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. Um 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.

Demonstração.

1. Por um lado, porque 1_H é elemento neutro de H, temos que $1_H 1_H = 1_H$; por outro lado, como 1_G é elemento neutro de G e $1_H \in G$, temos que $1_H 1_G = 1_H$. Logo, $1_H 1_H = 1_H 1_G$, pelo que, pela lei do corte, $1_H = 1_G$.
2. Sejam $h \in H$, h^{-1} o inverso de h em G e h' o inverso de h em H. Então,
$$hh' = 1_H = 1_G = hh^{-1}.$$
Logo, pela lei do corte, $h' = h^{-1}$. □

Exemplo 12. O grupóide $(\mathbb{Q}\setminus\{0\},\cdot)$ é subgrupo de $(\mathbb{R}\setminus\{0\},\cdot)$.

Exemplo 13. 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 14. 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, $(\mathbb{Z}_4,+)$ é grupo e os seus subgrupos 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. $x \in H \Rightarrow x^{-1} \in H$.

Demonstração. Suponhamos que $H < G$. Então:

1. $H \neq \emptyset$, pois $1_G \in H$;
2. dados $x, y \in H$, como H é um grupóide, $xy \in H$;
3. dado $x \in H$, como todo o elemento de H admite inverso em H e este é igual ao inverso em G, então $x^{-1} \in H$.

Reciprocamente, suponhamos que $H \subseteq G$ satisfaz as condições 1, 2 e 3. Então

(a) H é grupóide por 2;

(b) dado $x \in H$ (este elemento existe por 1), $x^{-1} \in H$ (por 3), pelo que $1_G = xx^{-1} \in H$ (por 2);

(c) qualquer elemento de H admite inverso em H (por 3).

Como a operação é associativa em G, também o é obviamente em H e, portanto, concluímos que $H < G$. □

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 15.
Seja $G = \{e, p, q, a, b, c\}$ o grupo cuja operação é dada pela tabela anexa. Então,
$C(e) = G$, $C(p) = C(q) = \{e, p, q\}$,
$C(a) = \{e, a\}$, $C(b) = \{e, b\}$
e $C(c) = \{e, c\}$.

$\cdot$	e	p	q	a	b	c
e	e	p	q	a	b	c
p	p	q	e	c	a	b
q	q	e	p	b	c	a
a	a	b	c	e	p	q
b	b	c	a	q	e	p
c	c	a	b	p	q	e

.

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 16. Se G é o grupo do exemplo 15, então, $Z(G) = \{e\}$.

Exemplo 17. 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, $H \cap K < G$.

Demonstração. Sejam G um grupo e $H, K < G$. Então,

1. $H \cap K \neq \emptyset$, pois $1_G \in H$ e $1_G \in K$, pelo que $1_G \in H \cap K$;
2. dados $x, y \in H \cap K$, temos que $x, y \in H$ e $x, y \in K$, pelo que $xy \in H$ e $xy \in K$. Logo, $xy \in H \cap K$.
3. dado $x \in H \cap K$, temos que $x \in H$ e $x \in K$, pelo que $x^{-1} \in H$ e $x^{-1} \in K$ e, portanto, $x^{-1} \in H \cap K$.

Logo, $H \cap K < G$. □

Corolário. Seja G um grupo. Então, a intersecção de uma família não vazia de subgrupos de G é ainda 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 18. Se $G = \{e, a, b, c\}$ é o grupo 4-Klein, cujos subgrupos são $\{e, a, b, c\}, \{e\}, \{e, a\}, \{e, b\}$ e $\{e, c\}$ (Exemplo 13.), então, $< a >= \{e, a\}$ e $< \{a, b\} >= G$.

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

Demonstração. Seja $B = \{a^n \mid n \in \mathbb{Z}\}$. Então,

1. $B \neq \emptyset$, pois $1_G = a^0$ e, portanto, $1_G \in B$;
   Dados $x, y \in B$, sabemos que existem $n, m \in \mathbb{Z}$ tais que $x = a^n$ e $y = a^m$ e, por isso,
   $$xy^{-1} = a^n \left(a^m\right)^{-1} = a^n a^{-m} = a^{n-m}.$$
   Como $n - m \in \mathbb{Z}$, temos que $xy^{-1} \in B$. Logo, $B < G$.
2. Como $1 \in \mathbb{Z}$, temos que $a \in B$.
3. Seja $H < G$ tal que $a \in H$. Então,
   $$x \in B \Rightarrow (\exists n \in \mathbb{Z}) \quad x = a^n \Rightarrow x \in H (\text{pois } H < G)$$
   e, portanto $B \subseteq H$.

Logo, $\langle a \rangle = B$. □

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 reduz-se ao 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 19. 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 20. 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 21. 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.

Demonstração. É óbvio que $o(1_G) = 1$. Provemos agora que é único elemento nestas condições. Suponhamos que $a \in G$ é tal que $o(a) = 1$. Então, $a^1 = 1_G$, i.e., $a = 1_G$. □

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. $\langle a \rangle = \left\{1_G, a^1, a^2, \ldots, a^{k-1}\right\}$;
4. $\langle a \rangle$ tem exatamente k elementos.

Demonstração.

1. Sejam $n \in \mathbb{Z}$ e $0 \leq r < k$ para os quais existe $q \in \mathbb{Z}$ tal que $n = qk + r$. Então,

$$a^n = a^{qk+r} = a^{qk} a^r = \left(a^k\right)^q a^r = 1_G^q a^r = 1_G a^r = a^r.$$

2. Pretendemos provar que $a^m = 1_G \Leftrightarrow k \mid m$, ou seja, que

$$a^m = 1_G \Leftrightarrow m = kp \quad \text{para algum } p \in \mathbb{Z}.$$

Suponhamos primeiro que $m = kp$ para algum $p \in \mathbb{Z}$. Então,

$$a^m = a^{kp} = \left(a^k\right)^p = 1_G^p = 1_G.$$

Reciprocamente, suponhamos que $a^m = 1_G$. Sabemos que, pelo algoritmo da divisão, existem $p \in \mathbb{Z}$ e $0 \leq r < k$ tais que $m = kp + r$ e, portanto,

$$1_G = a^m = a^{kp+r} = \left(a^k\right)^p a^r = 1_G^p a^r = 1_G a^r = a^r.$$

Como $o(a) = k$, temos que $r = 0$ (pois $0 \leq r < k$ e $k \leq r$ se $r \geq 1$). Logo, $m = kp$.

3. Sabemos que $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Obviamente, temos que $\left\{1_G, a, a^2, a^3, \ldots, a^{k-1}\right\} \subseteq \langle a \rangle$.
Seja $x \in \langle a \rangle$. Então,

$$x = a^p \qquad \text{para algum} \qquad p \in \mathbb{Z}.$$

Se $p \in \{0, 1, 2, 3, \ldots, k-1\}$ então $x \in \left\{1_G, a, a^2, a^3, \ldots, a^{k-1}\right\}$.
Se $p \notin \{0, 1, 2, 3, \ldots, k-1\}$ então sabemos, por 1, que existe $0 \leq r \leq k-1$ tal que $a^p = a^r$.
Logo, $\langle a \rangle \subseteq \left\{e, a, a^2, a^3, \ldots, a^{k-1}\right\}$ e a igualdade verifica-se.

4. Pretendemos provar que, na lista $1_G, a, a^2, a^3, \ldots, a^{k-1}$ não há repetição de elementos.
Suponhamos que sim, i.e., suponhamos que

$$a^p = a^q \qquad \text{com } 0 \leq q < p \leq k-1.$$

Então, $p - q > 0$ e

$$a^{p-q} = a^p a^{-q} = a^q a^{-q} = 1_G,$$

pelo que $k \leq p - q \leq k - 1$, o que é impossível. Logo, não há qualquer repetição e o subgrupo $\langle a \rangle$ tem exatamente k elementos. □