subgrupos

Definição. Seja G um grupo. Um seu subconjunto não vazio H diz-se um *subgrupo de* G se H for grupo para a operação de G restringida a H. Neste caso escrevemos $H < G$.

Observação. Num grupo G, identificam-se sempre os subgrupos: $\{1_G\}$ (*subgrupo trivial*) e G (*subgrupo impróprio*).

Proposição. Sejam G um grupo e $H < G$. Então:

1. O elemento neutro de H, 1_H, é o mesmo que o elemento neutro de G, 1_G;
2. Para cada $h \in H$, o inverso de h em H é o mesmo que o inverso de h em G.

Exemplo 10. O grupo $(\mathbb{Q}\setminus\{0\},\cdot)$ é subgrupo de $(\mathbb{R}\setminus\{0\},\cdot)$.

Exemplo 11. Seja $G=\{e,a,b,c\}$ o grupo de *4-Klein,* i.e., o grupo cuja operação é definida pela tabela anexa.
Os seus subgrupos são:
$\{e,a,b,c\},\{e\},\{e,a\},\{e,b\}$ e $\{e,c\}$.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Exemplo 12. Seja $\mathbb{Z}_4=\{\bar{0},\bar{1},\bar{2},\bar{3}\}$ o conjunto das classes módulo-4 algebrizado com a adição usual de classes.
Então, os subgrupos do grupo $(\mathbb{Z}_4,+)$ são: $\{\bar{0},\bar{1},\bar{2},\bar{3}\},\{\bar{0}\}$ e $\{\bar{0},\bar{2}\}$.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

.

Proposição. Sejam G um grupo e $H \subseteq G$. Então, $H < G$ se e só se são satisfeitas as seguintes condições:

1. $H \neq \emptyset$;
2. $x, y \in H \Rightarrow xy \in H$;
3. $x \in H \Rightarrow x^{-1} \in H$.

Proposição. Sejam G um grupo e $H \subseteq G$. Então, $H < G$ se e só se são satisfeitas as seguintes condições:

1. $H \neq \emptyset$;
2. $x, y \in H \Rightarrow xy^{-1} \in H$.

Observação. As duas últimas proposições são habitualmente referidas como critérios de subgrupo. São equivalentes e, por isso, a escolha de qual usar para provar que um subconjunto de um determinado grupo é ou não subgrupo deste depende do gosto e destreza de quem está a realizar a prova.

centralizador de um elemento

Definição. Sejam G um grupo e $a \in G$. Chama-se *centralizador de a* ao conjunto $C(a) = \{x \in G \mid ax = xa\}$.

Exemplo 13. Considere-se o grupo diedral do triângulo D_3. Então,
$C(\rho_1) = D_3$,
$C(\rho_2) = C(\rho_3) = \{\rho_1, \rho_2, \rho_3\}$,
$C(\theta_1) = \{\rho_1, \theta_1\}$, $C(\theta_2) = \{\rho_1, \theta_2\}$ e $C(\theta_3) = \{\rho_1, \theta_3\}$.

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

.

Proposição. Seja G um grupo. Então, para todo $a \in G$, $C(a) < G$.

Demonstração. Seja $a \in G$. Então,

1. $C(a) \neq \emptyset$, pois $1_G \in G$ é tal que $1_G a = a 1_G$ e, portanto, $1_G \in C(a)$;
2. dados $x, y \in C(a)$, temos que $xy \in G$ e
$$a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a,$$
pelo que $xy \in C(a)$;
3. dado $x \in C(a)$, temos que $x^{-1} \in G$ e
$$\begin{aligned} ax = xa \quad &\Rightarrow \quad x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} \\ &\Leftrightarrow \quad \left(x^{-1}a\right)\left(xx^{-1}\right) = \left(x^{-1}x\right)\left(ax^{-1}\right) \\ &\Leftrightarrow \quad \left(x^{-1}a\right)1_G = 1_G\left(ax^{-1}\right) \Leftrightarrow x^{-1}a = ax^{-1}, \end{aligned}$$
pelo que $x^{-1} \in C(a)$.

Logo, $C(a) < G$. □

centro de um grupo

Definição. Seja G um grupo. Chama-se *centro de* G ao conjunto

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

Exemplo 14. $Z(D_3) = \{\rho_1\}$.

Exemplo 15. Se G é um grupo abeliano, então, $Z(G) = G$.

Observação. É consequência imediata das definições de centro de um grupo e de centralizador de um elemento desse grupo que

$$Z(G) = \bigcap_{a \in G} C(a).$$

Proposição. Seja G um grupo. Então, $Z(G) < G$.

Demonstração. Seja G um grupo. Então,

1. $Z(G) \neq \emptyset$, pois $1_G \in G$ é tal que, para todo $a \in G$, $\quad 1_G a = a 1_G$ e, portanto, $1_G \in Z(G)$;
2. dados $x, y \in Z(G)$, temos que $xy \in G$ e, para todo $a \in G$,
$$a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a,$$
pelo que $xy \in Z(G)$;
3. dado $x \in Z(G)$, temos que $x^{-1} \in G$ e, para todo $a \in G$,
$$\begin{aligned} x^{-1}a &= \left(x^{-1}a\right)e = \left(x^{-1}a\right)\left(x^{-1}x\right) = \left(x^{-1}ax^{-1}\right)x = \\ &= x\left(x^{-1}ax\right) = \left(xx^{-1}\right)\left(ax^{-1}\right) = 1_G\left(ax^{-1}\right) = ax^{-1}, \end{aligned}$$
pelo que $x^{-1} \in Z(G)$.

Logo, $Z(G) < G$. □

intersecção de subgrupos

Proposição. Sejam G um grupo e $H, K < G$. Então, $H \cap K < G$.

Logo, $H \cap K < G$. $\square$

Corolário. Seja G um grupo. Então, a intersecção de uma família não vazia de subgrupos de G é ainda um subgrupo de G.

Questão: Será que a união de dois subgrupos de um grupo G é um subgrupo de G?

subgrupo gerado

Proposição. Sejam G um grupo e $\varnothing \neq X \subseteq G$. Consideremos o conjunto $\mathcal{H}$ de todos os subgrupos de G que contêm X. Então, $\bigcap_{H \in \mathcal{H}} H$ é o menor subgrupo de G que contém X.

Demonstração. Sejam G um grupo e $\mathcal{H} = \{H \subseteq G \mid H < G \quad \text{e} \quad X \subseteq H\}$. Então, como $\mathcal{H} \neq \emptyset$ (porque $G \in \mathcal{H}$), pelo corolário da proposição anterior, $\bigcap_{H \in \mathcal{H}} H < G$.

Mais ainda, pela definição de $\mathcal{H}$, temos que, $X \subseteq \bigcap_{H \in \mathcal{H}} H$.

Finalmente, seja $K < G$ tal que $X \subseteq K$. Então, $K \in \mathcal{H}$ e, portanto, $\bigcap_{H \in \mathcal{H}} H \subseteq K$.

Concluímos então que $\bigcap_{H \in \mathcal{H}} H$ é o menor subgrupo que contém X. □

Definição. Sejam G um grupo e $\varnothing \neq X \subseteq G$. Chama-se *subgrupo de G gerado por X*, e representa-se por $\langle X \rangle$, ao menor subgrupo que contém X.
Se $X = \{a\}$, então escrevemos $\langle a \rangle$ para representar $\langle X \rangle$ e falamos no *subgrupo de G gerado por a*.

Observação. Pela última proposição, temos que $\langle X \rangle$ é a intersecção de todos os subgrupos de G que contêm X.

Exemplo 16. Se $G = \{e, a, b, c\}$ é o grupo 4-Klein, cujos subgrupos são $\{e, a, b, c\}, \{e\}, \{e, a\}, \{e, b\}$ e $\{e, c\}$, então, $< a >= \{e, a\}$ e $< \{a, b\} >= G$.

Proposição. Sejam G um grupo e $a \in G$. Então, $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

ordem de um elemento

Dados um grupo G e $a \in G$, vimos que

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

É óbvio que, no caso de $a = 1_G$, o subgrupo é o subgrupo trivial.

Mais ainda, no grupo $(\mathbb{R}\backslash\{0\}, \cdot)$, é fácil ver que $\langle -1 \rangle = \{-1, 1\}$.

Torna-se, portanto, óbvio que, embora o subgrupo gerado esteja definido à custa do conjunto dos inteiros, nem sempre vamos obter um número infinito de elementos.

Definição. Sejam G um grupo e $a \in G$.

1. Diz-se que a tem *ordem infinita*, e escreve-se $o(a) = \infty$, se não existe nenhum $p \in \mathbb{N}$ tal que $a^p = 1_G$.
2. Diz-se que a tem *ordem* k ($k \in \mathbb{N}$), e escreve-se $o(a) = k$, se

$$\text{(a)} \quad a^k = 1_G;$$
$$\text{(b)} \quad p \in \mathbb{N} \quad \text{e} \quad a^p = 1_G \Rightarrow k \leq p.$$

Exemplo 17. Considerando o conjunto dos números reais:

- Em $(\mathbb{R}, +)$, a ordem de qualquer elemento não nulo a é infinita. Por outro lado, $o(0) = 1$.
- Em $(\mathbb{R}\backslash\{0\}, \times)$, temos que $o(1) = 1$, $o(-1) = 2$ e se $x \in \mathbb{R}\backslash\{-1, 0, 1\}$, então $o(x) = \infty$.

Exemplo 18. No grupo 4-Klein $G = \{1_G, a, b, c\}$ temos que:

1. $o(1_G) = 1$;
2. $o(a) = o(b) = o(c) = 2$.

Exemplo 19. No grupo $\mathbb{Z}_4 = \left\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\right\}$, temos que:

1. $o\left(\bar{0}\right) = 1$;
2. $o\left(\bar{1}\right) = 4$, pois $\bar{1} \neq \bar{0}, \bar{1}+\bar{1} = \bar{2} \neq \bar{0}, \bar{1}+\bar{1}+\bar{1} = \bar{3} \neq \bar{0}$ e $\bar{1}+\bar{1}+\bar{1}+\bar{1} = \bar{0}$;
3. $o\left(\bar{2}\right) = 2$, pois $\bar{2} \neq \bar{0}$ e $\bar{2}+\bar{2} = \bar{0}$
4. $o\left(\bar{3}\right) = 4$, pois $\bar{3} \neq \bar{0}, \bar{3}+\bar{3} = \bar{2} \neq \bar{0}, \bar{3}+\bar{3}+\bar{3} = \bar{1} \neq \bar{0}$ e $\bar{3}+\bar{3}+\bar{3}+\bar{3} = \bar{0}$.

Proposição. Num grupo G o elemento identidade é o único elemento que tem ordem 1.

Proposição. Sejam G um grupo e $a \in G$ um elemento com ordem infinita. Então, para $m, n \in \mathbb{Z}$,

$$a^m \neq a^n \qquad \text{se} \qquad m \neq n.$$

Demonstração. Sejam $m, n \in \mathbb{Z}$ tal que $a^m = a^n$. Então,

$$\begin{aligned} a^m = a^n \quad &\Rightarrow a^m a^{-n} = a^n a^{-m} = 1_G \\ &\Rightarrow a^{m-n} = a^{n-m} = 1_G \\ &\Rightarrow a^{|m-n|} = 1_G \\ &\Rightarrow |m-n| = 0 \qquad\qquad (o(a) = \infty) \\ &\Rightarrow m = n. \end{aligned}$$

Logo, se $m \neq n$ então $a^m \neq a^n$. □

Corolário. Sejam G um grupo e $a \in G$ um elemento com ordem infinita. Então, $\langle a \rangle$ tem um número infinito de elementos.

Corolário. Num grupo finito nenhum elemento tem ordem infinita.

Proposição. Sejam G um grupo, $a \in G$ e $k \in \mathbb{N}$ tal que $o(a) = k$. Então,

1. se um inteiro n tem r como resto na divisão por k então $a^n = a^r$;
2. para $n \in \mathbb{Z}$, $a^n = 1_G \Leftrightarrow k \mid n$;
3. $\langle a \rangle = \{1_G, a^1, a^2, \ldots, a^{k-1}\}$;
4. $\langle a \rangle$ tem exatamente k elementos.

Proposição. Sejam G um grupo e $a, b \in G$. Então, a e $b^{-1}ab$ têm a mesma ordem.

Demonstração. Suponhamos que $o(a) = n_0$ é finita. Sabemos que $(b^{-1}ab)^{n_0} = b^{-1}a^{n_0}b$ (ver exercício 9b da folha 2). Logo, como $a^{n_0} = 1_G$, obtemos

$$(b^{-1}ab)^{n_0} = b^{-1}1_G b = b^{-1}b = 1_G.$$

Suponhamos agora que k é um inteiro positivo tal que $(b^{-1}ab)^k = 1_G$. Então,

$$\begin{aligned}(b^{-1}ab)^k = 1_G &\Leftrightarrow b^{-1}a^k b = 1_G \\ &\Leftrightarrow b(b^{-1}a^k b)b^{-1} = b1_G b^{-1} \\ &\Leftrightarrow (bb^{-1})a^k(bb^{-1}) = 1_G \\ &\Leftrightarrow a^k = 1_G.\end{aligned}$$

Como a ordem de a é n_0, segue-se que $k \geq n_0$. Assim, n_0 é, de facto, o menor inteiro positivo n tal que $(b^{-1}ab)^n = 1_G$, ou seja, $o(b^{-1}ab) = n_0$.
Mostramos de seguida que, se a tiver ordem infinita, então, $b^{-1}ab$ também tem ordem infinita, usando a regra do contrarrecíproco. Suponhamos que $o(b^{-1}ab) = k$ é finita. Então, pelo que acabámos de provar, $o\left(b(b^{-1}ab)b^{-1}\right) = k$ e, portanto, $o(a) = k$ é finita. □

Observação. Se G é abeliano, o resultado anterior não tem qualquer interesse porque se reduz a $o(a) = o(a)$.

Proposição. Seja G um grupo e $a \in G$ um elemento de ordem finita n. Então, para qualquer $p \in \mathbb{N}$, $o(a^p) = \frac{n}{d}$, onde $d = \text{m.d.c.}(n, p)$.

Demonstração. Sejam $p \in \mathbb{N}$ e $d = \text{m.d.c.}(n, p)$. Então $\frac{n}{d}, \frac{p}{d} \in \mathbb{N}$ e $d = xn + yp$, para certos $x, y \in \mathbb{Z}$. Temos

$$(a^p)^{\frac{n}{d}} = (a^n)^{\frac{p}{d}} = 1_G^{\frac{p}{d}} = 1_G.$$

Se $k \in \mathbb{N}$ é tal que $(a^p)^k = 1_G$, então, como $o(a) = n$, temos que $n \mid pk$, i.e., $pk = nq$ para certo $q \in \mathbb{N}$.

$$\begin{aligned} d = xn + yp \quad &\Rightarrow dk = xnk + ypk = xnk + ynq = n(xk + yq) \\ &\Rightarrow k = \tfrac{n}{d}(xk + yq), \end{aligned}$$

pelo que $\frac{n}{d} \mid k$. Portanto, $o(a^p) = \frac{n}{d}$. □

Exemplo 20. Considere-se o grupo $(\mathbb{Z}_{31}^*, \otimes)$. Facilmente se verifica que, neste grupo, $o([2]_{31}) = 5$. Então,

$$o([8]_{31}) = o\left([2]_{31}^3\right) = \frac{5}{\text{m.d.c.}(5,3)} = 5.$$

Lema. Sejam G um grupo e $a, b \in G$. Então, para qualquer inteiro positivo k,

$$(ab)^k = 1_G \Leftrightarrow (ba)^k = 1_G.$$

Demonstração. Sejam a, b elementos arbitrários de um grupo G e k um inteiro positivo. Temos:

$$\begin{aligned}
(ab)^k = 1_G &\Leftrightarrow (ab)^{k+1} = ab \\
&\Leftrightarrow a(ba)^k b = ab \\
&\Leftrightarrow a^{-1}\left[a(ba)^k b\right] b^{-1} = a^{-1}(ab)b^{-1} \\
&\Leftrightarrow (a^{-1}a)(ba)^k(bb^{-1}) = (a^{-1}a)(bb^{-1}) \\
&\Leftrightarrow (ba)^k = 1_G. \qquad \square
\end{aligned}$$

Proposição. Sejam G um grupo e $a, b \in G$. Se ab tem ordem finita então $o(ba) = o(ab)$.

Proposição. Sejam G um grupo e $a \in G$. Então, $o(a^{-1}) = o(a)$.

Demonstração. O resultado é imediato tendo em conta que, para todo $k \in \mathbb{Z}$,

$$a^k = 1_G \Leftrightarrow (a^{-1})^k = 1_G. \qquad \square$$

Proposição. Se a e b são elementos de ordem finita de um grupo abeliano G, então $o(ab) \mid o(a)\, o(b)$.

Demonstração. Se G é abeliano, sabemos que, para todo $n \in \mathbb{Z}$, $(ab)^n = a^n b^n$ (exercício 12 da folha 2). Assim, temos que

$$(ab)^{o(a)\, o(b)} = a^{o(a)\, o(b)} b^{o(a)\, o(b)} = (a^{o(a)})^{o(b)} (b^{o(b)})^{o(a)} = (1_G)^{o(b)} (1_G)^{o(a)} = 1_G 1_G = 1_G.$$

Estamos em condições de concluir que $o(ab) \mid o(a)\, o(b)$. $\square$

Observação. Que relação terá de existir entre as ordens finitas de a e b para que a ordem de ab seja não só um divisor mas sim igual ao produto daquelas ordens?

Exemplo 21. No grupo aditivo $(\mathbb{Z}_6)$, temos que $o([2]_6) = 3$, $o([3]_6) = 2$ e $o([4]_6) = 3$.

Temos que

$$o([2]_6 \oplus [4]_6) = o([0]_6) = 1 \text{ e } o([2]_6)\, o([4]_6) = 3 \times 3 = 9.$$

Temos também que

$$o([2]_6 \oplus [3]_6) = o([5]_6) = 6 \text{ e } o([2]_6)\, o([3]_6) = 3 \times 2 = 6.$$