Elementos da Teoria de Grupos

lcc :: lmat :: 2.º ano

paula mendes martins

departamento de matemática :: uminho

generalidades

Definição. Um par $(S, *)$ diz-se um *grupóide* se S é um conjunto e $*$ é uma operação binária em S, i.e., se $*$ é definida por

$$\begin{array}{rcl} * : S \times S & \longrightarrow & S \\ (x, y) & \longmapsto & x * y. \end{array}$$

Definição. Seja $(S, *)$ um grupóide. A operação $*$ diz-se *comutativa* ou *abeliana* se

$$a * b = b * a, \qquad \forall a, b \in S.$$

Nestas condições, dizemos que $(S, *)$ é *comutativo* ou *abeliano*.

Exemplo 1.

- Se $*$ é definida por $x * y = \frac{x+y}{2}$ em $S = \mathbb{R}$, então, $(S, *)$ é um grupóide abeliano.
- Se $*$ é definida por $x * y = x - y$ em $S = \mathbb{N}$, então, $(N, *)$ não é um grupóide.
- Se $*$ é definida por $x * y = 3$ em $S = \mathbb{N}$, então, $(N, *)$ é um grupóide comutativo.
- Se $*$ é a adição ou a multiplicação usuais de classes em $\mathbb{Z}_n$, com $n \in \mathbb{N}$, então $(\mathbb{Z}_n, *)$ é um grupóide comutativo.

Exemplo 2. Sejam $S = \{a, b, c\}$ e $*$ a operação binária definida pela seguinte tabela (à qual se chama *tabela de Cayley*):

$*$	a	b	c
a	a	b	b
b	b	a	c
c	b	c	a

.

Então, $(S, *)$ é um grupóide comutativo.

Definição. Seja $(S, *)$ um grupóide. A operação $*$ diz-se *associativa* se

$$a * (b * c) = (a * b) * c, \quad \forall a, b, c \in S.$$

Nestas condições, escrevemos apenas $a * b * c$ e dizemos que o grupóide $(S, *)$ é um *semigrupo*.

Exemplo 3. O conjunto dos números inteiros constitui um semigrupo quando algebrizado com a multiplicação usual.

Exemplo 4. O grupóide do Exemplo 2 não é um semigrupo. De facto, temos que $a * (c * c) = a * a = a$ e $(a * c) * c = c$.

Definição. Seja $(S, *)$ um grupóide. Um elemento $a \in S$ diz-se um *elemento idempotente* se $a * a = a$.

Exemplo 5. No primeiro grupóide do Exemplo 1, todos os elementos são idempotentes. De facto, para todo $x \in S$, $x * x = \frac{x+x}{2} = x$.

Definição. Seja $(S, *)$ um grupóide. Um elemento $0 \in S$ diz-se *elemento zero* ou *nulo* se

$$0 * a = a * 0 = 0, \qquad \forall a \in S.$$

Um elemento $e \in S$ diz-se *elemento neutro* ou *elemento identidade* se

$$a * e = e * a = a, \qquad \forall a \in S.$$

Observação. Um elemento neutro ou um elemento zero de um grupóide é um elemento idempotente.

Proposição. Num grupóide $(S, *)$ existe, no máximo, um elemento neutro.

Demonstração. Suponhamos que $(S, *)$ admite dois elementos neutros, e e e'. Então, porque e é elemento neutro,

$$e * e' = e'.$$

Por outro lado, porque e' é elemento neutro,

$$e * e' = e.$$

Logo, $e = e'$. $\square$

Definição. Um semigrupo $(S, *)$ que admita elemento neutro diz-se um *monóide* ou um *semigrupo com identidade*. O único elemento neutro existente num monóide $(S, *)$ representa-se por 1_S.

Exemplo 6. O semigrupo $(\mathbb{N}, *)$ onde $*$ está definida por

$$a * b = 2ab, \qquad \forall a, b \in \mathbb{N},$$

não admite elemento neutro.

Exemplo 7. O semigrupo $(S, *)$, onde $S = \{a, b, c, d\}$ e $*$ é definida pela tabela

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

é um monóide, e a é o seu elemento neutro.

Definição. Sejam $(S,*)$ um semigrupo com identidade e $a \in S$. Um elemento $a' \in S$ diz-se *elemento oposto* de a se $a * a' = a' * a = 1_S$.

Proposição. Num semigrupo $(S,*)$ com identidade, um elemento $a \in S$ tem, no máximo, um elemento oposto.

Demonstração. Suponhamos que $a \in S$ admite dois elementos opostos, a' e a''. Então,

$$a' = a' * 1_S = a' * (a * a'') = (a' * a) * a'' = 1_S * a'' = a''.$$

Logo, quando existe, o oposto de um elemento é único. $\square$

Observação. Caso não haja ambiguidade quanto à operação $*$, referimo-nos muitas vezes ao grupóide (respetivamente, semigrupo, monóide) $(S,*)$ como o grupóide (respetivamente, semigrupo, monóide) S.

potência natural de um elemento num semigrupo

Para representarmos a operação binária definida num conjunto podemos usar dois tipos de linguagem: a multiplicativa e a aditiva. Nestes casos temos:

Linguagem multiplicativa	Linguagem aditiva
$a * b = ab$ (produto de a por b)	$a * b = a + b$ (a soma de a por b)
a^{-1} é o oposto ou *inverso* de a	$-a$ é o oposto ou *simétrico* de a

Dado um elemento a de um semigrupo S, utilizamos a seguinte notação para representar os seguintes produtos (ou somas):

Linguagem multiplicativa	Linguagem aditiva	
$a^2 = aa$	$2a = a + a$	
$a^3 = aaa$	$3a = a + a + a$	
$\vdots$	$\vdots$	
$a^n = \underbrace{aa \cdots aa}_{n \text{ vezes}}$	$na = \underbrace{a + a + \cdots + a + a}_{n \text{ vezes}}$	(com $n \in \mathbb{N}$)

A a^n chamamos *potência de a* e a na chamamos *múltiplo de a*.

A não ser que seja referido, trabalhamos com a linguagem multiplicativa.

Proposição. Sejam S um semigrupo, $m, n \in \mathbb{N}$ e $a \in S$. Então,

1. $a^m a^n = a^{m+n}$ $\qquad [\ ma + na = (m+n)\,a\ ]$;
2. $(a^m)^n = a^{mn}$ $\qquad [\ n\,(ma) = (nm)\,a\ ]$.

Demonstração. Trivial, tendo em conta a associatividade da operação. $\square$

Definição. Seja G um conjunto no qual está definida uma operação binária. Então, G diz-se um *grupo* se G é um semigrupo com identidade e no qual todos os elementos admitem um único elemento oposto, i.e., G é grupo se:

G1. A operação binária é associativa em G;

G2. $(\exists e \in G)\,(\forall a \in G) \qquad ae = ea = a$;

G3. $(\forall a \in G)\,\left(\exists^! a^{-1} \in G\right) \qquad aa^{-1} = a^{-1}a = e$.

Se a operação for comutativa, o grupo diz-se *comutativo* ou *abeliano.*

Representamos a identidade do grupo G por 1_G.

Exemplo 8. $(\mathbb{R}, +)$ é grupo abeliano ($+$ é a adição usual de números reais). $(\mathbb{R}, \cdot)$ não é grupo ($\cdot$ é a multiplicação usual de números reais), mas $(\mathbb{R} \setminus \{0\}, \cdot)$ é grupo abeliano.

Exemplo 9. Seja $n \in \mathbb{N}$. Sendo $\oplus$ e $\otimes$ as operações de adição e multiplicação usuais de classes de $\mathbb{Z}_n$, temos que $(\mathbb{Z}_n, \oplus)$ é grupo e $(\mathbb{Z}_n, \otimes)$ não é grupo. Sendo $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{[0]_n\}$, temos que $(\mathbb{Z}_n^*, \otimes)$ é grupo se e só se n é primo.

Exemplo 10. $(\mathbb{Z}, \cdot)$ não é grupo ($\cdot$ é a multiplicação usual de números inteiros), mas $(\mathbb{Z}, +)$ é grupo abeliano ($+$ é a adição usual de números inteiros).

Exemplo 11. Um conjunto singular, $\{x\}$, quando algebrizado com a única operação binária possível, $x * x = x$, é um grupo abeliano (chamado de *grupo trivial*).

Proposição. Num grupo G são válidas as leis do corte, i.e., para $x, y, a \in G$,

$$ax = ay \Rightarrow x = y \quad e \quad xa = ya \Rightarrow x = y.$$

Demonstração. Sejam $a, x, y \in G$. Então,

$$\begin{aligned} ax = ay \quad & \Longrightarrow \quad a^{-1}(ax) = a^{-1}(ay) \\ & \Rightarrow \quad \left(a^{-1}a\right)x = \left(a^{-1}a\right)y \\ & \Rightarrow \quad 1_G x = 1_G y \\ & \Rightarrow \quad x = y. \end{aligned}$$

A segunda implicação demonstra-se de modo análogo. □

Observação. Existem semigrupos que não são grupos nos quais se verifica a lei do corte, como, por exemplo, $\mathbb{Z} \setminus \{0\}$ algebrizado com a multiplicação usual de inteiros. Este semigrupo comutativo com identidade satisfaz as leis do corte, mas não é um grupo, pois os únicos elementos que admitem inverso são 1 e -1.

Teorema. Num grupo G, as equações $ax = b$ e $ya = b$, admitem uma única solução, para quaisquer $a, b \in G$.

Reciprocamente, um semigrupo S no qual as equações $ax = b$ e $ya = b$ admitem soluções únicas, para quaisquer $a, b \in S$, é um grupo.

Demonstração. Suponhamos, primeiro, que G é um grupo. Então, para $a, b \in G$, os elementos $a^{-1}b$ e ba^{-1} de G são soluções das equações $ax = b$ e $ya = b$, respetivamente. A unicidade destas soluções resulta do facto de as leis de corte serem válidas em G.

Reciprocamente, sejam S um semigrupo e $a \in S$. Então, existem soluções únicas das equações $ax = a$ e $ya = a$. Sejam e e e' essas soluções, respetivamente. Então, como para todo $b \in S$ existe um único $c \in S$ tal que $b = ca$, temos que

$$be = (ca)\,e = c\,(ae) = ca = b.$$

Logo, e é elemento neutro à direita em S. De modo análogo, provamos que e' é elemento neutro à esquerda. Assim,

$$e = e'e = e'$$

e, portanto, e é elemento neutro do semigrupo S.

Seja $a \in S$. Então, existem soluções únicas das equações $ax = e$ e $ya = e$. Sejam a' e a'' essas soluções, respetivamente. Temos então que $aa' = e$ e $a''a = e$. Logo,

$$a'' = a''e = a''\left(aa'\right) = \left(a''a\right)a' = ea' = a',$$

pelo que cada elemento $a \in S$ admite um oposto $a' \in S$. Portanto, S é um grupo. $\square$

Proposição. Seja S um semigrupo finito que satisfaz as leis do corte. Então S é um grupo.

Demonstração. Seja a um elemento qualquer de S. Então, as aplicações $\rho_a, \lambda_a : S \to S$ definidas por, respetivamente, $\rho_a(x) = xa$ e $\lambda_a(x) = ax$, $x \in S$, são injetivas. De facto, para $x, y \in S$, tendo em conta as leis do corte,

$$\rho_a(x) = \rho_a(y) \Leftrightarrow xa = ya \Rightarrow x = y$$

e

$$\lambda_a(x) = \lambda_a(y) \Leftrightarrow ax = ay \Rightarrow x = y.$$

Logo, sendo S um conjunto finito, temos que as duas aplicações são também sobrejetivas, pelo que as equações $ax = b$ e $ya = b$ têm soluções únicas em S. Assim, pelo teorema anterior, o semigrupo S é um grupo. $\square$

Proposição. Seja G um grupo. Então:

1. $1_G^{-1} = 1_G$;
2. $\left(a^{-1}\right)^{-1} = a, \quad \forall a \in G$;
3. $(ab)^{-1} = b^{-1}a^{-1}, \quad \forall a, b \in G$;
4. $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$, $(\forall n \in \mathbb{N})\,(\forall a_1, a_2, \ldots, a_n \in G)$.

Dado um elemento a de um grupo G e $p \in \mathbb{Z}$, define-se

$$\begin{aligned} a^P &= \underbrace{aa \cdots a}_{p \text{ vezes}} && \text{se } p \in \mathbb{Z}^+; \\ a^p &= 1_G && \text{se } p = 0; \\ a^p &= \left(a^{-1}\right)^{-p} = \left(a^{-p}\right)^{-1} && \text{se } p \in \mathbb{Z}^-. \end{aligned}$$

Em linguagem aditiva temos

$$\begin{aligned} pa &= \underbrace{a + a + \cdots + a}_{p \text{ vezes}} && \text{se } \mathbb{Z}^+; \\ pa &= 1_G && \text{se } p = 0; \\ pa &= (-p)(-a) = -((-p)\,a) && \text{se } p \in \mathbb{Z}^-. \end{aligned}$$

Proposição. Sejam G um grupo, $x \in G$ e $m, n \in \mathbb{Z}$. Então,

1. $x^m x^n = x^{m+n}$ (na linguagem aditiva: $mx + nx = (m+n)\,x$);
2. $(x^m)^n = x^{mn}$ (na linguagem aditiva: $n\,(mx) = (nm)\,x$).

Demonstração. Temos de considerar vários casos.

Caso 1: Sejam $m, n \in \mathbb{Z}^+$. O caso resulta imediatamente da definição.

Caso 2: Sejam $m, n \in \mathbb{Z}^-$. Então, $m = -l$ e $n = -k$ com $l, k > 0$, pelo que

$$x^m x^n = x^{-l} x^{-k} = \left(x^l\right)^{-1} \left(x^k\right)^{-1} = \left(x^k x^l\right)^{-1}$$
$$= \left(x^{k+l}\right)^{-1} = x^{-(k+l)} = x^{-k-l} = x^{n+m}.$$

Mais ainda,

$$\left(x^m\right)^n = \left(x^{-l}\right)^{-k} = \left[\left(\left(x^{-1}\right)^l\right)^k\right]^{-1} = \left[\left(x^{-1}\right)^{lk}\right]^{-1}$$
$$= \left[\left(x^{lk}\right)^{-1}\right]^{-1} = x^{lk} = x^{(-m)(-n)} = x^{mn}.$$

Caso 3: Sejam $m, n \in \mathbb{Z}$ tais que $m > 0,\ n < 0$ e $|m| > |n|$. Então, $n = -l$ com $m > l > 0$, pelo que

$$x^m x^n = x^{m-l+l} x^{-l} = x^{m-l} x^l \left(x^l\right)^{-1} = x^{m-l} 1_G = x^{m-l} = x^{m+n},$$

o que prova **1.** Por outro lado,

$$(x^m)^n = (x^m)^{-l} = \left[(x^m)^l\right]^{-1} = \left(x^{ml}\right)^{-1} = x^{-ml} = x^{mn},$$

o que prova a condição **2.**

Caso 4. Sejam $m, n \in \mathbb{Z}$ tais que $m > 0,\ n < 0$ e $|m| < |n|$. Então, $n = -l$ com $l > m > 0$, pelo que

$$\begin{aligned} x^m x^n &= x^m x^{-l} = x^m \left(x^l\right)^{-1} = x^m \left(x^{l-m+m}\right)^{-1} = x^m \left(x^{l-m} x^m\right)^{-1} = \\ &= x^m (x^m)^{-1} \left(x^{l-m}\right)^{-1} = 1_G x^{-(l-m)} = x^{-l+m} = x^{n+m}. \end{aligned}$$

A demonstração de **2.** é igual à do Caso 3.

Os casos em que pelo menos um dos inteiros é zero são triviais e qualquer outro caso é igual aos casos 3 ou 4. □

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 $\{\bar{0},\bar{2}\}$.

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

critérios de subgrupo

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, $C(a) < G$. $\square$

centro de um grupo

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

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

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, $Z(G) < G$. $\square$

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

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, $\bigcap\limits_{H\in\mathcal{H}} H$ 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, $\bigcap\limits_{H\in\mathcal{H}} H < G$.

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

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

Concluímos então que $\bigcap\limits_{H\in\mathcal{H}} H$ é o menor subgrupo que contém X. $\square$

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, $\langle a \rangle = B$. $\square$

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

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

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., $a = 1_G$. $\square$

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

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,

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

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. $\square$

ordem de um elemento (cont.)

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,

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

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. $\square$

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 $d = \mathrm{m.d.c.}(n, p)$.

Demonstração. Sejam $p \in \mathbb{N}$ e $d = \mathrm{m.d.c.}(n, p)$. Então $\frac{n}{d}, \frac{p}{d} \in \mathbb{N}$ e $d = xn + yp$, para certos $x, y \in \mathbb{N}$. 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 $n \mid pk$ (ponto 2 da Proposição do slide 35), 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 22. Considere-se o grupo $(\mathbb{Z}_{31}^*, \otimes)$. Facilmente se verifica que, neste grupo, $o([2]_{31}) = 5$. Então,

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

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:

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

Corolário. 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 9 da folha 2). Assim, temos que

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

Pelo ponto 2 da proposição do slide 35 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 23. No grupo aditivo $(\mathbb{Z}_6)$, temos que $o\left([2]_6\right) = 3$, $o\left([3]_6\right) = 2$ e $o\left([4]_6\right) = 3$.

Temos que

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

Temos também que

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

o teorema de Lagrange

Definição. Sejam G um grupo e $X, Y \subseteq G$. Chama-se *produto de X por Y*, e representa-se por XY, ao conjunto

$$XY = \begin{cases} \{xy \in G : x \in X \text{ e } y \in Y\} & \text{se } X \neq \emptyset \text{ e } Y \neq \emptyset; \\ \emptyset & \text{se } X = \emptyset \text{ ou } Y = \emptyset. \end{cases}$$

Se $X \neq \emptyset$, chama-se *inverso de X*, e representa-se por X^{-1}, ao conjunto $X^{-1} = \{x^{-1} : x \in X\}$.

Proposição. Sejam G um grupo e $\mathcal{P}(G) = \{X \mid X \subseteq G\}$. Então, $\mathcal{P}(G)$ é um semigrupo com identidade $\{1_G\}$, quando algebrizado com o produto de subconjuntos de G. $\square$

Observação. Na prática, a proposição anterior assegura que dados um grupo G e $A, B, C \subseteq G$, podemos falar no subconjunto ABC de G, uma vez que $ABC = A(BC) = (AB)C$. É também importante referir que, de um modo geral, no semigrupo $\mathcal{P}(G)$, o elemento A^{-1} não é elemento oposto de A , como mostra o seguinte exemplo.

Exemplo. Seja $G = \{e, a, b, c\}$ o grupo de *4-Klein*, i.e., o grupo cuja operação é dada pela tabela

$$\begin{array}{c|cccc} \cdot & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array}.$$

Se $A = \{a, b\}$, então, $A^{-1} = \{a^{-1}, b^{-1}\} = \{a, b\}$, pelo que

$$A^{-1}A = \{aa, ab, ba, bb\} = \{e, c\} \neq \{e\}.$$

Logo, no semigrupo $\mathcal{P}(G)$, o elemento A^{-1} não é o oposto do elemento A.

Notação. Dados $a \in G$ e $Y \subseteq G$, escreve-se aY para representar $\{a\}\, Y$ e Ya para representar $Y\{a\}$. Assim,

$$aY = \{ay \in G \mid y \in Y\}, \qquad Ya = \{ya \in G \mid y \in Y\}.$$

Recordar. Dado um conjunto X, chamamos *relação binária* em X a qualquer subconjunto R de $X \times X$. Para $x, y \in X$, dizemos que x *está* R *relacionado com* y se $(x, y) \in R$ e podemos escrever $x \, R \, y$ em vez de $(x, y) \in R$.

Uma relação binária R num dado conjunto X diz-se uma *relação de equivalência* se R é:

- *Reflexiva* $(\forall x \in X, \; x \, R \, x)$;
- *Simétrica* $(\forall x, y \in X, \; x \, R \, y \Rightarrow y \, R \, x)$;
- *Transitiva* $(\forall x, y, z \in X, \; (x \, R \, y \wedge y \, R \, z \Rightarrow x \, R \, z)$.

Se num conjunto X estiver definida uma operação binária (como é o caso dos grupos), uma relação de equivalência ρ em X diz-se:

- *uma relação de congruência à esquerda* se: $\forall x, y, z \in X, \; x \, \rho \, y \Rightarrow zx \, \rho \, zy$;
- *uma relação de congruência à direita* se: $\forall x, y, z \in X, \; x \, \rho \, y \Rightarrow xz \, \rho \, yz$;
- *uma relação de congruência* se: $\forall x, y, z \in X, \; x \, \rho \, y \Rightarrow (zx \, \rho \, zy \wedge xz \, \rho \, yz)$.

Proposição. Sejam G um grupo e $H < G$. A relação $\equiv^e \pmod{H}$, definida em G por

$$\forall x, y \in G, \qquad x \equiv^e y \pmod{H} \iff x^{-1}y \in H$$

é uma relação de congruência à esquerda. $\square$

Demonstração. Primeiro, verifiquemos que $\equiv^e \pmod{H}$ é uma relação de equivalência. De facto:

(i) Para todo $x \in G$, $x^{-1}x = 1_G \in H$, pelo que a relação é reflexiva.

(ii) Sejam $x, y \in G$ tais que $x \equiv^e y \pmod{H}$. Então,

$$x \equiv^e y \pmod{H} \Leftrightarrow x^{-1}y \in H \Rightarrow y^{-1}x = \left(x^{-1}y\right)^{-1} \in H \Leftrightarrow y \equiv^e x \pmod{H}.$$

Logo, a relação é simétrica.

(iii) Sejam $x, y, z \in G$ tais que $x \equiv^e y \pmod{H}$ e $y \equiv^e z \pmod{H}$. Então,

$$\begin{aligned} x \equiv^e y \pmod{H} \text{ e } y \equiv^e z \pmod{H} &\iff x^{-1}y \in H \text{ e } y^{-1}z \in H \\ &\Rightarrow x^{-1}z = x^{-1}yy^{-1}z \in H \\ &\iff x \equiv^e z \pmod{H}, \end{aligned}$$

pelo que a relação é transitiva.

Verifiquemos agora que a relação é compatível com a multiplicação à esquerda:

Sejam $x, y \in G$ tal que $x \equiv^e y \pmod{H}$ e $a \in G$. Queremos provar que $ax \equiv^e ay \pmod{H}$. De facto,

$$\begin{aligned} x \equiv^e y \pmod{H} &\iff x^{-1}y \in H \\ &\iff x^{-1}ey \in H \\ &\iff x^{-1}a^{-1}ay \in H \\ &\iff (ax)^{-1}ay \in H \\ &\iff ax \equiv^e ay \pmod{H}. \end{aligned}$$

Concluímos então que $\equiv^e \pmod{H}$ é uma relação de congruência à esquerda. □

Analogamente, provamos que

Proposição. Sejam G um grupo e $H < G$. A relação $\equiv^d \pmod{H}$, definida em G por

$$\forall x, y \in G, \qquad x \equiv^d y \pmod{H} \iff xy^{-1} \in H$$

é uma relação de congruência à direita. □

Definição. Sejam G um grupo e $H < G$. À relação $\equiv^e \pmod{H}$ chama-se *congruência esquerda módulo H* e à relação $\equiv^d \pmod{H}$ chama-se *congruência direita módulo H*.

Cada uma destas relações de equivalência define em G uma partição (que pode não ser necessariamente a mesma). Representando por $[a]_e$ a classe de equivalência do elemento $a \in G$ quando consideramos a congruência esquerda módulo H, temos que

$$\begin{aligned} x \in [a]_e \quad &\Leftrightarrow \quad x \equiv^e a \pmod H \Leftrightarrow x^{-1}a \in H \Leftrightarrow \exists h \in H : x^{-1}a = h \\ &\Leftrightarrow \quad \exists h \in H : x^{-1} = ha^{-1} \Leftrightarrow \exists h \in H : x = ah^{-1} \Leftrightarrow x \in aH, \end{aligned}$$

pelo que

$$[a]_e = aH, \quad \forall a \in G.$$

De modo análogo, representando por $[a]_d$ a classe de equivalência do elemento $a \in G$ quando consideramos a congruência direita módulo H, temos que

$$[a]_d = Ha, \quad \forall a \in G.$$

Definição. Sejam G um grupo e $H < G$. Para cada $a \in G$, o subconjunto aH designa-se por *classe lateral esquerda de a módulo H* e o subconjunto Ha designa-se por *classe lateral direita de a módulo H*.

Exemplo 22. Seja $G = \{e, a, b, c\}$ o grupo de *4-Klein*, i.e., o grupo cuja operação é dada pela tabela

$$\begin{array}{c|cccc} \cdot & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array}.$$

Considerando o subgrupo $H = \{e, a\}$, as classes laterais esquerdas são

$$eH = H = aH \quad \text{e} \quad bH = \{b, c\} = cH$$

e as classes laterais direitas são iguais já que o grupo é comutativo.

Exemplo 23. Seja $G = \{e, p, q, a, b, c\}$ o grupo cuja operação é dada pela tabela

$$\begin{array}{c|cccccc}
\cdot & e & p & q & a & b & c \\ \hline
e & e & p & q & a & b & c \\
p & p & q & e & c & a & b \\
q & q & e & p & b & c & a \\
a & a & b & c & e & p & q \\
b & b & c & a & q & e & p \\
c & c & a & b & p & q & e
\end{array}.$$

Então, considerando o subgrupo $H = \{e, a\}$, as classes laterais esquerdas são

$$eH = H = aH, \quad bH = \{b, q\} = qH \quad \text{e} \quad cH = \{c, p\} = pH$$

e as classes laterais direitas são

$$He = H = Ha, \quad Hb = \{b, p\} = Hp \quad \text{e} \quad Hc = \{c, q\} = Hq.$$

Proposição. Sejam G um grupo e $H < G$. Se H é finito então cada classe módulo H tem a mesma cardinalidade que H.

Demonstração. Sejam G um grupo e $a \in G$. As aplicações

$$\begin{array}{rcl} \lambda_a : G & \longrightarrow & G \\ x & \longmapsto & ax \end{array} \quad \text{e} \quad \begin{array}{rcl} \rho_a : G & \longrightarrow & G \\ x & \longmapsto & xa \end{array}$$

são bijecções em G. Logo, $\lambda_a|_H$ e $\rho_a|_H$ são bijecções de H em $\lambda_a(H) = aH$ e de H em $\rho_a(H) = Ha$, respetivamente. Assim, se H for finito,

$$\sharp(aH) = \sharp H = \sharp(Ha).$$

□

Proposição. Sejam G um grupo finito e $H < G$. Se $a_1H, a_2H, \ldots, a_rH$ são exatamente as classes laterais esquerdas de H em G (com $r \geq 1$ e $a_1, a_2, \ldots, a_r \in G$), então, $Ha_1^{-1}, Ha_2^{-1}, \ldots, Ha_r^{-1}$ são exatamente as classes laterais direitas de H em G.

Demonstração. Cada elemento de G pertence exatamente a uma e uma só classe lateral esquerda $a_1H, a_2H, \ldots, a_rH$. Sejam $x \in G$ e $1 \leq i \leq r$. Então,

$$\begin{aligned} x \in Ha_i^{-1} \quad & \Leftrightarrow x\left(a_i^{-1}\right)^{-1} \in H \Leftrightarrow xa_i \in H \Leftrightarrow \left(x^{-1}\right)^{-1} a_i \in H \\ & \Leftrightarrow x^{-1} \in a_iH. \end{aligned}$$

Como a condição $x^{-1} \in a_iH$ é verdadeira para exatamente um valor de i, então também a expressão $x \in Ha_i^{-1}$ é verdadeira para exatamente um valor de i.

□

Observação. No seguimento desta proposição, escrevemos

$$G/_{\equiv^e (\mathrm{mod}\, H)} = \{a_1 H, a_2 H, \ldots, a_r H\}$$

se e só se

$$G/_{\equiv^d (\mathrm{mod}\, H)} = \left\{Ha_1^{-1}, Ha_2^{-1}, \ldots, Ha_r^{-1}\right\}.$$

Definição. Sejam G um grupo finito e $H < G$. Chama-se:

1. *ordem do grupo* G, e representa-se por $|G|$, ao número de elementos de G;
2. *índice de* H, e representa-se por $[G : H]$, ao número de classes laterais esquerdas (ou direitas) de H em G.

Teorema. (*Teorema de Lagrange*) Sejam G um grupo finito e $H < G$. Então,

$$|G| = [G : H] \cdot |H| .$$

Demonstração. Imediata, tendo em conta que, se se considerar a partição em G definida pela congruência esquerda módulo H, temos $[G : H]$ classes, cada uma das quais com $|H|$ elementos. $\square$

Corolário. Num grupo finito G, a ordem de cada elemento divide a ordem do grupo.

Demonstração. Imediata, tendo em conta que $o\,(a) = |\langle a \rangle|$, para todo $a \in G$. $\square$

Corolário. Sejam G um grupo finito e p um primo tal que $|G| = p$. Então, existe $b \in G$ tal que $G = \langle b \rangle$.

Demonstração. Como p é primo, $p \neq 1$, pelo que $G \neq \{1_G\}$. Seja $x \in G$ tal que $x \neq 1_G$. Então,

$$\begin{aligned} o\,(x) \mid p \quad &\Rightarrow o\,(x) = p \\ &\Rightarrow |\langle x \rangle| = p \\ &\Leftrightarrow G = \langle x \rangle\,. \end{aligned}$$

□

O recíproco do teorema de Lagrange nem sempre é verdadeiro: o facto de a ordem de um grupo admitir um determinado fator, não implica que exista necessariamente um subgrupo desse grupo cuja ordem é esse fator.

No entanto, se esse fator é um número primo, temos:

Teorema. (*Teorema de Cauchy*) Sejam G um grupo de ordem $n \in \mathbb{N}$ e p um primo divisor de n. Então, existe um elemento $a \in G$ tal que $o(a) = p$. □

subgrupos normais e grupos quociente

Definição. Sejam G um grupo e $H < G$. Diz-se que H é *subgrupo normal* ou *invariante* de G, e escreve-se $H \lhd G$, se

$$\forall x \in G,\ xH = Hx.$$

Exemplo 24. Seja $G = \{e, p, q, a, b, c\}$ o grupo cuja operação é dada pela tabela

$\cdot$	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

(ver Exemplo 23) e $H = \{e, a\}$. Então, como $bH = \{b, q\} \neq \{b, p\} = Hb$, concluímos que H não é subgrupo normal de G. No entanto, se considerarmos o subgrupo $K = \{e, p, q\}$, temos que $K \lhd G$, uma vez que

$$eK = Ke = pK = Kp = qK = Kq = K = \{e, p, q\}$$

e

$$aK = Ka = bK = Kb = cK = Kc = \{a, b, c\}.$$

Proposição. Dado um grupo G qualquer, o subgrupo trivial e o subgrupo impróprio são subgrupos normais de G.

Demonstração. Sejam G um grupo e $a \in G$. Então, como as equações $ax = b$ e $ya = b$ têm soluções únicas, para qualquer $b \in G$, temos que

$$aG = \{ag : g \in G\} = G = \{ga : g \in G\} = Ga,$$

o que permite concluir que $G \lhd G$.Além disso,

$$a\{1_G\} = \{a1_G\} = a = \{1_G a\} = \{1_G\}a,$$

ou seja, $\{1_G\} \lhd G$. $\square$

Proposição. Seja G um grupo abeliano. Então, qualquer subgrupo H de G é normal em G.

Demonstração. Basta ter em conta que, se G é abeliano e $a \in G$, então, $aH = \{ah \in G : h \in H\} = \{ha \in G : h \in H\} = Ha$. $\square$

Exemplo 25. Seja G um grupo. Então, $Z(G) \lhd G$. De facto, seja $g \in G$. Então,

$$\begin{aligned} x \in gZ(G) \quad & \Leftrightarrow (\exists a \in Z(G)) \quad x = ga \\ & \Leftrightarrow (\exists a \in Z(G)) \quad x = ag \Leftrightarrow x \in Z(G)g. \end{aligned}$$

Exemplo 26. Sejam G um grupo e $H < G$ tal que $[G : H] = 2$. Então, $H \lhd G$. De facto, de $[G : H] = 2$, temos que existe $x \in G \backslash H$ tal que $Hx = xH$. Assim, para todo $y \in G$, como

$$yH = \begin{cases} H & \text{se } y \in H \\ xH & \text{se } y \notin H \end{cases}$$

e

$$Hy = \begin{cases} H & \text{se } y \in H \\ Hx & \text{se } y \notin H, \end{cases}$$

temos que $yH = Hy$, qualquer que seja $y \in G$. $\square$

Vimos já que a comutatividade num grupo G implica a normalidade dos subgrupos. Assim, podemos afirmar que se H é um subgrupo de G tal que, para todos $a \in G$ e $h \in H$, $ah = ha$, então $H \lhd G$.

Reciprocamente, se H é um subgrupo normal de G o que podemos afirmar é que

$$\forall a \in G,\ \forall h_1 \in H,\ \exists h_2 \in H:\ \ ah_1 = h_2 a.$$

Teorema. Sejam G um grupo e $H < G$. Então,

$$H \lhd G \iff (\forall x \in G)\,(\forall h \in H) \quad xhx^{-1} \in H.$$

Demonstração. [$\Rightarrow$] Suponhamos que $H \lhd G$. Então, para todo $x \in G$,

$$xH = Hx.$$

Sejam $g \in G$ e $h \in H$. Temos que existe $h' \in H$

$$ghg^{-1} = (gh)\,g^{-1} = (h'g)\,g^{-1} = h'\left(gg^{-1}\right) = h',$$

pelo que $ghg^{-1} \in H$.

[$\Leftarrow$] Suponhamos que, para todos $x \in G$ e $h \in H$,

$$xhx^{-1} \in H.$$

Queremos provar que $H \lhd G$.

Seja $g \in G$. Então,

$$\begin{aligned} y \in gH \quad &\Leftrightarrow \quad (\exists h' \in H) \quad y = gh' \\ &\Leftrightarrow \quad (\exists h' \in H) \quad y = gh'\left(g^{-1}g\right) \\ &\Leftrightarrow \quad (\exists h' \in H) \quad y = \left(gh'g^{-1}\right)g \\ &\Rightarrow \quad y \in Hg \qquad \textit{por hipótese}, \end{aligned}$$

pelo que $gH \subseteq Hg$. De modo análogo, prova-se que $Hg \subseteq gH$ e, portanto, $Hg = gH$. □

Exemplo 27. O Teorema anterior pode ser usado para provar facilmente que a interseção de dois subgrupos normais de um mesmo grupo é ainda um subgrupo normal desse grupo.

Sejam G um grupo e H_1 e H_2 dois subgrupos normais de G. Sabemos já que $H_1 \cap H_2 < G$. Para provar que este subrupo é normal em G, basta considerar $x \in G$ e $h \in H_1 \cap H_2$ e provar que $xhx^{-1} \in H_1 \cap H_2$. De facto, se $h \in H_1 \cap H_2$, então $h \in H_1$ e $h \in H_2$.

Como $H_1 \lhd G$, $x \in G$ e $h \in H_1$, temos, pelo teorema anterior, que $xhx^{-1} \in H_1$. Analogamente, como $H_2 \lhd G$, temos que $xhx^{-1} \in H_2$. Logo $xhx^{-1} \in H_1 \cap H_2$ e, novamente pelo teorema anterior, $H_1 \cap H_2 \lhd G$.

Observação. É óbvio que, se um grupo G admite um subgrupo normal H, as relações $\equiv^e \pmod{H}$ e $\equiv^d \pmod{H}$ são uma e uma só relação de congruência. De facto,

$$\begin{aligned} x \equiv^e y \pmod{H} \quad &\Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH = Hx \\ &\Leftrightarrow yx^{-1} \in H \Leftrightarrow x \equiv^d y \pmod{H}. \end{aligned}$$

Assim, fala-se de uma única relação $\equiv \pmod{H}$, que, por sua vez, define um único conjunto quociente, que se representa por G/H. Logo,

$$G/H = \{xH \mid x \in G\} = \{Hx \mid x \in G\}.$$

Proposição. Sejam G um grupo e $H \lhd G$. Então, G/H é grupo, se considerarmos o produto de subconjuntos de G.

Demonstração. Sejam $x, y \in G$. Então,

$$xHyH = xyHH = xyH,$$

pelo que G/H é fechado para o produto.

Mais ainda, a operação é associativa, H é o seu elemento neutro e cada classe xH admite a classe $x^{-1}H$ como elemento inverso. □

Definição. Sejam G um grupo e $H \lhd G$. Ao grupo G/H chama-se *grupo quociente.*

Exemplo 28. Considere-se o subgrupo $3\mathbb{Z} = \{3k : k \in \mathbb{Z}\}$ do grupo (aditivo) $\mathbb{Z}$. Como a adição usual de inteiros é comutativa, concluímos que $3\mathbb{Z} \lhd \mathbb{Z}$. Como estamos a trabalhar com a linguagem aditiva, temos que, dados $x, y \in \mathbb{Z}$,

$$x \equiv y (\bmod 3\mathbb{Z}) \Leftrightarrow x+(-y) \in 3\mathbb{Z} \Leftrightarrow x-y = 3k, \text{ para algum } k \in \mathbb{Z} \Leftrightarrow x \equiv y (\bmod 3).$$

Assim, temos que

$$\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\} = \mathbb{Z}_3.$$

Proposição. Sejam G um grupo e θ uma relação de congruência definida em G. Então, a classe de congruência do elemento identidade, $[1_G]_\theta$, é um subgrupo normal de G. Mais ainda, para $x, y \in G$,

$$x\,\theta\,y \iff x^{-1}y \in [1_G]_\theta\,.$$

Demonstração. Seja G um grupo e θ uma relação de congruência em G.

Pretendemos provar, primeiro, que

$$[1_G]_\theta = \{x \in G \mid x\theta 1_G\} \lhd G.$$

De facto,

(i) $[1_G]_\theta \neq \emptyset$, pois é uma classe de congruência;
(ii) Sejam $x, y \in [1_G]_\theta$. Então,

$$x\,\theta\,1_G \Rightarrow xy\,\theta\,1_G y = y\,\theta\,1_G \Rightarrow xy\,\theta\,1_G,$$

pelo que $xy \in [1_G]_\theta$;
(iii) Seja $x \in [1_G]_\theta$. Então,

$$x\,\theta\,1_G \Rightarrow xx^{-1}\,\theta\,1_G x^{-1} \Leftrightarrow 1_G\,\theta\,x^{-1} \Rightarrow x^{-1}\,\theta\,1_G,$$

pelo que $x^{-1} \in [1_G]_\theta$.

Logo, $[1_G]_\theta$ é um subgrupo de G.

Mais ainda, sejam $x \in G$ e $a \in [1_G]_\theta$. Então,

$$a \, \theta \, 1_G \Rightarrow xax^{-1} \, \theta \, x1_Gx^{-1} = xx^{-1} = 1_G,$$

pelo que $xax^{-1} \in [1_G]_\theta$ e, portanto, $[1_G]_\theta$ é invariante.

Finalmente, sejam $x, y \in G$. Então,

$$x \, \theta \, y \Rightarrow x^{-1}x \, \theta \, x^{-1}y \Leftrightarrow 1_G \, \theta \, x^{-1}y \Leftrightarrow x^{-1}y \in [1_G]_\theta$$

e

$$x^{-1}y \in [1_G]_\theta \Leftrightarrow x^{-1}y \, \theta \, 1_G \Rightarrow xx^{-1}y \, \theta \, x1_G \Leftrightarrow y \, \theta \, x.$$

Logo,

$$x \, \theta \, y \Longleftrightarrow x^{-1}y \in [1_G]_\theta \, .$$

$\square$

Observação. Com o que vimos até agora, é claro que existe uma relação biunívoca entre o conjunto das congruências possíveis de definir num grupo e o conjunto dos subgrupos normais nesse mesmo grupo: Cada subgrupo normal H de um grupo G define uma relação de congruência em G (relação mod H) e cada relação de congruência em G origina um subgrupo normal de G (a classe do elemento identidade).

morfismos

Definição. Sejam G_1, G_2 grupos. Uma aplicação $\psi : G_1 \longrightarrow G_2$ diz-se um *morfismo* ou *homomorfismo* se

$$(\forall x, y \in G_1) \qquad \psi(xy) = \psi(x)\,\psi(y).$$

Um morfismo diz-se um *epimorfismo* se for uma aplicação sobrejetiva.
Um morfismo diz-se um *monomorfismo* se for uma aplicação injetiva.
Um morfismo diz-se um *isomorfismo* se for uma aplicação bijetiva. Neste caso, escreve-se $G_1 \cong G_2$ e diz-se que os dois grupos são *isomorfos*.
Um morfismo de um grupo nele mesmo diz-se um *endomorfismo*.
Um endomorfismo diz-se um *automorfismo* se for uma aplicação bijetiva.

Exemplo 29. Sejam G_1 e G_2 grupos e $\varphi : G_1 \to G_2$ definida por $\varphi(x) = 1_{G_2}$, para todo $x \in G_1$. Então, φ é um morfismo de grupos (conhecido por *morfismo nulo*).

De facto, dados $x, y \in G_1$, temos que $\varphi(xy) = 1_G = 1_G 1_G = \varphi(x)\varphi(y)$.

Exemplo 30. A aplicação $\varphi : \mathbb{R} \to \mathbb{R}\backslash\{0\}$, definida por $\varphi(x) = e^x$ para todo $x \in \mathbb{R}$, é um morfismo do grupo $(\mathbb{R}, +)$ no grupo $(\mathbb{R}\backslash\{0\}, \times)$.

A conclusão é imediata tendo em conta que, para todos os reais x e y, $e^{x+y} = e^x e^y$ e que $e^x \neq 0$.

Exemplo 31. A aplicação $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2$, definida por

$$\varphi([0]_4) = \varphi([2]_4) = [0]_2 \qquad \varphi([1]_4) = \varphi([3]_4) = [1]_2$$

é um morfismo de grupos.

Para provar esta afirmação, temos de verificar os 10 casos distintos possíveis (temos 16 somas possíveis, mas os dois grupos são comutativos):

$$\begin{aligned}
\varphi([0]_4 \oplus [0]_4) &= \varphi([0]_4) = [0]_2 = [0]_2 \oplus [0]_2 = \varphi([0]_4) \oplus \varphi([0]_4)\\
\varphi([0]_4 \oplus [1]_4) &= \varphi([1]_4) = [1]_2 = [0]_2 \oplus [1]_2 = \varphi([0]_4) \oplus \varphi([1]_4)\\
\varphi([0]_4 \oplus [2]_4) &= \varphi([2]_4) = [0]_2 = [0]_2 \oplus [0]_2 = \varphi([0]_4) \oplus \varphi([2]_4)\\
\varphi([0]_4 \oplus [3]_4) &= \varphi([3]_4) = [1]_2 = [0]_2 \oplus [1]_2 = \varphi([0]_4) \oplus \varphi([3]_4)\\
\varphi([1]_4 \oplus [1]_4) &= \varphi([2]_4) = [0]_2 = [1]_2 \oplus [1]_2 = \varphi([1]_4) \oplus \varphi([1]_4)\\
\varphi([1]_4 \oplus [2]_4) &= \varphi([3]_4) = [1]_2 = [1]_2 \oplus [0]_2 = \varphi([1]_4) \oplus \varphi([2]_4)\\
\varphi([1]_4 \oplus [3]_4) &= \varphi([0]_4) = [0]_2 = [1]_2 \oplus [1]_2 = \varphi([1]_4) \oplus \varphi([3]_4)\\
\varphi([2]_4 \oplus [2]_4) &= \varphi([0]_4) = [0]_2 = [0]_2 \oplus [0]_2 = \varphi([2]_4) \oplus \varphi([2]_4)\\
\varphi([2]_4 \oplus [3]_4) &= \varphi([1]_4) = [1]_2 = [0]_2 \oplus [1]_2 = \varphi([2]_4) \oplus \varphi([3]_4)\\
\varphi([3]_4 \oplus [3]_4) &= \varphi([2]_4) = [0]_2 = [1]_2 \oplus [1]_2 = \varphi([3]_4) \oplus \varphi([3]_4)
\end{aligned}$$

Este morfismo pode ser definido por $\varphi([x]_4) = [x]_2$, para todo $[x]_4 \in \mathbb{Z}_4$. Será que, dados $n, m \in \mathbb{N}$, a correspondência de $\mathbb{Z}_n$ para $\mathbb{Z}_m$, definida por $\varphi([x]_n) = [x]_m$ é um morfismo de grupos?

A resposta à pergunta do slide anterior é NÃO.

Se $n < m$, a correspondência nem sequer é uma aplicação, uma vez que $[m]_n = [m-n]_n$ e $\varphi([m]_n) = [0]_m \neq [-n]_m = \varphi([m-n]_n)$.

Se $n \geq m$, a correspondência é uma aplicação, mas não necessariamente um morfismo de grupos. Como contraexemplo, podemos considerar a aplicação $\varphi : \mathbb{Z}_5 \to \mathbb{Z}_6$, definida por $\varphi([x]_5) = [x]_6$. Temos

$$\varphi([2]_5 \oplus [4]_5) = \varphi([1]_5) = [1]_6 \neq [0]_6 = [2]_6 \oplus [4]_6 = \varphi([2]_5) \oplus \varphi([4]_5).$$

Prova-se que $\varphi : Z_n \to Z_m$, definida por $\varphi([x]_n) = [x]_m$ é um morfismo de grupos se e só se $m \mid n$.

Proposição. Sejam G_1 e G_2 dois grupos. Se $\psi : G_1 \longrightarrow G_2$ é um morfismo então $\psi(1_{G_1}) = 1_{G_2}$.

Demonstração. Temos que

$$1_{G_1} 1_{G_1} = 1_{G_1},$$

pelo que

$$\psi(1_{G_1})\,\psi(1_{G_1}) = \psi(1_{G_1} 1_{G_1}) = \psi(1_{G_1}).$$

Por outro lado, como $\psi(1_{G_1}) \in G_2$, temos que

$$\psi(1_{G_1})\, 1_{G_2} = \psi(1_{G_1}).$$

Logo,

$$\psi(1_{G_1})\,\psi(1_{G_1}) = \psi(1_{G_1})\, 1_{G_2},$$

pelo que, pela lei do corte,

$$\psi(1_{G_1}) = 1_{G_2}. \qquad \square$$

Proposição. Sejam G_1 e G_2 dois grupos e $\psi : G_1 \longrightarrow G_2$ um morfismo. Então $[\psi(x)]^{-1} = \psi\left(x^{-1}\right)$.

Demonstração. Seja $x \in G_1$. Então,

$$\psi(x)\,\psi\left(x^{-1}\right) = \psi\left(xx^{-1}\right) = \psi(1_{G_1}) = 1_{G_2}$$

e

$$\psi\left(x^{-1}\right)\psi(x) = \psi\left(x^{-1}x\right) = \psi(1_{G_1}) = 1_{G_2}.$$

Logo, pela própria definição de inverso, $[\psi(x)]^{-1} = \psi\left(x^{-1}\right)$. $\square$

Proposição. Sejam G_1 e G_2 dois grupos, $H \subseteq G_1$ e $\psi : G_1 \to G_2$ um morfismo. Então,

$$H < G_1 \Rightarrow \psi(H) < G_2.$$

Demonstração. Seja $H < G_1$. Então:

1. $\psi(H) \neq \emptyset$, pois
$$1_{G_1} \in H \Rightarrow \psi\left(1_{G_1}\right) \in \psi(H);$$
2. Sejam $a, b \in \psi(H)$. Então,
$$(\exists x, y \in H) \quad a = \psi(x) \quad \text{e} \quad b = \psi(y).$$
Assim,
$$(\exists x, y \in H) \quad ab = \psi(x)\psi(y) = \psi(xy),$$
pelo que $z = xy \in H$ é tal que $ab = \psi(z)$. Logo, $ab \in \psi(H)$;
3. Seja $a \in \psi(H)$. Então, existe $x \in H$ tal que $a = \psi(x)$. Como
$$a = \psi(x) \Rightarrow a^{-1} = [\psi(x)]^{-1} = \psi\left(x^{-1}\right)$$
e $x^{-1} \in H$, temos que $a^{-1} \in \psi(H)$.

Concluímos, assim, que $\psi(H) < G$. $\square$

Corolário. Seja $\psi : G_1 \longrightarrow G_2$ um morfismo de grupos. Se ψ é um monomorfismo então $G_1 \cong \psi(G_1)$. $\square$

Observação. Dois grupos finitos isomorfos têm a mesma ordem. Mas, dois grupos com a mesma ordem, não são necessariamente isomorfos. Como contraexemplo, basta pensar no grupo 4-Klein e no $\mathbb{Z}_4$.

De facto, se o grupo 4-Klein $G = \{e, a, b, c\}$ fosse isomorfo ao grupo aditivo $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ e $f : G \to \mathbb{Z}_4$ fosse um isomorfismo de grupos, teríamos

$$\overline{0} = f(e) = f(xx) = f(x) \oplus f(x),$$

para todo $x \in G$. Sendo f bijetiva, concluíamos que todos os elementos de $\mathbb{Z}_4$ eram simétricos de si próprios, o que é uma contradição, pois, em $\mathbb{Z}_4$, apenas as classes $\overline{0}$ e $\overline{2}$ são inversas de si próprias.

Proposição. Sejam G_1 e G_2 dois grupos, $H \subseteq G_1$ e $\psi : G_1 \to G_2$ um epimorfismo. Então,

$$H \lhd G_1 \Rightarrow \psi(H) \lhd G_2.$$

Demonstração. Considerando a proposição anterior, como $H < G_1$, temos que $\psi(H) <\lhd G_2$. Assim, falta apenas provar que, para $g \in G_2$ e $a \in \psi(H)$, temos que $gag^{-1} \in \psi(H)$. De facto,

$$\begin{aligned} g \in G_2, a \in \psi(H) \quad & \Rightarrow (\exists x \in G_1, h \in H)\ g = \psi(x), \quad a = \psi(h) \\ & \Rightarrow (\exists x \in G_1, h \in H)\ gag^{-1} = \psi(x)\,\psi(h)\,[\psi(x)]^{-1} \\ & \Rightarrow gag^{-1} = \psi\left(xhx^{-1}\right) \text{ com } xhx^{-1} \in H \\ & \to gag^{-1} \in \psi(H), \end{aligned}$$

pelo que $\psi(H) \lhd G_2$. $\square$

Definição. Seja $\psi : G_1 \longrightarrow G_2$ um morfimo de grupos. Chama-se *núcleo (*ou *kernel)* de ψ, e representa-se por $\mathrm{Nuc}\psi$ ou $\ker\psi$, ao subconjunto de G_1

$$\mathrm{Nuc}\psi = \{x \in G_1 \mid \psi(x) = 1_{G_2}\}.$$

Exemplo 32. Se $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2$ é o morfismo definido no Exemplo 31., temos que

$$\mathrm{Nuc}\varphi = \{[0]_4, [2]_4\}.$$

Exemplo 33. Sejam G_1 e G_2 grupos e $\varphi : G_1 \to G_2$ o morfismo nulo. Então, $\mathrm{Nuc}\varphi = G_1$.

Proposição. Seja $\psi : G_1 \longrightarrow G_2$ um morfismo de grupos. Então, $\mathrm{Nuc}\psi \lhd \mathrm{G}_1$.

Demonstração. Começamos por provar que $\mathrm{Nuc}\psi$ é subgrupo de G_1.

1. Observemos, primeiro, que $1_{G_1} \in \mathrm{Nuc}\psi$. De facto, $1_{G_1} \in G_1$ e $\psi\left(1_{G_1}\right) = 1_{G_2}$;
2. Sejam $a, b \in G_1$. Como $a^{-1}b \in G_1$ e

$$\begin{aligned} a, b \in \mathrm{Nuc}\psi \quad & \Rightarrow \psi(a) = \psi(b) = 1_{G_2} \\ & \Rightarrow \psi\left(a^{-1}\right) = [\psi(a)]^{-1} = 1_{G_2}^{-1} = 1_{G_2} = \psi(b) \\ & \Rightarrow \psi\left(a^{-1}b\right) = \psi\left(a^{-1}\right)\psi(b) = 1_{G_2}1_{G_2} = 1_{G_2} \end{aligned}$$

temos que

$$a, b \in \mathrm{Nuc}\psi \Rightarrow a^{-1}b \in \mathrm{Nuc}\psi.$$

Assim, concluímos que este subconjunto de G_1 é, de facto, um seu subgrupo.
Sejam $g \in G_1$ e $b \in \mathrm{Nuc}\psi$. Então,

$$gbg^{-1} \in G_1$$

e

$$\begin{aligned} \psi\left(gbg^{-1}\right) &= \psi(g)\,\psi(b)\,\psi\left(g^{-1}\right) \\ &= \psi(g)\,1_{G_2}\,[\psi(g)]^{-1} \\ &= 1_{G_2}, \end{aligned}$$

pelo que $gbg^{-1} \in \mathrm{Nuc}\psi$. Logo, $\mathrm{Nuc}\psi \lhd G_1$. $\square$

O núcleo de um morfismo de grupos $\psi : G_1 \to G_2$ define uma relação de congruência, a saber

$$\begin{aligned} x \equiv y \pmod{\mathrm{Nuc}\psi} &\Leftrightarrow xy^{-1} \in \mathrm{Nuc}\psi \\ &\Leftrightarrow \psi\left(xy^{-1}\right) = 1_{G_2} \\ &\Leftrightarrow \psi(x)\left[\psi(y)\right]^{-1} = 1_{G_2} \\ &\Leftrightarrow \psi(x) = \psi(y)\,. \end{aligned}$$

Pelo que acabámos de ver, a demonstração da proposição seguinte é trivial.

Proposição. Seja $\psi : G_1 \to G_2$ um morfismo de grupos. Então, ψ é um monomorfismo se e só se $\mathrm{Nuc}\psi = \{1_{\mathrm{G}_1}\}$. $\square$

Proposição. Sejam G um grupo e $H \lhd G$. Então,

$$\begin{aligned} \pi : G &\longrightarrow G/H \\ x &\longmapsto xH \end{aligned}$$

é um epimorfismo (ao qual se chama *epimorfismo canónico*) tal que $\mathrm{Nuc}\pi = H$.

Demonstração. Sejam G um grupo e $H \lhd G$.

Então, para $x, y \in G$,

$$\psi(xy) = (xy)H = xHyH = \psi(x)\psi(y),$$

pelo que π é um morfismo. Além disso, ψ é obviamente sobrejetiva (cada classe é imagem por π do seu representante). Por fim,

$$\begin{aligned} x \in \mathrm{Nuc}\pi &\Leftrightarrow \pi(x) = H \\ &\Leftrightarrow xH = H \Leftrightarrow x \in H. \qquad \square \end{aligned}$$

Os resultados que estudámos no final da secção anterior dizem-nos que:

(i) Dado um morfismo qualquer entre dois grupos, o seu núcleo é um subgrupo normal do domínio;

(ii) Dado um subgrupo normal de um grupo, existe um morfismo cujo núcleo é aquele subgrupo.

Considerando as duas situações em simultâneo, temos que:
se $\psi : G \to G'$ é um morfismo de grupos, então, por (i),

$$\mathrm{Nuc}\psi \lhd G.$$

Logo, por (ii), $\pi : G \to G/_{\mathrm{Nuc}\psi}$ é um epimorfismo tal que

$$\mathrm{Nuc}\pi = \mathrm{Nuc}\psi.$$

Teorema Fundamental do Homomorfismo. Seja $\theta : G \longrightarrow G'$ um morfismo de grupos. Então,

$$\operatorname{Im}\theta \cong G/_{\operatorname{Nuc}\theta}.$$

$$\begin{tikzcd} G \arrow[r, "\theta"] \arrow[d, "\pi"'] & G' \\ G/\operatorname{Nuc}\theta \arrow[ur, "\phi"'] & \end{tikzcd}$$

Demonstração. Sejam $K = \operatorname{Nuc}\theta$ e $\phi : G/_K \longrightarrow G'$ tal que

$$\phi(xK) = \theta(x), \qquad \forall x \in G.$$

Estará a função ϕ bem definida, i.e., se $xK = yK$ será que $\theta(x) = \theta(y)$? SIM. De facto,

$$\begin{aligned} xK = yK &\Leftrightarrow x^{-1}y \in K \, (= \mathrm{Nuc}\,\theta) \\ &\Leftrightarrow \theta\left(x^{-1}y\right) = 1_{G'} \\ &\Leftrightarrow \theta(x) = \theta(y). \end{aligned}$$

Além disso, demonstrámos ainda que $\theta(x) = \theta(y) \Rightarrow xK = yK$, i.e., que

$$\phi(xK) = \phi(yK) \Rightarrow xK = yK,$$

pelo que ϕ é injectiva.

Mais ainda,

$$\begin{aligned} \mathrm{Im}\,\phi &= \{\phi(xK) \mid x \in G\} \\ &= \{\theta(x) \mid x \in G\} \\ &= \mathrm{Im}\,\theta. \end{aligned}$$

Observamos, por último, que ϕ é um morfismo, já que

$$\phi(xKyK) = \phi(xyK) = \theta(xy) = \theta(x)\,\theta(y) = \phi(xK)\,\phi(yK)\,.$$

Concluímos, então, que ϕ é um monomorfismo cujo conjunto imagem (que é isomorfo ao seu domínio) é igual a $\mathrm{Im}\theta$.

Logo,

$$\mathrm{Im}\,\theta \cong G/_{K} = G/_{\mathrm{Nuc}\,\theta}.$$

$\square$

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,

$$\begin{aligned} [0]_4 &= 0\,[1]_4 = 0\,[3]_4 & \qquad [1]_4 &= 1\,[1]_4 = 3\,[3]_4 \\ [2]_4 &= 2\,[1]_4 = 2\,[3]_4 & \qquad [3]_4 &= 3\,[1]_4 = 1\,[3]_4 \end{aligned}$$

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, $H \lhd G$, 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 $H = \left\langle a^d \right\rangle \lhd G$. 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. $\square$

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

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

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

grupo simétrico

Definição. Seja A um conjunto. Uma *permutação* de A é uma aplicação bijetiva de A em A.

Observação. Se A é um conjunto finito com n elementos ($n \in \mathbb{N}$), podemos estabelecer uma bijeção entre A e o conjunto $\{1, 2, ..., n\}$, pelo que aqui iremos adoptar esta última notação para qualquer conjunto com n elementos. Assim, dizemos, por exemplo, que

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

é uma permutação de um conjunto com 4 elementos.

Observação. Se A é um conjunto finito com n elementos ($n \in \mathbb{N}$), sabemos que podemos definir $n!$ permutações de A distintas. Mais ainda, se algebrizarmos este conjunto de $n!$ elementos com a composição de aplicações obtemos, obviamente, um grupo.

(i) A composta de duas permutações é uma permutação;

(ii) A composição de aplicações, em particular de permutações, é associativa;

(iii) A função identidade é uma permutação e é o elemento neutro para a composição de aplicações;

(iv) A aplicação inversa de uma permutação é uma permutação.

Definição. Chama-se *grupo simétrico* de um conjunto com n elementos, e representa-se por S_n, ao grupo das permutações desse conjunto.

Exemplo 43. Se considerarmos um conjunto com dois elementos,

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\};$$

Exemplo 44. Se considerarmos um conjunto com 3 elementos,

$$
\begin{aligned}
S_3 \quad &= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \right. \\
&\left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.
\end{aligned}
$$

Exemplo 45. Se considerarmos um conjunto com 4 elementos, temos que

$$
\begin{aligned}
S_4 \quad = \quad & \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \right. \\
& \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \\
& \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \\
& \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \\
& \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \\
& \left. \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \right\}.
\end{aligned}
$$

Proposição. O grupo simétrico S_n é não comutativo, para todo $n \geq 3$.

Demonstração. Se f e g são as permutações de S_n definidas por

$$
\begin{gathered}
f(1) = 2,\ f(2) = 3,\ f(3) = 1,\ f(k) = k, \forall 4 \leq k \leq n, \\
g(1) = 2,\ g(2) = 1,\ g(k) = k, \forall 3 \leq k \leq n,
\end{gathered}
$$

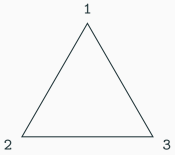
temos que

$$(f \circ g)(1) = 3 \neq 1 = (g \circ f)(1). \qquad \square$$

Definição. Chama-se *grupo diedral* ao grupo das simetrias e rotações de uma linha poligonal.

Representamos por D_n o grupo diedral de um polígono regular com n lados.

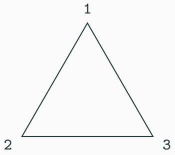
Exemplo 46. $D_3 = S_3$



Temos:

Rotações: 0^o; 120^o e 240^0;

Simetrias: 3 simetrias axiais.



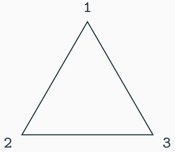
Representando as simetrias e rotações pelas permutações em $\{1, 2, 3\}$, temos:

Rotações de 0^o, 120^o e 240^o:

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix};$$

simetrias em relação às bissetrizes dos ângulos 1, 2 e 3:

$$\theta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \theta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ e } \theta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$



Considerando a composição de funções, obtemos a tabela:

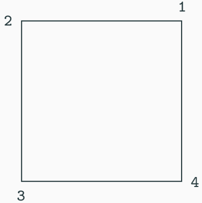
$\circ$	ρ_1	ρ_2	ρ_3	θ_1	θ_2	θ_3
ρ_1	ρ_1	ρ_2	ρ_3	θ_1	θ_2	θ_3
ρ_2	ρ_2	ρ_3	ρ_1	θ_3	θ_1	θ_2
ρ_3	ρ_3	ρ_1	ρ_2	θ_2	θ_3	θ_1
θ_1	θ_1	θ_2	θ_3	ρ_1	ρ_2	ρ_3
θ_2	θ_2	θ_3	θ_1	ρ_3	ρ_1	ρ_2
θ_3	θ_3	θ_1	θ_2	ρ_2	ρ_3	ρ_1

O grupo D_3 é (o menor grupo) não abeliano, $1_{D_3} = \rho_1$ e os seus subgrupos são:

$$\{\rho_1\}, \{\rho_1, \theta_1\}, \{\rho_1, \theta_2\}, \{\rho_1, \theta_3\}, \{\rho_1, \rho_2, \rho_3\} \text{ e } D_3.$$

Destes, quais são normais?

Exemplo 47. D_4 é um subgrupo próprio de S_4



Rotações de 0^o, 90^o, 180^o e 270^o:

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \ \rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ e } \rho_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix};$$

Simetrias em relação às bissectrizes $[1,3]$ e $[2,4]$:

$$\theta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ e } \theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix};$$

Simetrias em relação às mediatrizes do lado $[1,2]$ e do lado $[2,3]$:

$$\theta_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \text{ e } \theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Assim, D_4 tem 8 elementos enquanto que S_4 tem 24 elementos.

Considerando a composição de funções, obtemos a tabela

ρ_1	ρ_1	ρ_2	ρ_3	ρ_4	θ_1	θ_2	θ_3	θ_4
ρ_1	ρ_1	ρ_2	ρ_3	ρ_4	θ_1	θ_2	θ_3	θ_4
ρ_2	ρ_2	ρ_3	ρ_4	ρ_1	θ_2	θ_3	θ_4	θ_1
ρ_3	ρ_3	ρ_4	ρ_1	ρ_2	θ_3	θ_4	θ_1	θ_2
ρ_4	ρ_4	ρ_1	ρ_2	ρ_3	θ_4	θ_1	θ_2	θ_3
θ_1	θ_1	θ_4	θ_3	θ_2	ρ_1	ρ_4	ρ_3	ρ_2
θ_2	θ_2	θ_1	θ_4	θ_3	ρ_2	ρ_1	ρ_4	ρ_3
θ_3	θ_3	θ_2	θ_1	θ_4	ρ_3	ρ_2	ρ_1	ρ_4
θ_4	θ_4	θ_3	θ_2	θ_1	ρ_4	ρ_3	ρ_2	ρ_1

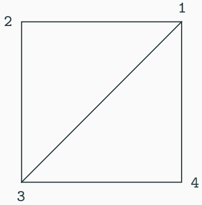
Os subgrupos de D_4 são

$$\{\rho_1\}, \{\rho_1, \theta_1\}, \{\rho_1, \theta_2\}, \{\rho_1, \theta_3\}, \{\rho_1, \theta_4\}, \{\rho_1, \rho_3\},$$

$$\{\rho_1, \rho_2, \rho_3, \rho_4\}, \{\rho_1, \rho_3, \theta_1, \theta_3\}, \{\rho_1, \rho_3, \theta_2, \theta_4\}, D_4\}.$$

Destes, quais são normais?

Exemplo 48. Relativamente à figura



o grupo diedral é composto pelas aplicações

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

$$\phi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ e } \phi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Definição. Diz-se que uma permutação σ de um conjunto finito A é um ciclo de comprimento n se existirem $a_1, a_2, \ldots, a_n \in A$ tais que

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \ldots, \quad \sigma(a_{n-1}) = a_n, \quad \sigma(a_n) = a_1$$

e se

$$\sigma(x) = x, \qquad \forall x \in A \setminus \{a_1, a_2, ..., a_n\}.$$

Neste caso, representa-se este facto por

$$\sigma = \begin{pmatrix} a_1 & a_2 & \ldots & a_{n-1} & a_n \end{pmatrix}.$$

Exemplo 49. Se $A = \{1, 2, 3, 4, 5\}$, temos que

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 3 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 5 & 4 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 5 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 3 & 5 \end{pmatrix}. \end{aligned}$$

Observação. Em S_n, o produto (composição) de dois ciclos pode ou não ser um ciclo, como o prova o seguinte exemplo: em S_6,

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

não é um ciclo. De facto, se representarmos este produto por σ, temos que $\sigma(2) = 4,\ \sigma(4) = 5,\ \sigma(5) = 2$ e $\sigma(1) \neq 1$.

Por outro lado,

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

Definição. Dado um conjunto A finito, dizemos que dois ciclos são *disjuntos* se não existir nenhum elemento de A que apareça simultaneamente na notação desses ciclos, i.e., se nenhum elemento de A for transformado simultaneamente pelos dois ciclos.

Exemplo 50. Em S_6,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1 \quad 6)\,(2 \quad 5 \quad 3)\,,$$

i.e., a permutação σ é o produto de dois ciclos disjuntos.

Teorema. Toda a permutação σ de um conjunto finito é um produto (composição) de ciclos disjuntos.

Demonstração. Suponhamos, sem perdas de generalidade, que $A = \{1, 2, 3, \ldots, n\}$. Consideremos então o primeiro elemento (1) e, para a permutação σ em A, consideremos a lista

$$1 \quad \sigma(1) \quad \sigma^2(1) \quad \sigma^4(1) \quad \ldots\ldots \qquad (*)$$

Como A é finito, sabemos que os elementos de (*) não podem ser todos distintos. Seja $\sigma^r(1)$ o primeiro elemento que aparece repetido. Então, $\sigma^r(1) = 1$.

De facto, se

$$\sigma^r(1) = \sigma^s(1), \qquad \text{para algum } s \in \{1, 2, \ldots, r-1\},$$

concluíamos que

$$\sigma^{r-s}(1) = \mathrm{id}(1) = 1 \qquad \text{e} \quad 0 < r - s < r,$$

pelo que $\sigma^r(1)$ não seria o primeiro elemento a aparecer repetido.

Formamos então o ciclo

$$\rho_1 = \begin{pmatrix} 1 & \sigma(1) & \sigma^2(1) & \cdots & \sigma^{r-1}(1) \end{pmatrix}.$$

Seja, então, i o primeiro elemento de A que não aparece em ρ_1. Aplicamos a i o raciocínio aplicado a 1 e formamos o ciclo

$$\rho_2 = \begin{pmatrix} i & \sigma(i) & \sigma^2(i) & \cdots & \sigma^{t-1}(i) \end{pmatrix}.$$

Por raciocínios análogos, "percorremos" todos os elementos de A. Suponhamos que são k os ciclos que formamos. Então, $\sigma = \rho_1 \cdots \rho_k$.

Vejamos agora que os ciclos são disjuntos dois a dois.

Consideremos os ciclos ρ_1 e ρ_2. Suponhamos que existe $j \in A$ tal que j aparece no ciclo ρ_1 e no ciclo ρ_2. Suponhamos, sem perdas de generalidade, que $j = \sigma^2(1)$ e que $j = \sigma^3(i)$. Então,

$$\begin{aligned} \rho_1 &= \begin{pmatrix} \sigma^2(1) & \sigma^3(1) & \cdots & \sigma^{r-1}(1) & 1 \end{pmatrix} \\ &= \begin{pmatrix} j & \sigma(j) & \sigma^2(j) & \cdots \end{pmatrix} \\ &= \begin{pmatrix} \sigma^3(i) & \sigma^4(i) & \sigma^5(i) & \cdots \end{pmatrix} = \rho_2, \end{aligned}$$

o que não acontece pois i não aparece em ρ_1.

Generalizando esta demonstração, provamos que todos os ciclos são disjuntos dois a dois. $\square$

Questão: Porque é que é importante escrever uma permutação como produto de ciclos disjuntos?

Resposta: Porque ciclos disjuntos comutam!

$$(1\quad 2\quad 3)\,(4\quad 5) = (4\quad 5)\,(1\quad 2\quad 3)$$

$$(1\quad 2\quad 3)\,(1\quad 2) = (1\quad 3) \neq (2\quad 3) = (1\quad 2)\,(1\quad 2\quad 3)$$

Observação. Relembrar que num grupo G, para $a, b \in G$,

$$ab = ba \Leftrightarrow \forall n \in \mathbb{Z},\ (ab)^n = a^n b^n.$$

Questão: Dada uma permutação σ num conjunto com n elementos, i.e., dado o elemento $\sigma \in S_n$, qual será a sua ordem?

Resposta:

1. se σ é um ciclo, então $o\left(\sigma\right)$ é o comprimento do ciclo.
2. se σ é um produto de pelo menos dois ciclos disjuntos, então $o\left(\sigma\right)$ é o m.m.c. entre os comprimentos dos ciclos em questão.

Exemplo 51. Em S_8, como
$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 1 & 7 & 8 & 5 & 6 \end{pmatrix} = (1 \quad 3 \quad 4)\,(5 \quad 7)\,(6 \quad 8)$, temos que $o\left(\phi\right) = 6$ pois o mínimo múltiplo comum entre as ordens dos três ciclos disjuntos é 6.

Definição. Uma *transposição* é um ciclo de comprimento 2.

Proposição. Qualquer ciclo é produto de transposições.

Demonstração. Imediata, tendo em conta que

$$(a_1 \quad a_2 \quad a_3 \quad \cdots \quad a_n) = (a_1 \quad a_n)(a_1 \quad a_{n-1}) \cdots (a_1 \quad a_3)(a_1 \quad a_2)\,.$$

$\square$

Observação. Considerando o teorema e a proposição anteriores, temos que qualquer permutação se escreve como produto de transposições.

Exemplo 52. Em S_7,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 1 & 7 & 5 & 6 \end{pmatrix} = (1 \quad 3 \quad 4)(5 \quad 7 \quad 6) = (1 \quad 4)(1 \quad 3)(5 \quad 6)(5 \quad 7)\,.$$

Teorema. Nenhuma permutação de um conjunto finito pode ser expressa simultaneamente como produto de um número par de transposições e como produto de um número ímpar de transposições. □

Definição. Uma permutação diz-se *par* se se escreve como o produto de um número par de transposições. Uma permutação diz-se *ímpar* se se escreve como produto de um número ímpar de transposições.

Exemplo 53.

- Em S_n, a identidade é uma permutação par. De facto, se A tem n elementos
$$\mathrm{id} = (a_i \quad a_j)\,(a_i \quad a_j)\,,$$
para quaisquer $a_i, a_j \in A$.
- Em S_n, um ciclo de comprimento ímpar é uma permutação par e um ciclo de comprimento par é uma permutação ímpar
$$(1 \quad 2 \quad 3) = (1 \quad 3)\,(1 \quad 2) \qquad\qquad (1 \quad 2 \quad 3 \quad 4) = (1 \quad 4)\,(1 \quad 3)\,(1 \quad 2)\,.$$

Teorema. Seja A um conjunto com n elementos. Então, o conjunto das permutações pares em A é um subgrupo de S_n de ordem $\frac{n!}{2}$.

Demonstração. Seja

$$A_n = \{\sigma : \sigma \text{ é uma permutação par}\}.$$

Sabemos que $\mathrm{id} \in A_n$, que a composição de duas permutações pares é ainda uma permutação par e que a inversa de uma permutação par é ainda uma permutação par. Logo, temos que A_n é um subgrupo do grupo S_n.

Para demonstrar que $|A_n| = \frac{n!}{2}$, basta considerar uma transposição $\tau \in S_n$ e a aplicação

$$\begin{aligned} \phi_\tau : A_n &\longrightarrow B_n \\ \sigma &\longmapsto \tau\sigma, \end{aligned}$$

onde B_n é o conjunto das permutações ímpares.

Provando que ϕ_τ é bijetiva, temos que $\#(A_n) = \#(B_n)$ e, como

$\#(A_n) + \#(B_n) = \#(S_n) = n!$, o resultado é imediato. $\square$

Definição. Seja A um conjunto com n elementos. Chama-se *grupo alterno de A*, e representa-se por A_n, ao subgrupo de S_n das permutações pares.

Exemplo 54. $A_2 = \{id\}$

$A_3 = \{id, (1\,2\,3), (1\,3\,2)\}$

$A_4 = \{id, (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,3\,4),$

$(2\,3\,4), (2\,4\,3), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$

o teorema de representação de Cayley

Para finalizarmos este capítulo sobre grupos, vamos mostrar a importância do estudo do grupo simétrico na Teoria de Grupos. De facto, como se prova no próximo teorema, qualquer grupo é isomorfo a um subgrupo de um dado grupo simétrico.

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

Demonstração. Para cada $x \in G$, a aplicação

$$\begin{array}{rcl} \lambda_x : G & \longrightarrow & G \\ a & \longmapsto & \lambda_x(a) = xa, \end{array}$$

é uma permutação em G.

Assim, se S é o grupo das permutações de G, consideramos a função

$$\begin{array}{rcl} \theta : G & \longrightarrow & S \\ x & \longmapsto & \lambda_x . \end{array}$$

Então, para $x, y, g \in G$,

$$(\lambda_x \circ \lambda_y)(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = x(yg) = (xy)g = \lambda_{xy}(g),$$

pelo que

$$\theta(x)\,\theta(y) = \theta(xy),$$

i.e., θ é um morfismo.

Mais ainda,

$$x \in \mathrm{Nuc}\theta \Leftrightarrow \theta(\mathrm{x}) = \mathrm{id_G} \Leftrightarrow \lambda_\mathrm{x} = \mathrm{id_G} \Rightarrow \mathrm{x} = \lambda_\mathrm{x}(1_\mathrm{G}) = \mathrm{id_G}(1_\mathrm{G}) = 1_\mathrm{G},$$

e, portanto,

$$\mathrm{Nuc}\theta = \{1_\mathrm{G}\}.$$

Logo, θ é um monomorfismo, pelo que $G \cong \mathrm{Im}\theta < S$. $\square$

Exemplo 55. Seja $G = \mathbb{Z}_4$. Então, como para todos $a, x \in \mathbb{Z}_4$, $\lambda_a(x) = a + x$, temos que

$$\begin{aligned}
\lambda_{\bar{0}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{1} & \bar{2} & \bar{3} \end{pmatrix} = \mathrm{id} \\
\lambda_{\bar{1}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{1} & \bar{2} & \bar{3} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \end{pmatrix} \\
\lambda_{\bar{2}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{2} & \bar{3} & \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{2} \end{pmatrix} \begin{pmatrix} \bar{1} & \bar{3} \end{pmatrix} \\
\lambda_{\bar{3}} &= \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{3} & \bar{0} & \bar{1} & \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{0} & \bar{3} & \bar{2} & \bar{1} \end{pmatrix}.
\end{aligned}$$

Assim, $\mathbb{Z}_4 \cong \{\lambda_{\bar{0}}, \lambda_{\bar{1}}, \lambda_{\bar{2}}, \lambda_{\bar{3}}\}$.

Elementos da Teoria de Anéis

lcc :: lmat :: 2.º ano

paula mendes martins

departamento de matemática :: uminho

generalidades

Definição. Seja A um conjunto não vazio e duas operações binárias, que representamos por $+$ e por $\cdot$, nele definidas. O triplo $(A, +, \cdot)$ diz-se um *anel* se

1. $(A, +)$ é um grupo comutativo (também chamado *módulo*);
2. $(A, \cdot)$ é um semigrupo;
3. A operação $\cdot$ é *distributiva* em relação à operação $+$, i.e., para todos $a, b, c \in A$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{e} \qquad (b + c) \cdot a = b \cdot a + c \cdot a.$$

O anel A diz-se *comutativo* se a multiplicação for comutativa.

Observação. Referimo-nos sempre à primeira operação (i.e., à operação para a qual temos um grupo) como *adição*. À segunda operação (i.e., à operação para a qual temos um semigrupo) chamamos *multiplicação*.

Definições. Seja $(A, +, \cdot)$ um anel.

- Ao elemento neutro do grupo chamamos *zero do anel* e representamos por 0_A.
- Quando existe, ao elemento neutro do semigrupo chamamos *identidade do anel* e representamos por 1_A.
- Ao elemento oposto de $a \in A$ para a adição chamamos *simétrico de a* e representamos por $-a$ (note-se que, sendo $(A, +)$ grupo, qualquer elemento do anel admite um único simétrico).
- No caso de o anel ter identidade, podem existir elementos que admitem elemento oposto para a multiplicação. Quando existe, referimo-nos ao elemento oposto de $a \in A$ para a multiplicação como o *inverso de a*. Neste caso, representamos o inverso de a por a^{-1}.

Observação. Se não houver ambiguidade, falamos no anel A quando nos referimos ao anel $(A, +, \cdot)$ e omitimos o sinal da multiplicação na escrita de expressões.

Exemplo 1. Seja $A = \{a\}$. Então, $(A, +, \cdot)$, onde $a + a = a$ e $a \cdot a = a$, é um anel comutativo com identidade, ao qual se chama *anel nulo*. Representa-se por $A = \{0_A\}$.

Exemplo 2. $(\mathbb{Z}, +, \times)$ e $(\mathbb{R}, +, \times)$ são anéis comutativos com identidade.

Exemplo 3. Dado $n \in \mathbb{N}$, $(\mathbb{Z}_n, +, \times)$ é um anel comutativo com identidade.

Exemplo 4. Dado o natural $n \geq 2$, $(n\mathbb{Z}, +, \times)$ é um anel comutativo sem identidade.

Exemplo 5. $(\mathcal{M}_2(\mathbb{R}), +, \times)$ é um anel não comutativo com identidade.

Proposição. Seja A um anel. Então, para todo $x \in A$, $0_A x = x 0_A = 0_A$.

Demonstração. Seja $x \in A$. Então, pela distributividade, temos que $0_A x + 0_A x = (0_A + 0_A)\, x$. Mas,

$$\begin{aligned} 0_A x + 0_A x = (0_A + 0_A)\, x \quad &\Leftrightarrow 0_A x + 0_A x = 0_A x \\ &\Leftrightarrow 0_A x + 0_A x = 0_A x + 0_A \\ &\Leftrightarrow 0_A x = 0_A. \end{aligned}$$

Logo, $0_A x = 0_A$. Analogamente, de

$$x 0_A + x 0_A = x\,(0_A + 0_A)$$

e de

$$x 0_A + x 0_A = x\,(0_A + 0_A) \Leftrightarrow x 0_A = 0_A,$$

obtemos $x 0_A = 0_A$. $\square$

Proposição. Se $A \neq \{0_A\}$ é um anel com identidade 1_A, então $1_A \neq 0_A$.

Demonstração. Se 0_A fosse a identidade do anel, então, para $x \neq 0_A$, teríamos $x = 0_A x$. Mas, pela proposição anterior, $0_A x = 0_A$, pelo que $x = 0_A$. $\square$

Proposição. Sejam A um anel e $x, y \in A$. Então:

1. $(-x)\,y = x\,(-y) = -xy$;
2. $(-x)\,(-y) = xy$.

Demonstração. Sejam $x, y \in A$. Então,

1. $(-x)\,y$ é o simétrico de xy já que
$$(-x)\,y + xy = (-x + x)\,y = 0_A y = 0_A$$
e $x\,(-y)$ é também o simétrico de xy pois
$$x\,(-y) + xy = x\,(-y + y) = x0_A = 0_A;$$
Logo, $-xy = (-x)y = x(-y)$.
2. $(-x)\,(-y)$ é o simétrico de $(-xy)$ já que
$$\begin{aligned}(-x)\,(-y) + (-xy) &= (-x)\,(-y) + (-x)\,y \\ &= (-x)\,(-y + y) = (-x)\,0_A = 0_A.\end{aligned}$$
Como o simétrico de $-xy$ é, de facto, xy, obtemos o resultado pretendido. $\square$

Proposição. Sejam A um anel, $n \in \mathbb{N}$ e $a, b_1, b_2, ..., b_n \in A$. Então,

1. $a\,(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n$;
2. $(b_1 + b_2 + \cdots + b_n)\,a = b_1 a + b_2 a + \cdots + b_n a$.

Observação. A propriedade apresentada na última proposição é conhecida, em Teoria de Anéis, como *propriedade distributiva generalizada*.

Seja $(A, +, \cdot)$ um anel. Então, $(A, +)$ é grupo, pelo que podemos falar nos múltiplos de expoente **inteiro** de $a \in A$. Assim, temos

i. $0a = 0_A$;
ii. $(n+1)\,a = na + a$, para todo $n \in \mathbb{N}_0$;
ii. $na = -(-na)$, para todo $n \in \mathbb{Z}^-$.

Proposição. Sejam A, um anel, $a, b \in A$ e $m, n \in \mathbb{Z}$. Então,

1. $(m+n)\,a = ma + na$;
2. $n\,(ma) = (nm)\,a$;
3. $n\,(a+b) = na + nb$.

Proposição. Sejam A um anel, $a, b \in A$ e $n \in \mathbb{Z}$. Então,

$$n\,(ab) = (na)\,b = a\,(nb)\,.$$

Demonstração. Temos de considerar três casos:

(i) $n = 0$. A demonstração é trivial.

(ii) $n > 0$. Resulta da propriedade distributiva generalizada:

$$(na)\,b = (\underbrace{a + a + \cdot + a}_{n\times})b = \underbrace{ab + ab + \cdots ab}_{n} \times = n(ab)$$

e

$$a\,(nb) = a(\underbrace{b + b + \cdot + b}_{n\times}) = \underbrace{ab + ab + \cdots ab}_{n} \times = n(ab).$$

(iii) $n < 0$. Para $a, b \in A$, temos que

$$n(ab) = -[(-n)(ab)] = -[((-n)a)b] = [-(-(na))]b = (na)b$$

e

$$n\,(ab) = -[(-n)(ab)] = -[a((-n)b)] = a[-(-n)b] = a(nb).$$

Seja $(A, +, \cdot)$ um anel. Então, $(A, \cdot)$ é semigrupo, pelo que podemos falar nas potências de expoente **natural** de $a \in A$. Assim, temos

i. $a^1 = a$;

ii. $a^{n+1} = a^n \cdot a$, para todo $n \in \mathbb{N}$.

Proposição. Sejam A um anel, $a \in A$ e $m, n \in \mathbb{N}$. Então,

1. $(a^n)^m = a^{nm}$;
2. $a^n a^m = a^{n+m}$. $\square$

Observação. Tendo em conta que estamos a trabalhar num anel e, portanto, a trabalhar com duas operações simultaneamente, distinguiremos as duas potências a^n e na (com $a \in A$ e $n \in \mathbb{N}$) falando em *múltiplo de a* para na e em *potência de a* para a^n.

Definição. Seja A um anel com identidade 1_A. Um elemento $a \in A$ diz-se uma *unidade* se admite um inverso em A. Representa-se por $\mathcal{U}_A$ o conjunto das unidades de um anel com identidade.

Exemplo 6. No anel $(\mathbb{Z}, +, \times)$, temos que $\mathcal{U}_A = \{-1, 1\}$.

Exemplo 7. No anel $(\mathbb{R}, +, \times)$, temos que $\mathcal{U}_A = \mathbb{R} \backslash \{0\}$.

Exemplo 8. No anel $(\mathcal{M}_2(\mathbb{R}), +, \times)$, temos que

$$\mathcal{U}_A = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{M}_2(\mathbb{R}) \mid ad - bc \neq 0 \right\}.$$

Quem são as unidades em $(\mathbb{Z}_n, +, \times)$, para $n \in \mathbb{N}$?São os elementos $[x]_n$, com $\mathrm{m.d.c.}(x, n) = 1$.

Definição. Seja A um anel. Um elemento $a \in A$ diz-se *simplificável* se, para todos $x, y \in A$

$$xa = ya \quad ou \quad ax = ay \Longrightarrow x = y.$$

Exemplo 9. Nos anéis $(\mathbb{Z}, +, \times)$ e $(\mathbb{R}, +, \times)$, qualquer elemento não nulo é simplificável.

Exemplo 10. No anel $(\mathcal{M}_2(\mathbb{R}), +, \times)$, o elemento $\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}$ não é simplificável. De facto,

$$\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ -1 & -2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ -3 & -2 \end{bmatrix}$$

e

$$\begin{bmatrix} 1 & 2 \\ -1 & -2 \end{bmatrix} \neq \begin{bmatrix} 3 & 2 \\ -3 & -2 \end{bmatrix}.$$

Observação. Num anel A, todo a unidade é simplificável, mas nem todo o elemento simplificável é uma unidade.

Definição. Seja A um anel. Um elemento $a \in A$ diz-se um *divisor de zero* se existe $b \in A \backslash \{0_A\}$ tal que

$$ab = 0_A \quad \text{ou} \quad ba = 0_A.$$

Observação. O elemento zero de um anel A só não é divisor de zero se $A = \{0_A\}$.

Exemplo 11. Nos anéis $(\mathbb{Z}, +, \times)$ e $(\mathbb{R}, +, \times)$, o único divisor de zero existente é o elemento 0.

Exemplo 12. No anel $(\mathcal{M}_2(\mathbb{R}), +, \times)$, qualquer matriz $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ tal que $ad - bc = 0$ é divisor de zero.

Quem são os divisores de zero em $(\mathbb{Z}_n, +, \times)$, para $n \in \mathbb{N}$?

Exemplo 13.

- Os divisores de zero do anel $(\mathbb{Z}_6, +, \times)$ são os elementos $[0]_6$, $[2]_6$, $[3]_6$ e $[4]_6$ pois
  $[0]_6 \times [1]_6 = [0]_6$, $[2]_6 \times [3]_6 = [0]_6$ e $[4]_6 \times [3]_6 = [0]_6$.

- No anel $(\mathbb{Z}_7, +, \times)$, o único elemento divisor de zero é $[0]_7$.

Proposição. No anel $(\mathbb{Z}_n, +, \times)$, os divisores de zero são os elementos $[x]_n$, onde $\mathrm{m.d.c.}(x, n) \neq 1$.

Demonstração. Se $1 \neq d = \mathrm{m.d.c.}(x, n)$, então, existem $a, b \in \mathbb{Z}$ tais que $d = ax + bn$ e existe $n = kd$. Assim, em $\mathbb{Z}_n$, $[d]_n = [a]_n[x]_n + [0]_n(*)$ e, portanto, $[0]_n = [kd]_n = [ka]_n[x]_n$ com $[ka]_n \neq [0]_n$. $\square$

característica de um anel

Sejam A um anel e $a \in A$. Considerando os múltiplos de a, i.e., os elementos da forma na com $n \in \mathbb{Z}$, temos duas situações a considerar:

(i) $(\exists m \in \mathbb{Z} \setminus \{0\})\ (\forall a \in A) \quad ma = 0_A$;

(ii) $(\forall m \in \mathbb{Z} \setminus \{0\})\, (\exists b \in A) \quad mb \neq 0_A$
(i.e., $nb = 0_A\ (\forall b \in A) \Rightarrow n = 0$).

Exemplo 14. São exemplos da situação (ii) o anel dos reais e o anel dos inteiros.

Exemplo 15. É exemplo da situação (i) o anel $(\mathbb{Z}_4, +, \cdot)$.

Definição. Seja A um anel.

1. Se
$$nb = 0_A,\ \forall b \in A \Rightarrow n = 0,$$
A diz-se um anel de *característica* 0 e escreve-se $c(A) = 0$;

2. Se
$$(\exists m \in \mathbb{Z} \setminus \{0\})\,(\forall a \in A) \quad ma = 0_A,$$
A diz-se um anel de *característica* q onde
$q = \min\{n \in \mathbb{N} : na = 0_A\ \forall a \in A\}$. Escreve-se $c(A) = q$.

Observação. A segunda parte da definição faz todo o sentido, pois se A é um anel que satisfaz 2., temos que, sendo

$$M = \{m \in \mathbb{Z} : ma = 0_A, \quad \forall a \in A\},$$

$(M, +)$ é um subgrupo do grupo cíclico $(\mathbb{Z}, +)$ e, portanto, é ele próprio um grupo cíclico e o seu gerador é o menor inteiro positivo de M.

Como $(A, +)$ é grupo, podemos falar da ordem de qualquer elemento de A.

Se A é um anel de característica q e $x \in A$ é tal que a ordem de x no grupo $(A, +)$ é $o\,(x) = p$, qual a relação de p com q?

A resposta é obviamente $p \mid q$. De facto, se q é a característica de A, temos que $qa = 0_A$, para todo $a \in A$. Em particular, para $a = x$ temos que $qx = 0_A$. Logo, como $p = o\,(x)$, vem, como consequência da definição de ordem de um elemento, que $p \mid q$.

Assim, podemos concluir que a característica de um anel finito A é o m.m.c. entre as ordens de todos os elementos de A.

Proposição. Sejam $A \neq \{0_A\}$ um anel com identidade 1_A e $n \in \mathbb{N}$. Então, a característica de A é n se e só se a ordem de 1_A é n.

Demonstração. $[\Rightarrow]$. Por hipótese, temos que $c(A) = n$, i.e., temos que:

(i) $\forall a \in A \quad na = 0_A$;

(ii) $(\exists p \in \mathbb{N} \forall a \in A \quad pa = 0_A) \implies n \mid p$.

Queremos provar que $o(1_A) = n$, i.e., queremos provar que:

(a) $n1_A = 0_A$;

(b) $(\exists p \in \mathbb{N} : p1_A = 0_A) \implies n \mid p$.

A condição (a) resulta naturalmente da condição (i). Para provarmos a condição (b) supomos que existe $p \in \mathbb{N}$ tal que $p1_A = 0_A$. Para aplicarmos (ii), temos que provar que $pa = 0_A$ para todo $a \in A$. De facto, $pa = p(1_A a) = (p1_A)a = 0_A a = 0_A$. Assim, por (ii), temos que $n \mid p$. Logo, verifica-se a condição (b).

$[\Leftarrow]$. Suponhamos agora que $p(1_A) = n$, i.e., que (a) e (b) são satisfeitos. Queremos provar que o anel satisfaz (i) e (ii):

(i) Para todo $a \in A$, temos que
$$na = n(1_A a) = (n1_A)a = 0_A a = 0_A.$$

(ii) Seja $p \in \mathbb{N}$ tal que, para todo $a \in A$, $pa = 0_A$. Em particular, como $1_A \in A$, temos que $p1_A = 0_A$. Então, por (b), concluímos que $n \mid p$, o que termina a nossa demonstração.

$\square$

Exemplo 16. Seja $n \in \mathbb{N}$. Como, em $\mathbb{Z}_n$, $o(\bar{1}) = n$, concluímos que $c(\mathbb{Z}_n) = n$.

Exemplo 17. O anel dos números inteiros e o anel dos números reais são anéis de característica 0, uma vez que, nestes anéis, $o(1)$ é infinita.

anéis especiais

Definição. Um anel comutativo com identidade A diz-se um *domínio* (ou *anel*) *de integridade* se admitir como único divisor de zero o elemento zero do anel.

Exemplo 18. Os anéis $(\mathbb{Z}, +, \times)$ e $(\mathbb{R}, +, \times)$ são domínios de integridade.

Exemplo 19. O anel das matrizes quadradas de ordem 2 não é um domínio de integridade.

Observação. Se A é um domínio de integridade, então, $A \neq \{0_A\}$.

Proposição. Seja A um anel comutativo com identidade. Então, as seguintes afirmações são equivalentes:

1. A é domínio de integridade;
2. $A \backslash \{0_A\} \neq \emptyset$ e todo o elemento de $A \backslash \{0_A\}$ é simplificável.

Demonstração. Suponhamos que A é um domínio de integridade. Então, $A \backslash \{0_A\} \neq \emptyset$. Sejam $y \in A \backslash \{0_A\}$ e $a, b \in A$ tais que $ya = yb$. Então, $ya - yb = 0_A$, pelo que

$$y\,(a-b) = 0_A.$$

Como A é domínio de integridade e $y \neq 0_A$, temos que

$$a - b = 0_A,$$

i.e.,

$$a = b.$$

Supondo que $ay = by$, faz-se o raciocínio análogo.
Reciprocamente, suponhamos que todo o elemento $y \in A \backslash \{0_A\} \neq \emptyset$ é simplificável. Como $A \backslash \{0_A\} \neq \emptyset$, temos que 0_A é um divisor de zero. Vejamos que é o único elemento nestas condições. Seja x_0 um divisor de zero de A, i.e., seja $x_0 \in A$ para o qual existe $b \in A \backslash \{0_A\}$ tal que

$$bx_0 = 0_A \qquad \text{ou} \qquad x_0 b = 0_A.$$

Suponhamos, sem perda de generalidade, que é a primeira condição que se verifica. Então,

$$bx_0 = 0_A = b0_A.$$

e, como b é simplificável (já que $b \neq 0_A$), temos que

$$x_0 = 0_A.$$

Logo, 0_A é o único dividor de zero, pelo que A é um domínio de integridade. $\square$

Proposição. Seja A um anel comutativo com identidade. Então, as seguintes afirmações são equivalentes:

1. A é domínio de integridade;
2. $A\setminus\{0_A\} \neq \emptyset$ e $A\setminus\{0_A\}$ é subsemigrupo de A relativamente ao produto.

Demonstração. Suponhamos que A é domínio de integridade. Então, $A\setminus\{0_A\} \neq \emptyset$. Provemos então que $(A\setminus\{0_A\}, \cdot)$ é subsemigrupo de $(A, \cdot)$. De facto:

(a) $A\setminus\{0_A\} \subseteq A$;

(b) se $a, b \in A\setminus\{0_A\}$, $ab \in A\setminus\{0_A\}$. Se $ab = 0_A$, com $a, b \in A\setminus\{0_A\}$, a e b seriam divisores de zero e, portanto, A não seria um domínio de integridade.

Reciprocamente, suponhamos que $A\setminus\{0_A\} \neq \emptyset$ e que $(A\setminus\{0_A\}, \cdot)$ é subsemigrupo de $(A, \cdot)$, ou seja, que

$$a \neq 0_A, b \neq 0_A \Longrightarrow ab \neq 0_A. \qquad (*)$$

De $A\setminus\{0_A\} \neq \emptyset$ concluímos que 0_A é divisor de zero. Provemos que é único. Seja x_0 um divisor de zero. Então, existe $y \in A\setminus\{0_A\}$ tal que

$$x_0 y = 0_A \qquad \text{ou} \qquad y x_0 = 0_A.$$

Comparando com (*), concluímos que $x_0 = 0_A$. $\square$

Proposição. Seja A um anel comutativo com identidade. Então, as seguintes afirmações são equivalentes:

1. A é domínio de integridade;
2. $A \setminus \{0_A\} \neq \emptyset$ e, se as equações $ax = b$ e $xa = b$ $(a \neq 0_A)$ tiverem solução, então, a solução é única.

Demonstração. Seja A um domínio de integridade. Então, $A \setminus \{0_A\} \neq \emptyset$. Suponhamos que, para $a, b \in A$ com $a \neq 0_A$,

$$(\exists x_0, y_0 \in A) \qquad ax_0 = b \quad \text{e} \quad y_0 a = b.$$

Sejam x_1 e y_1 outras soluções das equações $ax = b$ e $xa = b$, respetivamente. Então,

$$ax_0 = b = ax_1 \qquad \text{e} \qquad y_0 a = b = y_1 a$$

e, pelo facto de todos os elementos não nulos serem simplificáveis, temos que

$$x_0 = x_1 \qquad \text{e} \qquad y_0 = y_1 .$$

Logo, as soluções, quando existem, são únicas.

Reciprocamente, suponhamos que $A \setminus \{0_A\} \neq \emptyset$ e que, para $a \in A \setminus \{0_A\}$ e $b \in A$, se as equações $ax = b$ e $xa = b$ tiverem solução, então, a solução é única.

Como $x = 0_A$ é solução de $ax = 0_A$ e $xa = 0_A$, concluímos então que $x = 0_A$ é a única solução possível. Logo, 0_A é o único divisor de zero de A, pelo que A é um domínio de integridade. $\square$

Definição. Um anel A diz-se um *anel de divisão* se $(A\setminus\{0_A\},\cdot)$ é um grupo. Um anel de divisão comutativo diz-se um *corpo*.

Resulta da definição que qualquer corpo é um domínio de integridade, mas o recíproco não é verdadeiro.

Exemplo 20. O domínio de integridade $(\mathbb{Z},+,\times)$ não é um anel de divisão, pois $(\mathbb{Z}\setminus\{0\},\times)$ não é grupo.

Exemplo 21. O domínio de integridade $(\mathbb{R},+,\times)$ é um corpo e, portanto, um anel de divisão.

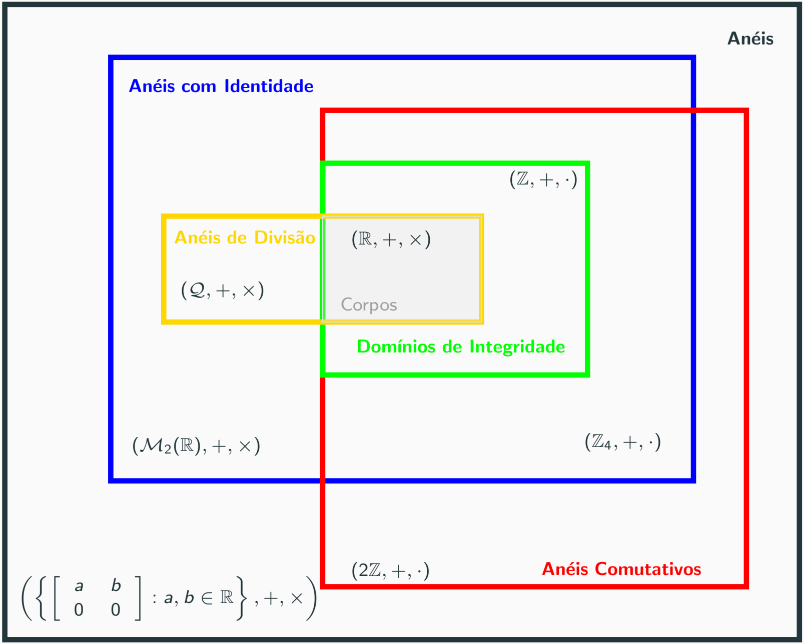
Exemplo 22. Seja $\mathcal{Q} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$, onde $i^2 = j^2 = k^2 = -1$, $ij = -ji = k, ki = -ik = j, jk = -kj = i$. Considere em $\mathcal{Q}$ as operações $+$ e $\times$ definidas por

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k)$$
$$= a + a' + (b + b')i + (c + c')j + (d + d')k$$

e

$$(a + bi + cj + dk) \times (a' + b'i + c'j + d'k) =$$
$$aa' - bb' - cc' - dd' + (ab' + a'b + cd' - c'd)i +$$
$$(ac' - bd' + a'c + b'd)j + (ad' + bc' - b'c + a'd)k.$$

Então, $(\mathcal{Q}, +, \times)$ é um anel de divisão não comutativo. Este anel designa-se por *Anel dos Quarteniões.*



Anéis
Anéis com Identidade
$(\mathbb{Z}, +, \cdot)$
Anéis de Divisão
$(\mathbb{R}, +, \times)$
$(\mathcal{Q}, +, \times)$
Corpos
Domínios de Integridade
$(\mathcal{M}_2(\mathbb{R}), +, \times)$
$(\mathbb{Z}_4, +, \cdot)$
$(2\mathbb{Z}, +, \cdot)$
Anéis Comutativos
$\left(\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{R}\right\}, +, \times\right)$

subanéis

Definição. Uma parte A' de um anel (respetivamente, domínio de integridade, anel de divisão, corpo) A diz-se um *subanel (respetivamente, subdomínio de integridade, subanel de divisão, subcorpo) de* A se for um anel (respetivamente, domínio de integridade, anel de divisão, corpo) relativamente às restrições das operações de adição e produto do anel.

Exemplo 23. Quando consideradas as operações usuais de adição e multiplicação, o anel $\mathbb{Z}$ é subanel e subdomínio de integridade de $\mathbb{R}$, mas não é seu subanel de divisão, nem subcorpo.

Exemplo 24. Quando consideradas as operações usuais de adição e multiplicação, o anel $n\mathbb{Z}$ ($n \in \mathbb{N} \backslash \{1\}$) é subanel mas não é subdomínio de integridade de $\mathbb{Z}$.

Exemplo 25. Dado um anel A, $\{0_A\}$ e A são subanéis de A. No entanto, dado um anel de divisão ou corpo A, $\{0_A\}$ não é subanel de divisão nem subcorpo de A.

Proposição. Sejam A um anel e $A' \subseteq A$. Então, A' é subanel de A se e só se:

1. $A' \neq \emptyset$;
2. $x, y \in A' \Rightarrow x - y \in A'$;
3. $x, y \in A' \Rightarrow xy \in A'$ $\square$

Proposição. Sejam A um domínio de integridade e $A' \subseteq A$. Então, A' é subdomínio de integridade de A se e só se:

1. $1_A \in A'$;
2. $x, y \in A' \Rightarrow x - y \in A'$;
3. $x, y \in A' \Rightarrow xy \in A'$ $\square$

Proposição. Sejam A um anel de divisão (respetivamente, corpo) e $A' \subseteq A$. Então, A' é subanel de divisão (respetivamente, subcorpo) de A se e só se:

1. $A' \neq \emptyset$;
2. $x, y \in A' \Rightarrow x - y \in A'$;
3. $x, y \in A' \setminus \{0_A\} \Rightarrow xy^{-1} \in A' \setminus \{0_A\}$. $\square$

INTERSECÇÃO Sejam A um anel e A_1 e A_2 subanéis de A. Então, $A_1 \cap A_2$ é subanel de A.

UNIÃO Sejam A um anel e A_1 e A_2 subanéis de A. A união $A_1 \cup A_2$ não é necessariamente um subanel de A.

SOMA Sejam A um anel e A_1 e A_2 subanéis de A. Como $(A_1, +)$ e $(A_2, +)$ são subgrupos do grupo comutativo $(A, +)$, sabemos que o subconjunto

$$A_1 + A_2 = \{a_1 + a_2 : a_1 \in A_1,\ a_2 \in A_2\}$$

de A é subgrupo de $(A, +)$ (Relembrar que se G é grupo e $H, K < G$ então $HK < G$ se e só se $HK = KH$; em linguagem aditiva, escrevemos $H + K < G$ se e só se $H + K = K + H$). No entanto, dados $a_1 + a_2, b_1 + b_2 \in A_1 + A_2$,

$$(a_1 + a_2)(b_1 + b_2) = a_1 b_1 + a_2 b_1 + a_1 b_2 + a_2 b_2$$

não é necessariamente um elemento de $A_1 + A_2$, pelo que $A_1 + A_2$ não é necessariamente um subanel de A.

ideais e relações de congruência num anel

Definição. Seja A um anel. Uma parte I de A diz-se um *ideal direito* (respetivamente, *ideal esquerdo*) de A se:

1. $(I, +) < (A, +)$;
2. $(\forall a \in A)\,(\forall x \in I) \quad xa \in I$ (respetivamente, $ax \in I$)

Se I for simultaneamente ideal esquerdo e ideal direito, então, I diz-se um *ideal de A*.

Exemplo 26. Consideremos o anel $(\mathbb{Z}, +, \times)$. O conjunto $2\mathbb{Z}$ é um seu ideal pois $(2\mathbb{Z}, +) < (\mathbb{Z}, +)$ e o produto de um inteiro qualquer por um inteiro par é um inteiro par.

Exemplo 27. Relativamente ao anel $(\mathbb{Z}_4, +, \cdot)$, o conjunto $\{\bar{0}, \bar{2}\}$ é um ideal pois

$$(\{\bar{0}, \bar{2}\}, +) < (\mathbb{Z}_4, +)$$

e

$$\begin{array}{l} \bar{0} \cdot \bar{0} = \bar{0} \cdot \bar{1} = \bar{0} \cdot \bar{2} = \bar{0} \cdot \bar{3} = \bar{0} \in \{\bar{0}, \bar{2}\} \\ \bar{2} \cdot \bar{0} = \bar{2} \cdot \bar{2} = \bar{0} \in \{\bar{0}, \bar{2}\} \quad e \quad \bar{2} \cdot \bar{1} = \bar{2} \cdot \bar{3} = \bar{2} \in \{\bar{0}, \bar{2}\}. \end{array}$$

Como o anel em questão é comutativo, concluímos que $\{\bar{0}, \bar{2}\}$ é um ideal de $\mathbb{Z}_4$.

Exemplo 28. Seja A um anel. Então, $\{0_A\}$ é um ideal de A (ao qual se chama *ideal trivial de* A).

Exemplo 29. Um anel A é um ideal de si próprio (ao qual se chama *ideal impróprio de* A).

Proposição. Todo o ideal de um anel A é um subanel de A. $\square$

Proposição. A intersecção de uma família de ideais de um anel A é um ideal de A. $\square$

Proposição. Num anel com identidade todo o ideal que contém essa identidade é impróprio.

Demonstração. Sejam A um anel com identidade 1_A e I um ideal de A tal que $1_A \in I$. Então,

$$\forall a \in A, \qquad a = a \cdot 1_A \in I.$$

Logo, $A \subseteq I$. Como, por definição, $I \subseteq A$, temos o resultado pretendido, i.e., $I = A$. $\square$

Proposição. Num anel de divisão existem apenas dois ideais: o trivial e o impróprio.

Demonstração. Vimos já que $\{0_A\}$ e A são ideais de qualquer anel A. Vejamos que, se A é um anel de divisão, estes ideais são de facto os únicos ideais de A. Seja $I \neq \{0_A\}$ um ideal de A. Então, existe $x \in A \setminus \{0_A\}$ tal que $x \in I$. Mas, como $(A \setminus \{0_A\}, \cdot)$ é um grupo, temos que $x^{-1} \in A \setminus \{0_A\} \subseteq A$. Assim, como I é um ideal de A, temos que

$$1_A = xx^{-1} \in I.$$

Logo, I é um ideal que contém a identidade do anel, pelo que, pela proposição anterior, é o ideal impróprio. $\square$

Exemplo 30. Os únicos ideias do corpo $\mathbb{R}$ são $\{0\}$ e o próprio $\mathbb{R}$.

O facto de $2\mathbb{Z}$ ser ideal de $\mathbb{Z}$ permite-nos concluir que $\mathbb{Z}$ não é corpo.

Podemos ter ideais de um anel A que sejam gerados por um elemento de a.

Definição. Sejam A um anel e $a \in A$. Chama-se *ideal principal direito* (respetivamente, *ideal principal esquerdo, ideal principal*) *gerado por a*, e representa-se por $(a)_d$ (respetivamente $(a)_e$, (a)) ao menor ideal direito (respetivamente, ideal esquerdo, ideal) que contém a.

Exemplo 31. Consideremos o anel $\mathbb{Z}_4$ com as operações usuais de adição e multiplicação de classes. Como a multiplicação é comutativa, todos os ideais esquerdos são direitos e viceversa, pelo que podemos falar simplesmente em ideais. Os ideais de $\mathbb{Z}_4$ são $\{\bar{0}\}$, $\{\bar{0}, \bar{2}\}$ e $\mathbb{Z}_4$. Assim, temos que

$$(\bar{0}) = \{\bar{0}\}, \quad (\bar{2}) = \{\bar{0}, \bar{2}\}, \quad (\bar{1}) = (\bar{3}) = \mathbb{Z}_4.$$

Proposição. Sejam A um anel e $a \in A$. Então,

1. $(a)_d$ é a intersecção de todos os ideais direitos de A que contêm a.
2. $(a)_e$ é a intersecção de todos os ideais esquerdos de A que contêm a.
3. (a) é a intersecção de todos os ideais de A que contêm a.

$\square$

Exemplo 32. No corpo $\mathbb{R}$, $(0) = \{0\}$ e $(x) = \mathbb{R}$, para todo $x \neq 0$.

Exemplo 33. No domínio de integridade $\mathbb{Z}$, $(-n) = (n) = n\mathbb{Z}$, para todo $n \in \mathbb{N}_0$.

Proposição. Sejam A um anel com identidade e $a \in A$. Então, $(a)_d = aA$ e $(a)_e = Aa$.

Demonstração. Seja A um anel com identidade 1_A e $a \in A$. Pretendemos provar que

$$aA = \{ax \mid x \in A\}$$

é o menor ideal direito que contém a.

De facto, $(aA, +)$ é um subgrupo de $(A, +)$, pois

(i) $aA \neq \emptyset$, já que $a = a \cdot 1_A \in aA$;

(ii) $ax, ay \in aA \Rightarrow ax - ay = a(x - y) \in A$;

Mais ainda,

$$x \in A, ay \in aA \Rightarrow (ay)x = a(xy) \in aA,$$

pelo que aA é um ideal de A.

Por outro lado, ao provar que $aA \neq \emptyset$, provamos que aA contém a.

Finalmente, seja J um ideal direito de A tal que $a \in J$. Então,

$$\begin{aligned} x \in aA \quad &\Rightarrow \quad x = ay \quad \text{com } y \in A \\ &\Rightarrow \quad x = ay \quad \text{com } a \in J \text{ e } y \in A \\ &\Rightarrow \quad x = ay \in J. \end{aligned}$$

De modo análogo, prova-se que $(a)_e = Aa$. $\square$

Corolário. Sejam A um anel comutativo com identidade e $a \in A$. Então, $(a) = Aa = aA$. $\square$

Definição. Seja A um anel. Uma relação de equivalência ρ definida em A diz-se uma *relação de congruência* se, para todos $x, x', y, y' \in A$,

$$x \,\rho\, x' \quad \text{e} \quad y \,\rho\, y' \Rightarrow (x+y) \,\rho\, \left(x'+y'\right) \quad \text{e} \quad (xy) \,\rho\, \left(x'y'\right).$$

Exemplo 34. Considere-se em $\mathbb{Z}$ a relação

$$a \,\rho\, b \Leftrightarrow a - b \in 2\mathbb{Z}.$$

Então, a relação ρ é de equivalência e é tal que

$$\begin{array}{rcl} a \,\rho\, b \quad \text{e} \quad a' \,\rho\, b' & \Leftrightarrow & a-b, a'-b' \in 2\mathbb{Z} \\ & \Rightarrow & a + a' - \left(b + b'\right) \in 2\mathbb{Z} \quad \text{e} \\ & & aa' - bb' = aa' - ba' + ba' - bb' = (a-b)\,a' + b\left(a' - b'\right) \in 2\mathbb{Z} \\ & \Leftrightarrow & \left(a + a'\right) \,\rho\, \left(b + b'\right) \quad \text{e} \quad aa' \,\rho\, bb', \end{array}$$

pelo que ρ é uma relação de congruência em $\mathbb{Z}$.

Proposição. Sejam A um anel e I um ideal de A. Então, a relação definida em A por

$$a \,\rho\, b \Leftrightarrow a - b \in I$$

é uma relação de congruência.

Demonstração. Comecemos por provar que ρ é uma relação de equivalência em A: Como $(I, +)$ é subgrupo comutativo de $(A, +)$, temos que:

(i) para todo $a \in A$, $a - a = 0_A \in I$ e, portanto, $a \,\rho\, a$. Assim, ρ é reflexiva;

(ii) se $a, b \in A$ são tais que $a \,\rho\, b$, temos que $a - b \in I$ e, portanto, $b - a = -(a - b) \in I$. Logo, $b \,\rho\, a$, o que nos permite concluir que ρ é simétrica;

(iii) se $a, b, c \in A$ são tais que $a \,\rho\, b$ e $b \,\rho\, c$, temos que $a - b \in I$ e $b - c \in I$ e, portanto,

$$a - c = (a - b) + (b - c) \in I.$$

Assim, $a \,\rho\, c$, o que nos permite concluir que ρ é transitiva.

Assim, ρ é uma relação de equivalência. Para concluir que ρ é uma relação de congruência basta verificar que

$$a \,\rho\, b, \;\; a' \,\rho\, b' \Rightarrow (a + a') \,\rho\, (b + b') \text{ e } aa' \,\rho\, bb'.$$

De facto, como I é ideal de A,

$$\begin{aligned} a \,\rho\, b, \;\; a' \,\rho\, b' \quad & \Rightarrow a - b, a' - b' \in I \\ & \Rightarrow (a + a') - (b + b') \in I, \\ & \qquad aa' - bb' = aa' - ba' + ba' - bb' = (a - b)a' + b(a' - b') \in I \\ & \Leftrightarrow (a + a') \,\rho\, (b + b'), \;\; aa' \,\rho\, bb'. \end{aligned}$$

$\square$

Proposição. Seja ρ uma relação de congruência definida num anel A. Então:

1. a classe $[0_A]_\rho$ é um ideal de A;
2. $a\,\rho\,b \Leftrightarrow a - b \in [0_A]_\rho$;
3. $(\forall a \in A) \quad [a]_\rho = a + [0_A]_\rho \, (= \{a + x \in A \mid x\,\rho\,0_A\})$.

Demonstração. (i) Sendo uma classe de equivalência, temos que $\neq \emptyset$. Sejam $a, b \in [0_A]_\rho$. Então, $a\,\rho\,0_A$ e $b\,\rho\,0_A$ e, portanto, $a - b\,\rho\,0_A$, pelo que $a - b \in [0_A]_\rho$. Então, $([0_A]_\rho, +) < (A, +)$. Sejam $a \in [0_A]_\rho$ e $x \in A$. Então $a\,\rho\,0_A$ e $x\,\rho\,x$ e, portanto, $ax\,\rho\,0_A x$ e $xa\,\rho\,x0_A$, i.e., $ax\,\rho\,0_A$ e $xa\,\rho\,0_A$. Assim, $ax, xa \in [0_A]_\rho$. Estamos em condições de concluir que $[0_A]_\rho$ é um ideal de A.

(ii) Sejam $a, b \in A$. Então,

$$a\,\rho\,b \Leftrightarrow a - b\,\rho\,b - b \Leftrightarrow a - b\,\rho\,0_A \Leftrightarrow a - b \in [0_A]_\rho .$$

(iii) Seja $a \in A$. Então,

$$b \in [a]_\rho \Leftrightarrow b\,\rho\,a \Leftrightarrow b - a \in [0_A]_\rho \Leftrightarrow b = a + [0_A] .$$

□

anéis quociente

definição

Se ρ é uma relação de congruência num anel A (e, portanto, de equivalência), podemos então falar no conjunto quociente

$$A/\rho = \left\{ [a]_\rho \mid a \in A \right\}.$$

Neste conjunto, definem-se duas operações binárias:

1. uma adição de classes: para $a, b \in A$,

$$[a]_\rho + [b]_\rho = [a + b]_\rho \,;$$

2. uma multiplicação de classes: para $a, b \in A$,

$$[a]_\rho \cdot [b]_\rho = [a \cdot b]_\rho \,.$$

Sendo ρ uma relação de congruência, prova-se que as operações estão bem definidas, i.e., não dependem da escolha do representante da classe:

Se $[a]_\rho = [a']_\rho$ e $[b]_\rho = [b']_\rho$, temos que

$$a \, \rho \, a' \text{ e } b \, \rho \, b',$$

pelo que

$$(a + b) \, \rho \, (a' + b') \quad \text{e} \quad (ab) \, \rho \, (a'b')$$

e, portanto,

$$[a + b]_\rho = [a' + b']_\rho \quad \text{e} \quad [ab]_\rho = [a'b']_\rho \, .$$

Teorema. Sejam A um anel e ρ uma relação de congruência definida em A. Então, considerando a adição e a multiplicação acima definidas, $(A/\rho, +, \cdot)$ é um anel. $\square$

Observação. Sabemos que existe uma relação biunívoca entre o conjunto das relações de congruência em A e o conjunto dos ideais de A. Assim, se I é ideal de A, podemos também falar num anel quociente:

Definição. Sejam A um anel e I é ideal de A. Chama-se *anel quociente módulo* I ao anel $(A/I, +, \cdot)$, onde

- $A/I = \{x + I : x \in A\}$ e
$$y \in x + I \Leftrightarrow y - x \in I.$$
- para todos $x, y \in A$,
$$(x + I) + (y + I) = (x + y) + I$$
e
$$(x + I)(y + I) = xy + I.$$

Proposição. Sejam A um anel e I um ideal de A.

1. Se A é uma anel comutativo, então A/I é um anel comutativo;
2. Se A é um anel com identidade 1_A, então A/I é um anel com identidade $1_A + I$. $\square$

Exemplo 32. Considerando o anel dos inteiros relativos, sabemos que, para cada $n \in \mathbb{N}$, $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$. Podemos então considerar o anel quociente $\mathbb{Z}/n\mathbb{Z}$. Mais ainda, para cada $x \in \mathbb{Z}$,

$$[x]_{n\mathbb{Z}} = x + n\mathbb{Z} = r + n\mathbb{Z} = [r]_n,$$

onde r é o resto da divisão inteira de x por n e, por isso, é tal que $0 \leq r \leq n - 1$.

Logo,

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

Definição. Seja A um anel comutativo com identidade. Um ideal I de A diz-se *maximal* se não existir um ideal K de A tal que

$$I \underset{\neq}{\subseteq} K \underset{\neq}{\subseteq} A.$$

Exemplo 33. O ideal $2\mathbb{Z}$ do anel $\mathbb{Z}$ é maximal. O ideal $4\mathbb{Z}$ não é maximal pois

$$4\mathbb{Z} \underset{\neq}{\subseteq} 2\mathbb{Z} \underset{\neq}{\subseteq} \mathbb{Z}.$$

Definição. Seja A um anel comutativo com identidade. Um ideal I de A diz-se *primo* se $A \backslash I \neq \emptyset$ e $A \backslash I$ é fechado para o produto.

Exemplo 34. O ideal $2\mathbb{Z}$ do anel $\mathbb{Z}$ é primo. De facto, $\mathbb{Z} \backslash 2\mathbb{Z} = 2\mathbb{Z} + 1$ é fechado para o produto, já que, para todos $n, m \in \mathbb{Z}$,

$$(2n+1)(2m+1) = 2(n+m+2nm) + 1.$$

Teorema. Sejam A um anel comutativo com identidade e I um ideal de A. Então, são equivalentes as seguintes afirmações:

1. I é maximal;
2. A/I é corpo.

Demonstração. $[(i) \Rightarrow (ii)]$. Como A é um anel comutativo com identidade, temos que A/I é um anel comutativo com identidade. Para provar que A/I é corpo, falta apenas provar que todo o elemento não nulo $x + I \in A/I$ admite um inverso.

Seja $a + I \in A/I$ tal que $a + I \neq I$. Então,

$$K = \{i + xa \in A \mid i \in I \text{ e } x \in A\}$$

é um ideal de A. De facto,

(a) $0_A = 0_A + 0_A a$, pelo que $0_A \in K$ e, portanto, $K \neq \emptyset$;

(b) para $i + xa, j + ya \in K$, temos que $i + xa - (j + ya) = (i - j) + (x - y)\, a \in K$;

(c) Para $i + xa \in K$ e $y \in A$, temos que $y\,(i + xa) = yi + (yx)\, a$. Como $yi \in I$ (porque I é ideal) e $yx \in A$, concluímos que $y\,(i + xa) \in K$.

Como o anel é comutativo, concluímos que K é um ideal de A.

Mais ainda, o ideal assim definido K é tal que $I \subsetneq K$. De facto,

$$i \in I \Rightarrow i = i + 0_A a \in K$$

e $a \notin I$ é tal que $a = 0_A + 1_A a \in K$.

Logo, porque I é um ideal maximal por hipótese, temos que $K = A$. Então, $1_A \in K$, pelo que existem $i_1 \in I$ e $x_1 \in A$ tais que $1_A = i_1 + x_1 a$, ou seja, $1_A - x_1 a = i_1 \in I$. Logo, $(1_A - x_1 a) + I = I$. Mas,

$$(1_A - x_1 a) + I = I \Leftrightarrow x_1 a + I = 1_A + I \Leftrightarrow (x_1 + I)(a + I) = 1_A + I,$$

pelo que $(a+I)^{-1} = x_1 + I$.

$[(ii) \Rightarrow (i)]$. Seja I um ideal de A tal que A/I é um corpo.

Suponhamos que existe um ideal K de A, tal que $I \subsetneqq K \subseteq A$. De $I \subsetneqq K$, concluímos que

$$(\exists x \in K) \qquad x \notin I.$$

Logo, $x + I \neq I$. Mas,

$$\begin{aligned} x + I \neq I \quad & \Rightarrow \quad \left(\exists x' + I \in (A/I) \setminus \{I\}\right) \quad (x+I)\left(x'+I\right) = 1_A + I \\ & \Rightarrow \quad \left(\exists x' \in A \backslash I\right) \quad xx' + I = 1_A + I \\ & \Rightarrow \quad \left(\exists x' \in A \backslash I\right) \quad xx' - 1_A = i \in I \\ & \Rightarrow \quad \left(\exists x' \in A\right) \quad 1_A = xx' - i, \quad \text{com } i, x \in K, \\ & \Rightarrow \quad 1_A \in K. \end{aligned}$$

Assim, $K = A$ e, portanto, I é maximal. □

Exemplo 35. Se considerarmos o anel $\mathbb{Z}$, um ideal é maximal se e só se é do tipo $p\mathbb{Z}$, com p primo, pois $\mathbb{Z}_p$ só é corpo se p for primo.

Teorema. Sejam A um anel comutativo com identidade e I um ideal de A. Então, são equivalentes as seguintes afirmações:

1. I é ideal primo;
2. A/I é um domínio de integridade.

Demonstração. $[(i) \Rightarrow (ii)]$. Como A é um anel comutativo com identidade, A/I também. Mais ainda, como I é primo, $A \backslash I \neq \emptyset$, pelo que $A/I \neq \{I\}$. Para provar que A/I é um domínio de integridade, falta então provar que

$$(x+I)(y+I) = I \Longrightarrow x+I = I \text{ ou } y+I = I.$$

De facto,

$$\begin{aligned}
(x+I)(y+I) = I \quad &\Longleftrightarrow \quad xy + I = I \\
&\Longleftrightarrow \quad xy \in I \\
&\Longrightarrow \quad x \in I \text{ ou } y \in I \qquad (I \text{ primo}) \\
&\Longleftrightarrow \quad x + I = I \text{ ou } y + I = I.
\end{aligned}$$

$[(ii) \Rightarrow (i)]$. Seja A um anel e I um ideal de A tal que A/I é um domínio de integridade. Então, $A/I \neq \{I\}$ e, portanto, $A \neq I$ pelo que $A \backslash I \neq \emptyset$.

Sejam $a, b \in A \backslash I$. Pretendemos provar que $ab \in A \backslash I$.

Suponhamos que $ab \in I$. Então, $ab + I = I$. Logo,

$$(a+I)(b+I) = I \Longrightarrow a+I = I \text{ ou } b+I = I,$$

o que contradiz a hipótese de $a, b \in A \backslash I$. $\square$

Como consequência dos dois últimos teoremas, temos que

Corolário. Qualquer anel maximal de um anel comutativo com identidade é ideal primo.

Demonstração. A demonstração é trivial, tendo em conta que todo o corpo é um domínio de integridade. Assim,

$$I \text{ ideal maximal} \iff A/I \text{ corpo} \implies A/I \text{ domínio de integridade} \iff I \text{ ideal primo.}$$

$\square$

morfismos

Definição. Sejam A e A' dois anéis. Uma aplicação $\varphi : A \to A'$ diz-se um *morfismo* (ou *homomorfismo*) *de anéis* se satisfaz as seguintes condições:

1. $(\forall a, b \in A) \qquad \varphi(a+b) = \varphi(a) + \varphi(b)\,;$
2. $(\forall a, b \in A) \qquad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)\,.$

Um morfismo diz-se um *monomorfismo* (respetivamente, *epimorfismo, isomorfismo*) se for injetivo (respetivamente, sobrejetivo, bijetivo)

Um morfismo diz-se um *endomorfismo* se $A = A'$. Um endomorfismo bijetivo diz-se um *automorfismo.*

Exemplo 36. Sejam A e A' anéis. Então, a aplicação $\varphi_0 : A \to A'$ definida por $\varphi_0(x) = 0_{A'}$, para todo $x \in A$, é um morfismo, ao qual chamamos *morfismo nulo.*

Exemplo 37. Seja A um anel. Então, a aplicação identidade em A é um automorfismo, ao qual chamamos *morfismo identidade.*

Exemplo 38. A aplicação $\varphi : \mathbb{Z} \to \mathbb{Z}_{10}$ definida por $\varphi(n) = [6n]_{10}$, para todo $n \in \mathbb{Z}$, é um homomorfismo de anéis. De facto, para $n, m \in \mathbb{Z}$ temos:

1. $\varphi(n+m) = [6(n+m)]_{10} = [6n+6m]_{10} = [6n]_{10} + [6m]_{10} = \varphi(n) + \varphi(m)$;
2. $\varphi(nm) = [6(nm)]_{10} = [36(nm)]_{10} = [(6n)(6m)]_{10} = [6n]_{10}[6m]_{10} = \varphi(n)\varphi(m)$, uma vez que $36 \equiv 6 (\mathrm{mod}\, 10)$.

Proposição. Sejam A e A' dois anéis e $\varphi : A \to A'$ um morfismo. Então, $\varphi(0_A) = 0_{A'}$.

Demonstração. De

$$0_{A'} + \varphi(0_A) = \varphi(0_A) = \varphi(0_A + 0_A) = \varphi(0_A) + \varphi(0_A)$$

concluímos, pela lei do corte, que

$$\varphi(0_A) = 0_{A'}. \qquad \square$$

Exemplo. 39. A aplicação $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida por $\varphi((n, m)) = 3n + m + 3$ não é um morfismo de anéis pois
$\varphi(0_{\mathbb{Z}\times\mathbb{Z}}) = \varphi((0, 0)) = 3 \times 0 + 0 + 3 = 3 \neq 0 = 0_{\mathbb{Z}}$.

Proposição. Sejam A e A' dois anéis e $\varphi : A \to A'$ um morfismo. Então, $(\forall a \in A) \quad \varphi(-a) = -\varphi(a)$.

Demonstração. Seja $a \in A$. Como

$$\varphi(-a) + \varphi(a) = \varphi(-a + a) = \varphi(0_A) = 0_{A'},$$

temos que

$$-\varphi(a) = \varphi(-a). \qquad \square$$

Proposição. Sejam A e A' dois anéis e $\varphi : A \to A'$ um morfismo. Então, $(\forall a \in A)\,(\forall k \in \mathbb{Z}) \quad \varphi\,(ka) = k\varphi\,(a)\,.$

Demonstração. Temos de considerar 3 casos:

- $k = 0$. Seja $a \in A$. Então,
$$\varphi\,(0a) = \varphi\,(0_A) = 0_{A'} = 0\varphi\,(a)\,;$$
- $k \in \mathbb{Z}^+$. Seja $a \in A$. Então, como $\varphi\,(1a) = \varphi\,(a) = 1\varphi\,(a)$ e, sempre que $\varphi\,(na) = n\varphi\,(a)\,,$ temos que
$$\varphi\,((n+1)\,a) = \varphi\,(na + a) = \varphi\,(na) + \varphi\,(a) = n\varphi\,(a) + \varphi\,(a) = (n+1)\,\varphi\,(a)\,,$$
concluímos, por indução, que $\varphi\,(ka) = k\varphi\,(a)$, para todo $k \in \mathbb{N}$.
- $k \in \mathbb{Z}^-$. Seja $a \in A$. Então,
$$\varphi\,(ka) = \varphi\,(-(-k)a) = -\varphi\,((-k)a) = -(-k)\varphi\,(a) = k\varphi\,(a)\,. \qquad \square$$

Proposição. Sejam $\varphi : A \to A'$ um morfismo de anéis e B um subanel de A. Então, $\varphi(B)$ é um subanel de A'. $\square$

Demonstração. Seja B um subanel de A. Então,

(i) $\varphi(B) \neq \emptyset$, pois $0_{A'} = \varphi(0_A)$ e $0_A \in B$;

(ii) dados $x, y \in \varphi(B)$, existem $a, b \in B$ tais que $x = \varphi(a)$ e $y = \varphi(b)$, pelo que

$$x - y = \varphi(a) - \varphi(b) = \varphi(a - b) \quad \text{com } a - b \in B$$

e

$$xy = \varphi(a)\varphi(b) = \varphi(ab) \quad \text{com } ab \in B.$$

Assim, $x - y, xy \in \varphi(B)$, pelo que $\varphi(B)$ é um subanel de A'.

Proposição. Sejam $\varphi : A \to A'$ um epimorfismo de anéis e I um ideal de A. Então, $\varphi(I)$ é um ideal de A'. $\square$

Demonstração. Pela proposição anterior, temos que $(\varphi(I), +) < (A', +)$. Por outro lado, sejam $a' \in A'$ e $x' \in \varphi(I)$. Então, existem $a \in A$ e $i \in I$ tais que $\varphi(a) = a'$ e $\varphi(i) = x'$, pelo que

$$a'x' = \varphi(a)\varphi(i) = \varphi(ai) \in \varphi(I)$$

e

$$x'a' = \varphi(i)\varphi(a) = \varphi(ia) \in \varphi(I).$$

Logo, $a'x', x'a' \in \varphi(I)$, pelo que $\varphi(I)$ é um ideal de A'. $\square$

Proposição. Sejam $\varphi : A \to A'$ um morfismo de anéis e B' um subanel de A'. Então,

$$\varphi^{-1}\left(B'\right) = \left\{x \in A \mid \varphi(x) \in B'\right\}$$

é um subanel de A.

Demonstração. Seja B' um subanel de A'. Então,

(i) $\varphi^{-1}\left(B'\right) \neq \emptyset$ pois $\varphi(0_A) = 0_{A'} \in B'$, pelo que $0_A \in \varphi^{-1}(B')$;

(ii) dados $x, y \in \varphi^{-1}\left(B'\right)$, temos que $\varphi(x), \varphi(y) \in B'$ e, portanto, $\varphi(x-y) = \varphi(x) - \varphi(y) \in B'$, pelo que $x - y \in \varphi^{-1}\left(B'\right)$;

(iii) dados $x, y \in \varphi^{-1}\left(B'\right)$, temos que $\varphi(x), \varphi(y) \in B'$ e, portanto, $\varphi(xy) = \varphi(x)\varphi(y) \in B'$, pelo que $xy \in \varphi^{-1}\left(B'\right)$.

Assim, $\varphi^{-1}\left(B'\right)$ é um subanel de A. $\square$

Proposição. Sejam $\varphi : A \to A'$ um morfismo de anéis e I' um ideal de A'. Então,

$$\varphi^{-1}\left(I'\right) = \left\{x \in A \mid \varphi(x) \in I'\right\}$$

é um ideal de A.

Demonstração. Seja I' um ideal de A'. Então, pela proposição anterior, $\varphi^{-1}\left(I'\right)$ é um subanel de A. Por outro lado, seja $a \in A$ e $x \in \varphi^{-1}\left(I'\right)$. Então, $\varphi(x) \in I'$ e, portanto, $\varphi(ax) = \varphi(a)\varphi(x) \in I'$, pelo que $ax \in \varphi^{-1}\left(I'\right)$ e, portanto, $\varphi^{-1}\left(I'\right)$ é um ideal de A. $\square$

Definição. Seja $\varphi : A \to A'$ um morfismo de anéis.

1. Chama-se *Núcleo de* φ (ou *kernel de* φ), e representa-se por $\mathrm{Nuc}\varphi$ (ou $\mathrm{Ker}\varphi$), ao subconjunto de A definido por

$$\mathrm{Nuc}\varphi = \{x \in A : \varphi(x) = 0_{A'}\};$$

2. Chama-se *imagem de* φ, e representa-se por $\mathrm{Im}\varphi$ ou $\varphi(A)$, ao subconjunto de A' definido por

$$\mathrm{Im}\varphi = \{\varphi(x) : x \in A\}.$$

Proposição. Seja $\varphi : A \to A'$ um morfismo de anéis. Então,

1. $\mathrm{Nuc}\varphi$ é um ideal de A;
2. $\mathrm{Im}\varphi$ é um subanel de A'.

1. Trivial, tendo em conta que $\mathrm{Nuc}\varphi = \varphi^{-1}\{0_{A'}\}$ e $\{0_{A'}\}$ é um ideal de A'.
2. Trivial, tendo em conta que $\mathrm{Im}\varphi = \varphi(A)$ e que A é um subanel de A. $\square$

Exemplo 40. Considere-se o morfismo de anéis $\varphi : \mathbb{Z} \to \mathbb{Z}_{10}$ definido por $\varphi(n) = [6n]_{10}$, para todo $n \in \mathbb{Z}$.

Por um lado, tendo em conta que $\mathrm{Nuc}\,\varphi = \{n \in \mathbb{Z} : \varphi(n) = [0]_{10}\}$ e que

$$\begin{aligned} \varphi(n) = [0]_{10} \quad &\Leftrightarrow [6n]_{10} = [0]_{10} \\ &\Leftrightarrow 6n \equiv 0 (\mathrm{mod}\, 10) \\ &\Leftrightarrow n \equiv 0 (\mathrm{mod}\, \tfrac{10}{\mathrm{m.d.c.}(6,10)}) \\ &\Leftrightarrow n \equiv 0 (\mathrm{mod}\, 5), \end{aligned}$$

concluímos que $\mathrm{Nuc}\,\varphi = 5\mathbb{Z}$.

Por outro lado,

$$\begin{aligned} \mathrm{Im}\varphi \quad &= \{\varphi(n) : n \in \mathbb{Z}\} \\ &= \{[6n]_{10} : n \in \mathbb{Z}\} = \{[0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}. \end{aligned}$$

Proposição. Sejam A um anel e I um seu ideal. Então, a aplicação $\pi : A \to A/I$ definida por $\pi(x) = x + I \; (x \in A)$, é um epimorfismo (ao qual se chama *epimorfismo canónico*).

Demonstração. Sejam A um anel e I um ideal de A. Então, em A/I, temos que

$$(x + I) + (y + I) = (x + y) + I$$

e

$$(x + I)(y + I) = xy + I.$$

Logo, a aplicação π é tal que

$$\pi(x) + \pi(y) = \pi(x + y)$$

e

$$\pi(x)\pi(y) = \pi(xy),$$

pelo que π é um morfismo. Além disso, o facto de qualquer elemento de A/I se definir à custa de um representante de A, permite-nos concluir que π é uma aplicação sobrejetiva. □

Teorema Fundamental do Homomorfismo. Seja $\varphi : A \to A'$ um morfismo de anéis. Então,

$$A/\mathrm{Nuc}\varphi \cong \varphi(A).$$

Demonstração. Seja $\varphi : A \to A'$ um morfismo de anéis. Então, $\mathrm{Nuc}\varphi$ é um ideal de A e, portanto, $\pi : A \to A/\mathrm{Nuc}\varphi$ é um epimorfismo. Seja θ a relação que a cada classe $x + \mathrm{Nuc}\varphi$ de $A/\mathrm{Nuc}\varphi$ faz corresponder o elemento $\varphi(x)$ de A'. Então,

(i) θ é uma aplicação injectiva, pois

$$(\forall x + \mathrm{Nuc}\varphi \in A/\mathrm{Nuc}\varphi) \qquad x \in A \text{ e } \varphi(x) \in A',$$

e

$$\begin{aligned} x + \mathrm{Nuc}\varphi = y + \mathrm{Nuc}\varphi \quad &\Longleftrightarrow \quad x - y \in \mathrm{Nuc}\varphi \\ &\Longleftrightarrow \quad \varphi(x - y) = 0_{A'} \\ &\Longleftrightarrow \quad \varphi(x) - \varphi(y) = 0_{A'} \\ &\Longleftrightarrow \quad \varphi(x) = \varphi(y). \end{aligned}$$

(ii) θ é um morfismo, pois

$$\begin{aligned} \pi((x + \mathrm{Nuc}\varphi) + (y + \mathrm{Nuc}\varphi)) \quad &= \quad \pi((x + y) + (\mathrm{Nuc}\varphi)) \\ &= \quad \varphi(x + y) \\ &= \quad \varphi(x) + \varphi(y) \\ &= \quad \pi(x + \mathrm{Nuc}\varphi) + \pi(y + \mathrm{Nuc}\varphi) \end{aligned}$$

e

$$\begin{aligned}
\pi\left((x+\mathrm{Nuc}\varphi)\cdot(y+\mathrm{Nuc}\varphi)\right) &= \pi\left((x\cdot y)+(\mathrm{Nuc}\varphi)\right)\\
&= \varphi\left(x\cdot y\right)\\
&= \varphi\left(x\right)\cdot\varphi\left(y\right)\\
&= \pi\left(x+\mathrm{Nuc}\varphi\right)\cdot\pi\left(y+\mathrm{Nuc}\varphi\right).
\end{aligned}$$

(iii) $\theta\left(A/\mathrm{Nuc}\varphi\right)=\mathrm{Im}\varphi$, porque

$$\begin{aligned}
y\in\theta\left(A/\mathrm{Nuc}\varphi\right) &\iff (\exists x\in A)\quad y=\theta\left(x+\mathrm{Nuc}\varphi\right)\\
&\iff (\exists x\in A)\quad y=\varphi\left(x\right)\\
&\iff y\in\mathrm{Im}\varphi.
\end{aligned}$$

Logo, concluímos que

$$A/\mathrm{Nuc}\varphi\cong\mathrm{Im}\varphi.$$

$\square$