SUMÁRIO

ÁLGEBRA I

Grupos, Subgrupos e Homomorfismos de Grupos

André Luiz Galdino

1. Grupos

A essência por trás da Teoria dos Grupos é tomar dois elementos de um conjunto, combinar eles de alguma maneira e retornar um terceiro elemento do mesmo conjunto, e é este o papel das *operações binárias*.

Definição 1.1. Seja G um conjunto não vazio. Uma *operação binária sobre* G é uma função $*$ que associa a cada par ordenado $(a, b) \in G \times G$ um elemento $a * b \in G$. De mais a mais, representamos uma operação binária sobre G da seguinte maneira:

$$\begin{aligned} * : G \times G &\to G \\ (a, b) &\mapsto a * b \end{aligned}$$

Observe que $a * b$ (lê-se: a estrela b) é uma outra forma de indicar a função $*(a, b)$, e que uma operação binária combina dois elementos, nem mais, nem menos. No mais, quando há qualquer operação $*$ definida sobre G, seja ela binária ou não, dizemos que G é um conjunto munido da operação $*$. Em particular, se $*$ é operação binária sobre G, então dizemos que G é *fechado* com relação à operação $*$.

Exemplo 1.2. Sejam $\mathbb{N}$ o conjunto dos números naturais, incluindo o número 0, $\mathbb{Z}$ o conjunto dos números inteiros, $\mathbb{Q}$ o conjunto dos números racionais, $\mathbb{R}$ o conjunto dos números reais e $\mathbb{C}$ o conjunto dos números complexos.

1. $* = +$: A adição sobre $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ é uma operação binária.
2. $* = -$: A subtração sobre $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ é uma operação binária.
3. $* = \cdot$: A multiplicação sobre $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ é uma operação binária.
4. $* = \div$: A divisão $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$ é uma operação binária.
5. $* = \circ$: A composição de funções é uma operação binária sobre o conjunto $\mathcal{F}(A) = \{f \mid f : A \to A\}$ de todas as funções de A em A.
6. A adição e multiplicação de matrizes são operações binárias sobre o conjunto $M_n(\mathbb{R})$ de todas as matrizes quadradas $n \times n$ com entradas em $\mathbb{R}$. Da mesma forma sobre $M_n(\mathbb{Q})$ e $M_n(\mathbb{C})$, respectivamente, os conjuntos das matrizes quadradas $n \times n$ com entradas racionais e complexos.

7. A adição de vetores em um espaço vetorial V é uma operação binária, pois,

$$\begin{aligned} + : V \times V &\to V \\ (u, v) &\mapsto u + v \end{aligned}$$

No entanto, a multiplicação por escalar não é uma operação binária, pois, tal multiplicação é definida por:

$$\begin{aligned} \cdot : \mathbb{R} \times V &\to V \\ (k, v) &\mapsto k \cdot v \end{aligned}$$

8. A função $\star : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, dada por $a \star b = a^b$, é uma operação binária sobre $\mathbb{N}$, chamada de potenciação. No entanto, esta mesma função sobre $\mathbb{Z}$ e $\mathbb{Q}$ não é uma operação binária. De fato, sendo $(3, -1) \in \mathbb{Z} \times \mathbb{Z}$ e $\left(5, \frac{1}{2}\right) \in \mathbb{Q} \times \mathbb{Q}$ temos, respectivamente, que:

$$3 \star (-1) = 3^{-1} = \frac{1}{3} \notin \mathbb{Z},$$

$$5 \star \frac{1}{2} = 5^{\frac{1}{2}} = \sqrt{5} \notin \mathbb{Q}.$$

Analogamente, a função de potenciação $\star$ não é uma operação binária sobre $\mathbb{R}$ pelo mesmo motivo anterior, já que $\sqrt{5} \notin \mathbb{R}$.

Definição 1.3. Seja G um conjunto não vazio munido de uma operação $*$. Dizemos que G é um *grupo* com respeito à operação $*$ se, e somente se, as seguintes acontecem:

i) $\forall a, b \in G \quad \Rightarrow \quad a * b \in G$;

ii) $\forall a, b, c \in G \quad \Rightarrow \quad a * (b * c) = (a * b) * c$;

iii) $\exists\ e \in G \ : \ \forall a \in G \quad \Rightarrow \quad e * a = a$;

iv) $\forall a \in G \quad \Rightarrow \quad \exists\ a^{-1} \in G \ : \ a^{-1} * a = e$.

Veja que na Definição 1.3 o item i) nos diz que G deve ser fechado com relação à operação $*$, ou seja, da operação $*$ sobre os elementos de G sempre resulta um elemento de G. O item ii) requer que $*$ seja uma operação associativa, isto é, a operação $*$ deve nos permitir operar mais de dois elementos sem a necessidade de usar parênteses, uma vez que qualquer associação entre os elementos nos fornece o mesmo resultado final. Por exemplo,

$$a * b * c * d = (a * b) * (c * d) = a * (b * (c * d)) = a * ((b * c) * d) = \cdots .$$

Na sequência, o item iii) exige a existência de um elemento especial $e \in G$, com relação à operação $*$, chamado de *elemento neutro*. Por fim, o item iv) pede a garantia de que todo elemento $a \in G$ possua, com relação à operação $*$, um *inverso* $a^{-1} \in G$.

Note que para se formar um grupo precisamos de um par de objetos: um conjunto G não vazio e uma operação $*$ definida sobre ele. Logo, uma notação intuitiva para grupo é $(G, *)$ e por vezes a usaremos, porém, por simplicidade costumamos dizer apenas que "G é um grupo" ou "o grupo G", o que evidentemente pressupõe a existência de uma operação $*$ definida sobre G. Contudo, quando falamos de um grupo G específico, devemos deixar claro qual operação esta associada a ele.

Exemplo 1.4.

1. Considere o conjunto $\mathbb{Z}$ com a operação usual de adição $(+)$. Como a operação $+$ é uma operação binária associativa sobre $\mathbb{Z}$ temos:

   i) $\forall a, b \in \mathbb{Z} \;\Rightarrow\; a + b \in \mathbb{Z}$;

   ii) $\forall a, b, c \in \mathbb{Z} \;\Rightarrow\; a + (b + c) = (a + b) + c$;

   iii) $\exists\, 0 \in \mathbb{Z} \;:\; \forall a \in \mathbb{Z} \;\Rightarrow\; 0 + a = a$;

   iv) $\forall a \in \mathbb{Z} \;\Rightarrow\; \exists\; -a \in \mathbb{Z} \;:\; (-a) + a = 0$.

   Logo, $(\mathbb{Z}, +)$ é um grupo.

2. Analogamente ao item anterior, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}, +)$ são grupos com suas respectivas operações usuais de adição, onde em todos os casos o 0 é o elemento neutro e o inverso de x é $-x$.

3. O conjunto $\mathbb{Z}$ munido da operação subtração $(-)$ não caracteriza um grupo. De fato, apesar da operação $-$ ser binária e associativa, o conjunto $\mathbb{Z}$ não possui elemento neutro com relação à $-$. Isto porque não existe um elemento $e \in \mathbb{Z}$ de forma que, para todo $x \in \mathbb{Z}$, se tenha:
$$e - x = x.$$

4. Seja $\mathbb{Q}^*$, conjunto dos números racionais sem o zero, munido da multiplicação usual em $\mathbb{Q}$. Afirmamos que $(\mathbb{Q}, \cdot)$ é um grupo. Vejamos:

   i) $\forall a, b \in \mathbb{Q}^* \;\Rightarrow\; a \neq 0 \text{ e } b \neq 0 \;\Rightarrow\; a \cdot b \neq 0 \;\Rightarrow\; a \cdot b \in \mathbb{Q}^*$.

   ii) Já é sabido que $\cdot$ é uma operação binária associativa, ou seja, para todo $a, b, c \in \mathbb{Q}^*$,
   $$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

iii) $\mathbb{Q}^*$ possui o 1 como elemento neutro da multiplicação, pois, para todo $a \in \mathbb{Q}^*$ temos:

$$1 \cdot a = a.$$

iv) Todo elemento $a \in \mathbb{Q}^*$ possui inverso multiplicativo que é $\frac{1}{a} \in \mathbb{Q}^*$. De fato,

$$\frac{1}{a} \cdot a = 1.$$

Logo, $(\mathbb{Q}^*, \cdot)$ é um grupo.

5. Analogamente ao item anterior, $(\mathbb{R}^*, \cdot)$ e $(\mathbb{C}^*, \cdot)$ são grupos com suas respectivas operações usuais de multiplicação, onde em todos os casos o 1 é o elemento neutro e o inverso de x é $\frac{1}{x}$.

6. O conjunto $\mathbb{R}^*$ munido da operação divisão $(\div)$ não é um grupo. De fato, a operação $\div$ é binária, porém não é associativa, pois:

$$\begin{aligned} (48 \div 12) \div 4 &= 4 \div 4 = 1 \\ 48 \div (12 \div 4) &= 48 \div 3 = 16 \end{aligned}$$

Logo, $(48 \div 12) \div 4 \neq 48 \div (12 \div 4)$.

7. Seja $G = \{1, -1\}$. Afirmamos que G é um grupo com a operação de multiplicação usual dos números reais. Vejamos, mas antes, sempre que possível e por simplicidade omitiremos a partir daqui o $\cdot$ que representa a multiplicação usual.

i) Para todo $a, b \in G$, temos $ab \in G$, pois,

$$1 \cdot 1 = 1 \qquad 1 \cdot (-1) = -1 \qquad (-1) \cdot 1 = -1 \qquad (-1) \cdot (-1) = 1$$

ii) Sem dúvida, para todo $a, b, c \in G$, tem-se $a(bc) = (ab)c$.

iii) G possui elemento neutro que é 1.

iv) Para todo $a \in G$, o própria a é seu inverso, ou seja, $a^{-1} = a$. De fato, para $a = 1$ ou $a = -1$ temos que $a^{-1}a = aa = 1$.

Logo, G é um grupo multiplicativo.

8. O conjunto $\mathbb{N}$ munido da operação de potenciação $\star$, dada por $a \star b = a^b$, não forma um grupo. Verdade, $\mathbb{N}$ é fechado para $\star$, mas $\star$ não é associativa. De fato, sendo $2, 3, 4 \in \mathbb{N}$ temos:

$$\begin{aligned} (2 \star 3) \star 4 &= 2^3 \star 4 = (2^3)^4 = 2^{3.4} = 2^{12} \\ 2 \star (3 \star 4) &= 2 \star 3^4 = 2^{(3^4)} = 2^{81} \end{aligned}$$

Portanto, $(2 \star 3) \star 4 \neq 2 \star (3 \star 4)$ e $(\mathbb{N}, \star)$ não é um grupo.

9. O conjunto $M_n(\mathbb{R})$ munido da operação de multiplicação usual das matrizes não constitui um grupo. De fato, sendo $\mathbf{I}_n \in M_n(\mathbb{R})$ a matriz identidade temos:

   i) $\forall A, B \in M_n(\mathbb{R}) \quad \Rightarrow \quad AB \in M_n(\mathbb{R})$.

   ii) $\forall A, B, C \in M_n(\mathbb{R}) \quad \Rightarrow \quad A(BC) = (AB)C$.

   iii) $\forall A \in M_n(\mathbb{R}) \quad \Rightarrow \quad \mathbf{I}_n A = A$.

   iv) Porém, nem toda matriz $A \in M_n(\mathbb{R})$ possui um inverso, pois, nem toda matriz quadrada possui determinante diferente de zero.

   Portanto, $M_n(\mathbb{R})$ não é um grupo com a operação de multiplicação usual das matrizes.

10. Considere o conjunto $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid det(A) \neq 0\}$. A operação de multiplicação usual de matrizes é uma operação binária sobre $GL_n(\mathbb{R})$. De fato, para todo $A, B \in GL_n(\mathbb{R})$ temos que $det(A) \neq 0$ e $det(B) \neq 0$, consequentemente,

$$det(AB) = det(A)det(B) \neq 0.$$

    Isto nos leva a concluir que $AB \in GL_n(\mathbb{R})$. Já é sabido que a operação de multiplicação de matrizes é associativa, e que a matriz identidade $\mathbf{I}_n$ é o elemento neutro de $GL_n(\mathbb{R})$. Além disso, toda matriz $A \in GL_n(\mathbb{R})$ possui um inverso A^{-1}, pois, toda matriz quadrada que possui determinante diferente de zero é inversível, e

$$det(A^{-1}) = \frac{1}{det(A)} \neq 0 \quad \Rightarrow \quad A^{-1} \in GL_n(\mathbb{R}).$$

    Portanto, $GL_n(\mathbb{R})$ é um grupo multiplicativo. Similarmente, também é um grupo multiplicativo o conjunto $GL_n(\mathbb{Q})$.

11. Sejam $n \in \mathbb{N}^*$, $X = \{x_1, x_2, x_3, \ldots, x_n\}$ e S_n o conjunto de todas as funções bijetoras de X em X, ou seja,

$$S_n = \{\phi : X \to X \mid \phi \text{ é uma função bijetora}\}.$$

    Afirmamos que S_n é um grupo com a operação de composição de funções, chamado de *Grupo Simétrico de grau n*. De fato, como a composição de funções bijetoras é também bijetora, temos que S_n é fechado com relação à composição de funções. Sem nenhuma dúvida, a operação composição de funções é associativa. Temos ainda que o elemento neutro de S_n é a função identidade, e como toda função bijetora possui inversa, que também é bijetora, concluímos a afirmação, isto é, $(S_n, \circ)$ é um grupo.

12. Seja $G = \{x \in \mathbb{R} \mid x \neq -1\}$. Vamos mostrar que G é um grupo com relação à operação $\oplus$ dada por:

$$x \oplus y = x + y + xy.$$

i) G é fechado para a operação $\oplus$. De fato, para todo $x, y \in G$, $x \neq -1$ e $y \neq -1$, temos:

$$x \oplus y = x + y + xy = (x+1)(y+1) - 1 \neq -1 \quad \Rightarrow \quad x \oplus y \in G.$$

ii) Para todo $x, y, z \in G$ vem que:

$$\begin{aligned} x \oplus (y \oplus z) &= x \oplus (y + z + yz) \\ &= x + (y + z + yz) + x(y + z + yz) \\ &= x + y + z + yz + xy + xz + x(yz) \\ &= x + y + z + yz + xy + xz + (xy)z \\ &= (x + y + xy) + z + (x + y + xy)z \\ &= (x + y + xy) \oplus z \\ &= (x \oplus y) \oplus z. \end{aligned}$$

Logo, a operação $\oplus$ é associativa.

iii) Para todo $x \in G$, verifiquemos se existe $e \in G$ tal que $e \oplus x = x$.

$$\begin{aligned} e \oplus x &= x \\ e + x + ex &= x \\ e + ex &= 0 \\ (1 + x)e &= 0 \\ e &= 0. \end{aligned}$$

Logo, G possui elemento neutro que é $e = 0$.

iv) Por fim, todo $x \in G$ possui um inverso $x^{-1} \in G$, pois,

$$\begin{aligned} x^{-1} \oplus x &= e \\ x^{-1} + x + x^{-1}x &= 0 \\ x^{-1} &= -\frac{x}{1+x} = -1 + \frac{1}{1+x} \neq -1. \end{aligned}$$

Logo, $(G, \oplus)$ é um grupo.

Definição 1.5. Dizemos que um grupo $(G, *)$ é *abeliano* ou *comutativo* se, e somente se, $*$ é uma operação comutativa.

Exemplo 1.6.

1. Para todo $a, b \in \mathbb{Z}$ temos $a + b = b + a$, ou seja, $(\mathbb{Z}, +)$ é um grupo aditivo abeliano. Analogamente, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ e $(\mathbb{C}, +)$, com suas respectivas operações usuais de adição, são grupos abelianos.

2. Para todo $a, b \in \mathbb{Q}^*$ temos $a \cdot b = b \cdot a$, isto é, $(\mathbb{Q}^*, \cdot)$ é um grupo multiplicativo abeliano. Igualmente, $(\mathbb{R}^*, \cdot)$ e $(\mathbb{C}^*, \cdot)$, com suas respectivas operações usuais de multiplicação, são grupos abelianos.

3. É fácil ver que o grupo multiplicativo $G = \{1, -1\}$ é um grupo abeliano.

4. O conjunto $\mathcal{F}(\mathbb{R})$, de todas as funções de $\mathbb{R}$ em $\mathbb{R}$, é um grupo abeliano com a operação de adição usual entre funções, a saber, para todo $x \in \mathbb{R}$:

   i) Para todo $f, g \in \mathcal{F}(\mathbb{R})$ temos $(f+g)(x) = f(x)+g(x) \in \mathcal{F}(\mathbb{R})$.

   ii) Para todo $f, g, h \in \mathcal{F}(\mathbb{R})$ temos

$$\begin{aligned}
[f + (g + h)](x) &= f(x) + (g + h)(x) \\
&= f(x) + (g(x) + h(x)) \\
&= (f(x) + g(x)) + h(x) \\
&= (f + g)(x) + h(x) \\
&= [(f + g) + h](x).
\end{aligned}$$

   iii) A função nula $f(x) = 0$ é o elemento neutro de $\mathcal{F}(\mathbb{R})$ com relação à operação $+$, pois, para todo $g \in \mathcal{F}(\mathbb{R})$ temos:

$$(f + g)(x) = f(x) + g(x) = 0 + g(x) = g(x).$$

   iv) Para todo $f \in \mathcal{F}(\mathbb{R})$, existe $-f \in \mathcal{F}(\mathbb{R})$ tal que:

$$(-f + f)(x) = -f(x) + f(x) = 0.$$

   Logo, $(\mathcal{F}(\mathbb{R}), +)$ é um grupo. Ademais,

   v) Para todo $f, g \in \mathcal{F}(\mathbb{R})$ temos:

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x).$$

   Portanto, $(\mathcal{F}(\mathbb{R}), +)$ é um grupo abeliano.

5. O conjunto $M_{n\times m}(\mathbb{Z})$ é um grupo aditivo abeliano com a operação de adição usual das matrizes. De fato, o elemento neutro de $M_{n\times m}(\mathbb{Z})$ é a matriz nula $n\times m$, denotada por $\mathbf{0}_{n\times m}$, e o inverso da matriz $A \in M_{n\times m}(\mathbb{Z})$ é a matriz $-A \in M_{n\times m}(\mathbb{Z})$. Assim temos:

   i) $\forall A, B \in M_{n\times m}(\mathbb{Z}) \quad \Rightarrow \quad A + B \in M_{n\times m}(\mathbb{Z})$.

   ii) $\forall A, B, C \in M_{n\times m}(\mathbb{Z}) \quad \Rightarrow \quad A + (B + C) = (A + B) + C$.

   iii) $\forall A \in M_{n\times m}(\mathbb{Z}) \quad \Rightarrow \quad \mathbf{0}_{n\times m} + A = A$.

   iv) $\forall A \in M_{n\times m}(\mathbb{Z}) \quad \Rightarrow \quad -A) + A = \mathbf{0}_{n\times m}$.

   v) $\forall A, B \in M_{n\times m}(\mathbb{Z}) \quad \Rightarrow \quad A + B = B + A$.

   Logo, $(M_{n\times m}(\mathbb{Z}), +)$ é um grupo abeliano aditivo. Também são grupos abelianos $(M_{n\times m}(\mathbb{Q}), +)$, $(M_{n\times m}(\mathbb{R}), +)$ e $(M_{n\times m}(\mathbb{C}), +)$.

6. Sejam $n > 1$ um inteiro e $\overline{r} = \{kn + r \mid k \in \mathbb{Z}, 0 \leq r < n\}$. Considerando o conjunto

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\},$$

   e definindo a operação de adição sobre $\mathbb{Z}_n$ como sendo

$$\overline{x} + \overline{y} = \overline{x + y},$$

   temos que $(\mathbb{Z}_n, +)$ é um grupo abeliano. De fato,

   i) Para todo $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n$ temos:

$$\begin{aligned} \overline{x} + (\overline{y} + \overline{z}) &= \overline{x} + \overline{(y + z)} = \overline{x + (y + z)} \\ &= \overline{(x + y) + z} = \overline{(x + y)} + \overline{z} \\ &= (\overline{x} + \overline{y}) + \overline{z}. \end{aligned}$$

   ii) Para todo $\overline{x} \in \mathbb{Z}_n$, existe $\overline{0} \in \mathbb{Z}_n$ tal que:

$$\overline{x} + \overline{0} = \overline{x + 0} = \overline{x}.$$

   iii) Para todo $\overline{x} \in \mathbb{Z}_n$, existe $\overline{n - x} \in \mathbb{Z}_n$ tal que:

$$\overline{x} + \overline{n - x} = \overline{x + (n - x)} = \overline{n} = \overline{0}.$$

   iv) Para todo $\overline{x}, \overline{y} \in \mathbb{Z}_n$,

$$\overline{x} + \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x}.$$

   Portanto, $(\mathbb{Z}_n, +)$ é um grupo abeliano.

7. Considere o conjunto $\mathcal{F}(\mathbb{R})$ das funções de $\mathbb{R}$ em $\mathbb{R}$ munido da operação composição de funções. Apesar do conjunto $\mathcal{F}(\mathbb{R})$ ser não vazio, ser fechado com relação à operação, possuir a função identidade $i_{\mathbb{R}}$ como elemento neutro e a operação composição ser associativa, ele não é um grupo, pois, nem toda $f \in \mathcal{F}(\mathbb{R})$ possui inverso f^{-1}. De fato, $f \in \mathcal{F}(\mathbb{R})$ possui uma inversa f^{-1} se, e somente se, f é bijetora. No entanto, nem toda $f \in \mathcal{F}(\mathbb{R})$ é bijetora, por exemplo, a função $f(x) = x^2$ não é injetora e nem sobrejetora.

8. Seja S_3 o grupo de todas as funções bijetoras de $X = \{x_1, x_2, x_3\}$ nele mesmo, ou seja,

$$S_3 = \left\{ \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}, \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}, \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}, \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix}, \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}, \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix} \right\},$$

onde a notação $\begin{pmatrix} x_1 & x_2 & x_3 \\ x_i & x_j & x_k \end{pmatrix}$ representa a função tal que:

$$x_1 \to x_i, \qquad x_2 \to x_j, \qquad x_3 \to x_k.$$

Como vimos no item 11 do Exemplo 1.4, S_3 é um grupo com a operação composição de funções. Porém, S_3 não é um grupo abeliano. De fato, considere as funções ϕ e ψ, dadas como segue:

$$\phi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix} \qquad \text{e} \qquad \psi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}.$$

Temos que:

(a) $\phi\psi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix}.$

(b) $\psi\phi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}.$

Portanto, $\phi\psi \neq \psi\phi$ e S_3 não é abeliano.

Lema 1.7. Sejam $(G, *)$ um grupo e $a \in G$. Se $a * a = a$, então $a = e$.

Demonstração: Como $a \in G$, existe $a^{-1} \in G$ tal que $a^{-1} * a = e$. Logo,

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

Por outro lado,

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

Portanto, $a = e$. ■

Teorema 1.8. Se $(G, *)$ é um grupo, então para todo $a \in G$ temos que:

1. $a * a^{-1} = e$.
2. $a * e = a$.

Demonstração: Se $(G, *)$ é um grupo, então para todo $a \in G$,

$$a^{-1} * a = e \qquad \text{e} \qquad e * a = a.$$

1. $(a * a^{-1}) * (a * a^{-1}) = (a * (a^{-1} * a)) * a^{-1} = (a * e) * a^{-1} = a * a^{-1}$, consequentemente, pelo Lema 1.7 temos o resultado desejado, que é, $a * a^{-1} = e$.
2. $a * e = a * (a^{-1} * a) = (a * a^{-1}) * a = e * a = a$. Como queríamos demonstrar. ■

O Teorema 1.8 nós diz que a ordem em que operamos o elemento neutro e o elemento inverso é indiferente, ou seja,

$$a^{-1} * a = a * a^{-1} = e \qquad \text{e} \qquad e * a = a * e = a.$$

Teorema 1.9. Seja $(G, *)$ um grupo. Então,

1. G possui um único elemento neutro.
2. cada elemento $a \in G$ possui um único inverso.

Demonstração: Para mostrar que o elemento neutro e o inverso são únicos, suponhamos que existem dois de cada e mostramos que eles são, respectivamente, iguais.

1. Sejam $e, e' \in G$ elementos neutros com relação à $*$. Logo,
   i) se e é um elemento neutro, então $e * e' = e'$.
   ii) se e' é um elemento neutro, então $e * e' = e$.

   De i) e ii) temos $e = e'$, isto é, o elemento neutro é único.

2. Suponhamos que a^{-1} e b sejam dois inversos de $a \in G$, isto é,

$$a^{-1} * a = a * a^{-1} = e \qquad \text{e} \qquad b * a = a * b = e.$$

Então,

$$b = e * b = (a^{-1} * a) * b = a^{-1} * (a * b) = a^{-1} * e = a^{-1}.$$

Logo, $b = a^{-1}$. Isto é, o inverso de cada elemento $a \in G$ é único.

■

O Teorema 1.9 mostra que se o elemento neutro existe, então ele é único. Em particular, por definição, temos $e * e = e$, ou seja, $e^{-1} = e$.

Corolário 1.10. Se G é um grupo e $a \in G$, então $(a^{-1})^{-1} = a$.

Demonstração: Seja a^{-1} o inverso de a, ou seja, $a * a^{-1} = e$. Pelo Teorema 1.9 o inverso é único, consequentemente, observando esta última igualdade podemos concluir, por definição, que a é o inverso de a^{-1}, ou seja, $(a^{-1})^{-1} = a$. ■

Lema 1.11. Sejam G um grupo e $a, x, y \in G$. Então, as seguintes leis de cancelamento são válidas:

1. $a * x = a * y \quad \Rightarrow \quad x = y.$
2. $x * a = y * a \quad \Rightarrow \quad x = y.$

Demonstração:

1. Suponha que $a * x = a * y$. Então,

$$\begin{aligned} x = e * x = (a^{-1} * a) * x &= a^{-1} * (a * x) \\ &= a^{-1} * (a * y) \\ &= (a^{-1} * a) * y = e * y = y. \end{aligned}$$

Logo, $x = y$.

2. Suponha que $x * a = y * a$. Então,

$$\begin{aligned} x = x * e = x * (a * a^{-1}) &= (x * a) * a^{-1} \\ &= (y * a) * a^{-1} \\ &= y * (a * a^{-1}) = y * e = y. \end{aligned}$$

Portanto, $x = y$. ■

Lema 1.12. Seja $(G, *)$ um grupo. Mostre que para todo $a, b \in G$,

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

Demonstração: Para todo $a, b \in G$ temos:

$$(a * b) * (a * b)^{-1} = e \quad \Rightarrow \quad a * (b * (a * b)^{-1}) = e.$$

Pelo item 1 do Lema 1.11, podemos operar a^{-1} à esquerda de ambos os lados da última igualdade, sem que a mesma se altere:

$$\begin{aligned} a * (b * (a * b)^{-1}) = e \quad &\Rightarrow \quad a^{-1} * a * (b * (a * b)^{-1}) = a^{-1} * e \\ &\Rightarrow \quad e * (b * (a * b)^{-1}) = a^{-1} * e \\ &\Rightarrow \quad b * (a * b)^{-1} = a^{-1}. \end{aligned}$$

Do mesmo modo, sem que a última igualdade se altere, podemos operar b^{-1} à esquerda de ambos os lados:

$$\begin{aligned} b * (a * b)^{-1} = a^{-1} \quad &\Rightarrow \quad b^{-1} * b * (a * b)^{-1} = b^{-1} * a^{-1} \\ &\Rightarrow \quad e * (a * b)^{-1} = b^{-1} * a^{-1} \\ &\Rightarrow \quad (a * b)^{-1} = b^{-1} * a^{-1}. \end{aligned}$$

Como queríamos demonstrar. ■

Lema 1.13. Seja G um grupo. Se $a, b \in G$ e x é uma variável em G, então a equação $a * x = b$ possui uma única solução em G, que é $x = a^{-1} * b$.

Demonstração: Claramente $x = a^{-1} * b$ é uma solução da equação $a * x = b$, pois,

$$a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b.$$

Por outro lado, se x_0 é uma solução da equação, então $a * x_0 = b$. Donde obtemos,

$$x_0 = e * x_0 = (a^{-1} * a) * x_0 = a^{-1} * (a * x_0) = a^{-1} * b.$$

Portanto, a equação $a * x = b$ possui uma única solução em G, que é $x = a^{-1} * b$. ■

Como consequência do Lema 1.13 temos: para mostrar que um determinando elemento $x \in G$ é igual ao elemento neutro do grupo G, basta mostrar que $a * x = a$ para algum $a \in G$.

Lema 1.14. Sendo $(G, *)$ um grupo e $n \in \mathbb{Z}$, definida recursivamente a n-ésima potência de $a \in G$ da seguinte forma:

$$\begin{aligned} a^0 &= e, \\ a^{n+1} &= a^n * a \qquad n > 0, \\ a^n &= (a^{-n})^{-1} \qquad n < 0. \end{aligned}$$

Então, para todo $n, m \in \mathbb{Z}$:

1. $a^n * a^m = a^{n+m}$
2. $(a^n)^m = a^{nm}$

Demonstração: As provas se dão por indução em m e, sem perca de generalidade, vamos supor $n > 0$ e $m > 0$. Os casos $n = 0$ ou $m = 0$ são triviais e de fácil entendimento. Já os casos onde $n < 0$ ou $m < 0$, basta levar em conta a definição da n-ésima potência para o caso de expoente negativo, se valer da propriedade apresentada pelo Lema 1.12, e aplicar a propriedade para o caso em que os expoentes são positivos.

1. **BI -** Para $m = 1$ temos: $a^n * a^1 = a^{n+1}$. Portanto, a igualdade é verdadeira para $m = 1$.

   HI - Vamos supor que a igualdade seja verdadeira para $m = k$, ou seja, $a^n * a^k = a^{n+k}$.

   PI - Na sequência, vamos verificar se a igualdade é verdadeira para $m = k + 1$, ou seja, verificar se $a^n * a^{k+1} = a^{n+(k+1)}$.

   $$a^n * a^{k+1} = a^n * a^k * a \overset{HI}{=} a^{n+k} * a = a^{(n+k)+1} = a^{n+(k+1)}.$$

   Logo, a igualdade é verdadeira para $m = k+1$ e, consequentemente, a igualdade é verdadeira para todo $a \in G$ e para todo $n, m \in \mathbb{N}$.

2. **BI -** Para $m = 1$ temos: $(a^n)^1 = a^n = a^{n.1}$. Portanto, a igualdade é verdadeira para $m = 1$.

   HI - Vamos supor que a igualdade seja verdadeira para $m = k$, ou seja, $(a^n)^k = a^{nk}$.

   PI - Verifiquemos se a igualdade é verdadeira para $m = k + 1$, ou seja, vamos verificar se $(a^n)^{k+1} = a^{n(k+1)}$.

   $$(a^n)^{k+1} = (a^n)^k * a^n \overset{HI}{=} a^{nk} * a^n = a^{nk+n} = a^{n(k+1)}.$$

   Portanto, a igualdade é verdadeira para $m = k + 1$. Consequentemente, a igualdade é verdadeira para todo $a \in G$ e todo $n, m \in \mathbb{N}$.

■

Definição 1.15. A *ordem* de um grupo G é definida como sendo o número de elementos em G e é denotada por $|G|$.

Exemplo 1.16.

1. O grupo $G = \{-1, 1\}$ é um grupo finito de ordem 2, que é, $|G| = 2$.
2. Como $\mathbb{Z}$ é infinito, então o grupo $(\mathbb{Z}, +)$ possui ordem infinita.

Deste ponto em diante, sempre que possível e não causar prejuízos ou dúvidas, não mais explicitaremos a operação $*$ de um grupo $(G, *)$. Isto posto, em vez de $a * b$ apenas escreveremos ab. Além disso, lembremos que por definição a n-ésima potência de $a \in G$ é dada por:

$$a^n = \underbrace{aaa \cdots a}_{n}.$$

Definição 1.17. Seja G um grupo. Dizemos que um elemento $a \in G$ possui *ordem* n se, e somente se, $n > 0$ e é o menor inteiro tal que $a^n = e$. No mais, se $a \in G$ possui ordem n, então denotamos por $|a| = n$.

Exemplo 1.18.

1. Considere o grupo $\mathbb{Z}_6$. O elemento $\overline{2} \in \mathbb{Z}_6$ possui ordem 3. De fato,

$$\overline{2}^1 = \overline{2}, \qquad \overline{2}^2 = \overline{2} + \overline{2} = \overline{4}, \qquad \overline{2}^3 = \overline{2} + \overline{2} + \overline{2} = \overline{6} = \overline{0}.$$

2. Os elementos $-1, i \in \mathbb{C}^*$ possuem, respectivamente, ordens 2 e 4. Vejamos,

$$(-1)^1 = -1, \qquad (-1)^2 = (-1)(-1) = 1.$$

$$i^1 = i, \qquad i^2 = -1, \qquad i^3 = i^2 i = -i, \qquad i^4 = i^2 i^2 = 1.$$

Lema 1.19. Seja $a \in G$, onde G é um grupo. Se $|a| = n$, então $a^m = e$ se, e somente se, $n \mid m$.

Demonstração: ($\Rightarrow$) Seja $|a| = n$ e suponha que $a^m = e$. Pelo algoritmo da divisão de Euclides temos que existem únicos $q, r \in \mathbb{Z}$, tal que $m = qn + r \quad \text{e} \quad 0 \leq r < n$. Sendo assim temos:

$$a^m = e \;\Rightarrow\; a^{qn+r} = e \;\Rightarrow\; a^{qn}a^r = e \;\Rightarrow\; (a^n)^q a^r = e \;\Rightarrow\; a^r = e.$$

Como $|a| = n$, isto é, n é o menor inteiro tal que $a^n = e$, concluímos de $r < n$ e $a^r = e$ que a única possibilidade é termos $r = 0$. Consequentemente, $m = qn$ e, por definição, $n \mid m$.

($\Leftarrow$) Por outro lado, se $n \mid m$, então $m = kn$ e $a^m = a^{kn} = (a^n)^k = e$. ■

Corolário 1.20. Seja $a \in G$ tal que $|a| = n$. Para todo $k, t \in \mathbb{Z}$, temos $a^k = a^t$ se, e somente se, $k \equiv t(mod\ n)$.

Demonstração: $a^k = a^t \Leftrightarrow a^{k-t} = e \Leftrightarrow n \mid (k-t) \Leftrightarrow k \equiv t(mod\ n)$. ■

Na verdade, sendo $a \in G$ de ordem finita n, podemos comparar ou correlacionar as ordens de a e a^k. De fato, observe que

$$(a^k)^n = (a^n)^k = e.$$

Então, pelo Lema 1.19, a ordem de a^k divide n. Em outras palavras, a ordem de a^k divide a ordem de a. Por exemplo, suponhamos que $a \in G$ tenha ordem 12. Pela observação feita anteriormente, sabemos que a ordem de qualquer potência de a, digamos a^k, divide a ordem de a, que é 12. Neste sentido é natural pensar que a ordem de a^2 é 6. De fato,

$$(a^2)^1 = a^2, \quad (a^2)^2 = a^4, \quad (a^2)^3 = a^6,$$

$$(a^2)^4 = a^8, \quad (a^2)^5 = a^{10}, \quad (a^2)^6 = a^{12} = e.$$

Isto é, $|a^2| = 6 = \dfrac{12}{2}$.

Mas, de maneira geral, sendo $|a| = n$ será que podemos adotar como regra que $|a^k| = \dfrac{n}{k}$? Infelizmente não, pois, dessa forma teríamos que $|a^8| = \dfrac{12}{8}$, o que nos leva a um absurdo, uma vez que $\dfrac{12}{8} \notin \mathbb{Z}$. Não obstante,

$$(a^8)^1 = a^8, \qquad (a^8)^2 = a^{16} = a^{12}a^4 = a^4, \qquad (a^8)^3 = a^{24} = (a^{12})^2 = e.$$

Portanto, concluímos que de fato $|a^8| = 3 = \dfrac{12}{4}$.

Sendo assim, a pergunta que surge naturalmente é: Já que a ordem de a^k divide $|a|$, então qual é sua ordem? Ou de outra forma, qual é o fator de $|a|$ que é a ordem de a^k? Ou ainda, qual é a correlação entre $|a^k|$ e $|a|$? A resposta para essa pergunta vem através da seguinte proposição.

Proposição 1.21. Sejam G um grupo e $a \in G$. Se $|a| = n$, então $|a^k| = \dfrac{n}{mdc(n,k)}$.

Demonstração: Seja $|a| = n$ e $|a^k| = m$. Observe que:

$$(a^k)^{n/mdc(n,k)} = (a^n)^{k/mdc(n,k)} = e.$$

Isto implica, pelo Lema 1.19, que m divide $\dfrac{n}{mdc(n,k)}$. Por outro lado,

$$a^{km} = (a^k)^m = e,$$

o que, de acordo com o Lema 1.19, nos diz que n divide km. Donde obtemos que $\dfrac{n}{mdc(n,k)}$ divide $\dfrac{km}{mdc(n,k)} = \dfrac{k}{mdc(n,k)}m$. Por fim,

$$mdc\left(\frac{n}{mdc(n,k)}, \frac{k}{mdc(n,k)}\right) = 1,$$

concluímos que $\dfrac{n}{mdc(n,k)}$ divide m. Portanto, $m = \dfrac{n}{mdc(n,k)}$.

■

Corolário 1.22. Sejam G um grupo e $a \in G$ tal que $|a| = n$. Se $k \mid n$, então $|a^k| = \dfrac{n}{k}$.

Demonstração: Se $k \mid n$, então $n = qk$ e $mdc(n,k) = mdc(qk,k) = k$. Pela Proposição 1.21,

$$|a^k| = \frac{n}{mdc(n,k)} = \frac{n}{k}.$$

■

Corolário 1.23. Sejam G um grupo e $a \in G$ tal que $|a| = n$. Se $mdc(n,k) = 1$, então $|a^k| = n$.

Demonstração: Se $mdc(n,k) = 1$, então pela Proposição 1.21,

$$|a^k| = \frac{n}{mdc(n,k)} = n.$$

■

Corolário 1.24. Seja G um grupo. Se $a \in G$ e $|a| = n$, então $|a^{-1}| = n$.

Demonstração: Como $mdc(n,-1) = 1$, é fácil ver que $|a^{-1}| = n$.

■

Exemplo 1.25. Seja $a \in G$ tal que $|a| = 12$. Como $|a^k| = \dfrac{12}{mdc(12,k)}$ temos:

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$mdc(12,k)$	12	1	2	3	4	1	6	1	4	3	2	1	12
$\lvert a^k\rvert$	1	12	6	4	3	12	2	12	3	4	6	12	1

k	-1	-2	-3	-4	-5	-6	-7	-8	-9	-10
$mdc(12,k)$	1	2	3	4	1	6	1	4	3	2
$\lvert a^k\rvert$	12	6	4	3	12	2	12	3	4	6

1.1 Exercícios

1. Em cada item abaixo, considere a operação binária $*$ sobre A e verifique se ela é associativa e se ela é comutativa.

   a) $A = \mathbb{R}$ e $x * y = \dfrac{x+y}{2}$.

   b) $A = \mathbb{Z}$ e $x * y = x + xy$.

   c) $A = \mathbb{R}^*$ e $x * y = \dfrac{x}{y}$.

   d) $A = \mathbb{R}$ e $x * y = x^2 + y^2$.

2. Seja $B = \mathbb{Z} \times \mathbb{Z}$. Considerando as operações a seguir, verifique se elas são associativas e/ou comutativas.

   a) $(a, b) * (x, y) = (ax, 0)$

   b) $(a, b) \circ (x, y) = (a + x, b + y)$

   c) $(a, b) \diamond (x, y) = (a + x, by)$

   d) $(a, b) \oplus (x, y) = (ax - by, ay + bx)$

3. Seja $*$ a operação sobre $\mathbb{Z}$ dada por $a * b = ma + nb$. Que condições devem satisfazer $m, n \in \mathbb{Z}$ de forma que $*$ seja associativa? e para ser comutativa?

4. Considere o grupo $(\mathcal{F}(\mathbb{R}), \circ)$ e seja $f \in \mathcal{F}(\mathbb{R})$ a função dada por $f(x) = 2x + 3$ para todo $x \in \mathbb{R}$. Calcule $f^3 \in \mathcal{F}(\mathbb{R})$.

5. Sejam $n > 1$ um inteiro e $\overline{r} = \{kn + r \mid k \in \mathbb{Z}, 0 \leq r < n\}$. Considerando o conjunto das *classes de restos módulo n* dado por $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$, mostre que as operações $\oplus$ e $\odot$ definidas sobre $\mathbb{Z}_n$ a seguir são associativas e comutativas.

   a) $\overline{x} \oplus \overline{y} = \overline{x + y}$

   b) $\overline{x} \odot \overline{y} = \overline{xy}$

6. Prove que é associativa a operação $*$ sobre $\mathbb{Z}^3$ dada por:

$$(a, b, c) * (x, y, z) = (ax, by, cz).$$

7. Mostre que a multiplicação de matrizes 2×2 sobre o conjunto dos números reais é associativa, mas não comutativa.

8. Mostre que o conjunto dos números inteiros positivos $\mathbb{Z}^+$ não é fechado sob a operação de subtração usual.

9. Prove que o conjunto G a seguir é um grupo com a operação de multiplicação usual de matrizes.

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}.$$

10. Considere o grupo $(GL_2(\mathbb{R}), \cdot)$. Determine o inverso de $A = \begin{bmatrix} 1 & 3 \\ -2 & -5 \end{bmatrix} \in GL_2(\mathbb{R})$.

11. Mostre que se G é um grupo abeliano, então para todo $a, b \in G$ e para todo $n \in \mathbb{N}$ temos que:

$$(a * b)^n = a^n * b^n.$$

12. Seja G um grupo. Mostre que se $x^2 = e$ para todo $x \in G$, então G é abeliano.

13. Seja G um grupo. Mostre que se $a, b \in G$ e x é uma variável em G, então a equação $x * a = b$ possui uma única solução em G, que é $x = b * a^{-1}$.

14. Mostre que se $(ab)^2 = a^2b^2$ para todo $a, b \in G$, então G é um grupo abeliano.

15. Verifique se $(\mathbb{R}, \otimes)$ é um grupo abeliano, onde $\otimes$ é dada por:

$$a \otimes b = a + b - 3.$$

16. Seja $\mathbb{R}^2$ o produto cartesiano de $\mathbb{R}$ por ele mesmo. Considerando a soma de vetores usual em $\mathbb{R}^2$,

$$(x, y) + (a, b) = (x + a, y + b),$$

verifique se $(\mathbb{R}^2, +)$ é um grupo.

17. Seja S_3 o grupo das permutações dos 3 elementos x_1, x_2 e x_3. Considere as funções ϕ e ψ, dadas como segue:

$$\phi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix} \qquad \text{e} \qquad \psi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}.$$

Mostre que:

a) $\phi^2 = e$.
b) $\psi^3 = e$.
c) $\psi^{-1} = \psi^2$.
d) $\phi\psi = \psi^{-1}\phi$.

18. Sejam $(G, *)$ um grupo e $a \in G$. Mostre que a função $T_a : G \to G$, definida por $T_a(x) = a * x$, é bijetora.

19. Considere o conjunto $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, tal que:

$$ij = k, \quad jk = i, \quad ki = j, \quad kj = -i, \quad ik = -j,$$

$$ji = -k, \quad (\pm i)^2 = (\pm j)^2 = (\pm k)^2 = 1.$$

Mostre que Q_8 é um grupo, chamado de *Grupo dos Quatérnios*.

20. Mostre que $D_3 = \{e, r, r^2, s, rs, r^2s\}$ é um grupo, onde

$$r^3 = e, \quad s^2 = e \quad sr = r^2s.$$

O grupo D_3 é chamado de *Grupo Diedral de Ordem* 3.

21. Mostre que $D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$ é um grupo, onde

$$r^4 = e, \quad s^2 = e, \quad sr = r^3s.$$

O grupo D_4 é chamado de *Grupo Diedral de Ordem* 4.

22. Mostre que $E = \{a + b\sqrt{2} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$ é um grupo multiplicativo abeliano.

23. Seja $\mathcal{P}_n$ o conjunto de todos os polinômios de grau n com variável real x, ou seja, se $p(x) \in \mathcal{P}_n$, então

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0.$$

Mostre que $(\mathcal{P}_n, +)$ é um grupo, onde a operação $+$ é a adição usual dos polinômios.

24. Determine as ordens de $A, B \in GL_2(\mathbb{R})$.

a) $A = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$ b) $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$

25. Determine a ordem de $\eta = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix} \in S_3$.

26. Seja $a \in G$ tal que $|a| = 5$. Determine a $|a^k|$ para $-8 \leq k \leq 8$.

27. Seja G um grupo finito. Mostre que as seguintes condições são equivalentes:

a) Para todo $a \in G$, $a^{|G|} = e$.

b) Para todo $a \in G$, $|a|$ divide $|G|$.

2. Subgrupos

Definição 2.1. Sejam G um grupo e H subconjunto não vazio de G. Dizemos que H é um *subgrupo* de G, e denotamos por $H \leq G$, se, e somente se, H é um grupo com a operação binária de G.

Observe que $\{e\}$ e G são sempre subgrupos de G, chamados de *subgrupos triviais*, e cujo interesse de estudo é diminuto.

Definição 2.2. Dizemos que H é um subgrupo *próprio* ou *não trivial* de G, e denotamos por $H < G$, se H é um subgrupo de G com $H \neq G$ e $H \neq \{e\}$.

Exemplo 2.3. É fácil ver que:

1. $\mathbb{Z} < \mathbb{Q} < \mathbb{R}$ com relação a operação usual de adição.
2. $\mathbb{Q}^* < \mathbb{R}^*$ e $\mathbb{R}^+ < \mathbb{R}^*$ com relação a operação usual de multiplicação.
3. o conjunto de todos os números pares, a saber, $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$, é um subgrupo de $(\mathbb{Z}, +)$.

Na sequência, apresentamos formas de verificar se um determinando subconjunto H de G é um subgrupo de G, sem ter que mostrar que ele por si só é um grupo com a operação de G.

Teorema 2.4. Se H é um subconjunto de um grupo $(G, *)$, então H é um subgrupo de G se, e somente se, as seguintes acontecem:

i) $e \in H$; (elemento neutro de G)

ii) $\forall a \in H \quad \Rightarrow \quad a^{-1} \in H$; (fechado para inverso)

iii) $\forall a, b \in H \quad \Rightarrow \quad a * b \in H$. (fechado para a operação)

Demonstração: ($\Rightarrow$) Suponhamos que $H \leq G$ e mostremos que as condições i), ii) e iii) são satisfeitas. Se e_h é o elemento neutro de H, então $e_h * e_h = e_h$. Além disso, $e_h \in H \subseteq G$, consequentemente, sendo e o elemento neutro de G temos $e * e_h = e_h$. Dessas duas igualdades concluímos que $e * e_h = e_h * e_h$. Portanto, pelo Lema 1.11, vem que $e = e_h \in H$, o que prova a condição i).

Desde que $(H, *)$ é um grupo, temos que H é fechado com relação à operação $*$, ou seja, para todo $a, b \in H$ temos $a * b \in H$. Além disso, temos que para todo $a \in H$ existe o inverso de a em H, isto é, $a^{-1} \in H$. Consequentemente, se verifica as condições ii) e iii).

($\Leftarrow$) Agora suponhamos que as condições i), ii) e iii) são satisfeitas, e provemos que H é um subgrupo de G, ou seja, provemos que $(H, *)$ é um grupo. De fato, de i) temos que $H \neq \emptyset$ e possui elemento neutro, pois, $e \in H$. Por iii) vem que H é fechado com relação à operação $*$. Como a operação $*$ é a mesma operação sobre o grupo G, segue imediatamente que $*$ é uma operação associativa sobre H. Finalmente, por ii), todo elemento de H possui inverso, donde concluímos que H é um grupo.

■

Teorema 2.5. Se H é um subconjunto de um grupo $(G, *)$, então H é um subgrupo de G se, e somente se, as seguintes acontecem:

i) $H \neq \emptyset$;

ii) $\forall a, b \in H \quad \Rightarrow \quad a * b^{-1} \in H$.

Demonstração: ($\Rightarrow$) Suponhamos que H é um subgrupo de G. Pelo Teorema 2.4 sabemos que $e \in H$, ou seja, $H \neq \emptyset$. Além disso, para todo $b \in H$ temos que $b^{-1} \in H$. Sendo assim, para todo $a, b \in H$ vem que $a, b^{-1} \in H$, donde concluímos que $a * b^{-1} \in H$. Logo, se H é um subgrupo de G, então as condição i) e ii) são satisfeitas.

($\Leftarrow$) Agora suponhamos que as condições i) e ii) são satisfeitas, e provemos que H é um subgrupo de G. Pelo item i) temos que $H \neq \emptyset$, ou seja, existe $a \in H$. Agora pelo item ii) temos:

$$a * a^{-1} \in H \quad \Rightarrow \quad e \in H.$$

Ainda pelo item ii) vem que:

$$\forall a \in H \quad \Rightarrow \quad e * a^{-1} \in H \quad \Rightarrow \quad a^{-1} \in H.$$

Por fim, observando a implicação anterior, para todo $b \in H$ temos que $b^{-1} \in H$. Dessa forma,

$$\forall a, b \in H \quad \Rightarrow \quad a, b^{-1} \in H \quad \Rightarrow \quad a * (b^{-1})^{-1} \in H \quad \Rightarrow \quad a * b \in H.$$

Portanto, pelo Teorema 2.4, H é um subgrupo de G.

■

Daqui em diante, por uma questão de simplicidade e sem prejuízo, usaremos a notação ab, em vez de $a * b$, para representar a operação entre dois elementos quaisquer de um grupo qualquer, com uma operação qualquer. Porém, sempre que houver a possibilidade de uma interpretação dúbia, ou se fazer necessário, recorremos à explicitação da operação envolvida.

Na sequência, apresentamos "roteiros" com intuito de fornecer uma orientação de como provar ou não, que determinando subconjunto H de um grupo G é um subgrupo ou não.

De acordo com o Teorema 2.4, para provar que um subconjunto não vazio H de um grupo G é um subgrupo de G, é necessário e suficiente que se verifique *todas* as seguintes:

i) Mostre que o elemento neutro de G pertence a H.

ii) Assuma que $a \in H$ e mostre que $a^{-1} \in H$.

iii) Assuma que $a, b \in H$ e mostre que $ab \in H$.

Já de acordo com o Teorema 2.5, para provar que um subconjunto não vazio H de um grupo G é um subgrupo de G, é necessário e suficiente que *todas* as seguintes sejam verdadeiras:

i) Mostre que H não é vazio. Em particular, mostre que o elemento neutro de G pertence a H.

ii) Assuma que $a, b \in H$ e mostre que $ab^{-1} \in H$.

Por outro lado, para provar que um subconjunto não vazio H de um grupo G *não é um subgrupo* de G, é necessário e suficiente que *apenas uma* das seguintes se verifique:

i) Mostre que o elemento neutro de G não pertence a H.

ii) Ou encontre um elemento $a \in H$ e mostre que $a^{-1} \notin H$.

iii) Ou encontre dois elementos $a, b \in H$ e mostre que $ab \notin H$.

Exemplo 2.6.

1. Considere o grupo $(\mathbb{R}^*, \cdot)$ e $\mathbb{R}^*_+ = \{x \in \mathbb{R} \mid x > 0\}$. Afirmamos que $\mathbb{R}^*_+$ é um subgrupo de $\mathbb{R}^*$. De fato, pois,

   i) Como $1 > 0$ temos que $1 \in \mathbb{R}^*_+$, ou seja, $\mathbb{R}^*_+ \neq \emptyset$.

   ii) Para todo $b \in \mathbb{R}^*_+$ temos que $b > 0$. Portanto, $b^{-1} = \dfrac{1}{b} > 0$ e

   $$\forall a, b \in \mathbb{R}^*_+ \;\Rightarrow\; a > 0 \text{ e } b^{-1} > 0 \;\Rightarrow\; ab^{-1} > 0 \;\Rightarrow\; ab^{-1} \in \mathbb{R}^*_+.$$

   Consequentemente, pelo Teorema 2.5, $\mathbb{R}^*_+ \leq \mathbb{R}^*$.

2. O conjunto dos números inteiros pares $2\mathbb{Z} = \{\ldots, -2, 0, 2, 4, \ldots\}$ é um subgrupo de $(\mathbb{Z}, +)$. De fato, a identidade de $\mathbb{Z}$ é o 0, e seguramente $0 \in 2\mathbb{Z}$. A soma de dois números inteiros pares é um número inteiro par, assim $2\mathbb{Z}$ é fechado para a adição de inteiros. Por fim, se $x \in 2\mathbb{Z}$, isto é, x é um inteiro par, então o seu inverso aditivo $-x$ também é um número inteiro par, que é $-x \in 2\mathbb{Z}$. Portanto, $2\mathbb{Z} \leq \mathbb{Z}$.

3. O subconjunto $\mathbb{N}$ de $\mathbb{Z}$ não é um subgrupo de $(\mathbb{Z}, +)$, pois, $\mathbb{N}$ não contém todos os inversos de seus elementos. Neste sentido, e pelo mesmo motivo, $\mathbb{N}$ não é um subgrupo de $\mathbb{Q}^*$ com relação à operação de multiplicação.

4. Seja $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z} \right\}$. Afirmamos que $H \leq GL_2(\mathbb{R})$.

   De fato,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H \qquad \text{e} \qquad \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} \in H.$$

   Além disso,

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n+m \\ 0 & 1 \end{bmatrix} \in H.$$

   Portanto, pelo Teorema 2.4, $H \leq GL_2(\mathbb{R})$.

5. O conjunto $SL_2(\mathbb{R})$, de toda matriz 2×2 com determinante igual a 1, é subgrupo de $GL_2(\mathbb{R})$ com a multiplicação usual de matrizes. De fato,

$$SL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \quad \text{e} \quad ad - bc = 1 \right\}.$$

   Uma vez que $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ pertence a $SL_2(\mathbb{R})$, temos $SL_2(\mathbb{R}) \neq \emptyset$.

   Além disso, $SL_2(\mathbb{R})$ é fechado para a multiplicação usual de matrizes. Verdade, se $A, B \in SL_2(\mathbb{R})$, então $AB \in SL_2(\mathbb{R})$, pois,

$$det(AB) = det(A)det(B) = 1.1 = 1.$$

   Por fim, $SL_2(\mathbb{R})$ é fechado para inverso, pois, se $A \in SL_2(\mathbb{R})$, então $det(A) \neq 0$. Consequentemente, existe A^{-1} e

$$det(A^{-1}) = \frac{1}{det(A)} = \frac{1}{1} = 1.$$

   Portanto, $SL_2(\mathbb{R})$ é subgrupo de $GL_2(\mathbb{R})$.

Lema 2.7. Seja G um grupo, $H \leq G$ e $K \leq G$. Então $H \cap K \leq G$.

Demonstração: Como $H \leq G$ e $K \leq G$ temos que $e \in H$ e $e \in K$, ou seja, $e \in H \cap K$. Consequentemente, $H \cap K \neq \emptyset$. Agora suponhamos que $a, b \in H \cap K$, ou seja, $a, b \in H$ e $a, b \in K$. Uma vez que por hipótese $H \leq G$ e $K \leq G$ temos que $ab^{-1} \in H$ e $ab^{-1} \in K$, isto é, $ab^{-1} \in H \cap K$. Portanto, pelo Teorema 2.5, $H \cap K \leq G$.

■

Na verdade, o Lema 2.7 é verdadeiro para uma família qualquer $\{H_a\}_{a \in A}$ de subgrupos de um grupo G. Por outro lado, se $H, K \leq G$, então $H \cup K$ não é necessariamente um subgrupo de G, como mostra o exemplo a seguir.

Exemplo 2.8. Seja o grupo $\mathbb{Z}$ com a operação adição usual. Temos que,

$$2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\} \leq \mathbb{Z} \qquad \text{e} \qquad 3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\} \leq \mathbb{Z}.$$

No entanto,

$$2\mathbb{Z} \cup 3\mathbb{Z} \not\leq \mathbb{Z}.$$

De fato, por exemplo,

$$2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z},$$

ou seja, $2\mathbb{Z} \cup 3\mathbb{Z}$ não é fechado para a operação adição.

Definição 2.9. Seja G um grupo e $a \in G$. Definimos o conjunto *gerado por* a, denotado por $\langle a \rangle$, como sendo o conjunto de todas as potências inteiras de a, ou seja,

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

Exemplo 2.10. Considere o grupo $(\mathbb{R}^*, \cdot)$ e $-2, -1 \in \mathbb{R}^*$. Assim temos:

1. $\langle -2 \rangle = \{(-2)^n \mid n \in \mathbb{Z}\} = \left\{\ldots, -\frac{1}{8}, -\frac{1}{4}, -\frac{1}{2}, 1, -2, 4, -8, 16, \ldots\right\}$.
2. $\langle -1 \rangle = \{(-1)^n \mid n \in \mathbb{Z}\} = \{-1, 1\}$.

Lema 2.11. Seja G um grupo e $a \in G$. Então $\langle a \rangle$ é um subgrupo abeliano de G, chamado de *subgrupo cíclico gerado por a*.

Demonstração: Claramente $\langle a \rangle \neq \emptyset$, pois, $a = a^1 \in \langle a \rangle$. Agora, se $x, y \in \langle a \rangle$, então por definição temos que $x = a^n$ e $y = a^m$ para algum $n, m \in \mathbb{Z}$. Sendo assim, temos:

$$xy^{-1} = a^n(a^m)^{-1} = a^n a^{-m} = a^{n-m} \in \langle a \rangle.$$

Finalmente,

$$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx.$$

Portanto, $\langle a \rangle$ é um subgrupo abeliano G.

■

Proposição 2.12. Seja G um grupo. Se $a \in G$ e $|a| = n$, então:

1. $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.
2. $|\langle a \rangle| = n$.

Demonstração: Note que para mostrar a primeira afirmação é suficiente mostrar que $\langle a \rangle \subset \{e, a, a^2, \ldots, a^{n-1}\}$, isto porque $\{e, a, a^2, \ldots, a^{n-1}\} \subset \langle a \rangle$.

Seja $|a| = n$ e considere uma potência qualquer de a, digamos a^k. Pelo algoritmo da divisão de Euclides existem inteiros q e r tais que $k = qn + r$ onde $0 \leq r < n$. Logo,

$$a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = a^r,$$

ou seja, toda potência $a^k \in \langle a \rangle$ é igual a alguma potência a^r, onde $0 \leq r < n$, isto é, $a^k \in \{e, a, a^2, \ldots, a^{n-1}\}$. Portanto, $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

Por fim, para mostrar a segunda afirmação, ou seja, mostrar que $|\langle a \rangle| = n$, é suficiente mostrar que todos os elementos do conjunto $\{e, a, a^2, \ldots, a^{n-1}\}$ são distintos. Para isto, por contradição, suponhamos que existem duas potências iguais no conjunto $\{e, a, a^2, \ldots, a^{n-1}\}$, que é,

$$a^i = a^j \qquad \text{com} \qquad 1 \leq i < j < n.$$

Donde obtemos, $a^{j-i} = e$. Como $0 < j - i < n$ temos uma contradição, pois, n é o menor inteiro tal que $a^n = e$. Portanto, todos os elementos do conjunto $\{e, a, a^2, \ldots, a^{n-1}\}$ são distintos e concluímos que $|\langle a \rangle| = n$. ■

Definição 2.13. Um grupo G é chamado *cíclico* se, e somente se, existe $a \in G$ tal que $G = \langle a \rangle$. Neste caso, diz-se que G *é cíclico gerado por* a.

Exemplo 2.14. Seja o grupo $(\mathbb{Z}, +)$ e $1 \in \mathbb{Z}$. Então $\mathbb{Z}$ é um grupo cíclico gerado por 1, ou seja, $\mathbb{Z} = \langle 1 \rangle$. De fato, com a operação adição temos que $a^n = \underbrace{a + a + \cdots + a}_{n} = n.a$, ou seja:

$$\begin{array}{lll} 0 = 0.1 = 1^0 & 4 = 4.1 = 1^4 & 8 = 8.1 = 1^8 \\ 1 = 1.1 = 1^1 & 5 = 5.1 = 1^5 & \vdots \\ 2 = 2.1 = 1^2 & 6 = 6.1 = 1^6 & n = n.1 = 1^n \\ 3 = 3.1 = 1^3 & 7 = 7.1 = 1^7 & \vdots \end{array}$$

Não obstante, $\mathbb{Z}$ também é um grupo cíclico gerado por -1, ou seja, $\mathbb{Z} = \langle -1 \rangle$, donde podemos concluir que um grupo pode ter mais de um gerador.

Lema 2.15. Todo subgrupo de um grupo cíclico é cíclico.

Demonstração: Seja $G = \langle a \rangle$ um grupo cíclico. Se $H \leq G$, então existem duas posibilidades, que é: H é um subgrupo trivial, ou seja, $H = \{e\}$ ou $H = G$. Em qualquer um desses casos temos que H é cíclico. A outra possibilidade é H ser um subgrupo próprio de G, ou seja, $H \neq \{e\}$ e $H \neq G$. Neste caso, existe um inteiro positivo mínimo n tal que $a^n \in H$. Claramente, temos que $\langle a^n \rangle \subseteq H$. Por outro lado, se $h \in H$, então h é da forma a^m, pois H é um subgrupo de G. Pelo algoritmo da divisão de Euclides existem inteiros q e r tais que:

$$a^m = a^{nq+r} = a^{nq}a^r, \quad \text{com} \quad 0 \leq r < n,$$

ou seja,

$$a^r = a^{-nq}a^m \in H.$$

Dessa forma, somente podemos ter $r = 0$, já que supomos que n é o menor menor inteiro positivo para o qual $a^n \in H$. Assim todo elemento $h \in H$ é da forma $a^{qn} = (a^n)^q$, o que nos leva a concluir que $H \subseteq \langle a^n \rangle$. Consequentemente, temos $H = \langle a^n \rangle$ e, portanto, H é cíclico.

■

Definição 2.16. Seja G um grupo. O *centro* de G, denotado por $Z(G)$, é o conjunto de todos os elementos $a \in G$ tal que a comuta com todo elemento de G. De outra forma,

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

Note que $Z(G)$ é sempre não vazio. De fato, desde que $ex = xe$ para todo $x \in G$, temos que $e \in Z(G)$, ou seja, $Z(G) \neq \emptyset$. Além disso, é fácil ver que o centro $Z(G)$ é sempre abeliano.

Exemplo 2.17. Vamos determinar o centro do grupo $GL_2(\mathbb{R})$ de todas as matrizes 2×2 inversíveis. Para isto, vamos supor que $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Z(GL_2(\mathbb{R}))$. Dessa forma, a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ comuta com *todas* as matrizes pertencentes a $GL_2(\mathbb{R})$. Em outras palavras, para *toda* matrix $\begin{bmatrix} x & y \\ z & w \end{bmatrix} \in GL_2(\mathbb{R})$ temos:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} x & y \\ z & w \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Donde obtemos,

$$\begin{bmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{bmatrix} = \begin{bmatrix} ax+cy & bx+dy \\ az+cw & bz+dw \end{bmatrix}.$$

Note que da igualdade anterior devemos ter:

$$ax + bz = ax + cy \quad \Rightarrow \quad bz = cy.$$

Como $b, c \in \mathbb{R}$ são fixos e a escolha de $y, z \in \mathbb{R}$ é arbitrária, a única forma da igualdade $bz = cy$ ser verdadeira para todo $y, z \in \mathbb{R}$ é fazendo $b = 0$ e $c = 0$. Daí, consequentemente,

$$ay + bw = bx + dy \quad \Rightarrow \quad ay = dy \quad \Rightarrow \quad a = d.$$

Portanto, o centro de $GL_2(\mathbb{R})$ é dado por:

$$Z(GL_2(\mathbb{R})) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \neq 0 \right\}.$$

Lema 2.18. Se G é um grupo, então $Z(G)$ é um subgrupo de G.

Demonstração: Claramente, $Z(G) \neq \emptyset$, pois, $e \in Z(G)$. Também, se $g \in Z(G)$, então $g^{-1} \in Z(G)$. Isto porque, para todo $x \in G$ temos:

$$g^{-1}x = g^{-1}xe = g^{-1}(xg)g^{-1} = g^{-1}(gx)g^{-1} = exg^{-1} = xg^{-1}.$$

Agora, se $a, b \in Z(G)$, então $ab^{-1} \in Z(G)$. De fato, se $a, b \in Z(G)$, então para todo $x \in G$ temos:

$$ax = xa \qquad \text{e} \qquad bx = xb.$$

Além disso, como vimos anteriormente, ambos a^{-1} e b^{-1} pertencem ao $Z(G)$. Sendo assim,

$$(ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}).$$

Portanto, $Z(G)$ é um subgrupo de G.

■

Definição 2.19. Seja G um grupo e $x \in G$. O *centralizador* de x em G, denotado por $C_G(x)$, é o conjunto de todos os elementos $x \in G$ tal que a comuta com x. Em outras palavras,

$$C_G(x) = \{a \in G \mid ax = xa\}.$$

Exemplo 2.20. Sendo $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \in GL_2(\mathbb{R})$, vamos determinar o $C_{GL_2(\mathbb{R})}(A)$. Por definição, uma matriz $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C_{GL_2(\mathbb{R})}(A)$ se, e somente se, $AB = BA$, a saber:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Donde obtemos,

$$\begin{bmatrix} a & 2b \\ c & 2d \end{bmatrix} = \begin{bmatrix} a & b \\ 2c & 2d \end{bmatrix}.$$

Esta última igualdade é verdadeira se, e somente se, $2b = b$ e $c = 2c$, isto é, se, e somente se, $b = 0$ e $c = 0$. Portanto,

$$C_{GL_2(\mathbb{R})}(A) = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \mid a, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

Lema 2.21. Seja G um grupo. Se $x \in G$, então $C_G(x)$ é um subgrupo de G.

Demonstração: É fácil ver que $e \in C_G(x)$, ou seja, $C_G(x) \neq \emptyset$. Agora, se $g \in C_G(x)$, então $g^{-1} \in C_G(x)$, pois,

$$g^{-1}x = g^{-1}xe = g^{-1}(xg)g^{-1} = g^{-1}(gx)g^{-1} = exg^{-1} = xg^{-1}.$$

Por fim, se $a, b \in C_G(x)$, então $ab^{-1} \in C_G(x)$. De fato,

$$(ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}).$$

Portanto, $C_G(x)$ é um subgrupo de G.

■

2.1 Exercícios

1. Verifique se $H_2 = \{1, 2, 3, 4, 5, 6, \ldots\} \subseteq \mathbb{Z}$, o conjunto dos números inteiros positivos, é um subgrupo de $(\mathbb{Z}, +)$. E o que podemos dizer sobre o conjunto $H_3 = \{\ldots, -3, -1, 1, 3, 5, 7, \ldots\} \subseteq \mathbb{Z}$?

2. É verdade que $\mathbb{Q} \leq \mathbb{R}$? Justifique sua resposta!

3. Mostre que $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ é um subgrupo de $\mathbb{Z}$ com a operação de adição usual.

4. Seja S_3 o grupo das permutações dos 3 elementos x_1, x_2 e x_3. Considere as aplicações ϕ e ψ dadas por:

$$\phi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix} \qquad \psi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}$$

Mostre que $S_3 = \{e, \psi, \psi^2, \phi, \phi\psi, \phi\psi^2\}$. Além disso, mostre que os seguintes são subgrupos de S_3.

$$\begin{array}{lcllcl} H_1 & = & \{e\} & H_4 & = & \{e, \phi\psi^2\} \\ H_2 & = & \{e, \phi\} & H_5 & = & \{e, \psi, \psi^2\} \\ H_3 & = & \{e, \phi\psi\} & H_6 & = & \{e, \psi, \psi^2, \phi, \phi\psi, \phi\psi^2\} \end{array}$$

5. a) Mostre que $GL_2(\mathbb{R})$ é um grupo com a operação de multiplicação de matrizes usual.

   b) Mostre que o conjunto $D = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in \mathbb{R} \quad \text{e} \quad a \neq 0 \right\}$ é um subgrupo de $GL_2(\mathbb{R})$.

   c) Mostre que o conjunto $SL_2(\mathbb{R})$ das matrizes 2×2 cujo determinante é igual a 1, é um subgrupo de $GL_2(\mathbb{R})$.

6. Seja $\mathbb{Q}^*$ o grupo dos números racionais não nulos sob a operação de multiplicação usual, e considere o conjunto

$$H = \left\{ \frac{1}{2^m} \mid m \in \mathbb{Z} \right\}.$$

H é um subgrupo de $\mathbb{Q}^*$?

7. Seja $\mathbb{R}^2$ o produto cartesiano de $\mathbb{R}$ por ele mesmo. Considerando a soma de vetores usual em $\mathbb{R}^2$, ou seja, $(x, y) + (a, b) = (x + a, y + b)$, responda:

   a) $(\mathbb{R}^2, +)$ é um grupo?

   b) $A = \{(a, 0) \mid a \in \mathbb{R}\}$ é um subgrupo de $\mathbb{R}^2$?

   c) $B = \{(0, b) \mid b \in \mathbb{R}\}$ é um subgrupo de $\mathbb{R}^2$?

   d) $A \cup B$ é um subgrupo de $\mathbb{R}^2$?

8. Verifique se:

   a) $\left\{ \dfrac{1+2m}{1+2n} \mid m, n \in \mathbb{Z} \right\}$ é um subgrupo de $(\mathbb{Q}^*, \cdot)$.

   b) $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$ é um subgrupo de $(\mathbb{Q}^* \setminus \{1\}, *)$, onde $x * y = x + y - xy$.

   c) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ é um subgrupo de $(\mathbb{R}, +)$.

   d) $\{a + b\sqrt{2} \in \mathbb{R}^* \mid a, b \in \mathbb{Q}\}$ é um subgrupo de $(\mathbb{R}^*, \cdot)$.

   e) $\left\{ \begin{bmatrix} cos(x) & sen(x) \\ -sen(x) & cos(x) \end{bmatrix} \mid x \in \mathbb{R} \right\}$ é subgrupo de $(GL_2(\mathbb{R}), \cdot)$.

9. Seja G o grupo dos números reais não nulos com a operação de multiplicação usual. Verifique se o conjunto H dado a seguir é um subgrupo de G.

$$H = \{x \in G \mid x = 1 \text{ ou } x \text{ é um número irracional}\}.$$

10. Considere o grupo $\mathbb{Q}^*$ com a operação multiplicação usual, e o conjunto $\mathbb{Q}_+^* = \{x \in \mathbb{Q} \mid x > 0\}$ de todos os racionais positivos. Podemos afirmar que $\mathbb{Q}_+^*$ é um subgrupo de $\mathbb{Q}^*$?

11. Mostre que:

    a) o grupo aditivo dos inteiros $\mathbb{Z}$ é cíclico gerado pelo número -1.

    b) o grupo multiplicativo $G = \{-1, 1, -i, i\}$ é cíclico gerado por i, com $i^2 = -1$.

    c) o grupo multiplicativo $G = \{-1, 1, -i, i\}$ é cíclico gerado por $-i$, onde $i^2 = -1$.

    d) o grupo aditivo $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ é cíclico gerado por 2.

    e) o grupo aditivo $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ é cíclico gerado por n.

    f) o grupo aditivo $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ é cíclico gerado por $-n$.

12. Seja $\{H_a\}_{a \in A}$ uma família de subgrupos de um grupo G. Mostre que a interseção $H = \cap_{a \in A} H_a$, da família de subgrupos $\{H_a\}_{a \in A}$, ainda é um subgrupo.

13. Seja $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. Mostre que $Z = \{1, -1\}$ é um subgrupo de Q_8.

14. Mostre que $Z(S_3) = \{e\}$.

15. Mostre que se G é abeliano, então $Z(G) = G$.

16. Sejam G um grupo e S um subconjunto de G. Considere os seguintes conjuntos:

    a) $S^{-1} = \{a^{-1} \mid a \in S\}$.

    b) $\langle S \rangle = \{a_1 a_2 a_3 \cdots a_n \mid n \in \mathbb{N},\ a_i \in S \text{ ou } a_i \in S^{-1}\}$.

    Mostre que o conjunto $\langle S \rangle$ é um subgrupo de G, chamado de *Subgrupo gerado por S*.

17. Seja $G = GL_2(\mathbb{R})$ com a multiplicação de matrizes usual. Determine $C_G(x)$, onde

$$x = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

18. Prove que se G é um grupo e $x \in G$, então $Z(G) \leq C_G(x)$.

19. Prove que o grupo G é abeliano se, e somente se, $G = C_G(x)$ para todo $x \in G$.

3. Homomorfismo de Grupos e Aplicações

Definição 3.1. Sejam $(G, *)$ e $(H, \otimes)$ grupos.

1. Uma aplicação $f : G \to H$ é um *homomorfismo* se, e somente se,
$$\forall a, b \in G,\ f(a * b) = f(a) \otimes f(b).$$
2. Uma aplicação $f : G \to H$ é um *isomorfismo* se, e somente se, f é um homomorfismo bijetor. Neste caso, dizemos que G e H são grupos isomorfos e denotamos por $G \cong H$.

Exemplo 3.2.

1. Sejam os grupos $G = (\mathbb{R}_+^*, \cdot)$ e $H = (\mathbb{R}, +)$. Defina a aplicação $f : G \to H$ por $f(x) = log(x)$. A aplicação f assim definida é um homomorfismo. De fato, para todo $x, y \in \mathbb{R}_+^*$ temos:
$$f(xy) = log(xy) = log(x) + log(y) = f(x) + f(y).$$
2. Os grupos $G = (\mathbb{R}, +)$ e $H = (\mathbb{R}^+, \cdot)$ são isomorfos. De fato, a aplicação $f : G \to H$ definida por $f(x) = 2^x$ é um isomorfismo, pois:
   i) a aplicação f é um homomorfismo.
   $$f(x + y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y).$$
   ii) a aplicação f é injetora.
   $$\forall x, y \in G,\ f(x) = f(y) \quad \Rightarrow \quad 2^x = 2^y \quad \Rightarrow \quad x = y.$$
   iii) a aplicação f é sobrejetora.
   $$\forall y \in H \quad \Rightarrow \quad \exists\, x = log_2(y) \in G : \quad f(x) = 2^{log_2(y)} = y.$$
3. Obviamente, por definição, todo isomorfismo é um homomorfismo. No entanto, nem todo homomorfismo é um isomorfismo. De fato, seja $\psi : \mathbb{Z}_6 \to \mathbb{Z}_6$ dada por:
$$\psi(\overline{x}) = \overline{2x}.$$
A aplicação ψ assim definida é um homomorfismo, pois
$$\psi(\overline{x + y}) = \overline{2(x + y)} = \overline{2x + 2y} = \overline{2x} + \overline{2y} = \psi(\overline{x}) + \psi(\overline{y}).$$
Porém, a aplicação ψ não é bijetiva, pois, ψ não é sobrejetiva, uma vez que:
$$\psi(\mathbb{Z}_6) = \{\overline{0}, \overline{2}, \overline{4}\}.$$

Definição 3.3. Seja G um grupo.

1. Uma aplicação $\phi : G \to G$ é um *endomorfismo* se, e somente se, ϕ é um homomorfismo.

2. Uma aplicação $\phi : G \to G$ é um *automorfismo* se, e somente se, ϕ é um isomorfismo.

Exemplo 3.4.

1. A aplicação $\phi : (\mathbb{R}, +) \to (\mathbb{R}, +)$ definida por $\phi(x) = x^3$ não é um automorfismo. De fato, apesar de ϕ ser bijetiva, ϕ não é um homomorfismo, pois existem números reais x e y tais que

$$(x + y)^3 \neq x^3 + y^3.$$

   ou seja,

$$\phi(x + y) \neq \phi(x) + \phi(y).$$

2. A aplicação $\eta : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ definida por $\eta(x) = x^3$ é um automorfismo. De fato, a aplicação η é um homomorfismo, pois para todo $x, y \in \mathbb{R}^*$ temos

$$\eta(xy) = (xy)^3 = x^3y^3 = \eta(x)\eta(y).$$

   Além disso, a aplicação η é bijetora, pois para todo $y \in \mathbb{R}^*$ a equação $\eta(x) = y$ possui uma única solução, que é $x = \sqrt[3]{y}$. Logo, η é um automorfismo sobre $\mathbb{R}^*$.

Na sequência, omitiremos a indicação da operação dos grupos. No entanto, sendo $(G, *)$ e $(H, \otimes)$ grupos, e a aplicação $f : G \to H$, fica subentendido que quando escrevemos $f(ab)$ a operação aplicada entre ab é a operação $*$ de G, domínio da aplicação f. Da mesma forma, que a operação aplicada entre $f(a)f(b)$ é a operação $\otimes$ de H, contradomínio da aplicação f.

Lema 3.5. Sejam G e H grupos, e $f : G \to H$ um homomorfismo. Então:

1. $f(e_{_G}) = e_{_H}$ onde $e_{_G} \in G$, $e_{_H} \in H$ são os elementos neutros.
2. $f(a^{-1}) = f(a)^{-1}$ para todo $a \in G$.
3. $f(a^n) = f(a)^n$ para todo $n \in \mathbb{Z}$.

Demonstração: Sejam $e_{_G}$ e $e_{_H}$ os respectivos elementos neutros de G e H. Se $a \in G$, $n \in \mathbb{Z}$, e $f : G \to H$ é um homomorfismo, então:

1. $f(e_{_G}) = e_{_H}$. De fato, $\quad f(e_{_G}) = f(e_{_G}e_{_G}) = f(e_{_G})f(e_{_G})$.
   Logo, como $f(e_{_G}) \in H$, pelo Lema 1.7 vem que $f(e_{_G}) = e_{_H}$.

2. $f(a^{-1}) = f(a)^{-1}$. De fato, $\; f(a)f(a^{-1}) = f(aa^{-1}) = f(e_{_G}) = e_{_H}$.
   Consequentemente, pela unicidade do elemento inverso vem que $f(a)^{-1} = f(a^{-1})$.

3. $f(a^n) = f(a)^n$. De fato,

$$f(a^n) = f(\underbrace{aa\cdots a}_{n}) = \underbrace{f(a)f(a)\cdots f(a)}_{n} = f(a)^n.$$

■

Geralmente, os algebristas não fazem qualquer distinção entre grupos isomorfos. Em outras palavras, não se preocupam com a natureza dos elementos que compõem os grupos, mas apenas com a forma como eles se operam. Neste sentindo, como mostra o lema a seguir, não fazemos nenhuma distinção entre um grupo cíclico infinito e o grupo aditivo dos inteiros, a menos possivelmente da natureza de seus elementos.

Lema 3.6. Todo grupo cíclico infinito é isomorfo ao grupo aditivo dos inteiros.

Demonstração: Seja G um grupo cíclico infinito, ou seja, existe $a \in G$ tal que $G = \langle a \rangle$. Defina $f : \mathbb{Z} \to G$ por $f(n) = a^n$. A aplicação f é um homomorfismo:

$$f(n+m) = a^{n+m} = a^n a^m = f(n) + f(m).$$

Por outro lado,

$$f(n) = f(m) \quad \Rightarrow \quad a^n = a^m.$$

Como G é um grupo cíclico infinito gerado por a, então todas as potências de a são distintas, o que nos leva a concluir que $a^n = a^m$ se, e só se, temos $n = m$. Isto é, f é injetiva. Que f é sobrejetiva é fácil ver. Logo, a aplicação f é um isomorfismo e, portanto, $G \cong \mathbb{Z}$.

■

Lema 3.7. Seja G um grupo cíclico finito de ordem n. Então, $G \cong \mathbb{Z}_n$.

Demonstração: Sejam $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$ e G um grupo cíclico gerado por a, isto é,

$$G = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Considere a aplicação $\phi : \mathbb{Z}_n \to G$ dada por $\phi(\overline{m}) = a^m$. Afirmamos que ϕ assim definida é um isomorfismo. De fato, a aplicação ϕ é injetora, pois,

$$\phi(\overline{r}) = \phi(\overline{s}) \;\Rightarrow\; a^r = a^s \;\Rightarrow\; a^{r-s} = e \;\Rightarrow\; n \mid (r-s) \;\Rightarrow\; r \equiv s(mod\ n).$$

Donde concluímos que $\overline{r} = \overline{s}$. Obviamente, ϕ é sobrejetora. Resta então mostrar que ϕ é um homomorfismo. Note que:

$$\phi(\overline{r} + \overline{s}) = \phi(\overline{r+s}) = a^{r+s} = a^r a^s = \phi(\overline{r})\phi(\overline{s}).$$

Portanto, ϕ é um isomorfismo e, consequentemente, $G \cong \mathbb{Z}_n$.

■

Note que para mostrar que dois grupos G e H são isomorfos, basta seguir os seguintes passos, não necessariamente na ordem:

i) Defina uma aplicação $f : G \to H$.

ii) Mostre que f é injetora.

iii) Mostre que f é sobrejetora.

iv) Mostre que f é um homomorfismo.

Não obstante, seguindo a linha de pensamento dos algebristas, quando desejamos mostrar que dois grupos *não* são isomorfos, uma das formas é encontrar uma propriedade algébrica que seria preservada pela existência de qualquer isomorfismo entre os dois grupos, mas que é satisfeita somente por um dos grupos envolvidos. Por exemplo, se há um isomorfismo entre dois grupos e um deles é abeliano, então o outro tem por obrigação ser também abeliano, como mostramos a seguir.

Lema 3.8. Sejam G e H grupos, e $f : G \to H$ um isomorfismo. Se G é abeliano, então H é abeliano.

Demonstração: Se G é um grupo abeliano, então para todo $a, b \in G$ temos $ab = ba$. Sendo assim,

$$f(ab) = f(ba) \quad \Rightarrow \quad f(a)f(b) = f(b)f(a),$$

ou seja, para todo $a, b \in G$ vem que $f(a)f(b) = f(b)f(a)$. Como f é bijetora concluímos que H é abeliano.

■

Em geral, um homomorfismo de grupo $f : G \to H$ envia subgrupos de G em subgrupos de H, como mostra o Lema 3.9 a seguir. Mas antes relembremos que dados dois conjuntos G e H, e uma aplicação $f : G \to H$, o conjunto *imagem de* f, denotado por $Im(f)$, é dado por:

$$Im(f) = \{y \in H \mid y = f(x) \text{ para algum } x \in G\}.$$

Além disso, dado $S \subseteq G$, a imagem de S por f, denotada por $f(S)$, é:

$$f(S) = \{f(x) \mid x \in S\}.$$

Também, sendo $E \subseteq H$, a *imagem inversa* de E por f, denotada por $f^{-1}(E)$, é o subconjunto de G dado por:

$$f^{-1}(E) = \{x \in G \mid f(x) \in E\}.$$

Lema 3.9. Sejam G e H grupos, S um subgrupo de G, e $f : G \to H$ um homomorfismo. Então, $f(S)$ é um subgrupo de H. Em particular, $Im(f) = f(G)$ é um subgrupo de H.

Demonstração: Sejam $e_{_G}$ e $e_{_H}$ os respectivos elementos neutros de G e H. Como S é um subgrupo de G temos que $e_{_G} \in S$. Logo, sendo

$$f(S) = \{f(x) \mid x \in S\},$$

temos que:

1. $f(e_{_G}) = e_{_H} \in f(S)$, ou seja, $f(S) \neq \emptyset$.
2. Para todo $x, y \in f(S)$ existem $a, b \in S$ tal que $f(a) = x$ e $f(b) = y$. Como S é um subgrupo de G temos que $ab^{-1} \in S$, consequentemente,

$$xy^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) \in S.$$

Portanto, $f(S)$ é um subgrupo de H.

■

Lema 3.10. Sejam G e H grupos, e $f : G \to H$ um homomorfismo. Se f é injetiva, então $G \cong Im(f)$.

Demonstração: Pelo Lema 3.9, a $Im(f)$ é um subgrupo de H. Defina a aplicação $\phi : G \to Im(f)$ por $\phi(x) = f(x)$. Como $f : G \to H$ é um homomorfismo, obviamente, ϕ também é um homomorfismo. Além disso, como f é injetora e sobrejetora de G em $Im(f)$, vemos claramente que ϕ é bijetora. Portanto, ϕ é um isomorfismo e $G \cong Im(f)$.

■

Lema 3.11. Seja G um grupo cíclico gerado por a. Se $\phi : G \to H$ é um homomorfismo de grupos, então para todo $x \in G$, $\phi(x)$ é completamente determinado por $\phi(a)$.

Demonstração: Para todo $x \in G = \langle a \rangle$ temos $x = a^k$, para algum $k \in \mathbb{Z}$. Logo, $\phi(x) = \phi(a^k) = \phi(a)^k$, isto é, todo $\phi(x)$ pode ser escrito como uma potência de $\phi(a)$, como queríamos demonstrar.

■

Na verdade, o Lema 3.11 nos diz que: Se $G = \langle a \rangle$ e $\phi, \psi : G \to H$ são isomorfismos, tais que $\phi(a) = \psi(a)$, então $\phi(x) = \psi(x)$ para todo $x \in G$. Isto é, ϕ e ψ são o mesmo isomorfismo.

Lema 3.12. Sejam G, H e J grupos. Se $g : G \to H$ e $f : H \to J$ são homomorfismos, então $f \circ g : G \to J$ é um homomorfismo.

Demonstração: Sejam $g : G \to H$ e $f : H \to J$ homomorfismos. Então, para todo $a, b \in G$ temos:

$$(f \circ g)(ab) = f(g(ab)) = f(g(a)g(b)) = f(g(a))f(g(b)) = (f \circ g)(a)(f \circ g)(b).$$

Portanto, $f \circ g : G \to J$ é um homomorfismo.

■

Lema 3.13. Se $f : G \to H$ é um isomorfismo, então $f^{-1} : H \to G$ também é um isomorfismo.

Demonstração: Seja $f : G \to H$ um isomorfismo. Como f é bijetora, a inversa $f^{-1} : H \to G$ de f existe e também é bijetora. Logo, nos resta provar apenas que f^{-1} é um homomorfismo de grupos. Sendo assim,

$$\forall x, y \in H \Rightarrow \exists a, b \in G \text{ tal que } x = f(a) \text{ e } y = f(b) \Rightarrow f^{-1}(x) = a \text{ e } f^{-1}(y) = b$$

Portanto, f^{-1} é um homomorfismo pois:

$$f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x)f^{-1}(y)$$

■

Definição 3.14. Sejam G e H grupos, e $f : G \to H$ um homomorfismo. Definimos o *núcleo* de f, denotado por $Ker(f)$, como segue:

$$Ker(f) = \{x \in G \mid f(x) = e_{_H}\}.$$

Exemplo 3.15.

1. Seja $f : \mathbb{Z} \to \mathbb{C}$ dada por $f(n) = i^n$. Lembrando que o elemento neutro de $\mathbb{C}$ é igual a 1 e que $i^2 = -1$, então

$$\begin{aligned} Ker(f) &= \{n \in \mathbb{Z} \mid f(n) = e_{_{\mathbb{C}}}\} \\ &= \{n \in \mathbb{Z} \mid i^n = 1\} \\ &= \{n \in \mathbb{Z} \mid i^n = (-1)^{2m}, \text{ com } m \in \mathbb{Z}\} \\ &= \{n \in \mathbb{Z} \mid i^n = (i^2)^{2m} = i^{4m}, \text{ com } m \in \mathbb{Z}\} \\ &= \{n \in \mathbb{Z} \mid n = 4m, \text{ com } m \in \mathbb{Z}\} \\ &= \{0, \pm 4, \pm 8, \pm 12, \ldots\}. \end{aligned}$$

2. Seja $\phi : \mathbb{Z} \to \mathbb{Z}$ definida por $\phi(x) = 2x$ para todo $x \in \mathbb{Z}$. Claramente, ϕ é um homomorfismo e

$$Ker(\phi) = \{x \in \mathbb{Z} \mid \phi(x) = 0\} = \{x \in \mathbb{Z} \mid 2x = 0\} = \{0\}.$$

O resultado apresentando a seguir é uma ferramenta muito útil para determinar quando um homomorfismo é injetor ou não.

Lema 3.16. Seja $f : G \to H$ um homomorfismo. Então:

1. $Ker(f)$ é um subgrupo de G.
2. f é injetora se, e somente se, $Ker(f) = \{e_{_G}\}$.

Demonstração: Considere $e_{_G}$ e $e_{_H}$ os respectivos elementos neutros de G e H, e $f : G \to H$ um homomorfismo.

1. $Ker(f)$ é um subgrupo de G. De fato, como $f(e_{_G}) = e_{_H}$, vem que $e_{_G} \in Ker(f)$. Além disso, para todo $x, y \in Ker(f)$ temos $f(x) = e_{_H}$ e $f(y) = e_{_H}$, então:

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e_{_H}e_{_H}^{-1} = e_{_H}.$$

   Portanto, $xy^{-1} \in Ker(f)$ e, consequentemente, $Ker(f) \leq G$.

2. ($\Rightarrow$) Suponhamos que f seja injetora. Para todo $x \in Ker(f)$ temos $f(x) = e_{_H}$. Como $f(e_{_G}) = e_{_H}$ vem que $f(x) = f(e_{_G})$. Uma vez que f é injetora injetora, por definição, temos que $x = e_{_G}$. Logo, para todo $x \in Ker(f)$ temos $x = e_{_G}$, ou seja, $Ker(f) = \{e_{_G}\}$.

   ($\Leftarrow$) Suponhamos que $Ker(f) = \{e_{_G}\}$. Sejam $a, b \in G$ tais que $f(a) = f(b)$. Temos que:

$$f(a) = f(b) \quad \Rightarrow \quad f(a)f(b)^{-1} = f(ab^{-1}) = e_{_H} \quad \Rightarrow \quad ab^{-1} \in Ker(f).$$

   Como $Ker(f) = \{e_{_G}\}$, temos que $ab^{-1} = e_{_G}$, o que nos leva a concluir que $a = b$. Portanto, f é injetora e concluímos a demonstração. ∎

Exemplo 3.17.

1. A aplicação $\phi : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ dada por $\phi(x) = |x|$ é um homomorfismo, porém não um isomorfismo. De fato,

$$\phi(xy) = |xy| = |x||y| = \phi(x)\phi(y)$$

   mas

$$Ker(\phi) = \{x \in \mathbb{R}^* \mid \phi(x) = 1\} = \{x \in \mathbb{R}^* \mid |x| = 1\} = \{-1, 1\} \neq \{1\}$$

   Portanto, ϕ não é injetiva, e consequentemente, ϕ não é um isomorfismo.

2. Vimos no Exemplo 3.15 que $\phi : \mathbb{Z} \to \mathbb{Z}$, definida por $\phi(x) = 2x$ para todo $x \in \mathbb{Z}$, é um homomorfismo cujo $Ker(\phi) = \{0\}$. Portanto, ϕ é injetiva.

Um dos principais resultados da Teoria de Grupos é, incontestavelmente, o Teorema de Cayley. Este teorema coloca todos os grupos num mesmo nível, e mostra que estudar o *Grupo das Permutações*, definido na sequência, é de extrema relevância, pois ele mostra que todo grupo é isomorfo a um grupo de permutações. Respondendo assim a seguinte pergunta: De que realmente são formados os grupos abstratos?

Definição 3.18. Seja X um conjunto não vazio. Definimos o *grupo das permutações* sobre X, denotado por S_X, como sendo o conjunto de todas as aplicações bijetoras de X em X munido da operação binária composição de aplicações. Em particular, quando X é finito com n elementos, digamos $X = \{x_1, x_2, x_3, \ldots, x_n\}$, escrevemos S_n em vez de S_X, e chamamos S_n de *Grupo Simétrico de grau n*.

Teorema 3.19 (Teorema de Cayley)**.** Todo grupo é isomorfo a um grupo de permutações.

Demonstração: Seja G um grupo. Para todo $a \in G$ defina a aplicação $T_a : G \to G$ por

$$T_a(x) = ax$$

Como vimos no Exercício 18 do Capítulo **??**, a aplicação T_a é bijetora, ou seja, uma permutação dos elementos de G pela esquerda.

Seja $H = \{T_a \mid a \in G\}$ o conjunto de todas as permutações T_a. Considerando a composição de aplicações, H é um grupo. De fato, para todo $a, b \in G$ temos

$$(T_a \circ T_b)(x) = T_a(T_b(x)) = T_a(bx) = (ab)x = T_{ab}(x).$$

Logo, para todo $x \in G$ temos $(T_a \circ T_b)(x) = T_{ab}(x)$, donde resulta que $T_a \circ T_b = T_{ab}$.

Sendo assim T_e é o elemento neutro de H e, para todo $T_a \in H$, $(T_a)^{-1} = T_{a^{-1}}$. Como a composição de aplicações é associativa, concluímos que H é um grupo.

Agora defina $\phi : G \to H$ como sendo $\phi(a) = T_a$ para todo $a \in G$. Dessa forma, ϕ é um homomorfismo, pois, para todo $a, b \in G$ temos:

$$\phi(ab) = T_{ab} = T_a \circ T_b = \phi(a) \circ \phi(b).$$

Temos também que ϕ é injetora, pois, se $\phi(a) = \phi(b)$, então $T_a = T_b$, em particular, $T_a(e) = T_b(e)$, ou seja, $ae = be$ o que nos leva a concluir que $a = b$. Por fim, pela própria definição de H, ϕ é sobrejetora.

Portanto, ϕ é um isomorfismo e, consequentemente, $G \cong H$, o que conclui a demonstração. ∎

3.1 Exercícios

1. Seja V um espaço vetorial qualquer. Mostre que V é um grupo abeliano com relação a adição usual de vetores.

2. Sejam V e W espaços vetoriais. Considerando a adição usual de vetores, mostre que toda transformação linear $T : V \to W$ é um homomorfismo de grupo.

3. Sejam G, H, I e J grupos. Se $f : G \to I$ e $g : H \to J$ são isomorfismos, então mostre que $\phi : G \times H \to I \times J$ dada por

$$\phi(x, y) = (f(x), g(y)),$$

para todo $(x, y) \in G \times H$, é também um isomorfismo.

4. Seja $H = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mid x \in \mathbb{R} \right\}$. Mostre que:
   (a) $H \leq GL_2(\mathbb{R})$.
   (b) $\mathbb{R} \cong H$.

5. Mostre o Lema 3.8 por contradição.

6. Sejam G e H grupos, e $\phi : G \to H$. Mostre que, se H não é abeliano, então G não é abeliano ou $G \ncong H$.

7. Seja $G = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \mid b, m \in \mathbb{R} \text{ e } m \neq 0 \right\}$. Mostre que:
   (a) $(G, \cdot)$ é um grupo.
   (b) $G \ncong \mathbb{R}^* \times \mathbb{R}$.
   (c) Dado $u \in \mathbb{Z}$, $f_u : G \to \mathbb{R}$ definida por

$$f_u \left(\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \right) = a^u$$

   é um homomorfismo.

8. Seja $\phi : \mathbb{Z} \to \mathbb{Z}$ definida por $\phi(x) = 2x$ para todo $x \in \mathbb{Z}$. Determine $Im(\phi)$.

9. Seja $\phi : \mathbb{Z}_3 \to \mathbb{Z}_6$ definida por $\phi(\overline{x}) = \overline{2x}$. Mostre que ϕ é um homomorfismo e determine $Ker(\phi)$ e $Im(\phi)$.

10. Seja $\psi : \mathbb{Z}_6 \to \mathbb{Z}_3$ definida por $\psi(\overline{x}) = \overline{x}$. Mostre que ϕ é um homomorfismo e determine $Ker(\psi)$ e $Im(\psi)$.

11. Seja $f : G \to H$ umhomomorfismo, e K o núcleo de f, isto é, $K = Ker(f)$. Mostre que para todo $k \in K$ e $x \in G$, temos que $xkx^{-1} \in K$.

12. Seja $\phi : \mathbb{R} \to \mathbb{C}^*$ dada por $\phi(x) = e^{ix}$, para todo $x \in \mathbb{R}$. Mostre que ϕ é um homomorfismo, determine o $Ker(\phi)$ e a $Im(\phi)$.

13. Sejam G um grupo e H um subgrupo de G. Prove que se $a \in G$, então o subconjunto

$$aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ para algum } h \in H\}$$

é um subgrupo de G e $H \cong aHa^{-1}$.

Sugestão: Considere $\phi : G \to G$ dada por $\phi(x) = axa^{-1}$.