dots, -n, 0, n, 2n, \dots\}.$$

**Proposição 1.12.1.** Há  $n$  classes de congruência módulo  $n$  (denotamos esse conjunto por  $\mathbb{Z}/n\mathbb{Z}$ ), isto é, o índice  $[\mathbb{Z} : n\mathbb{Z}]$  é  $n$ . São elas

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

**Definição 1.12.2** (Soma e produto). Seja  $\bar{a}$  e  $\bar{b}$  as classes de congruência representadas pelos inteiros  $a$  e  $b$ . Define-se a *soma* como a classe de congruência de  $a + b$  e o *produto* pela classe de congruência  $ab$ , isto é,

$$\bar{a} + \bar{b} = \overline{a + b} \quad \text{e} \quad \bar{a}\bar{b} = \overline{ab}.$$

**Proposição 1.12.2.** Se  $a' \equiv b' \pmod{n}$  e  $b' \equiv b \pmod{n}$ , então  $a' + b' \equiv a + b \pmod{n}$  e  $a'b' \equiv ab \pmod{n}$ .

**Observação 1.12.1.** Além disso, a soma e produto também continuam respeitando as propriedades associativas, comutativas e distributivas, desde que o mesmo se mantém para soma e multiplicação de inteiros.

**Exemplo 1.12.2.** Seja  $n = 13$ , então

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{12}\}.$$

Com isso,

$$(\bar{7} + \bar{9})(\bar{11} + \bar{6}) = \bar{3} \cdot \bar{4} = \bar{12}.$$

## 1.13 Estrutura de grupos abelianos finitamente gerados

**Teorema 1.13.1** (Teorema fundamental dos grupos abelianos finitamente gerados). Todo grupo abeliano finitamente gerado  $G$  é isomorfo a um produto de grupos cíclicos na forma

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

onde os  $p_i$  são primos, não necessariamente distintos, e os  $r_i$  são inteiros positivos. O produto é único, exceto por possíveis rearranjos dos fatores; isso é, o número (chamado número Betti de  $G$ ) de fatores  $\mathbb{Z}$  é único e as potências de primos  $(p_i)^{r_i}$  são únicas.

**Exemplo 1.13.1.** Queremos encontrar todos os grupos abelianos de ordem 360, a menos de isomorfismos. Dizer a menos de isomorfismo significa que qualquer grupo abeliano de ordem 360 deve ser estruturalmente idêntico — isto é, isomorfo — a um

*Solução.* Já que nossos grupos são da ordem finita 360, não aparecerão  $\mathbb{Z}$  no produto. Primeiro, vamos expressar 360 como um produto de potências de primos:  $360 = 2^3 3^2 5$ . Então, pelo Teorema 1.13.1, temos as seguintes possibilidades

1.  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
2.  $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
3.  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

$$4. \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$

$$5. \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

$$6. \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$

Então, esses são os seis diferentes grupos abelianos (a menos de isomorfismos) de ordem 360.  $\triangle$

**Definição 1.13.1** (Grupo redutível e irredutível). Um grupo é dito *redutível* se ele é isomorfo a um produto direto de dois subgrupos não triviais. Do contrário, é dito *irredutível*.

**Proposição 1.13.1.** *Os grupos abelianos finitos irredutíveis são exatamente os grupos cíclicos que possuem a ordem de uma potência prima.*

**Proposição 1.13.2.** *Se  $m$  divide a ordem de um grupo abeliano finito  $G$ , então  $G$  tem um subgrupo de ordem  $m$ .*

**Proposição 1.13.3.** *Se  $m$  é um quadrado inteiro livre, isto é,  $m$  não é divisível por nenhum quadrado de primo, então todo grupo abeliano de ordem  $m$  é cíclico.*

## 1.14 Grupos de Quociente

**Proposição 1.14.1.** *Seja  $N$  um subgrupo normal de um grupo  $G$ . Então, o produto de duas classe laterais  $aN, bN$  também é uma classe lateral*

$$(aN)(bN) = abN.$$

**Definição 1.14.1** (Produto de coclases). Sejam as classe laterais  $C_1, C_2$  e os elementos  $a \in C_1$  e  $b \in C_2$ , então  $C_1 = aN$  e  $C_2 = bN$ . Chamamos de *produto das classe laterais*  $C_1$  e  $C_2$  a classe lateral  $C_1C_2 = abN$ , isto é, a classe lateral que contém  $ab$ .

**Observação 1.14.1** (Notação para conjunto de classe laterais). É conveniente denotar o *conjunto de classe laterais de um subconjunto normal  $N$  de um grupo  $G$*  pela simbologia

$$G/N = \text{conjunto de classe laterais de } N \text{ em } G.$$

Também pode-se usar a notação em barra  $G/N = \bar{G}$  e  $aN = \bar{a}$ , tomando o cuidado para diferenciar que  $\bar{a}$  denota a classe lateral que contém  $a$ .

**Proposição 1.14.2.** *Seja o mapeamento  $\pi : G \longrightarrow \bar{G} = G/N$ , da forma  $a \rightsquigarrow \bar{a} = aN$ , isto é,  $\bar{G}$  é um grupo e o mapeamento  $\pi$  é um homomorfismo com núcleo  $N$ . Então a ordem de  $G/N$  é o índice  $[G : N]$ .*

**Proposição 1.14.3.** *Todo subgrupo normal de um grupo  $G$  é o núcleo de um homomorfismo.*

**Proposição 1.14.4.** *Sejam  $G$  um grupo e  $S$  um conjunto qualquer com uma lei de composição. Seja também  $\varphi : G \longrightarrow S$  um mapeamento sobrejetivo tal que  $\varphi(a)\varphi(b) = \varphi(ab)$  para todo  $a, b \in G$ . Então  $S$  é um grupo.*

**Proposição (Primeiro teorema do isomorfismo):** Sejam  $\varphi : G \longrightarrow G'$  um homomorfismo de grupo sobrejetivo e  $N$  o núcleo de  $\varphi$ . Então  $G/N$  é isomórfico a  $G'$  pelo mapeamento  $\bar{\varphi}$  que transporta a classe lateral  $\bar{a} = aN$  para  $\varphi(a)$ :

$$\bar{\varphi}(\bar{a}) = \varphi(a).$$

Esse é o método fundamental para identificar grupos de quocientes.



## Referências Bibliográficas