# Teoria de Grupos: notas de estudo

Guilherme Philippi

22 de janeiro de 2021

# Sumário

**1 Grupos** **2**
1.1 Lei de composição . . . . . 2
1.2 Grupos . . . . . 3
1.3 Subgrupos . . . . . 3
1.4 Homomorfismos . . . . . 4
1.5 Isomorfismos . . . . . 5

**Referências Bibliográficas** **6**

# Capítulo 1

# Grupos

## 1.1 Lei de composição

**Definição 1.1.1** (Lei de Composição)**.** Uma *Lei de Composição* sobre $S$ é uma função $F : S \times S \longrightarrow S$.

**Definição 1.1.2.** Para $a, b, c \in S$, uma Lei de Composição $F$ é dita

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

**Observação 1.1.1.** Usaremos a notação $F(a,b) = ab$, para simplificar a escrita de propriedades.

**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 $a_1, \ldots, a_n \in S$ (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 $\vec{1}$ para representar a identidade multiplicativa e $\vec{0}$ 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 as seguintes propriedades são satisfeitas:

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 simbolo, omitindo a lei de composição quando não houver necessidade.

**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 $\{\vec{1}\}$, formado pela identidade de $G$. Diz-se que um subgrupo é um *subgrupo apropriado* se for diferente desses dois.

**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 $x$: $H = \{\dots, x^{-2}, x^{-1}, \vec{1}, x, x^2, \dots\}$.

**Definição 1.3.3.** 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 espressos 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

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

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

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

## 1.4 Homomorfismos

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

$$\varphi(ab) = \varphi(a)\varphi(b), \ \forall \ a, b \ \in G.$$

Quando isso acontece, dizemos que o mapeamento $\varphi$ *preserva a estrutura algébrica de grupo.*

**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 $\varphi(a^{-1}) = \varphi(a)^{-1}$.*

**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

Se dois grupos $G$ e $G'$ estão relacionados por uma *correspondência biunívoca entre seus elementos compatível com suas respectivas leis de composição*, isto é, uma bijeção

$$G \longleftrightarrow G'$$

onde, se $a, b \in G$ corresponde respectivamente ao $a', b' \in G'$ então o produto $ab \in G$ corresponde ao produto $a'b' \in G'$, então dizemos que a correspondência *preserva as propriedades da estrutura algébrica de grupo*. Isso é, temos um homomorfismo bijetivo. Para essa bijeção dá-se o nome de *relação de isomorfismo*.

**Definição 1.5.1** (Isomorfismo de grupos)**.** Dois grupos $G$ e $G'$ são ditos *isomórfos* se possuírem um homomorfismo bijetivo entre si, isto é, há um mapeamento *bijetivo* $\varphi : G \longrightarrow G'$ que preserva a estrutura algébrica de grupo:

$$\varphi(ab) = \varphi(a)\varphi(b) \Rightarrow (ab)' = a'b', \text{ para todo } a, b \in G \text{ e } a', b' \in G'.$$

**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 multiplicação no grupo:

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

- 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 multiplicação no grupo.

**Observação 1.5.2.** Se o grupo é abeliano, a conjugação é o mapa identidade: $bab^{-1} = abb^{-1} = a$. Porém, qualquer grupo não comutativo tem alguma conjugação não trivial, logo possui também um automorfismo não trivial.

**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.** *Se $a \in \operatorname{nu}\varphi$ e $b$ é qualquer elemento do grupo $G$, então o conjugado $bab^{-1} \in \operatorname{nu}\varphi$.*

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

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 (se $G$ é abeliano, então $bab^{-1} = a$). Mas isso não é necessáriamente verdade em subgrupos de grupos não abelianos.

**Definição 1.5.6** (Centro de um grupo)**.** O *centro* $Z(G)$ de um grupo $G$ é o conjunto de elementos que comutam com todo elemento de $G$:

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

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

# Referências Bibliográficas