grupos cíclicos

Definição. Um grupo G diz-se *cíclico* se

$$(\exists a \in G) \quad G = \langle a \rangle \,,$$

i.e., se existe $a \in G$ tal que

$$(\forall x \in G)\,(\exists n \in \mathbb{Z}) \quad x = a^n.$$

Exemplo 34. O grupo $(\mathbb{Z}, +)$ é cíclico, já que $\mathbb{Z} = \langle 1 \rangle$, pois para todo $n \in \mathbb{Z}$, temos que $n = n \cdot 1$.

Exemplo 35. O grupo $(\mathbb{R}, +)$ não é cíclico. Não existe nenhum real x tal que

$$\forall a \in \mathbb{R},\ \exists n \in \mathbb{Z}: \ a = nx.$$

Exemplo 36. O grupo $(\mathbb{Z}_4, +)$ é cíclico, já que $\mathbb{Z}_4 = \left\langle [1]_4 \right\rangle = \left\langle [3]_4 \right\rangle$. De facto,

$$[0]_4 = 0\,[1]_4 = 0\,[3]_4 \qquad [1]_4 = 1\,[1]_4 = 3\,[3]_4$$
$$[2]_4 = 2\,[1]_4 = 2\,[3]_4 \qquad [3]_4 = 3\,[1]_4 = 1\,[3]_4$$

Exemplo 37. Para qualquer $n \in \mathbb{N}$, temos que $(\mathbb{Z}_n, +)$ é cíclico, já que $\mathbb{Z}_n = \left\langle [1]_n \right\rangle$.

Exemplo 38. O conjunto $G = \{i, -i, 1, -1\}$, quando algebrizado pela multiplicação usual de complexos, é um grupo cíclico. De facto, $G = \langle i \rangle$.

Exemplo 39. O grupo trivial $G = \{1_G\}$ é um grupo cíclico. De facto, $\langle 1_G \rangle = \{1_G\}$.

Proposição. Todo o grupo cíclico é abeliano.

Demonstração. Sejam $G = \langle a \rangle$ e $x, y \in G$. Então, existem $n, m \in \mathbb{Z}$ tais que $x = a^n$ e $y = a^m$. assim,

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

Observação. Observe-se que o recíproco do teorema anterir não é verdadeiro.

Exemplo 40. O grupo 4-Klein é um grupo abeliano. No entanto, não é cíclico, pois $\langle 1_G \rangle = \{1_G\} \neq G$, $\langle a \rangle = \{1_G, a\} \neq G$, $\langle b \rangle = \{1_G, b\} \neq G$ e $\langle c \rangle = \{1_G, c\} \neq G$. Assim, podemos concluir que não existe $x \in G$ tal que $G = \langle x \rangle$.

Teorema. Qualquer subgrupo de um grupo cíclico é cíclico.

Demonstração. Sejam $G = \langle a \rangle$, para algum $a \in G$, e $H < G$.

Se $H = \{1_G\}$, então $H = \langle 1_G \rangle$ e, portanto, H é cíclico.

Se $H \neq \{1_G\}$, então, existe $x = a^n \in G$ $(n \neq 0)$ tal que $x \in H$. Então, H tem pelo menos uma potência positiva de a. Seja d o menor inteiro positivo tal que $a^d \in H$. Vamos provar que $H = \left\langle a^d \right\rangle$:

(i) Por um lado $a^d \in H$, logo $\left\langle a^d \right\rangle \subseteq H$;

(ii) Reciprocamente, seja $y \in H$. Como $y \in G$, $y = a^m$ para algum $m \in \mathbb{Z} \setminus \{0\}$. Então, existem $q, r \in \mathbb{Z}$ com $0 \leq r < d$, tais que

$$y = a^m = a^{dq+r} = a^{qd} a^r.$$

Assim, $a^r = \left(a^d\right)^{-q} a^m \in H$, pelo que $r = 0$. Logo, $a^m = a^{qd} \in \left\langle a^d \right\rangle$, pelo que $H \subseteq \left\langle a^d \right\rangle$. $\square$

Observação. Se o grupo G é cíclico e tem ordem n, isto é, se existe $a \in G$ tal que $G =< a >= \{1_G, a, a^2, ..., a^{n-1}\}$, então, para qualquer divisor positivo k de n, $< a^{\frac{n}{k}} >$ é um subgrupo de G com ordem k.

Exemplo 41. Os subgrupos do grupo cíclico $\mathbb{Z}$ são todos do tipo $n\mathbb{Z}$. De facto, para todo $n \in \mathbb{Z}$, $\langle n \rangle = n\mathbb{Z}$.

Observação. Resulta da definição de grupo cíclico que qualquer elemento que tenha ordem igual à ordem do grupo é um seu gerador e que qualquer gerador de um grupo cíclico finito tem ordem igual à ordem do grupo.

Exemplo 42. Em $\mathbb{Z}_4$ tem-se que: $o\left(\bar{3}\right) = 4$ e $\mathbb{Z}_4 = \left\langle \bar{3} \right\rangle$.
Em geral, para $n \geq 2$, como $o([x]_n) = \frac{n}{\mathrm{m.d.c.}(x,n)}$, temos que

$$\mathbb{Z}_n =< [x]_n > \Longleftrightarrow \mathrm{m.d.c.}(x, n) = 1.$$

Para um grupo $G = \langle a \rangle$, G é abeliano e se $H < G$, $H = \left\langle a^d \right\rangle$, para algum $d \in \mathbb{N}$. Assim, $H \triangleleft G$, pelo que podemos falar no grupo G/H. Vejamos de seguida como são os elementos deste grupo:

Proposição. Seja $G = \langle a \rangle$ um grupo infinito e $H = \left\langle a^d \right\rangle \triangleleft G$. Então, $H, aH, a^2H, ..., a^{d-1}H$ é a lista completa de elementos de G/H.

Demonstração. Observemos primeiro que, para todo $x \in G$, $xH = a^r H$, para algum $r \in \{0, 1, 2, ..., d-1\}$.
De facto, se $x \in G = \langle a \rangle$, então existe $p \in \mathbb{Z}$ para o qual $x = a^p$. Mas, se $p \in \mathbb{Z}$, existem $q \in \mathbb{Z}$ e $0 \leq r \leq d-1$ tais que $p = qd + r$, pelo que $a^p = a^{qd+r} = a^r \cdot \left(a^d\right)^q \in a^r H$. Logo, $a^p H = a^r H$.
Provemos agora que, para $0 \leq i, j \leq d-1$,

$$i \neq j \Longrightarrow a^i H \neq a^j H.$$

Suponhamos que $i < j$. Então, $0 \leq j - i \leq d-1$, pelo que

$$\begin{aligned} a^i H = a^j H \quad & \Leftrightarrow \left(a^i\right)^{-1} a^j \in H \Leftrightarrow a^{j-i} \in H \\ & \Leftrightarrow j - i = kd, \text{ para algum } k \in \mathbb{Z} \\ & \Leftrightarrow j - i = 0 \Leftrightarrow j = i. \end{aligned}$$

Logo, a implicação verifica-se e, portanto, $G/_H = \left\{H, aH, ..., a^{d-1}H\right\}$. $\square$

Proposição. Dois grupos cíclicos finitos são isomorfos se e só se tiverem a mesma ordem.

Demonstração. Sejam G e T dois grupos cíclicos e finitos. Então, existem $a \in G$ e $b \in T$ tais que $G = \langle a \rangle$ e $T = \langle b \rangle$.
Se $G \cong T$, então obviamente G e T têm a mesma ordem.
Se G e T têm a mesma ordem n, então, $o(a) = o(b) = n$ e

$$G = \left\{1_G, a, a^2, \ldots, a^{n-1}\right\}, \qquad T = \left\{1_T, b, b^2, \ldots, b^{n-1}\right\}.$$

Logo, a aplicação $\psi : G \to T$ definida por

$$\psi = \begin{pmatrix} 1_G & a & a^2 & \cdots & a^{n-1} \\ 1_T & b & b^2 & \cdots & b^{n-1} \end{pmatrix}$$

é obviamente um isomorfismo. □

Corolário. Sejam $n \in \mathbb{N}$ e G um grupo cíclico de ordem n. Então, $G \cong \mathbb{Z}_n$.

Observação. Vimos já que se G é um grupo e $a \in G$ é tal que $o(a) = \infty$, então, para $m, n \in \mathbb{Z}$

$$m \neq n \Longrightarrow a^m \neq a^n.$$

Assim, se G é infinito e cíclico, temos que $G = \langle a \rangle$ para algum $a \in G$ tal que $o(a) = \infty$, pelo que

$$G = \left\{ \ldots, a^{-2}, a^{-1}, 1_G, a, a^2, a^3, \ldots \right\}.$$

Proposição. Se G é um grupo cíclico infinito, então, $G \cong \mathbb{Z}$. $\square$