

1 Noções de grupos

Definição 1. Um **grupo** é um conjunto G munido de uma operação

$$\begin{aligned} * : G \times G &\rightarrow G \\ (x, y) &\mapsto x * y \end{aligned}$$

que satisfaz as seguintes condições:

(G1) A operação é associativa, isto é,

$$x * (y * z) = (x * y) * z, \quad \forall x, y, z \in G.$$

(G2) Existe um elemento neutro, isto é,

$$\exists e \in G \text{ tal que } e * x = x * e = x, \quad \forall x \in G.$$

(G3) Todo elemento possui um elemento simétrico, isto é,

$$\forall x \in G, \exists x' \in G \text{ tal que } x * x' = e = x' * x.$$

Além disso, o grupo é dito **comutativo** (ou **abeliano**) se a seguinte condição é satisfeita:

(G4) A operação é comutativa, isto é,

$$x * y = y * x, \quad \forall x, y \in G.$$

Notação. Exceto quando se fizer necessário, não indicaremos a operação do grupo. Além disso, quando não existir ambiguidade, escreveremo xy no lugar de $x * y$.

O seguinte lema será útil para construirmos nossos primeiros exemplos de grupos.

Lema 1. *Seja G um grupo.*

1. Vale a lei do cancelamento, isto é, se $xa = xb$ ou $ax = bx$, com $a, b, x \in G$, então $a = b$.
2. O elemento neutro e é único.
3. Cada elemento $x \in G$ possui um único simétrico. (Daqui em diante, denotaremos tal elemento por x^{-1} .)
4. $(x^{-1})^{-1} = x$, para todo $x \in G$.
5. $(xy)^{-1} = y^{-1}x^{-1}$ para quaisquer $x, y \in G$.

Demonstração. Provaremos a primeira afirmação, as demais ficaram a cargo do leitor. Sejam a, b, x elementos de G , tais que $xa = xb$. Como G é um grupo, segue de (G3) que existe $x' \in G$, tal que $xx' = x'x = e$, e além disso, operando com x' a esquerda em ambos os lados da equação temos $x'(xa) = x'(xb)$. Mas de (G1) segue que $(x'x)a = (x'x)b$, ou seja, $ea = eb$. Mas de (G2) temos que $a = b$ como queríamos. $\square$

Exemplo 1. 1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ são grupos abelianos, onde “+” e “.” denotam a soma e o produto usual.

2. Seja $X = \{a, b, c\}$. Para que X seja um grupo, precisamos fixar uma operação. Isso pode ser feito através de uma tabela de multiplicação

$\times$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

3. Seja $\text{Mat}(n, \mathbb{R})$ o conjunto das matrizes quadradas de ordem n . Então $(\text{Mat}(n, \mathbb{R}), +)$ onde “+” denota a soma usual de matrizes é um grupo abeliano, no entanto $(\text{Mat}(n, \mathbb{R}), \cdot)$, onde “.” denota o produto usual de matrizes, não é um grupo.
4. Seja $\text{GL}(n, \mathbb{R})$, o subconjunto de $\text{Mat}(n, \mathbb{R})$, consistindo das matrizes invertíveis. $(\text{GL}(n, \mathbb{R}), +)$ onde “+” denota a soma usual de matrizes

não é um grupo, no entanto $(GL(n, \mathbb{R}), \cdot)$, onde “ $\cdot$ ” denota o produto usual de matrizes é um grupo. $(GL(n, \mathbb{R}), \cdot)$ é dito **grupo geral linear**, e frequentemente omitimos a operação.

5. Sejam G_1 e G_2 grupos. Seja $G_1 \times G_2$ o conjunto dos pares ordenados (x_1, x_2) com $x_1 \in G_1$ e $x_2 \in G_2$. Defina a operação

$$\begin{aligned} (G_1 \times G_2) \times (G_1 \times G_2) &\rightarrow G_1 \times G_2 \\ ((x_1, x_2), (x'_1, x'_2)) &\mapsto (x_1 x'_1, x_2 x'_2) \end{aligned}$$

Então $G_1 \times G_2$ é um grupo, chamado **produto direto** de G_1 e G_2 .

A seguir, veremos como podemos dividir os grupos, em pedaços “menores”.

Definição 2. Sejam $(G, *)$ um grupo e $H \subseteq G$. Dizemos que H é um **subgrupo** de G , se $(H, *)$ é um grupo. Neste caso escrevemos $H \leq G$.

Proposição 1. Sejam G um grupo e $\emptyset \neq H \subseteq G$. Então $H \leq G$ se, e somente se, as seguintes condições são satisfeitas

1. $\forall h_1, h_2 \in H$, temos $h_1 h_2 \in H$.
2. $\forall h \in H$, temos $h^{-1} \in H$.

Demonstração. Se $(H, *)$ é subgrupo de $(G, *)$ é imediato verificar as propriedades 1) e 2). Faremos a outra direção. Por outro lado, suponha que H satisfaz 1) e 2), e vamos provar que $(H, *)$ é um grupo. Como $*$ é associativa para todos os elementos de G , o é, em particular para os elementos de H , uma vez que H é subconjunto de G . Para verificar G2), basta notar que o elemento neutro da operação de G , 1_G está em H . Seja $h \in H$. Por 2) temos que $h^{-1} \in H$ e por 1) temos que $h * h^{-1} = 1_G \in H$. Por fim, a condição 2) implica G3), assim $(H, *)$ é um grupo. $\square$

Exemplo 2. 1. Dado um grupo H , $\{e\}$ e G são subgrupos de G .

2. Seja G um grupo. Então $\{e\}$ é um subgrupo de G , dito **subgrupo trivial**.

3. Seja G um grupo, então $G \leq G$.
4. $(\mathbb{Z}, +)$ e $(\mathbb{Q}, +)$ são subgrupos de $(\mathbb{R}, +)$,
5. Seja G um grupo. Definimos por

$$Z(G) := \{x \in G ; xy = yx \text{ para todo } y \in G\},$$

o **centro** de G . Tal subconjunto é um subgrupo de G .

Definição 3. Sejam $(G; *)$ um grupo e $x \in G$. Para cada $n \in \mathbb{Z}$, denotaremos por

$$x^n = \begin{cases} e, & \text{se } n = 0. \\ x * x^{n-1}, & \text{se } n > 0. \\ (x^{-1})^{-n}, & \text{se } n < 0. \end{cases}$$

Definimos $\langle x \rangle := \{x^n ; n \in \mathbb{Z}\}$ o **subconjunto das potências de x** . Se G é um grupo aditivo, escrevemos na em vez de a^n .

É imediato verificar que:

Proposição 2. Sejam G um grupo e $x \in G$. Então $\langle x \rangle$ é um subgrupo de G , chamado de **subgrupo gerado por x** .

Definição 4. Sejam G um grupo e S é um subconjunto qualquer de um grupo G . O conjunto $\{a_1 a_2 \cdots a_n ; n \in \mathbb{N}, a_i \in S \text{ ou } a_i^{-1} \in S\}$, denotado por $\langle S \rangle$ é um subgrupo de G , chamado de **subgrupo gerado por S** .

Definição 5. Um grupo G é dito **cíclico** quando pode ser gerado por um elemento, isto é, quando $G = \langle g \rangle$, para algum $g \in G$.

É imediato ver que se G é um grupo cíclico e $H \leq G$, então H é cíclico.

Exemplo 3. Considere o grupo $(\mathbb{Z}, +)$. Temos que $\mathbb{Z}$ é um grupo cíclico gerado por 1

Definição 6. Seja G um grupo. O subgrupo $\langle \{xyx^{-1}y^{-1} ; x, y \in G\} \rangle$ é dito **subgrupo dos comutadores de G** e será denotado por $[G, G]$.

Note que G é abeliano se, e somente se $[G, G] = \{e\}$.

Definição 7. Se G é um grupo finito, diremos seu número de elementos é a **ordem** de G , e denotaremos por $|G|$. Se G é um grupo infinito, diremos que G possui ordem infinita.

Definição 8. Sejam G um grupo e $x \in G$. A **ordem do elemento** g , denotada por $o(x)$, é a ordem do subgrupo gerado por x , ou seja, $o(x) = |\langle x \rangle|$.

É imediato verificar que

Proposição 3. Sejam G um grupo e $x \in G$, tal que $o(x) = n < \infty$. Então $n = \min\{N \in \mathbb{N} \setminus \{0\} ; x^N = e\}$ e $\langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$.

Definição 9. Sejam G um grupo e $H \leq G$. Para cada $x \in G$, definamos a **classe lateral de x à esquerda** por $xH := \{xh ; h \in H\}$ e a **classe lateral de x à direita** por $Hx := \{hx ; h \in H\}$.

Proposição 4. Sejam G um grupo, $H \leq G$ e $x, y \in G$. Então:

- 1) $xH = yH$ se, e somente se, $y^{-1}x \in H$. Em particular, $xH = H$ se, e somente se, $x \in H$.
- 2) $f_x : H \rightarrow xH$ tal que $f_x(h) = xh$ é bijetora. Em particular, $|H| = |xH|$.
- 3) Seja

$$\begin{aligned} \varphi : \{\text{classes laterais à esquerda}\} &\rightarrow \{\text{classes laterais à direita}\} \\ xH &\mapsto Hx^{-1}, \end{aligned}$$

então φ é bijetora.

- 4) Considere a relação dada por

$$x \sim y \Leftrightarrow xH = yH.$$

Temos que:

- (a) $xH \neq \emptyset$.
- (b) $xH = yH$ ou $xH \cap yH = \emptyset$.
- (c) $G = \bigcup_{x \in G} xH$.

Demonstração. Os itens 1) 2) e 3) serão deixados como exercício aos leitores. Provaremos 4).

- (a) Como pelo item 2) $|H| = |xH|$ segue que $|xH| \neq 0$ e portanto $xH \neq \emptyset$.
- (b) Suponha $xH \cap yH \neq \emptyset$. Provaremos que $xH = yH$. Seja $z \in xH \cap yH$, então existem $h_1, h_2 \in H$ tais que $z = xh_1 = yh_2$. Assim para todo $h \in H$, temos $xh = zh_1^{-1}h = yh_2h_1^{-1}h$. Portanto $xH \subseteq yH$. Analogamente vemos que $yH \subseteq xH$ e temos nosso resultado.
- (c) Segue diretamente de (b).

□

Notação. Denotaremos por $(G : H)$ o número de classes laterais à esquerda (igual ao número de classes laterais à direita, pelo item (3) da proposição acima.), tal número é dito **índice** do subgrupo H em G .

Exemplo 4. Seja $(\mathbb{Z}, +)$ o grupo aditivo dos inteiros, $H = \langle n \rangle$. Teremos n classes laterais dadas por $[0], \dots, [n-1]$. Deste modo $(G : H) = n$.

Teorema 1 (Lagrange). *Se G é um grupo finito e $H \leq G$, então*

$$|G| = |H|(G : H).$$

Em particular, $|H|$ divide $|G|$ e $\frac{|G|}{|H|} = (G : H)$.

Demonstração. Como G é finito, se $|G| = s$, podemos considerar $G = \{a_1, \dots, a_s\}$. Então, pelo item (4) da Proposição 4, temos

$$G = a_1H \cup \dots \cup a_sH,$$

com $a_i H \cap a_j H = \emptyset$, para $i \neq j$. Assim $(G : H) = r$.

Pelo item (2) da Proposição 4, temos $|a_i H| = |a_j H| = |H|$, segue que:

$$|G| = |a_1 H| + \cdots + |a_r H| = r|H| = (G : H)|H|.$$

Portanto $\frac{|G|}{|H|} = (G : H)$. □

Corolário 1. *Se G é um grupo finito e $x \in G$, então $o(x)$ divide $|G|$. Em particular, $x^{|G|} = e$.*

Demonstração. Como $[x] \leq G$ e $|\langle x \rangle| = o(x)$, pelo Teorema de Lagrange temos que $o(x)$ divide $|G|$. Assim, existe, $t \in \mathbb{Z}$ tal que $|G| = o(x)t$, então $x^{|G|} = (x^{o(x)})^t = e$. □

Corolário 2. *Todo grupo de ordem prima é cíclico.*

Demonstração. Suponha que $|G| = p$, onde p é um número primo. Seja $x \in G \setminus \{e\}$, então $o(x) | p$. Segue que $o(x) = 1$ ou $o(x) = p$. Como $x \neq e$, temos que $o(x) = p$. Portanto $G = \langle x \rangle$. □

2 Exemplo: Grupos de Permutações

Nessa seção discutiremos os grupos de permutações. Eles merecem uma seção a parte da nossa discussão sobre grupos, pois eles foram os blocos fundamentais para a construção da teoria de grupos. Quando Galois pensava em grupos, na ocasião do estudo de raízes de equações polinômiais, ele pensava nos grupos de permutações (das raízes dos polinômios).

Definição 10. Seja X um conjunto. Dizemos que σ é uma **permutação** de X se $\sigma : X \rightarrow X$ é uma função bijetiva.

Definição 11. Seja X um conjunto e considere:

$$S_X := \{\sigma : X \rightarrow X; \sigma \text{ é uma permutação}\},$$

não é difícil ver que quando consideramos a operação de composição de funções, o conjunto S_X é um grupo. Dizemos que S_X é o **grupo simétrico**

de X . Quando X é um conjunto finito com cardinalidade n , denotamos S_X por S_n e dizemos que S_n é o **grupo simétrico de n elementos**.

Note que no caso em que $X = \{1, 2, \dots, n\}$, uma forma possível de descrever os elementos $\sigma \in S_n$ é

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & j \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(j) \cdots & \sigma(n) \end{pmatrix}.$$

Outra forma mais conveniente de descrever um tal elemento é a seguinte:

Definição 12. Sejam $\{i_1, i_2, \dots, i_r\}$ um subconjunto de $X = \{1, 2, \dots, n\}$, e $\sigma \in S_n$, de modo que σ fixa os complementar de $\{i_1, i_2, \dots, i_r\}$ em X . Isto é $\sigma(x) = x$ para todo $x \in X$ com $x \notin \{i_1, i_2, \dots, i_r\}$, e tal que $\sigma(i_1) = i_2; \sigma(i_2) = i_3; \dots; \sigma(i_{r-1}) = i_r; \sigma(i_r) = i_1$. Então σ é dito um **r -ciclo**, ou um **ciclo de comprimento r** , que denotaremos por $\sigma = (i_1 \ i_2 \ \cdots \ i_r)$.

Ademais, diremos que um 2-ciclo é dito uma **transposição**.

Note que um 1-ciclo é a identidade, pois fixa o elemento em questão, assim, todos os 1-ciclos são iguais.

Veremos a seguir, que podemos escrever qualquer permutação como o produto de transposições. Para isso, precisaremos do seguinte lema.

Lema 2. *Toda permutação $\sigma \in S_n$, é um ciclo, ou um produto de ciclos disjuntos.*

Demonstração. Procederemos por indução no número k de elementos que não são fixos por σ . Se $k = 0$ então σ é a identidade e portanto é um 1-ciclo. Caso o leitor se sinta desconfortável com a indução com o caso base se iniciando no zero,

Se σ não move nenhum elemento então σ é a identidade que é um 1-ciclo. Suponha que σ move pelo menos 1 elemento. Note que não podemos ter uma permutação que move apenas 1 elemento, caso contrário ela não seria bijetiva. Assim o próximo caso possível seria $k = 2$. Assim, sejam $\{i_1, i_2\}$ os elementos que são movidos por σ . Note que necessariamente $\sigma(i_1) = i_2$ e $\sigma(i_2) = i_1$, caso contrário σ moveria mais elementos. Assim podemos escrever $\sigma = (i_1 \ i_2)$.

Suponha, que se σ move $k \geq 2$ elementos, e seja i_1 um elemento que não é fixo por σ . Defina $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$, $\dots$, $i_{r+1} = \sigma(i_r)$. Onde r é o menor inteiro tal que $i_{r+1} \in \{i_1, \dots, i_r\}$ (note que temos no máximo n na lista $\{i_1, \dots, i_r\}$, e portanto em algum momento começaremos repetição). Perceba que necessariamente $\sigma(i_r) = i_1$. Caso contrário, se $\sigma(i_r) = i_j$, com $i_j \neq i_1$, teríamos $\sigma(i_r) = \sigma(i_{j-1}) = i_j$, uma contradição pois σ é permutação, logo injetiva. Seja $\alpha_1 = (i_1 \ i_2 \ \dots \ i_r)$. Se $r = k$, então $\sigma = \alpha_1$ e o lema está demonstrado. Caso contrário, se $r < n$, então η fixa cada um dos elementos em $Y_1 = \{i_1, \dots, i_r\}^c$. Como $\sigma(Y_1) = Y_1$. Defina a permutação β_1 de Y_1 tal que $\alpha_1(x) = \sigma(x)$ para todo $x \in Y$ e que fixa todos os elementos em Y^c . Segue que $\sigma = \alpha_1\beta_1$, com as α_1 e β_1 disjuntas. Repetindo o mesmo argumento para β_1 , encontramos um ciclo com s_1 elementos $\alpha_2 = (j_1 \ \dots \ j_{s_1})$, de modo que se $s_1 = n - r$ então $\beta_1 = \alpha_2$ e $\sigma = \alpha_1\alpha_2$, e temos nosso resultado. Caso contrário, teríamos $\beta_1 = \alpha_2\beta_2$ com α_2 sendo um s_1 -ciclo e β_2 uma permutação num conjunto com $n - r - s_1$ elementos. Note que ao repetir esse procedimento, ele deve terminar em algum momento, pois a cada iteração, o número $n - r - s_1 - \dots - s_k$ decresce, mas deve permanecer ser positivo. Assim teremos nosso resultado. $\square$

Corolário 3. *Todo elemento $\alpha \in S_n$ pode ser escrito como produto de transposições.*

Demonstração. Exercício ao leitor. $\square$

Exercícios

1. Prove as afirmações 2, 3, 4 e 5 do Lema 1.
2. Defina um grupo com o conjunto $X = \{a, b, c, d\}$, $Y = \{e, f, g, h\}$, e $Z = \{a, b, c, d, e\}$.
3. Prove que $(\text{GL}(n, \mathbb{R}), +)$ não é um grupo, e que $(\text{GL}(n, \mathbb{R}), \cdot)$ o é.
4. Seja $\text{O}(n, \mathbb{R}) := \{A \in \text{Mat}(n, \mathbb{R}); A * A^{\text{tr}} = A^{\text{tr}} * A = I\}$, onde I denota a matriz identidade. Prove que $(\text{O}(n, \mathbb{R}), *)$ é subgrupo de $\text{GL}(n, \mathbb{R})$. $\text{O}(n, \mathbb{R})$ é dito **grupo ortogonal**.

5. Seja $\text{SO}(n, \mathbb{R}) := \{A \in \text{O}(n, \mathbb{R}); \det A = 1\}$. Prove que $(\text{SO}(n, \mathbb{R}), *)$ é um grupo. $\text{SO}(n, \mathbb{R})$ é dito **grupo ortogonal especial**.
6. Sejam $\text{Mat}(n, \mathbb{C})$ o conjunto das matrizes quadradas de ordem n com entradas complexas. Prove que $\text{GL}(n, \mathbb{C}) := \{A \in \text{Mat}(n, \mathbb{C}); A \text{ é invertível}\}$ é um grupo. Analogamente aos exercícios anteriores, prove que $\text{U}(n) := \{A \in \text{Mat}(n, \mathbb{C}); A * \overline{A}^{\text{tr}} = \overline{A}^{\text{tr}} * A = I\}$, onde $\overline{A}$ denota o conjugado complexo das entradas de A , é um subgrupo de $\text{GL}(n, \mathbb{C})$. Faça o mesmo para $\text{SU}(n) := \{A \in \text{U}(n); \det A = 1\}$. $\text{U}(n)$ é dito **grupo unitário** e $\text{SU}(n)$ é dito **grupo unitário especial**.
7. Seja n um número natural, e $\Omega_n := \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$. Prove que $\text{Sp}(2n, \mathbb{R}) := \{A \in \text{GL}(2n, \mathbb{R}); A^{\text{tr}} \Omega_n A = \Omega_n\}$ é um subgrupo de $\text{GL}(2n, \mathbb{R})$. $\text{Sp}(2n, \mathbb{R})$ é dito **grupo simplético**.
8. Escreva a permutação

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 6 & 3 \end{pmatrix},$$

em notação de ciclos.

9. Duas permutações são ditas **disjuntas** se elementos não fixos de uma permutação são fixos pela outra. Prove que permutações disjuntas de S_n comutam.
10. Prove que todo elemento $\alpha \in S_n$ pode ser escrito como produto de transposições.
11. Escreva a tabela de multiplicação de S_3 , e descreva todos os seus subgrupos.
12. Calcule a ordem de S_n para todo n .
13. O grupo das simetrias de um polígono regular de n lados, denotado por D_n , consiste do grupo gerado por todas as possíveis produtos de

2 EXEMPLO: GRUPOS DE PERMUTAÇÕES

dois elementos r (rotação) e s (reflexão) de modo que eles satisfazem as seguintes relações: $r^n = 1$, $s^2 = 1$ e $srs = r^{-1}$.

- a) Interprete geometricamente o significado das relações $r^n = 1$, $s^2 = 1$ e $srs = r^{-1}$.
 - b) Calcule a ordem de D_n
 - c) Descreva os elementos de D_3 e D_4 (use desenhos!).
 - d) D_4 é um grupo cíclico?
 - e) Mostre que $D_n < S_n$.
14. Prove o pequeno teorema de Fermat: Sejam p um número primo, então $a^{p-1} \equiv 1 \pmod{p}$, para todo a que não é múltiplo de p .