Grupos

lcc :: 2.º ano
paula mendes martins

departamento de matemática :: uminho

conceitos e resultados básicos

Definição. Seja G um conjunto no qual está definida uma operação binária. Então, G diz-se um *grupo* se G é um semigrupo com identidade e no qual todos os elementos admitem um único elemento oposto, i.e., G é grupo se:

G1. A operação binária é associativa em G;

G2. $(\exists e \in G)\,(\forall a \in G) \qquad ae = ea = a;$

G3. $(\forall a \in G)\,\left(\exists^! a^{-1} \in G\right) \qquad aa^{-1} = a^{-1}a = e.$

Se a operação for comutativa, o grupo diz-se *comutativo* ou *abeliano.*

Representamos a identidade do grupo G por 1_G.

Exemplo 1. $(\mathbb{R}, +)$ é grupo abeliano ($+$ é a adição usual de números reais). $(\mathbb{R}, \cdot)$ não é grupo ($\cdot$ é a multiplicação usual de números reais), mas $(\mathbb{R} \setminus \{0\}, \cdot)$ é grupo abeliano.

Exemplo 2. $(\mathbb{Z}, \cdot)$ não é grupo ($\cdot$ é a multiplicação usual de números inteiros), mas $(\mathbb{Z}, +)$ é grupo abeliano ($+$ é a adição usual de números inteiros).

Exemplo 3. Seja $n \in \mathbb{N}$. Sendo $\oplus$ e $\otimes$ as operações de adição e multiplicação usuais de classes de $\mathbb{Z}_n$, temos que $(\mathbb{Z}_n, \oplus)$ é grupo e $(\mathbb{Z}_n, \otimes)$ não é grupo. Sendo $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{[0]_n\}$, temos que $(\mathbb{Z}_n^*, \otimes)$ é grupo se e só se n é primo.

Exemplo 4. Um conjunto singular, $\{x\}$, quando algebrizado com a única operação binária possível, $x * x = x$, é um grupo abeliano (chamado de *grupo trivial*).

Exemplo 5. O conjunto $G = \{x, e\}$, quando algebrizado com a operação definida pela tabela

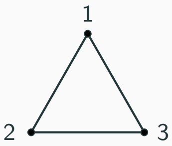
$$\begin{array}{c|cc} \cdot & e & x \\ \hline e & e & x \\ x & x & e \end{array},$$

é um grupo abeliano.

Exemplo 6. Seja $n \in \mathbb{N}$. O conjunto das matrizes reais quadradas de ordem n, quando algebrizado com a multiplicação usual de matrizes, não é um grupo. No entanto, o conjunto das matrizes reais quadradas de ordem n invertíveis é um grupo não abeliano quando considerada a mesma multiplicação. A este grupo chama-se *grupo linear geral de ordem n* e representa-se por $GL_n(\mathbb{R})$ ou $GL(n, \mathbb{R})$.

Exemplo 7. Seja X um conjunto não vazio. O conjunto $\mathcal{F}(X)$ das funções de X em X é um semigrupo não abeliano quando algebrizado com a composição usual de funções. Já o conjunto $\mathcal{S}_X = \{f \in \mathcal{F}(X) : f \text{ é bijetiva}\}$ é um grupo quando algebrizado com a mesma operação. Prova-se este grupo é não abeliano se o conjunto X tiver pelo menos três elementos distintos. Este tipo de grupos, aos quais chamamos *grupos simétricos*, têm grande importância na Teoria de Grupos e serão estudados com algum detalhe no final deste capítulo.

Exemplo 8. Seja D_3 o conjunto das isometrias num triângulo equilátero.

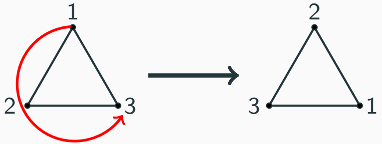


O conjunto D_3 tem exatamente seis elementos, três rotações e três simetrias axiais.

As rotações, de ângulos com 0^o, 120^o e 240^o de amplitude, são, respetivamente:

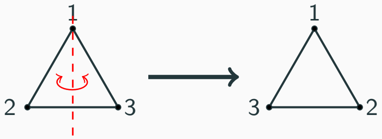
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

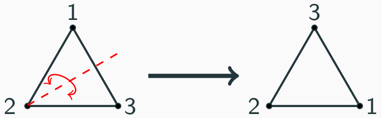


$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

As simetrias, em relação às bissetrizes dos ângulos 1, 2 e 3, são, repetivamente:



$$\theta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$



$$\theta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\theta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Considerando a composição usual de funções, obtemos a tabela:

$\circ$	ρ_1	ρ_2	ρ_3	θ_1	θ_2	θ_3
ρ_1	ρ_1	ρ_2	ρ_3	θ_1	θ_2	θ_3
ρ_2	ρ_2	ρ_3	ρ_1	θ_3	θ_1	θ_2
ρ_3	ρ_3	ρ_1	ρ_2	θ_2	θ_3	θ_1
θ_1	θ_1	θ_2	θ_3	ρ_1	ρ_2	ρ_3
θ_2	θ_2	θ_3	θ_1	ρ_3	ρ_1	ρ_2
θ_3	θ_3	θ_1	θ_2	ρ_2	ρ_3	ρ_1

O grupo D_3 é o menor grupo não abeliano que se pode definir, no sentido em que qualquer grupo com um número inferior de elementos é abeliano. A este grupo é costume chamarmos *grupo diedral do triângulo*. Este grupo não é mais do que o grupo simétrico $\mathcal{S}_X$, com $X = \{1, 2, 3\}$, referido no exemplo anterior.

Proposição. Num grupo G são válidas as leis do corte, i.e., para $x, y, a \in G$,

$$ax = ay \Rightarrow x = y \quad e \quad xa = ya \Rightarrow x = y.$$

Observação. Existem semigrupos que não são grupos nos quais se verifica a lei do corte, como, por exemplo, $\mathbb{Z} \setminus \{0\}$ algebrizado com a multiplicação usual de inteiros. Este semigrupo comutativo com identidade satisfaz as leis do corte, mas não é um grupo, pois os únicos elementos que admitem inverso são 1 e -1.

Teorema. Num grupo G, as equações $ax = b$ e $ya = b$, admitem uma única solução, para quaisquer $a, b \in G$.

Reciprocamente, um semigrupo S no qual as equações $ax = b$ e $ya = b$ admitem soluções únicas, para quaisquer $a, b \in S$, é um grupo.

Exemplo 9. Sejam $S = \{a, b, c\}$ e $*$ a operação binária definida pela tabela de Cayley:

$$\begin{array}{c|ccc} * & a & b & c \\ \hline a & a & b & b \\ b & b & a & c \\ c & b & c & a \end{array}.$$

Então, $(S, *)$ não é um grupo, pois b e c são soluções distintas da equação $a * x = b$.

Proposição. Seja S um semigrupo finito que satisfaz as leis do corte. Então S é um grupo.

Demonstração. Seja a um elemento qualquer de S. Então, as aplicações $\rho_a, \lambda_a : S \to S$ definidas por, respetivamente, $\rho_a(x) = xa$ e $\lambda_a(x) = ax$, $x \in S$, são injetivas. De facto, para $x, y \in S$, tendo em conta as leis do corte,

$$\rho_a(x) = \rho_a(y) \Leftrightarrow xa = ya \Rightarrow x = y$$

e

$$\lambda_a(x) = \lambda_a(y) \Leftrightarrow ax = ay \Rightarrow x = y.$$

Logo, sendo S um conjunto finito, temos que as duas aplicações são também sobrejetivas, pelo que as equações $ax = b$ e $ya = b$ têm soluções únicas em S. Assim, pelo teorema anterior, o semigrupo S é um grupo. $\square$

Proposição. Seja G um grupo. Então:

1. $1_G^{-1} = 1_G$;
2. $\left(a^{-1}\right)^{-1} = a, \quad \forall a \in G$;
3. $(ab)^{-1} = b^{-1}a^{-1}, \quad \forall a, b \in G$;
4. $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$, $(\forall n \in \mathbb{N})\,(\forall a_1, a_2, \ldots, a_n \in G)$.

Dado um elemento a de um grupo G e $p \in \mathbb{Z}$, define-se

$$
\begin{aligned}
a^P &= \underbrace{aa\cdots a}_{p \text{ vezes}} && \text{se } p \in \mathbb{Z}^+;\\
a^p &= 1_G && \text{se } p = 0;\\
a^p &= \left(a^{-1}\right)^{-p} = \left(a^{-p}\right)^{-1} && \text{se } p \in \mathbb{Z}^-.
\end{aligned}
$$

Em linguagem aditiva temos

$$
\begin{aligned}
pa &= \underbrace{a + a + \cdots + a}_{p \text{ vezes}} && \text{se } p \in \mathbb{Z}^+;\\
pa &= 1_G && \text{se } p = 0;\\
pa &= (-p)\,(-a) = -\left((-p)\,a\right) && \text{se } p \in \mathbb{Z}^-.
\end{aligned}
$$

Proposição. Sejam G um grupo, $x \in G$ e $m, n \in \mathbb{Z}$. Então,

1. $x^m x^n = x^{m+n}$ (na linguagem aditiva: $mx + nx = (m+n)\,x$);
2. $(x^m)^n = x^{mn}$ (na linguagem aditiva: $n\,(mx) = (nm)\,x$).

Observação. A demonstração é feita considerando sempre que, para cada $n \in \mathbb{Z}$, se pode ter $n \in \mathbb{Z}^-$, $n = 0$ ou $n \in \mathbb{Z}^+$