

Universidade do Minho - 2021/22  
Licenciatura em Ciências de Computação

# Álgebra

Paula Mendes Martins  
Departamento de Matemática



<b>1</b>	<b>apresentação</b>	<b>1</b>
<b>2</b>	<b>preliminares</b>	<b>3</b>
2.1	semigrupos - conceitos básicos . . . . .	3
2.2	potência natural de um elemento num semigrupo . . . . .	6
<b>3</b>	<b>elementos da teoria de grupos</b>	<b>9</b>
3.1	generalidades . . . . .	9
3.1.1	potência inteira de um elemento num grupo . . . . .	14
3.2	subgrupos . . . . .	15
3.2.1	critérios de subgrupo . . . . .	17
3.2.2	exemplos de subgrupos importantes . . . . .	18
3.3	ordem de um elemento . . . . .	22
3.3.1	algumas propriedades . . . . .	25
3.4	o teorema de Lagrange . . . . .	27
3.5	subgrupos normais, relações de congruência e grupos quociente . . . . .	34
3.6	morfismos . . . . .	37
3.6.1	teoremas de isomorfismo . . . . .	44
3.7	grupos cíclicos . . . . .	48
3.7.1	conceito e exemplos . . . . .	48
3.7.2	propriedades elementares . . . . .	49
3.7.3	morfismos entre grupos cíclicos . . . . .	51

3.8	grupo simétrico . . . . .	52
3.8.1	O grupo diedral . . . . .	54
3.8.2	ciclos . . . . .	55
3.8.3	grupo alterno . . . . .	58
3.8.4	o teorema de representação de Cayley . . . . .	59
<b>4</b>	<b>elementos da teoria de anéis</b>	<b>63</b>
4.1	generalidades . . . . .	63
4.1.1	domínios de integridade . . . . .	70
4.1.2	anéis de divisão e corpos . . . . .	72
4.2	característica de um anel . . . . .	73
4.3	subanéis . . . . .	77
4.4	ideais e relações de congruência num anel . . . . .	78
4.4.1	anel quociente . . . . .	83
4.4.2	ideais primos e ideais maximais . . . . .	84
4.5	morfismos . . . . .	87
4.5.1	teorema fundamental do homomorfismo . . . . .	91
4.5.2	teoremas do isomorfismo . . . . .	92
<b>5</b>	<b>divisibilidade em domínios de integridade</b>	<b>97</b>
5.1	definições básicas . . . . .	97
5.2	domínios de fatorização única . . . . .	105
5.3	domínios de ideais principais . . . . .	107
5.4	domínios euclidianos . . . . .	109
5.5	Corpo de frações de um domínio de integridade . . . . .	114

# 1 apresentação

Estas notas servem de apoio à teoria lecionada em Álgebra, unidade curricular do 2º ano da Licenciatura em Ciências da Computação e da Licenciatura em Matemática. Nelas são apresentados os conceitos e os resultados fundamentais para a introdução desta área do saber matemático. Uma vasta lista de exemplos é também apresentada para melhor compreensão da teoria apresentada.

outubro 2021

Paula Mendes Martins



### 2.1 semigrupos - conceitos básicos

**Definição 2.1.** 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

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

**Definição 2.2.** Seja  $(S, *)$  um grupóide. A operação  $*$  diz-se comutativa se

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

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

**Exemplo 2.3.** ■ 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,  $(S, *)$  não é um grupóide.
- Se  $*$  é definida por  $x * y = 3$  em  $S = \mathbb{N}$ , então,  $(S, *)$  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 2.4.** 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. O facto de todas as entradas da tabela serem elementos de  $S$  permite concluir que  $*$  é uma operação binária e o facto de a tabela ser simétrica relativamente à sua diagonal principal permite concluir que a operação binária  $*$  é comutativa.

**Definição 2.5.** 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 2.6.** O conjunto dos números inteiros constitui um semigrupo quando algebrizado com a multiplicação usual.

**Exemplo 2.7.** O primeiro grupóide do Exemplo 2.3 não é um semigrupo. De facto,

$$x * (y * z) = \frac{x + \frac{y+z}{2}}{2} = \frac{2x + y + z}{4} \neq \frac{x + y + 2z}{4} = \frac{\frac{x+y}{2} + z}{2} = (x * y) * z.$$

**Exemplo 2.8.** O grupóide do Exemplo 2.4 não é um semigrupo. De facto, temos que  $a * (c * c) = a * a = a$  e  $(a * c) * c = b * c = c$ .

**Observação.** Quando uma operação binária está definida por uma tabela de Cayley, para se verificar que a operação é associativa, é necessário verificar todos os casos possíveis de operar três elementos (se o conjunto tem  $n$  elementos, será necessário verificar  $n^3$  igualdades, o que obriga a efetuar  $4 \times n^3$  cálculos. Existe um teste de verificação da associatividade em tabelas de Cayley - teste de associatividade de Light - que simplifica aquele procedimento, mas que não o otimiza significativamente.

Num grupóide ou semigrupo, destacam-se alguns elementos, tendo em conta os resultados obtidos quando os operamos com eles próprios ou com outros elementos. De seguida, apresentamos alguns desses elementos.



**Definição 2.9.** *Seja  $(S, *)$  um grupóide. Um elemento  $a \in S$  diz-se um elemento idempotente se  $a * a = a$ .*

**Exemplo 2.10.** *No grupóide do Exemplo 2.3, todos os elementos são idempotentes. De facto, para todo  $x \in S$ ,  $x * x = \frac{x+x}{2} = x$ .*

**Definição 2.11.** *Seja  $(S, *)$  um grupóide. Um elemento  $0 \in S$  diz-se elemento zero ou nulo se*

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

**Definição 2.12.** *Seja  $(S, *)$  um grupóide. Um elemento  $e \in S$  diz-se elemento neutro ou elemento identidade se*

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

Resulta imediatamente das definições anteriores que um elemento neutro e um elemento zero de um grupóide são elementos idempotentes. Vejamos que num grupóide não podem existir simultaneamente dois elementos neutros. Assim, quando existe, podemos referir-nos ao elemento neutro e destacá-lo com notação própria.

**Proposição 2.13.** *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,  $e = e'$ . □

De modo análogo, provamos que, num grupóide, existe no máximo um elemento zero.

**Definição 2.14.** *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 2.15.** *O semigrupo  $(\mathbb{N}, *)$  onde  $*$  está definida por*

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

*não admite elemento neutro.*

**Exemplo 2.16.** No semigrupo  $S = \{a, b, c, d\}$  algebrizado com a operação  $*$  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, pois  $a$  é elemento neutro.

**Definição 2.17.** 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 2.18.** 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. □

## 2.2 potência natural de um elemento num semigrupo

Caso não haja ambiguidade quanto à operação  $*$ , referimo-nos muitas vezes ao grupóide (respetivamente, semigrupo, monóide)  $(S, *)$  como o grupóide (respetivamente, semigrupo, monóide)  $S$ . 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 <i>inverso</i> de $a$	$-a$ é o oposto ou <i>simétrico</i> de $a$

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

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

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

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

A potenciação natural em semigrupos satisfaz as propriedades apresentadas na seguinte proposição.

**Proposição 2.19.** *Sejam  $S$  um semigrupo,  $m, n \in \mathbb{N}$  e  $a \in S$ . Então,*

$$(i) \quad a^m a^n = a^{m+n} \quad [ \quad ma + na = (m+n)a \quad ];$$

$$(ii) \quad (a^m)^n = a^{mn} \quad [ \quad n(ma) = (nm)a \quad ].$$

**Demonstração:** A demonstração é feita por indução (exercício). □



## 3 elementos da teoria de grupos

### 3.1 generalidades

**Definição 3.1.** *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)  $(\exists e \in G) (\forall a \in G) \quad ae = ea = a$ ;

(G2)  $(\forall a \in G) (\exists! a^{-1} \in G) \quad aa^{-1} = a^{-1}a = e$ .

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

**Exemplo 3.2.**  $(\mathbb{R}, +)$  é grupo abeliano ( $+$  é a adição usual de números reais).

**Exemplo 3.3.**  $(\mathbb{R}, \cdot)$  não é grupo ( $\cdot$  é a multiplicação usual de números reais), mas  $(\mathbb{R} \setminus \{0\}, \cdot)$  é grupo abeliano.

**Exemplo 3.4.**  $(\mathbb{Z}, \cdot)$  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 3.5.** *Um conjunto singular,  $\{x\}$ , quando algebrizado com a única operação binária possível,  $x * x = x$ , é um grupo abeliano (chamado, obviamente, de grupo trivial).*

**Exemplo 3.6.** *O conjunto  $G = \{x, e\}$ , quando algebrizado com a operação definida pela tabela*

$\cdot$	$e$	$x$
$e$	$e$	$x$
$x$	$x$	$e$

é um grupo abeliano.

**Exemplo 3.7.** 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. No caso de  $n = 4$ , as operações  $\oplus$  e  $\otimes$  em  $\mathbb{Z}_4$  podem ser definidas pelas tabelas

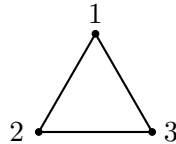
$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$		$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$e$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$		$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$		$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$		$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Repare-se que, neste caso,  $(\mathbb{Z}_4^*, \otimes)$  não é um grupóide, pois  $\bar{2} \otimes \bar{2} = \bar{0} \notin \mathbb{Z}_4^*$ . Uma situação análoga verifica-se em qualquer  $\mathbb{Z}_n^*$ , com  $n$  não primo.

**Exemplo 3.8.** Seja  $n \in \mathbb{N}$ . O conjunto das matrizes reais quadradas de ordem  $n$ , quando algebrizado com a multiplicação usual de matrizes, não é um grupo. No entanto, o conjunto das matrizes reais quadradas de ordem  $n$  invertíveis é um grupo não abeliano quando considerada a mesma multiplicação. A este grupo chama-se grupo linear geral de ordem  $n$  e representa-se por  $GL_n(\mathbb{R})$  ou  $GL(n, \mathbb{R})$ .

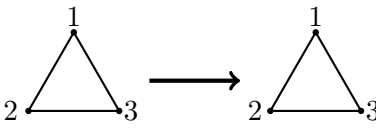
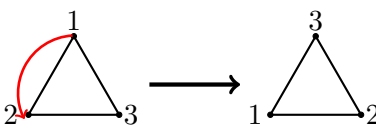
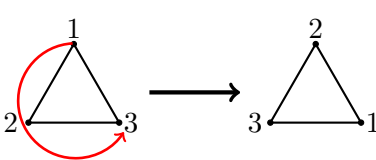
**Exemplo 3.9.** Seja  $X$  um conjunto não vazio. O conjunto  $\mathcal{F}(X)$  das funções de  $X$  em  $X$  é um semigrupo não abeliano quando algebrizado com a composição usual de funções. Já o conjunto  $S_X = \{f \in \mathcal{F}(X) : f \text{ é bijetiva}\}$  é um grupo quando algebrizado com a mesma operação. Prova-se este grupo é não abeliano se o conjunto  $X$  tiver pelo menos três elementos distintos. Este tipo de grupos, aos quais chamamos grupos simétricos, têm grande importância na Teoria de Grupos e serão estudados com algum detalhe no final deste capítulo.

**Exemplo 3.10.** Seja  $D_3$  o conjunto das isometrias num triângulo equilátero.

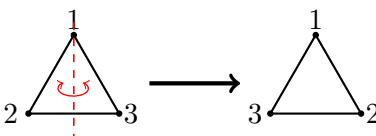
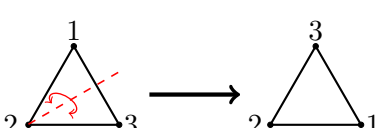
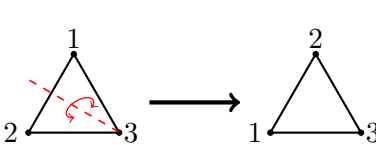


O conjunto  $D_3$  tem exatamente seis elementos, três rotações e três simetrias axiais.

As rotações, de ângulos com  $0^\circ$ ,  $120^\circ$  e  $240^\circ$  de amplitude, são, respetivamente:

-  que podemos representar por  $\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ ;
-  que podemos representar por  $\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
-  que podemos representar por  $\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

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

-  que podemos representar por  $\theta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ ;
-  que podemos representar por  $\theta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ ;
-  que podemos representar por  $\theta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ .

Considerando a composição usual de funções, obtemos a tabela:

$\circ$	$\rho_1$	$\rho_2$	$\rho_3$	$\theta_1$	$\theta_2$	$\theta_3$
$\rho_1$	$\rho_1$	$\rho_2$	$\rho_3$	$\theta_1$	$\theta_2$	$\theta_3$
$\rho_2$	$\rho_2$	$\rho_3$	$\rho_1$	$\theta_3$	$\theta_1$	$\theta_2$
$\rho_3$	$\rho_3$	$\rho_1$	$\rho_2$	$\theta_2$	$\theta_3$	$\theta_1$
$\theta_1$	$\theta_1$	$\theta_2$	$\theta_3$	$\rho_1$	$\rho_2$	$\rho_3$
$\theta_2$	$\theta_2$	$\theta_3$	$\theta_1$	$\rho_3$	$\rho_1$	$\rho_2$
$\theta_3$	$\theta_3$	$\theta_1$	$\theta_2$	$\rho_2$	$\rho_3$	$\rho_1$

O grupo  $D_3$  é o menor grupo não abeliano que se pode definir, no sentido em que qualquer grupo com um número inferior de elementos é abeliano. A este grupo é costume chamarmos grupo diedral

do triângulo. Este grupo não é mais do que o grupo simétrico  $S_X$ , com  $X = \{1, 2, 3\}$ , referido no exemplo anterior.

De seguida, apresentamos alguns resultados básicos na teoria de grupos.

**Proposição 3.11.** 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,

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

A segunda implicação demonstra-se de modo análogo. □

Repare-se que existem semigrupos que não são grupos nos quais se verifica a lei do corte. O exemplo seguinte ilustra esta situação.

**Exemplo 3.12.** Seja  $\mathbb{Z} \setminus \{0\}$  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 3.13.** 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,

$$a'' = a''e = a''(aa') = (a''a)a' = ea' = a',$$

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

**Proposição 3.14.** *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  $\rho_a, \lambda_a : S \rightarrow S$  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 duas equações

$$ax = b \text{ e } ya = b$$

têm soluções únicas em  $S$ . Assim, pela proposição anterior, o semigrupo  $S$  é um grupo.  $\square$

**Proposição 3.15.** *Seja  $G$  um grupo. Então:*

- (i)  $1_G^{-1} = 1_G$ ;
- (ii)  $(a^{-1})^{-1} = a$ ,  $\forall a \in G$ ;
- (iii)  $(ab)^{-1} = b^{-1}a^{-1}$ ,  $\forall a, b \in G$ ;
- (iv)  $(a_1a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1}a_1^{-1}$ ,  $(\forall n \in \mathbb{N}) (\forall a_1, a_2, \dots, a_n \in G)$ .

**Demonstração:** Exercício.  $\square$

### 3.1.1 potência inteira de um elemento num grupo

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

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

Em linguagem aditiva temos

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

**Proposição 3.16.** *Sejam  $G$  um grupo,  $x \in G$  e  $m, n \in \mathbb{Z}$ . Então,*

- i)  $x^m x^n = x^{m+n}$  (na linguagem aditiva:  $mx + nx = (m+n)x$ );
- ii)  $(x^m)^n = x^{mn}$  (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

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

Por outro lado,

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

*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

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

o que prova (i). 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 (ii).

**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

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

A demonstração de (ii) é igual ao 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.  $\square$

## 3.2 subgrupos

**Definição 3.17.** 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  $H < G$ .

**Exemplo 3.18.** Um grupo não trivial  $G$  tem, pelo menos, dois subgrupos:  $\{1_G\}$  (subgrupo trivial) e  $G$  (subgrupo impróprio).

O grupo trivial  $G = \{1_G\}$  tem exatamente um subgrupo: o subgrupo impróprio (que é igual ao subgrupo trivial).

**Exemplo 3.19.** O grupóide  $(\mathbb{Z}, +)$  é subgrupo de  $(\mathbb{R}, +)$ .

**Exemplo 3.20.** O grupóide  $(\mathbb{Z} \setminus \{0\}, \cdot)$  não é subgrupo de  $(\mathbb{R} \setminus \{0\}, \cdot)$  pois  $(\mathbb{Z} \setminus \{0\}, \cdot)$  não é um grupo.

**Exemplo 3.21.** Seja  $G = \{e, a, b, c\}$  o grupo de 4-Klein, i.e., o grupo cuja operação é dada pela seguinte tabela

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

Os seus subgrupos são:  $\{e, a, b, c\}$ ,  $\{e\}$ ,  $\{e, a\}$ ,  $\{e, b\}$  e  $\{e, c\}$ .

**Exemplo 3.22.** Seja  $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  o conjunto das classes módulo-4 algebrizado com a adição, i.e.,

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

Então,  $(\mathbb{Z}_4, +)$  é grupo e os seus subgrupos são:  $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ ,  $\{\bar{0}\}$  e  $\{\bar{0}, \bar{2}\}$ .

**Exemplo 3.23.** Relativamente ao grupo não comutativo  $D_3 = \{\rho_1, \rho_2, \rho_3, \theta_1, \theta_2, \theta_3\}$  apresentado no Exemplo 3.10, cuja tabela de Cayley é

$\circ$	$\rho_1$	$\rho_2$	$\rho_3$	$\theta_1$	$\theta_2$	$\theta_3$
$\rho_1$	$\rho_1$	$\rho_2$	$\rho_3$	$\theta_1$	$\theta_2$	$\theta_3$
$\rho_2$	$\rho_2$	$\rho_3$	$\rho_1$	$\theta_3$	$\theta_1$	$\theta_2$
$\rho_3$	$\rho_3$	$\rho_1$	$\rho_2$	$\theta_2$	$\theta_3$	$\theta_1$
$\theta_1$	$\theta_1$	$\theta_2$	$\theta_3$	$\rho_1$	$\rho_2$	$\rho_3$
$\theta_2$	$\theta_2$	$\theta_3$	$\theta_1$	$\rho_3$	$\rho_1$	$\rho_2$
$\theta_3$	$\theta_3$	$\theta_1$	$\theta_2$	$\rho_2$	$\rho_3$	$\rho_1$

os seus subgrupos são  $\{\rho_1\}$ ,  $\{\rho_1, \rho_2, \rho_3\}$ ,  $\{\rho_1, \theta_1\}$ ,  $\{\rho_1, \theta_2\}$  e  $\{\rho_1, \theta_3\}$ .

Trabalhando apenas com a definição, o único modo de listarmos todos os subgrupos de um grupo (como nos exemplos anteriores) é verificar se cada um dos seus subconjuntos é ou não grupo para a restrição da operação. Se o grupo tem  $n$  elementos, o conjunto admite  $2^n$  subconjuntos, o que pode tornar o procedimento bastante longo. De seguida, apresentamos alguns resultados que permitem facilitar o processo.

**Proposição 3.24.** Sejam  $G$  um grupo e  $H < G$ . Então:

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

**Demonstração:** (i) 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,

$$1_H = 1_G.$$

(ii) 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,

$$h' = h^{-1}.$$

□

### 3.2.1 critérios de subgrupo

As duas proposições apresentadas nesta secção permitem simplificar a verificação se um dado subconjunto do grupo é ou não um seu subgrupo.

**Proposição 3.25.** *Sejam  $G$  um grupo e  $H \subseteq G$ . Então,  $H < G$  se e só se são satisfeitas as seguintes condições:*

- (i)  $H \neq \emptyset$ ;
- (ii)  $x, y \in H \Rightarrow xy \in H$ ;
- (iii)  $x \in H \Rightarrow x^{-1} \in H$ .

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

- (i)  $H \neq \emptyset$ , pois  $1_G \in H$ ;
- (ii) dados  $x, y \in H$ , como  $H$  é um grupóide,  $xy \in H$ ;
- (iii) 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 (i), (ii) e (iii). Então

- (a)  $H$  é grupóide por (ii);
- (b) dado  $x \in H$  (este elemento existe por (i)),  $x^{-1} \in H$  (por (iii)), pelo que  $1_G = xx^{-1} \in H$  (por (ii));
- (c) qualquer elemento de  $H$  admite inverso em  $H$  (por (iii)).

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

**Proposição 3.26.** *Sejam  $G$  um grupo e  $H \subseteq G$ . Então,  $H < G$  se e só se são satisfeitas as seguintes condições:*

- (i)  $H \neq \emptyset$ ;
- (ii)  $x, y \in H \Rightarrow xy^{-1} \in H$ .

**Demonstração:** Basta provar que  $i) + ii) \leftrightarrow a) + b) + c)$ , onde a), b) e c) são as condições da proposição anterior. (Exercício)  $\square$

**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.

### 3.2.2 exemplos de subgrupos importantes

Dado um grupo  $G$ , é possível identificar subgrupos sem ter de percorrer a lista de subconjuntos de  $G$ . Nesta secção apresentamos alguns exemplos.

#### • centralizador de um elemento

**Definição 3.27.** *Sejam  $G$  um grupo e  $a \in G$ . Chama-se centralizador de  $a$  ao conjunto*

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

**Exemplo 3.28.** Considere-se o grupo diedral do triângulo  $D_3$ , cuja tabela é

$\circ$	$\rho_1$	$\rho_2$	$\rho_3$	$\theta_1$	$\theta_2$	$\theta_3$
$\rho_1$	$\rho_1$	$\rho_2$	$\rho_3$	$\theta_1$	$\theta_2$	$\theta_3$
$\rho_2$	$\rho_2$	$\rho_3$	$\rho_1$	$\theta_3$	$\theta_1$	$\theta_2$
$\rho_3$	$\rho_3$	$\rho_1$	$\rho_2$	$\theta_2$	$\theta_3$	$\theta_1$
$\theta_1$	$\theta_1$	$\theta_2$	$\theta_3$	$\rho_1$	$\rho_2$	$\rho_3$
$\theta_2$	$\theta_2$	$\theta_3$	$\theta_1$	$\rho_3$	$\rho_1$	$\rho_2$
$\theta_3$	$\theta_3$	$\theta_1$	$\theta_2$	$\rho_2$	$\rho_3$	$\rho_1$

Então,

$$C(\rho_1) = D_3, C(\rho_2) = C(\rho_3) = \{\rho_1, \rho_2, \rho_3\}, C(\theta_1) = \{\rho_1, \theta_1\}, C(\theta_2) = \{\rho_1, \theta_2\} \\ \text{e } C(\theta_3) = \{\rho_1, \theta_3\}.$$

**Observação.** Da definição, resulta que, se  $G$  é um grupo abeliano, então  $C(a) = G$ , para todo  $a \in G$ .

**Proposição 3.29.** Seja  $G$  um grupo. Então, para todo  $a \in G$ ,  $C(a) < G$ .

**Demonstração:** Seja  $a \in G$ . Então,

- (i)  $C(a) \neq \emptyset$ , pois  $1_G \in G$  é tal que  $1_G a = a 1_G$  e, portanto,  $1_G \in C(a)$ ;
- (ii) 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  $xy \in C(a)$ ;

- (iii) dado  $x \in C(a)$ , temos que  $x^{-1} \in G$  e

$$\begin{aligned} ax = xa &\Rightarrow x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} \\ &\Leftrightarrow (x^{-1}a)(xx^{-1}) = (x^{-1}x)(ax^{-1}) \\ &\Leftrightarrow (x^{-1}a)1_G = 1_G(ax^{-1}) \\ &\Leftrightarrow x^{-1}a = ax^{-1}, \end{aligned}$$

pelo que  $x^{-1} \in C(a)$ .

Logo,  $C(a) < G$ .

□

• centro de um grupo

**Definição 3.30.** *Seja  $G$  um grupo. Chama-se centro de  $G$  ao conjunto*

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

**Exemplo 3.31.**  $Z(D_3) = \{\rho_1\}$ .

**Observação.** Da definição, resulta que, se  $G$  é um grupo abeliano, então  $Z(G) = G$ .

**Proposição 3.32.** *Seja  $G$  um grupo. Então,  $Z(G) < G$ .*

**Demonstração:** Seja  $G$  um grupo. Então,

- (i)  $Z(G) \neq \emptyset$ , pois  $1_G \in G$  é tal que, para todo  $a \in G$ ,  $1_G a = a 1_G$  e, portanto,  $1_G \in Z(G)$ ;
- (ii) 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  $xy \in Z(G)$ ;

- (iii) dado  $x \in Z(G)$ , temos que  $x^{-1} \in G$  e, para todo  $a \in G$ ,

$$\begin{aligned} x^{-1}a &= (x^{-1}a)e = (x^{-1}a)(x^{-1}x) = (x^{-1}ax^{-1})x = \\ &= x(x^{-1}ax) = (xx^{-1})(ax^{-1}) = 1_G(ax^{-1}) = ax^{-1}, \end{aligned}$$

pelo que  $x^{-1} \in Z(G)$ . Logo,  $Z(G) < G$ . □

• intersecção de subgrupos

**Proposição 3.33.** *Sejam  $G$  um grupo e  $H, K < G$ . Então,  $H \cap K < G$ .*

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

- (i)  $H \cap K \neq \emptyset$ , pois  $1_G \in H$  e  $1_G \in K$ , pelo que  $1_G \in H \cap K$ ;
- (ii) 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,  $xy \in H \cap K$ .
- (iii) dado  $x \in H \cap K$ , temos que  $x \in H$  e  $x \in K$ , pelo que  $x^{-1} \in H$  e  $x^{-1} \in K$  e, portanto,  $x^{-1} \in H \cap K$ .

Logo,  $H \cap K < G$ . □



**Corolário 3.34.** *Seja  $G$  um grupo. Então, a intersecção de uma família não vazia de subgrupos de  $G$  é ainda um subgrupo de  $G$ .*

**Observação.** Sempre que se fala na intersecção de subconjuntos, é natural questionar o que acontece com a união desses mesmos subconjuntos. No geral, a união de dois subgrupos de um grupo  $G$  não é um subgrupo de  $G$ . Por exemplo, a união dos subgrupos  $2\mathbb{Z}$  e  $3\mathbb{Z}$  do grupo  $(\mathbb{Z}, +)$  não é um subgrupo de  $\mathbb{Z}$ , uma vez que  $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$  e  $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ . Facilmente se prova que a união de dois subgrupos de um grupo  $G$  é um subgrupo de  $G$  se e só se um dos subgrupos está contido no outro.

#### • subgrupo gerado

**Proposição 3.35.** *Sejam  $G$  um grupo e  $\emptyset \neq X \subseteq G$ . Consideremos*

$$\mathcal{H} = \{H \subseteq G \mid H < G \text{ e } X \subseteq H\}$$

(i.e.,  $\mathcal{H}$  é o conjunto de todos os subgrupos de  $G$  que contêm  $X$ ). Então,  $\bigcap_{H \in \mathcal{H}} H$  é o menor subgrupo de  $G$  que contém  $X$ .

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

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

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

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

**Definição 3.36.** *Sejam  $G$  um grupo e  $\emptyset \neq X \subseteq G$ . 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 proposição anterior, temos que  $\langle X \rangle$  é a intersecção de todos os subgrupos de  $G$  que contêm  $X$ .

**Proposição 3.37.** *Sejam  $G$  um grupo e  $a \in G$ . Então,  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ .*

**Demonstração:** Sejam  $G$  um grupo e  $a \in G$ . Seja  $B = \{a^n \mid n \in \mathbb{Z}\}$ . Então,

- (i)  $B \neq \emptyset$ , pois  $1_G = a^0$  e, portanto,  $1_G \in B$ ;
- (ii) dados  $x, y \in B$ , sabemos que existem  $n, m \in \mathbb{Z}$  tais que  $x = a^n$  e  $y = a^m$ ,

$$y^{-1} = (a^m)^{-1} = a^{-m}$$

e

$$xy^{-1} = a^n a^{-m} = a^{n-m}.$$

Como  $-m, n - m \in \mathbb{Z}$ , temos que  $xy^{-1} \in B$ . Logo,  $B < G$ .

Mais ainda, como  $1 \in \mathbb{Z}$ , temos que  $a \in B$ .

Finalmente, seja  $H < G$  tal que  $a \in H$ . Então,

$$\begin{aligned} x \in B &\Rightarrow (\exists n \in \mathbb{Z}) \quad x = a^n \\ &\Rightarrow x \in H \quad (\text{pois } H < G). \end{aligned}$$

Logo,  $B \subseteq H$  e, portanto,  $\langle a \rangle = B$ . □

### 3.3 ordem de um elemento

Terminamos a última secção provando que, dados um grupo  $G$  e  $a \in G$ ,  $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ . É óbvio que, no caso de  $a = 1_G$ , o subgrupo reduz-se ao subgrupo trivial. Mais ainda, no grupo  $(\mathbb{R} \setminus \{0\}, \cdot)$ , 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. Nesta secção vamos explorar esta ideia.

**Definição 3.38.** Sejam  $G$  um grupo e  $a \in G$ .

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

(ii) Diz-se que  $a$  tem ordem  $k$  ( $k \in \mathbb{N}$ ), e escreve-se  $o(a) = k$ , se

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

**Exemplo 3.39.** No grupo  $(\mathbb{R}, +)$  a ordem de qualquer elemento não nulo  $a$  é infinita. Por outro lado,  $o(0) = 1$ .

**Exemplo 3.40.** Seja  $G = \{e, a, b, c\}$  o grupo 4-Klein. Então, a tabela de Cayley é

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

Facilmente se verifica que  $o(e) = 1$  e  $o(a) = o(b) = o(c) = 2$ .

**Exemplo 3.41.** No grupo  $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ , temos que:

- (i)  $o(\bar{0}) = 1$ ;
- (ii)  $o(\bar{1}) = 4$ , 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  $\bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{0}$ ;
- (iii)  $o(\bar{2}) = 2$ , pois  $\bar{2} \neq \bar{0}$  e  $\bar{2} + \bar{2} = \bar{0}$
- (iv)  $o(\bar{3}) = 4$ , 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  $\bar{3} + \bar{3} + \bar{3} + \bar{3} = \bar{0}$ .

Não é coincidência o facto de, nos exemplos apresentados, o único elemento com ordem 1 ser a identidade do grupo. Este é um resultado da Teoria de Grupos que provamos de seguida.

**Proposição 3.42.** 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.,  $a = 1_G$ .  $\square$

Os próximos resultados permitem-nos estudar a cardinalidade do subgrupo gerado por um elemento de um grupo em função da ordem desse elemento.

**Proposição 3.43.** Sejam  $G$  um grupo e  $a \in G$  um elemento com ordem infinita. Então, para  $m, n \in \mathbb{Z}$ ,

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

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

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

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

**Corolário 3.44.** *Sejam  $G$  um grupo e  $a \in G$  um elemento com ordem infinita. Então,  $\langle a \rangle$  tem um número infinito de elementos.*

**Demonstração:** Imediata, tendo em conta que  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$  e a proposição anterior.  $\square$

**Corolário 3.45.** *Num grupo finito nenhum elemento tem ordem infinita.*

**Demonstração:** Sejam  $G$  um grupo finito e  $a \in G$ . Se  $o(a) = \infty$ , então,  $\langle a \rangle$  é infinito e, portanto, não pode ser um subconjunto de  $G$ .  $\square$

**Proposição 3.46.** *Sejam  $G$  um grupo,  $a \in G$  e  $k \in \mathbb{N}$  tal que  $o(a) = k$ . Então,*

- (i) *se um inteiro  $n$  tem  $r$  como resto na divisão por  $k$  então  $a^n = a^r$ ;*
- (ii) *para  $n \in \mathbb{Z}$ ,  $a^n = 1_G \Leftrightarrow k \mid n$ ;*
- (iii)  *$\langle a \rangle = \{1_G, a^1, a^2, \dots, a^{k-1}\}$ ;*
- (iv)  *$\langle a \rangle$  tem exatamente  $k$  elementos.*

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

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

(ii) 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,

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

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,

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

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

(iii) Sabemos que  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ . Obviamente, temos que  $\{1_G, a, a^2, a^3, \dots, a^{k-1}\} \subseteq \langle a \rangle$ . Provemos agora a inclusão contrária.

Seja  $x \in \langle a \rangle$ . Então,

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

Se  $p \in \{0, 1, 2, 3, \dots, k-1\}$  então  $x \in \{1_G, a, a^2, a^3, \dots, a^{k-1}\}$ .

Se  $p \notin \{0, 1, 2, 3, \dots, k-1\}$  então sabemos, por (i), que existe  $0 \leq r \leq k-1$  tal que  $a^p = a^r$ .

Logo,  $\langle a \rangle \subseteq \{e, a, a^2, a^3, \dots, a^{k-1}\}$  e a igualdade verifica-se.

(iv) pretendemos provar que, na lista  $1_G, a, a^2, a^3, \dots, a^{k-1}$  não há repetição de elementos.

Suponhamos que sim, i.e., suponhamos que

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

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 exactamente  $k$  elementos.  $\square$

### 3.3.1 algumas propriedades

**Proposição 3.47.** *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. Porque a operação é associativa, temos que  $(b^{-1}ab)^{n_0} = b^{-1}a^{n_0}b$ . Logo, como  $a^{n_0} = 1_G$ , obtemos

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

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

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

Como a ordem de  $a$  é  $n_0$ , segue-se que  $k \geq n_0$ . Assim,  $n_0$  é, de facto, o menor inteiro positivo  $n$  tal que  $(b^{-1}ab)^n = 1_G$ , ou seja,  $o(b^{-1}ab) = n_0$ .

Mostramos de seguida que, se  $a$  tiver ordem infinita, então,  $b^{-1}ab$  também tem ordem infinita, usando a regra do contrarrecíproco. Suponhamos que  $o(b^{-1}ab) = k$  é finita. Então, pelo que acabámos de provar,  $o(b(b^{-1}ab)b^{-1}) = k$  e, portanto,  $o(a) = k$  é finita.  $\square$

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

**Proposição 3.48.** *Seja  $G$  um grupo e  $a \in G$  um elemento de ordem finita  $n$ . Então, para qualquer  $p \in \mathbb{N}$ ,  $o(a^p) = \frac{n}{d}$ , onde  $d = \text{m.d.c.}(n, p)$ .*

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

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

Se  $k \in \mathbb{N}$  é tal que  $(a^p)^k = 1_G$ , então, como  $o(a) = n$ , temos que  $n \mid pk$  (ponto 2 da Proposição 3.46, i.e.,  $pk = nq$  para certo  $q \in \mathbb{N}$ ).

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

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

**Exemplo 3.49.** *Considere-se o grupo  $(\mathbb{Z}_{31}^*, \otimes)$ . Facilmente se verifica que, neste grupo,  $o([2]_{31}) = 5$ . Então,*

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

**Lema 3.50.** *Sejam  $G$  um grupo e  $a, b \in G$ . Então, para qualquer inteiro positivo  $k$ ,*

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

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

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

**Proposição 3.51.** *Sejam  $G$  um grupo e  $a, b \in G$ . Se  $ab$  tem ordem finita então  $o(ba) = o(ab)$ .*

**Demonstração:** Trivial, tendo em conta o lema anterior.  $\square$

**Proposição 3.52.** *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  $k \in \mathbb{Z}$ ,

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

**Proposição 3.53.** *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, então, para todo  $n \in \mathbb{Z}$ ,  $(ab)^n = a^n b^n$ . 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 3.46 estamos em condições de concluir que  $o(ab) \mid o(a)o(b)$ .  $\square$

**Exemplo 3.54.** *No grupo aditivo  $(\mathbb{Z}_6)$ , temos que  $o([2]_6) = 3$ ,  $o([3]_6) = 2$  e  $o([4]_6) = 3$ .*

*Temos que*

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

*Temos também que*

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

### 3.4 o teorema de Lagrange

Nesta secção apresentamos um resultado fundamental no estudo dos subgrupos de um grupo. Para o fazer, começamos por observar que, partindo da operação de um grupo  $G$ , podemos definir uma operação no conjunto dos subconjuntos de  $G$  que confere a este conjunto a estrutura de semigrupo com identidade.

**Definição 3.55.** Sejam  $G$  um grupo e  $X, Y \subseteq G$ . Chama-se produto de  $X$  por  $Y$ , e representa-se por  $XY$ , ao conjunto

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

**Exemplo 3.56.** No grupo  $D_3$ , se  $X = \{\rho_1, \rho_2\}$  e  $Y = \{\rho_1, \rho_2, \theta_1\}$ , temos que

$$\begin{aligned} XY &= \{\rho_1\rho_1, \rho_1\rho_2, \rho_1\theta_1, \rho_2\rho_1, \rho_2\rho_2, \rho_2\theta_1\} \\ &= \{\rho_1, \rho_2, \theta_1, \rho_2, \rho_3, \theta_3\} \\ &= \{\rho_1, \rho_2, \theta_1, \rho_3, \theta_3\}. \end{aligned}$$

O exemplo anterior mostra que, se os subconjuntos  $X$  e  $Y$  de um grupo  $G$  forem finitos, com  $m$  e  $n$  elementos, o conjunto  $XY$  tem, no máximo,  $mn$  elementos.

**Proposição 3.57.** Sejam  $G$  um grupo e  $\mathcal{P}(G) = \{X \mid X \subseteq G\}$ . Então,  $\mathcal{P}(G)$  é um semigrupo, 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 3.58.** Seja  $G = \{e, a, b, c\}$  o grupo de 4-Klein, i.e., o grupo cuja operação é dada pela tabela

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

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  $A$ .



Para o estudo que vamos efetuar, interessa sobretudo considerar produtos de um subconjunto singular por outro subconjunto. Assim, adoptamos a seguinte notação, para facilitar a escrita.

**Notação.** Escreve-se  $aY$  para representar

$$\{a\}Y = \{ay \in G \mid y \in Y\}$$

e escreve-se  $Xb$  para representar

$$X\{b\} = \{xb \in G \mid x \in X\}.$$

A multiplicação de subconjuntos de um grupo  $G$  está associada a duas relações binárias definidas por um seu subgrupo que apresentamos de seguida.

**Proposição 3.59.** *Sejam  $G$  um grupo e  $H < G$ . A relação  $\equiv^e (\text{mod } H)$ , definida em  $G$  por*

$$\forall x, y \in G, \quad x \equiv^e y (\text{mod } H) \iff x^{-1}y \in H$$

*é uma relação de congruência à esquerda.*

**Demonstração:** Primeiro, verifiquemos que  $\equiv^e (\text{mod } H)$  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  $x \equiv^e y (\text{mod } H)$ . Então,

$$x \equiv^e y (\text{mod } H) \iff x^{-1}y \in H \Rightarrow y^{-1}x = (x^{-1}y)^{-1} \in H \iff y \equiv^e x (\text{mod } H).$$

Logo, a relação é simétrica.

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

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

pelo que a relação é transitiva.

Verifiquemos agora que a relação é congruente 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,

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

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

Analogamente, provamos que

**Proposição 3.60.** *Sejam  $G$  um grupo e  $H < G$ . A relação  $\equiv^d \pmod{H}$ , definida em  $G$  por*

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

*é uma relação de congruência à direita.*  $\square$

**Definição 3.61.** *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

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

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 3.62.** *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  $H$ .*

**Proposição 3.63.** *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

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

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,

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

□

**Exemplo 3.64.** *Seja  $G = \{e, a, b, c\}$  o grupo de 4-Klein, i.e., o grupo cuja operação é dada pela seguinte tabela*

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

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

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

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

**Exemplo 3.65.** *Relativamente ao grupo não comutativo  $D_3 = \{\rho_1, \rho_2, \rho_3, \theta_1, \theta_2, \theta_3\}$  apresentado no Exemplo 3.10, considerando o subgrupo  $H = \{\rho_1, \theta_1\}$ , as classes laterais esquerdas são*

$$\rho_1 H = H = \theta_1 H, \quad \theta_2 H = \{\theta_2, \rho_3\} = \rho_3 H \quad e \quad \theta_3 H = \{\theta_3, \rho_2\} = \rho_2 H$$

e as classes laterais direitas são

$$H\rho_1 = H = H\theta_1, \quad H\theta_2 = \{\theta_2, \rho_2\} = H\rho_2 \quad e \quad H\theta_3 = \{\theta_3, \rho_3\} = H\rho_3.$$

Os exemplos anteriores mostram que as classes laterais direitas definidas por um subgrupo de um grupo não são necessariamente iguais às classes laterais esquerdas definidas pelo mesmo subgrupo. No entanto, em cada exemplo, podemos verificar que o número de classes esquerdas é igual ao número de classes direitas e que o número de elementos de cada classe (direita ou esquerda) mantém-se constante. São estas duas caraterísticas das classes laterais direitas que provamos de seguida.

**Proposição 3.66.** *Sejam  $G$  um grupo finito e  $H < G$ . Se  $a_1H, a_2H, \dots, a_rH$  são exatamente as classes laterais esquerdas de  $H$  em  $G$  (com  $a_1, a_2, \dots, a_n \in G$ ), então,  $Ha_1^{-1}, Ha_2^{-1}, \dots, Ha_r^{-1}$  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  $a_1H, a_2H, \dots, a_rH$ . Sejam  $x \in G$  e  $1 \leq i \leq r$ . Então,

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

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  $i$ .  $\square$

**Observação.** No seguimento desta proposição, escrevemos

$$G/\equiv^e(\text{ mod } H) = \{a_1H, a_2H, \dots, a_rH\}$$

se e só se

$$G/\equiv^d(\text{ mod } H) = \{Ha_1^{-1}, Ha_2^{-1}, \dots, Ha_r^{-1}\}.$$

**Definição 3.67.** *Sejam  $G$  um grupo finito e  $H < G$ . Chama-se:*

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

**Teorema 3.68. (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 3.69.** *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 3.70.** *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,

$$o(x) \mid p \Rightarrow o(x) = p \Rightarrow |\langle x \rangle| = p \iff G = \langle x \rangle.$$

$\square$

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 (ver exercício 26 das folhas de exercícios). No entanto, se esse fator é um número primo, podemos afirmar a existência desse subgrupo.

**Teorema 3.71.** (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  $o(a) = p$ .*

$\square$

### 3.5 subgrupos normais, relações de congruência e grupos quociente

Na secção anterior, vimos que nem sempre a classe lateral esquerda de um elemento coincide com a sua classe lateral direita. Neste capítulo veremos que o facto de exigirmos que tal aconteça para todos os elementos de grupo, permite-nos falar num outro grupo - o grupo quociente.

**Definição 3.72.** *Sejam  $G$  um grupo e  $H < G$ . Diz-se que  $H$  é subgrupo normal ou invariante de  $G$ , e escreve-se  $H \triangleleft G$ , se*

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

Assim, um subgrupo  $H$  de  $G$  é invariante se, para cada  $x \in G$  e  $h_1 \in H$ , existe  $h_2 \in H$  tal que

$$xh_1 = h_2x.$$

**Exemplo 3.73.** *Dado um grupo  $G$  qualquer, o subgrupo trivial e o subgrupo impróprio são subgrupos invariantes de  $G$ .*

**Exemplo 3.74.** *Seja  $G$  um grupo. Então,  $Z(G) \triangleleft G$ . De facto, seja  $g \in G$ . Então,*

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

**Exemplo 3.75.** *No grupo  $D_3 = \{\rho_1, \rho_2, \rho_3, \theta_1, \theta_2, \theta_3\}$  e subgrupo  $H = \{\rho_1, \theta_1\}$  referidos no Exemplo 3.65, como*

$$\theta_2 H = \{\theta_2, \rho_3\} \neq \{\theta_2, \rho_2\} = H\theta_2,$$

*concluimos que  $H$  não é subgrupo normal de  $D_3$ . No entanto, se considerarmos o subgrupo  $K = \{\rho_1, \rho_2, \rho_3\}$ , temos que  $K \triangleleft D_3$ , uma vez que*

$$\rho_1 K = K\rho_1 = \rho_2 K = K\rho_2 = \rho_3 K = K\rho_3 = K = \{\rho_1, \rho_2, \rho_3\}$$

e

$$\theta_1 K = K\theta_1 = \theta_2 K = K\theta_2 = \theta_3 K = K\theta_3 = \{\theta_1, \theta_2, \theta_3\}.$$

**Proposição 3.76.** *Sejam  $G$  um grupo e  $H < G$  tal que  $|G : H| = 2$ . Então,  $H \triangleleft G$ .*

**Demonstração:** Seja  $H < G$  tal que  $|G : H| = 2$ . Então, existe  $x \in G \setminus H$  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  $y \in G$ . □

**Proposição 3.77.** *Todo o subgrupo de um grupo abeliano é um subgrupo invariante.* □

O teorema seguinte apresenta uma importante caracterização dos subgrupos normais.

**Teorema 3.78.** *Sejam  $G$  um grupo e  $H < G$ . Então,*

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

**Demonstração:** Suponhamos primeiro que  $H \triangleleft G$ . Então, para todo  $x \in G$ ,

$$xH = Hx.$$

Sejam  $g \in G$  e  $h \in H$ . Então,

$$ghg^{-1} = (gh)g^{-1} = (h'g)g^{-1} = h'(gg^{-1}) = h' \in H.$$

Reciprocamente, suponhamos que, para todos  $x \in G$  e  $h \in H$ ,

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

Seja  $g \in G$ . Então,

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

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

É óbvio que, se um grupo  $G$  admite um subgrupo invariante  $H$ , as relações  $\equiv^e (\text{mod } H)$  e  $\equiv^d (\text{mod } H)$  são uma e uma só relação de congruência. De facto,

$$x \equiv^e y (\text{mod } H) \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH = Hx \Leftrightarrow yx^{-1} \in H \Leftrightarrow x \equiv^d y (\text{mod } H).$$

Assim, fala-se de uma única relação  $\equiv (\text{mod } H)$ , que, por sua vez, define um único conjunto quociente, que se representa por  $G/H$ . Temos, assim, que

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

**Proposição 3.79.** *Sejam  $G$  um grupo e  $H \triangleleft G$ . 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.  $\square$

**Definição 3.80.** *Sejam  $G$  um grupo e  $H \triangleleft G$ . Ao grupo  $G/H$  chama-se grupo quociente.*

**Proposição 3.81.** *Sejam  $G$  um grupo e  $\theta$  uma relação de congruência definida em  $G$ . Então, a classe de congruência do elemento identidade,  $[1_G]_\theta$ , é um subgrupo invariante 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  $\theta$  uma relação de congruência em  $G$ . Pretendemos provar, primeiro, que

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

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,

$$a\theta 1_G \Rightarrow xax^{-1}\theta x1_G x^{-1} = xx^{-1} = 1_G,$$

pelo que  $xxa^{-1} \in [1_G]_\theta$  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,

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

□

O que acabamos de ver permite-nos concluir 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). Assim, basta estudar os subgrupos normais de um grupo para conhecermos as congruências possíveis de definir nesse grupo (ou vice-versa).

### 3.6 morfismos

**Definição 3.82.** Sejam  $G_1, G_2$  grupos. Uma aplicação  $\psi : G_1 \longrightarrow G_2$  diz-se um morfismo ou homomorfismo se

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

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 bijectiva. 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 bijectiva.

**Exemplo 3.83.** Sejam  $G_1$  e  $G_2$  grupos e  $\varphi : G_1 \rightarrow G_2$  definida por  $\varphi(x) = 1_{G_2}$ , para todo  $x \in G_1$ . Então,  $\varphi$  é um morfismo de grupos (conhecido por morfismo nulo)

**Exemplo 3.84.** A aplicação  $\varphi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2$ , definida por

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

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):

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

Para evitar todos estes cálculos, uma vez que  $[2]_2 = [0]_2$  e  $[3]_2 = [1]_2$ , podemos definir este por morfismo por  $\varphi([x]_4) = [x]_2$ , para todo  $[x]_4 \in \mathbb{Z}_4$  e trabalhar apenas com a expressão. Assim, para provarmos que temos um morfismo, basta observar que, para  $[x]_4, [y]_4 \in \mathbb{Z}_4$ , temos que

$$\varphi([x]_4 + [y]_4) = \varphi([x + y]_4) = [x + y]_2 = [x]_2 + [y]_2 = \varphi([x]_4) + \varphi([y]_4).$$

No seguimento do exemplo anterior, coloca-se uma pergunta natural: 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 é NÃO. De facto, prova-se que

**Proposição 3.85.**  $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ , definida por  $\varphi([x]_n) = [x]_m$  é um morfismo de grupos se e só se  $m \mid n$ . □

**Proposição 3.86.** 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,

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

□

**Proposição 3.87.** Sejam  $G_1$  e  $G_2$  dois grupos e  $\psi : G_1 \longrightarrow G_2$  um morfismo. Então

$$[\psi(x)]^{-1} = \psi(x^{-1}).$$

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

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

e

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

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

**Proposição 3.88.** *Sejam  $G_1$  e  $G_2$  dois grupos,  $H \subseteq G_1$  e  $\psi : G_1 \longrightarrow G_2$  um morfismo. Então,*

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

**Demonstração:** Seja  $H < G_1$ . Então:

(i)  $\psi(H) \neq \emptyset$ , pois

$$1_{G_1} \in H \Rightarrow \psi(1_{G_1}) \in \psi(H);$$

(ii) Sejam  $a, b \in \psi(H)$ . Então,

$$(\exists x, y \in H) \quad a = \psi(x) \quad \text{e} \quad b = \psi(y).$$

Então,

$$(\exists x, y \in H) \quad ab = \psi(x)\psi(y) = \psi(xy),$$

pelo que

$$(\exists z = xy \in H) \quad ab = \psi(z),$$

e, portanto,  $ab \in \psi(H)$ ;

(iii) Seja  $a \in \psi(H)$ . Então,

$$a = \psi(x) \quad \text{com } x \in H \Rightarrow a^{-1} = [\psi(x)]^{-1} = \psi(x^{-1}) \quad \text{com } x^{-1} \in H.$$

Logo,  $a^{-1} \in \psi(H)$ .

Concluimos, assim, que  $\psi(H) < G$ . □

**Corolário 3.89.** *Seja  $\psi : G_1 \longrightarrow G_2$  um morfismo de grupos. Se  $\psi$  é um monomorfismo então*

$$G_1 \cong \psi(G_1).$$

□

Sabemos que, dados dois conjuntos finitos, só é possível definir uma aplicação bijetiva entre eles se ambos tiverem a mesma cardinalidade. Assim, podemos concluir que dois grupos finitos isomorfos têm a mesma ordem. Mas, dois grupos com a mesma ordem não são necessariamente isomorfos. Como contra-exemplo, 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  $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  e  $f : G \rightarrow \mathbb{Z}_4$  fosse um isomorfismo de grupos, teríamos

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

para todo  $x \in G$ . Sendo  $f$  bijetiva, concluamos 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  $\bar{0}$  e  $\bar{2}$  são simétricas de si próprias.

**Proposição 3.90.** *Sejam  $G_1$  e  $G_2$  dois grupos,  $H \subseteq G_1$  e  $\psi : G_1 \longrightarrow G_2$  um epimorfismo. Então,*

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

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

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

pelo que  $\psi(H) \triangleleft G_2$ . □

**Definição 3.91.** *Seja  $\psi : G_1 \longrightarrow G_2$  um morfismo de grupos. Chama-se núcleo (ou kernel) de  $\psi$ , e representa-se por  $\text{Nuc}\psi$  ou  $\ker \psi$ , ao subconjunto de  $G_1$*

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

**Proposição 3.92.** *Seja  $\psi : G_1 \longrightarrow G_2$  um morfismo de grupos. Então,  $\text{Nuc}\psi \triangleleft G_1$ .*

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

- (i) Observemos, primeiro, que  $1_{G_1} \in \text{Nuc}\psi$ . De facto,  $1_{G_1} \in G_1$  e  $\psi(1_{G_1}) = 1_{G_2}$ ;
- (ii) Sejam  $a, b \in \text{Nuc}\psi$ . Então,

$$\begin{aligned} a, b \in \text{Nuc}\psi &\Rightarrow a, b \in G_1 \text{ e } \psi(a) = \psi(b) = 1_{G_2} \\ &\Rightarrow a^{-1}, b \in G_1, \psi(a^{-1}) = [\psi(a)]^{-1} = 1_{G_2}^{-1} = 1_{G_2} = \psi(b) \\ &\Rightarrow a^{-1}b \in G_1 \text{ e } \psi(a^{-1}b) = \psi(a^{-1}) \psi(b) = 1_{G_2} 1_{G_2} = 1_{G_2} \\ &\Rightarrow a^{-1}b \in \text{Nuc}\psi. \end{aligned}$$

Assim, concluimos que este subconjunto de  $G_1$  é, de facto, um seu subgrupo.

Sejam  $g \in G_1$  e  $b \in \text{Nuc}\psi$ . Então,

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

e

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

pelo que  $gbg^{-1} \in \text{Nuc}\psi$ . Logo,  $\text{Nuc}\psi \triangleleft G_1$ . □

Assim sendo, o núcleo de um morfismo  $\psi : G_1 \longrightarrow G_2$  de grupos define uma relação de congruência, a saber

$$\begin{aligned}x \equiv y \pmod{\text{Nuc}\psi} &\iff xy^{-1} \in \text{Nuc}\psi \\ &\iff \psi(xy^{-1}) = 1_{G_2} \\ &\iff \psi(x)[\psi(y)]^{-1} = 1_{G_2} \\ &\iff \psi(x) = \psi(y).\end{aligned}$$

**Proposição 3.93.** *Sejam  $G$  um grupo e  $H \triangleleft G$ . Então,*

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

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

**Demonstração:** Sejam  $G$  um grupo e  $H \triangleleft G$ .

Então, para  $x, y \in G$ ,

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

pelo que  $\pi$  é um morfismo. Além disso,  $\psi$  é obviamente sobrejetiva (cada classe é imagem por  $\pi$  do seu representante). Por fim,

$$\begin{aligned}x \in \text{Nuc}\pi &\iff \pi(x) = H \\ &\iff xH = H \\ &\iff x \in H.\end{aligned}$$

□

As duas últimas proposições dizem-nos que:

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

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

Considerando as duas situações em simultâneo, temos que:

Seja  $\psi : G \longrightarrow G'$  um morfismo de grupos. Então, por (i),

$$\text{Nuc}\psi \triangleleft G.$$

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

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

O teorema seguinte, conforme o nome indica, é fundamental no estudo dos morfismos de grupos. Permite-nos perceber que qualquer morfismo pode ser escrito como a composta de dois morfismos, o que muitas vezes facilita o estudo do morfismo original.

**Teorema 3.94. Teorema Fundamental do Homomorfismo.** *Seja  $\theta : G \longrightarrow G'$  um morfismo de grupos. Então,*

$$\text{Im}\theta \cong G/\text{Nuc}\theta.$$

**Demonstração:** Sejam  $K = \text{Nuc}\theta$  e  $\phi : G/K \longrightarrow G'$  tal que

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

$$\begin{array}{ccc} G & \xrightarrow{\theta} & G' \\ \pi \downarrow & \nearrow \phi & \\ G/\text{Nuc}\theta & & \end{array}$$

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

$$\begin{aligned} xK = yK &\iff x^{-1}y \in K (= \text{Nuc}\theta) \\ &\iff \theta(x^{-1}y) = 1_{G'} \\ &\iff \theta(x) = \theta(y). \end{aligned}$$

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

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

pelo que  $\phi$  é injetiva.

Mais ainda,

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

Observamos, por último, que  $\phi$  é um morfismo, já que

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

Concluimos, então, que  $\phi$  é um monomorfismo cujo conjunto imagem (que é isomorfo ao seu domínio) é igual a  $\text{Im}\theta$ . Logo,

$$\text{Im}\theta \cong G/K = G/\text{Nuc}\theta.$$

□

### 3.6.1 teoremas de isomorfismo

Terminamos esta secção apresentando dois resultados envolvendo isomorfismos entre grupos. Estes resultados são muitas vezes referenciados como *Teoremas de Isomorfismo*.

Para provarmos o 1º Teorema de Isomorfismo, começamos por enunciar e demonstrar o seguinte lema.

**Lema 3.95.** *Sejam  $\psi : G \rightarrow G'$  um morfismo de grupos e  $K < G$ . Então,*

$$\text{Nuc}\psi \subseteq K \Rightarrow \psi^{-1}(\psi(K)) = K.$$



**Demonstração:** Precisamos apenas de provar que  $\psi^{-1}(\psi(K)) \subseteq K$ , já que a outra inclusão acontece sempre. Assim,

$$\begin{aligned}
 x \in \psi^{-1}(\psi(K)) &\iff (\exists y \in \psi(K)) \quad y = \psi(x) \\
 &\iff (\exists a \in K) \quad y = \psi(a) = \psi(x) \\
 &\iff (\exists a \in K) \quad \psi(a^{-1}x) = [\psi(a)]^{-1} \psi(x) = 1_{G'} \\
 &\iff (\exists a \in K) \quad a^{-1}x \in \text{Nuc}\psi \\
 &\Rightarrow (\exists a \in K) \quad a^{-1}x \in K \\
 &\Rightarrow x = a \cdot a^{-1}x \in K.
 \end{aligned}$$

□

**Teorema 3.96. (1º Teorema do Isomorfismo)** Sejam  $G$  e  $G'$  dois grupos e  $\psi : G \rightarrow G'$  um epimorfismo. Seja  $K \triangleleft G$  tal que  $\text{Nuc}\psi \subseteq K$ . Então,

$$G/K \cong G'/\psi(K).$$

**Demonstração:** Observemos, primeiro, que, sendo  $\psi$  um epimorfismo,

$$K \triangleleft G \Rightarrow \psi(K) \triangleleft G',$$

pelo que faz sentido falar no grupo quociente  $G'/\psi(K)$ .

Seja  $\theta : G/K \rightarrow G'/\psi(K)$  definida por  $\theta(xK) = \psi(x)\psi(K)$

$$\begin{array}{ccc}
 G & \xrightarrow{\psi} & G' \\
 \pi \downarrow & & \downarrow \pi' \\
 G/K & \xrightarrow{\theta} & G'/\psi(K)
 \end{array}$$

Estará  $\theta$  bem definida? De facto, para todo  $x \in G$ ,  $\psi(x) \in G'$  e

$$\begin{aligned}
 xK = yK &\iff x^{-1}y \in K \\
 &\Rightarrow \psi(x^{-1}y) \in \psi(K) \\
 &\iff [\psi(x)]^{-1} \psi(y) \in \psi(K) \\
 &\iff \psi(x) \psi(K) = \psi(y) \psi(K) \\
 &\iff \theta(xK) = \theta(yK).
 \end{aligned}$$

Por outro lado, porque  $\text{Nuc}\psi \subseteq K$ , temos que  $\psi^{-1}(\psi(K)) = K$  e, portanto,

$$\begin{aligned}
 \theta(xK) = \theta(yK) &\iff \psi(x) \psi(K) = \psi(y) \psi(K) \\
 &\iff \psi(x^{-1}y) \in \psi(K) \\
 &\Rightarrow x^{-1}y \in \psi^{-1}(\psi(K)) = K \\
 &\iff xK = yK,
 \end{aligned}$$

pelo que  $\psi$  é injetiva. Mais ainda, como  $\psi$  é sobrejetiva, temos que

$$(\forall y \in G') (\exists x \in G) \quad \psi(x) = y,$$

o que equivale a dizer que

$$(\forall y \psi(K) \in G'/\psi(K)) (\exists xK \in G/K) \quad \theta(xK) = y\psi(K),$$

pelo que  $\theta$  é também sobrejetiva.

Falta então verificar que  $\theta$  é um morfismo. De facto,

$$\begin{aligned}
 \theta(xKyK) &= \theta(xyK) = \psi(xy) \psi(K) = \psi(x) \psi(y) \psi(K) \\
 &= \psi(x) \psi(K) \psi(y) \psi(K) = \theta(xK) \theta(yK).
 \end{aligned}$$

Logo,  $\theta$  é um isomorfismo e o resultado verifica-se. □

Para demonstrarmos o 2º teorema do isomorfismo necessitamos dos seguintes lemas:

**Lema 3.97.** *Sejam  $G$  um grupo e  $H < G$  e  $H' \triangleleft G$ . Então,  $HH' < G$ .* □

**Lema 3.98.** *Sejam  $G$  um grupo e  $H < G$  e  $H' \triangleleft G$ . Então, se  $H' \subseteq H$ , então,  $H' \triangleleft H$ .* □

**Teorema 3.99. (2º Teorema do Isomorfismo)** Sejam  $G$  um grupo e  $H, T < G$  tal que  $T \triangleleft G$ . Então,

$$(HT)/T \cong H/(H \cap T).$$

**Demonstração:** Pelos lemas anteriores,  $HT < G$  e  $T \triangleleft HT$ . Faz então sentido falar no grupo quociente  $(HT)/T$ .

Por outro lado,  $H \cap T \triangleleft H$ . De facto, sabemos que  $H \cap T < G$ , e, portanto,  $H \cap T < H$ . Mais ainda

$$\begin{aligned} x \in H \cap T \quad \text{e} \quad a \in H &\Rightarrow x \in T \quad \text{e} \quad a \in G \\ &\Rightarrow xax^{-1} \in T \quad (T \triangleleft G), \end{aligned}$$

pelo que  $H \cap T \triangleleft H$ . Logo, podemos falar no grupo quociente  $H/(H \cap T)$ .

Provemos agora que os dois grupos quocientes são isomorfos.

Seja  $\pi : HT \rightarrow HT/T$  o epimorfismo canónico. Como  $H \subseteq HT$ , consideremos

$$\begin{aligned} \pi|_H : H &\rightarrow HT/T \\ x_1 &\mapsto x_1T (= x_1 1_G T) \end{aligned}$$

Como  $\pi|_H$  é uma restrição de um morfismo é ainda um morfismo. Mais ainda, este morfismo é sobrejectivo. De facto,

$$\begin{aligned} &(\forall yT \in HT/T) (\exists x_1 \in H, x_2 \in T) \quad yT = x_1 x_2 T \\ \iff &(\forall yT \in HT/T) (\exists x_1 \in H) \quad yT = x_1 T. \\ \iff &(\forall yT \in HT/T) (\exists x_1 \in H) \quad yT = \pi|_H(x_1). \end{aligned}$$

Assim,  $H/T = \text{Im} \pi|_H = HT/T$ .

Por outro lado,  $\text{Nuc} \pi|_H = H \cap T$ , já que

$$\begin{aligned} x \in \text{Nuc} \pi|_H &\iff x \in H \text{ e } \pi|_H(x) = T \\ &\iff x \in H \text{ e } xT = T \\ &\iff x \in H \text{ e } x \in T \\ &\iff x \in H \cap T. \end{aligned}$$

Assim, pelo teorema fundamental do homomorfismo, concluímos que

$$H/(H \cap T) = H/\text{Nuc} \pi|_H \cong \text{Im} \pi|_H = HT/T.$$

□

## 3.7 grupos cíclicos

Vimos, no final da subsecção 3.2.2, o conceito de subgrupo gerado por um subconjunto singular  $\{a\}$  de um grupo  $G$ . Este conceito revela-se de grande importância para a Teoria de Grupos se pensarmos que pode esse subgrupo gerado ser o próprio grupo. Justifica-se, por isso, a existência de uma secção a ele dedicada.

### 3.7.1 conceito e exemplos

**Definição 3.100.** 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 3.101.** O grupo  $(\mathbb{Z}, +)$  é cíclico, já que  $\mathbb{Z} = \langle 1 \rangle$ , pois

$$(\forall n \in \mathbb{Z}) \quad n = n \cdot 1.$$

**Exemplo 3.102.** O grupo  $(\mathbb{R}, +)$  não é cíclico.

**Exemplo 3.103.** O grupo  $(\mathbb{Z}_4, +)$  é cíclico, já que  $\mathbb{Z}_4 = \langle \bar{1} \rangle = \langle \bar{3} \rangle$ , pois

$$\bar{0} = 0 \cdot \bar{1} = 0 \cdot \bar{3}$$

$$\bar{1} = 1 \cdot \bar{1} = 3 \cdot \bar{3}$$

$$\bar{2} = 2 \cdot \bar{1} = 2 \cdot \bar{3}$$

$$\bar{3} = 3 \cdot \bar{1} = 1 \cdot \bar{3}$$

**Exemplo 3.104.** Para qualquer  $n \in \mathbb{N}$ , temos que  $(\mathbb{Z}_n, +)$  é cíclico, já que  $\mathbb{Z}_n = \langle \bar{1} \rangle$ .

**Exemplo 3.105.** 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 3.106.** O grupo trivial  $G = \{1_G\}$  é um grupo cíclico. De facto, em qualquer grupo  $G$ ,  $\langle 1_G \rangle = \{1_G\}$ .

### 3.7.2 propriedades elementares

Apresentamos algumas propriedades de grupos cíclicos que resultam da própria definição.

**Proposição 3.107.** *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,

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

Observe-se que o recíproco do teorema anterior não é verdadeiro, como mostra o seguinte exemplo.

**Exemplo 3.108.** *O grupo 4-Klein apresentado no Exemplo 3.40 é obviamente 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 3.109.** *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  $H = \langle a^d \rangle$ :

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

(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,

$$a^m = a^{qd} \in \langle a^d \rangle,$$

pelo que  $H = \langle a^d \rangle$ . □

**Observação.** A demonstração do teorema anterior permite-nos concluir que se o grupo  $G$  é cíclico e tem ordem  $n$ , isto é, se existe  $a \in G$  tal que  $G = \langle a \rangle = \{1_G, a, a^2, \dots, a^{n-1}\}$ , então, para qualquer divisor positivo  $k$  de  $n$ ,  $\langle a^{\frac{n}{k}} \rangle$  é um subgrupo de  $G$  com ordem  $k$ . Mais ainda, um grupo cíclico  $G$  de ordem finita  $n$  tem um e um só subgrupo de ordem  $k$ , para cada  $k$  divisor de  $n$ .

**Exemplo 3.110.** Os subgrupos de  $\mathbb{Z}$  são todos do tipo  $n\mathbb{Z}$ . De facto, para todo  $n \in \mathbb{Z}$ ,  $\langle n \rangle = n\mathbb{Z}$ .

O próximo resultado deduz-se facilmente dos resultados anteriores, pelo que a sua demonstração será omitida.

**Proposição 3.111.** Qualquer gerador de um grupo cíclico finito tem ordem igual à ordem do grupo.

□

**Exemplo 3.112.** Em  $\mathbb{Z}_4$  tem-se que:  $o(\bar{3}) = 4$  e  $\mathbb{Z}_4 = \langle \bar{3} \rangle$ .

Vimos já que, para um grupo  $G = \langle a \rangle$ ,  $G$  é abeliano e se  $H < G$ ,  $H = \langle a^d \rangle$ , para algum  $d \in \mathbb{N}$ .

Assim,  $H \triangleleft G$ , pelo que podemos falar no grupo  $G/H$ . Vejamos de seguida como são os elementos deste grupo:

**Proposição 3.113.** Seja  $G = \langle a \rangle$  um grupo infinito e  $H = \langle a^d \rangle \triangleleft G$ . Então,

$$H, aH, a^2H, \dots, a^{d-1}H$$

é a lista completa de elementos de  $G/H$ .

**Demonstração:** Observemos primeiro que, para todo  $x \in G$ ,

$$xH = a^rH, \quad \text{para algum } r \in \{0, 1, 2, \dots, d-1\}.$$

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

$$a^p = a^{qd+r} = a^r \cdot (a^d)^q \in a^rH.$$

Logo,

$$a^pH = a^rH.$$

Provemos agora que, para  $0 \leq i, j \leq d-1$ ,

$$i \neq j \Rightarrow a^iH \neq a^jH.$$

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

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

Logo, a implicação verifica-se e, portanto,

$$G/H = \{H, aH, \dots, a^{d-1}H\}.$$

□

### 3.7.3 morfismos entre grupos cíclicos

Vimos, na secção anterior, que dois grupos com a mesma ordem não são necessariamente isomorfos. Tal não se verifica quando falamos em grupos cíclicos.

**Proposição 3.114.** *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

$$\begin{aligned}
 G &= \{1_G, a, a^2, \dots, a^{n-1}, a^n\} \\
 &\text{e} \\
 T &= \{1_T, b, b^2, \dots, b^{n-1}, b^n\}.
 \end{aligned}$$

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

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

é obviamente um isomorfismo.

□

**Corolário 3.115.** *Sejam  $n \in \mathbb{N}$  e  $G$  um grupo cíclico de ordem  $n$ . Então,  $G \cong \mathbb{Z}_n$ .*

**Demonstração:** Imediata, tendo em conta o exemplo 3.104. □

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

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

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

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

Podemos então concluir que:

**Proposição 3.116.** *Se  $G$  é um grupo cíclico infinito, então,  $G \cong \mathbb{Z}$ .* □

### 3.8 grupo simétrico

**Definição 3.117.** *Seja  $A$  um conjunto. Uma permutação de  $A$  é uma aplicação bijetiva de  $A$  em  $A$ .*

**Observação 1.** Se  $A$  é um conjunto finito com  $n$  elementos ( $n \in \mathbb{N}$ ), podemos estabelecer uma bijecção entre  $A$  e o conjunto  $\{1, 2, \dots, n\}$ , 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 2.** 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 (ver Exemplo 3.9).

**Definição 3.118.** *Chama-se grupo simétrico de um conjunto com  $n$  elementos, e representa-se por  $S_n$ , ao grupo das permutações desse conjunto.*



**Exemplo 3.119.** 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 3.120.** Se considerarmos um conjunto com 3 elementos,

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

**Exemplo 3.121.** Se considerarmos um conjunto com 4 elementos, temos que

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

A classe dos grupos simétricos é uma boa fonte de grupos não abelianos, conforme garante a proposição seguinte.

**Proposição 3.122.** 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

$$f(1) = 2, f(2) = 3, f(3) = 1, f(k) = k, \forall 4 \leq k \leq n,$$

$$g(1) = 2, \quad g(2) = 1, \quad g(k) = k, \quad \forall 3 \leq k \leq n,$$

temos que

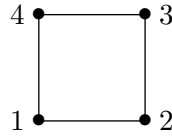
$$(f \circ g)(1) = 3 \neq 1 = (g \circ f)(1). \quad \square$$

### 3.8.1 O grupo diedral

**Definição 3.123.** Chama-se grupo diedral ao grupo das simetrias e rotações de uma linha poligonal.

**Exemplo 3.124.** O grupo diedral  $D_3$ , grupo das simetrias e rotações de um triângulo equilátero, foi apresentado no exemplo 3.10. Temos que  $D_3 = S_3$ .

**Exemplo 3.125.** O grupo diedral  $D_4$ :



Neste caso, no grupo diedral existem menos elementos do que no grupo simétrico. De facto, se considerarmos:

(i) as rotações de  $0^\circ$ ,  $90^\circ$ ,  $180^\circ$  e  $270^\circ$ , temos, respetivamente:

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

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

(ii) as simetrias em relação às bissetrizes  $[1, 3]$  e  $[2, 4]$  temos, respetivamente:

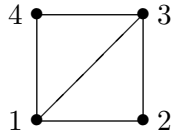
$$\theta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ e } \theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix};$$

(iii) as simetrias em relação às mediatrizes do lado  $[1, 2]$  e do lado  $[2, 3]$  temos, respetivamente:

$$\theta_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \text{ e } \theta_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

assim,  $D_4$  tem 8 elementos enquanto que  $S_4$  tem 24 elementos.

**Exemplo 3.126.** *Relativamente à figura*



*o grupo diedral é composto pelas aplicações*

$$\begin{aligned}\phi_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \\ \phi_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ e } \phi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.\end{aligned}$$

### 3.8.2 ciclos

Quando trabalhamos com permutações, seja com o grupo simétrico ou com o grupo diedral, a notação até agora usada para a descrição das aplicações, embora simples, pode tornar-se pesada com envolvem muitos números e também permutações. Nesta seção estudaremos conceitos associados ao conceito de permutação que nos permitirá simplificar não só a notação na representação das diferentes permutações, como possíveis cálculos a fazer.

**Definição 3.127.** *Diz-se que uma permutação  $\sigma$  de um conjunto finito  $A$  é um ciclo de comprimento  $n$  se existirem*

$$a_1, a_2, \dots, a_n \in A$$

*tais que*

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

*e se*

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

*Representa-se este facto por  $\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \end{pmatrix}$ .*

**Exemplo 3.128.** *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.** O produto (composta) de dois ciclos nem sempre é 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.

**Definição 3.129.** 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 movido simultaneamente pelos dois ciclos.

**Observação.** A noção de ciclos disjuntos é importante quando falamos no produto de ciclos. Vimos já que a multiplicação (composição) de dois ciclos (casos particulares de permutações) de  $S_n$  (com  $n \geq 3$ ) não é necessariamente comutativa. Por exemplo,

$$(12)(13) = (132) \neq (123) = (13)(12),$$

No entanto, é fácil perceber da definição que ciclos disjuntos comutam. É importante aqui recordar que, se  $G$  é grupo e  $a, b \in G$ , então,

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

O próximo resultado é fundamental no estudo dos grupos simétricos. Antes de o enunciar e demonstrar vejamos os seguintes exemplos.

**Exemplo 3.130.** Em  $S_6$ ,  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1 \ 6)(2 \ 5 \ 3)$ , i.e., a permutação  $\sigma$  é produto de dois ciclos disjuntos.

**Exemplo 3.131.** Em  $S_6$ , se  $\pi_1 = (123)$  e  $\pi_2 = (241)$ , então,

$$\pi_1 \pi_2 = (123)(241) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 5 & 6 \end{pmatrix} = (1 \ 3)(2 \ 4),$$

i.e., o produto de dois ciclos não disjuntos é produto de dois ciclos disjuntos.

**Teorema 3.132.** *Toda a permutação  $\sigma$  de um conjunto finito é um produto de ciclos disjuntos.*

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

$$1 \quad \sigma(1) \quad \sigma^2(1) \quad \sigma^4(1) \quad \dots \quad (*)$$

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

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

concluíamos que

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

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

Formamos então o ciclo

$$\rho_1 = (1 \quad \sigma(1) \quad \sigma^2(1) \quad \dots \quad \sigma^{r-1}(1)).$$

Seja, então,  $i$  o primeiro elemento de  $A$  que não aparece em  $\rho_1$ . Aplicamos a  $i$  o raciocínio aplicado a 1 e formamos o ciclo

$$\rho_2 = (i \quad \sigma(i) \quad \sigma^2(i) \quad \dots \quad \sigma^{t-1}(i)).$$

Por raciocínios análogos, “percorremos” todos os elementos de  $A$ . Suponhamos que são  $k$  os ciclos que formamos. Então

$$\sigma = \rho_1 \rho_2 \dots \rho_k.$$

Vejamos agora que os ciclos são disjuntos dois a dois.

Consideremos os ciclos  $\rho_1$  e  $\rho_2$ . Suponhamos que existe  $j \in A$  tal que  $j$  aparece no ciclo  $\rho_1$  e no ciclo  $\rho_2$ . Suponhamos, sem perdas de generalidade, que  $j = \sigma^2(1)$  e que  $j = \sigma^3(i)$ . Então,

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

o que não acontece pois  $i$  não aparece em  $\rho_1$ .

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

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

**Resposta:**

(i) se  $\sigma$  é **um ciclo**, então  $o(\sigma)$  é o comprimento do ciclo.

(ii) se  $\sigma$  é **um produto de pelo menos dois ciclos disjuntos**, então  $o(\sigma)$  é o m.m.c. entre os comprimentos dos ciclos em questão.

**Exemplo 3.133.** Em  $S_8$ , como  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 4 & 3 & 7 & 6 & 1 & 8 \end{pmatrix} = (1 \ 2 \ 5 \ 7)(3 \ 4)$ , temos que  $o(\sigma) = 4$ .

De facto,  $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 3 & 4 & 1 & 6 & 2 & 8 \end{pmatrix}$ ,  $\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 1 & 4 & 3 & 2 & 6 & 5 & 8 \end{pmatrix}$  e  $\sigma^4 = id$ .

**Exemplo 3.134.** Em  $S_8$ , como  $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 1 & 7 & 8 & 5 & 6 \end{pmatrix} = (1 \ 3 \ 4)(5 \ 7)(6 \ 8)$ , temos que  $o(\phi) = 6$ .

### 3.8.3 grupo alterno

**Definição 3.135.** Uma transposição é um ciclo de comprimento 2.

**Proposição 3.136.** Qualquer ciclo é produto de transposições.

**Demonstração:** Imediata, tendo em conta que

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

$\square$

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

O resultado seguinte, de certo modo intuitivo, tem uma demonstração que n

**Teorema 3.137.** *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 3.138.** *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 permutações.*

**Exemplo 3.139.** *A identidade é uma permutação par. De facto, se  $A$  tem  $n$  elementos*

$$id = (a_i \ a_j)(a_i \ a_j),$$

*para quaisquer  $a_i, a_j \in A$ .*

**Teorema 3.140.** *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  $id \in A_n$ , 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  $A_n < S_n$ .

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  $\phi_\tau$  é bijectiva, temos que  $\#(A_n) = \#(B_n)$  e, como  $\#(A_n) + \#(B_n) = \#(S_n) = n!$ , o resultado é imediato. □

**Definição 3.141.** *Seja  $A$  um conjunto com  $n$  elementos. Chama-se grupo alterno de  $A$ , e representa-se por  $A_n$ , ao subgrupo das permutações pares.*

### 3.8.4 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 3.142. (Teorema de representação de Cayley)** *Todo o grupo é isomorfo a um grupo de permutações.*

**Demonstração:** Para cada  $x \in G$ , a aplicação

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

é uma permutação em  $G$ .

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

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

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.,  $\theta$  é um morfismo.

Mais ainda,

$$x \in \text{Nuc}\theta \Leftrightarrow \theta(x) = \text{id}_G \Leftrightarrow \lambda_x = \text{id}_G \Rightarrow x = \lambda_x(1_G) = \text{id}_G(1_G) = 1_G,$$

e, portanto,

$$\text{Nuc}\theta = \{1_G\}.$$

Logo,  $\theta$  é um monomorfismo, pelo que  $G \cong \text{Im}\theta < S$ . □

**Exemplo 3.143.** Seja  $G = \mathbb{Z}_4$ . Então, com para todos  $a, x \in \mathbb{Z}_4$ ,  $\lambda_a(x) = a + x$ , temos que

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



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



## 4 elementos da teoria de anéis

### 4.1 generalidades

**Definição 4.1.** Seja  $A$  um conjunto não vazio e duas operações binárias  $[+ \text{ e } \cdot]$  nele definidas. O triplo  $(A, +, \cdot)$  diz-se um anel se

A1.  $(A, +)$  é um grupo comutativo (também chamado módulo);

A2.  $(A, \cdot)$  é um semigrupo;

A3. A operação de multiplicação é distributiva em relação à operação de adição, i.e., para todos  $a, b, c \in A$ ,

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

Tendo em conta que temos duas operações definidas num mesmo conjunto, é natural haver uma maior complexidade de notação. Para tornarmos a abordagem mais simples, 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*. 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  $1_A$ . Por último, 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 que diz respeito à multiplicação, 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  $a^{-1}$ .

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

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

**Exemplo 4.2.** 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 4.3.**  $(\mathbb{Z}, +, \times)$  é um anel comutativo com identidade.

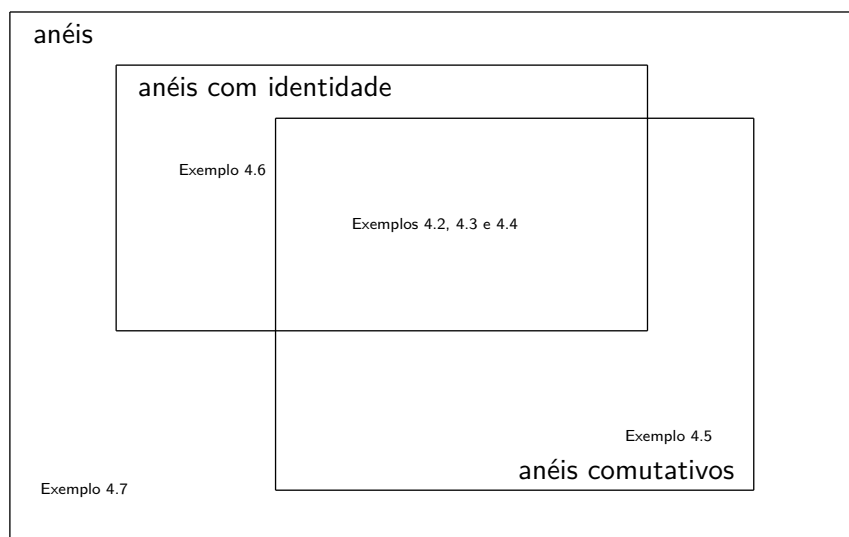
**Exemplo 4.4.**  $(\mathbb{R}, +, \times)$  é um anel comutativo com identidade.

**Exemplo 4.5.**  $(2\mathbb{Z}, +, \times)$  é um anel comutativo sem identidade.

**Exemplo 4.6.**  $(\mathcal{M}_2(\mathbb{R}), +, \times)$  é um anel não comutativo com identidade.

**Exemplo 4.7.** O conjunto  $A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{R} \right\}$ , quando algebrizado com a adição e multiplicação usuais de matrizes quadradas de ordem 2, é um anel não comutativo e sem identidade.

Os exemplos que acabámos de apresentar permitem-nos entender o diagrama seguinte, onde estão representadas as relações existentes entre a classe dos anéis, a classe dos anéis comutativos e a classe dos anéis com identidade



As quatro proposições que apresentamos de seguida apresentam propriedades satisfeitas por qualquer anel, que usaremos constantemente ao longo deste capítulo.

**Proposição 4.8.** *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,

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

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

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

e

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

obtemos  $x 0_A = 0_A$ . □

**Proposição 4.9.** *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  $x = 0_A$ . □

**Proposição 4.10.** *Sejam  $A$  um anel e  $x, y \in A$ . Então:*

- (i)  $(-x) y = x (-y) = -xy$ ;
- (ii)  $(-x) (-y) = xy$ .

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

(i)  $(-x)y$  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,  $-xy = (-x)y = x(-y)$ .

(ii)  $(-x)(-y)$  é o simétrico de  $(-xy)$  já que

$$(-x)(-y) + (-xy) = (-x)(-y) + (-x)y = (-x)(-y + y) = (-x)0_A = 0_A.$$

Como o simétrico de  $-xy$  é, de facto,  $xy$ , obtemos o resultado pretendido.  $\square$

**Proposição 4.11.** Sejam  $A$  um anel,  $n \in \mathbb{N}$  e  $a, b_1, b_2, \dots, b_n \in A$ . Então,

$$(i) \ a(b_1 + b_2 + \dots + b_n) = ab_1 + ab_2 + \dots + ab_n;$$

$$(ii) \ (b_1 + b_2 + \dots + b_n)a = b_1a + b_2a + \dots + b_na.$$

**Demonstração:** Por indução.  $\square$

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 nas potências de expoente inteiro de  $a \in A$ . Assim, temos

$$(i) \ 0a = 0_A;$$

$$(ii) \ (n+1)a = na + a, \text{ para todo } n \in \mathbb{N}_0;$$

$$(iii) \ na = -(-na), \text{ para todo } n \in \mathbb{Z}^-.$$

**Proposição 4.12.** Sejam  $A$ , um anel,  $a, b \in A$  e  $m, n \in \mathbb{Z}$ . Então,

$$(i) \ (m+n)a = ma + na;$$

$$(ii) \ n(ma) = (nm)a;$$

$$(iii) \ n(a+b) = na + nb.$$

**Demonstração:** Os dois primeiros resultados são consequência imediata do facto de  $(A, +)$  ser grupo. Provemos (iii):

(a)  $n = 0$ . Neste caso, temos

$$0_A(a + b) = 0_A = 0_A + 0_A = 0_A a + 0_A b.$$

(b)  $n > 0$ . Vamos usar o Método de Indução Matemática. Se  $n = 1$ , o resultado é imediato. Supondo que o resultado é válido para  $n$ , provemos para  $n + 1$ . Como  $(A, +)$  é grupo comutativo, temos que

$$(n + 1)(a + b) = n(a + b) + (a + b) = na + nb + a + b = (na + a) + (nb + b) = (n + 1)a + (n + 1)b.$$

Concluimos, então, que, para todo  $n \geq 1$ ,  $n(a + b) = na + nb$ .

(c)  $n < 0$ . Neste caso, temos

$$\begin{aligned} n(a + b) &= (-(-n))(a + b) = -[(-n)(a + b)] = -[(-n)a + (-n)b] \\ &= -(-n)a + -(-n)b = na + nb. \end{aligned}$$

□

**Proposição 4.13.** *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)  $n > 0$ . Vamos usar o Método de Indução Matemática. Para  $n = 1$ , o resultado é imediato. Supondo que o resultado é válido para  $n$ , provemos para  $n + 1$ . Temos que

$$(n + 1)(ab) = n(ab) + ab = a(nb) + ab = a(nb + b) = a[(n + 1)b]$$

e

$$(n + 1)(ab) = n(ab) + ab = (na)b + ab = (na + a)b = [(n + 1)a]b.$$

Concluimos, então, que, para todo  $n \geq 1$ ,  $n(ab) = a(nb) = (na)b$ .

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

- (i)  $(a^n)^m = a^{nm}$ ;
- (ii)  $a^n a^m = a^{n+m}$ .

□

**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  $a^n$ .

Consoante as especificidades de um anel, podemos destacar alguns dos seus elementos. É o que vamos fazer de seguida.

**Definição 4.15.** *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 4.16.** *No anel  $(\mathbb{Z}, +, \times)$ , temos que  $\mathcal{U}_A = \{-1, 1\}$ .*

**Exemplo 4.17.** *No anel  $(\mathbb{R}, +, \times)$ , temos que  $\mathcal{U}_A = \mathbb{R} \setminus \{0\}$ .*

**Exemplo 4.18.** *No anel  $(\mathcal{M}_2(\mathbb{R}), +, \times)$ , temos que*

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

**Definição 4.19.** *Seja  $A$  um anel. Um elemento  $a \in A$  diz-se simplificável se, para todos  $x, y \in A$*

$$xa = ya \quad \text{ou} \quad ax = ay \Rightarrow x = y.$$



**Exemplo 4.20.** Nos anéis  $(\mathbb{Z}, +, \times)$  e  $(\mathbb{R}, +, \times)$ , qualquer elemento não nulo é simplificável.

**Exemplo 4.21.** 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

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

**Definição 4.22.** Seja  $A$  um anel. Um elemento  $a \in A$  diz-se um divisor de zero se existe  $b \in A \setminus \{0_A\}$  tal que

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

**Exemplo 4.23.** No anel  $(\mathbb{Z}, +, \times)$ , o único divisor de zero existente é o elemento 0.

**Exemplo 4.24.** No anel  $(\mathbb{R}, +, \times)$ , o único divisor de zero é o elemento 0.

**Exemplo 4.25.** 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. De facto,

(i) se  $a = b = c = d = 0$ , para qualquer matriz  $M$ , quadrada de ordem 2, temos que

$$M \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix};$$

(ii) se  $d \neq 0$  ou  $c \neq 0$ , temos que

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} d & d \\ -c & -c \end{bmatrix} = \begin{bmatrix} ad - bc & ad - bc \\ cd - dc & cd - dc \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix};$$

(iii) se  $a \neq 0$  ou  $b \neq 0$ , temos que

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} -b & -b \\ a & a \end{bmatrix} = \begin{bmatrix} -ab + ba & -ab + ba \\ -cb + da & -cb + da \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

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

### 4.1.1 domínios de integridade

**Definição 4.26.** 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 4.27.** Os anéis  $(\mathbb{Z}, +, \times)$  e  $(\mathbb{R}, +, \times)$  são domínios de integridade.

**Exemplo 4.28.** O anel das matrizes quadradas de ordem 2 não é um domínio de integridade.

Resulta imediatamente da definição que, se  $A$  é um domínio de integridade, então,  $A \neq \{0_A\}$ . As três proposições seguintes apresentam caracterizações diferentes de um domínio de integridade.

**Proposição 4.29.** Seja  $A$  um anel comutativo com identidade. Então, as seguintes afirmações são equivalentes:

- (i)  $A$  é domínio de integridade;
- (ii)  $A \setminus \{0_A\} \neq \emptyset$  e todo o elemento de  $A \setminus \{0_A\}$  é simplificável.

**Demonstração:** Suponhamos que  $A$  é um domínio de integridade. Então,  $A \setminus \{0_A\} \neq \emptyset$ . Sejam  $y \in A \setminus \{0_A\}$  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  $y \in A \setminus \{0_A\} \neq \emptyset$  é simplificável. Como  $A \setminus \{0_A\} \neq \emptyset$ , 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  $b \in A \setminus \{0_A\}$  tal que

$$bx_0 = 0_A \quad \text{ou} \quad x_0b = 0_A.$$

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 divisor de zero, pelo que  $A$  é um domínio de integridade. □

**Proposição 4.30.** *Seja  $A$  um anel comutativo com identidade. Então, as seguintes afirmações são equivalentes:*

- (i)  $A$  é domínio de integridade;
- (ii)  $A \setminus \{0_A\} \neq \emptyset$  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

$$a \neq 0_A, b \neq 0_A \Rightarrow ab \neq 0_A. \quad (*)$$

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

$$x_0y = 0_A \quad \text{ou} \quad yx_0 = 0_A.$$

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

**Proposição 4.31.** *Seja  $A$  um anel comutativo com identidade. Então, as seguintes afirmações são equivalentes:*

(i)  $A$  é domínio de integridade;

(ii)  $A \setminus \{0_A\} \neq \emptyset$  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  $a \neq 0_A$ ,

$$(\exists x_0, y_0 \in A) \quad ax_0 = b \quad \text{e} \quad y_0a = b.$$

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

$$ax_0 = b = ax_1 \quad \text{e} \quad y_0a = b = y_1a$$

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

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

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.  $\square$

#### 4.1.2 anéis de divisão e corpos

**Definição 4.32.** *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, como demonstra o seguinte exemplo.

**Exemplo 4.33.** *O domínio de integridade  $(\mathbb{Z}, +, \times)$  não é um anel de divisão, pois  $(\mathbb{Z} \setminus \{0\}, \times)$  não é grupo.*

**Exemplo 4.34.** *O domínio de integridade  $(\mathbb{R}, +, \times)$  é um corpo e, portanto, um anel de divisão.*

**Exemplo 4.35.** 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 de adição e de multiplicação definidas por

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

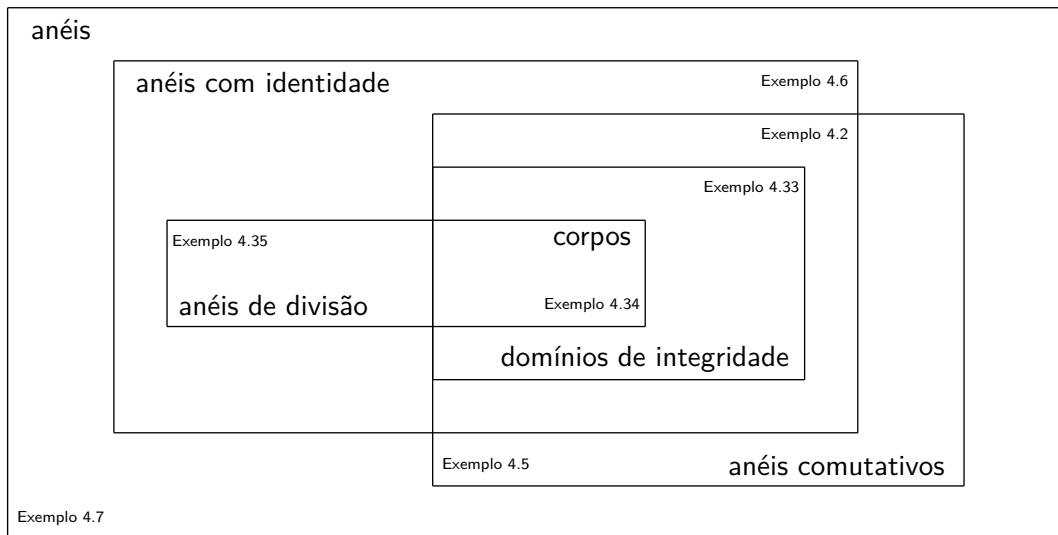
e

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

em que as somas dos elementos  $a, a', b, b', c, c', d, d'$  são efectuadas em  $\mathbb{R}$ .

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

De seguida, completamos o diagrama já apresentado, incluindo os conceitos de domínio de integridade, anel de divisão e corpo.



## 4.2 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 4.36.** São exemplos da situação (ii) o anel dos reais e o anel dos inteiros.

**Exemplo 4.37.** É exemplo da situação (i) o anel  $(\mathbb{Z}_4, +, \cdot)$ , onde

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

De facto, para  $m = 4$ , temos que

$$\begin{aligned} 4 \cdot \bar{0} &= \bar{0} + \bar{0} + \bar{0} + \bar{0} = \bar{0}, \\ 4 \cdot \bar{1} &= \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{0}, \\ 4 \cdot \bar{2} &= \bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{0}, \\ 4 \cdot \bar{3} &= \bar{3} + \bar{3} + \bar{3} + \bar{3} = \bar{0}. \end{aligned}$$

**Exemplo 4.38.** Seja  $A$  um anel tal que  $a^2 = a$ , para todo  $a \in A$ . (tal anel existe; basta pensar em  $A = \{0_A\}$ ). Então,  $A$  é um exemplo de anel que satisfaz a condição (i). De facto, para todo  $a \in A$ ,

$$2a = a + a = (a + a)^2 = (a + a)(a + a) = a^2 + a^2 + a^2 + a^2 = 4a^2 = 4a,$$

pelo que

$$4a - 2a = 0_A,$$

i.e.,

$$2a = 0_A.$$

Assim, para todo  $a \in A$ , existe  $m = 2 \in \mathbb{Z} \setminus \{0\}$  tal que  $ma = 0_A$ .

Vamos distinguir estas duas situações através da definição de *característica de um anel*, que de seguida apresentamos.

**Definição 4.39.** 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 tal que

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

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  $M$ .

Seja  $A$  um anel. Fazendo a ligação com o conceito de ordem de um elemento num grupo (neste caso, o grupo  $(A, +)$ ), levanta-se imediatamente a seguinte questão:

*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  $A$  é o m.m.c. entre as ordens de todos os elementos de  $A$ .

Se o anel tiver identidade, então a característica desse anel é determinada em função da ordem da identidade, como nos mostra o próximo resultado:

**Proposição 4.40.** *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)  $(\exists p \in \mathbb{N} \forall a \in A \quad pa = 0_A) \Rightarrow n \mid p$ .

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

- (a)  $n1_A = 0_A$ ;
- (b)  $(\exists p \in \mathbb{N} : p1_A = 0_A) \Rightarrow n \mid p$ .

A condição (a) resulta naturalmente da condição (i) pois, se  $na = 0_A$  para todo  $a \in A$ , então, como  $1_A \in A$ , temos que  $n1_A = 0_A$ . 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.

□

**Exemplo 4.41.** *Seja  $n \in \mathbb{N}$ . Como, em  $\mathbb{Z}_n$ ,  $p(\bar{1}) = n$ , concluímos que  $c(\mathbb{Z}_n) = n$ .*

**Exemplo 4.42.** *O anel dos números inteiros e o anel dos números reais são anéis de característica 0.*



### 4.3 subanéis

**Definição 4.43.** 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 4.44.** 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 4.45.** Quando consideradas as operações usuais de adição e multiplicação, o anel  $n\mathbb{Z}$  ( $n \in \mathbb{N} \setminus \{1\}$ ) é subanel mas não é subdomínio de integridade de  $\mathbb{Z}$ .

**Exemplo 4.46.** 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  $A$ .

De modo análogo àquele efetuado para os subgrupos, podemos estabelecer critérios de subanel, subdomínio de integridade, subanel de divisão e subcorpo. Por serem semelhantes, as demonstrações são deixadas como exercício.

**Proposição 4.47.** Sejam  $A$  um anel e  $A' \subseteq A$ . Então,  $A'$  é subanel de  $A$  se e só se:

- (i)  $A' \neq \emptyset$ ;
- (ii)  $x, y \in A' \Rightarrow x - y \in A'$ ;
- (iii)  $x, y \in A' \Rightarrow xy \in A'$

□

**Proposição 4.48.** Sejam  $A$  um domínio de integridade e  $A' \subseteq A$ . Então,  $A'$  é subdomínio de integridade de  $A$  se e só se:

- (i)  $1_A \in A'$ ;
- (ii)  $x, y \in A' \Rightarrow x - y \in A'$ ;
- (iii)  $x, y \in A' \Rightarrow xy \in A'$

□

**Proposição 4.49.** 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:

- (i)  $A' \neq \emptyset$ ;
- (ii)  $x, y \in A' \Rightarrow x - y \in A'$ ;
- (iii)  $x, y \in A' \setminus \{0_A\} \Rightarrow xy^{-1} \in A' \setminus \{0_A\}$ .

□

Acabamos esta secção com a seguinte observação: 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 de  $A$

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

é subgrupo de  $(A, +)$ . No entanto, dados  $a_1 + a_2, b_1 + b_2 \in A_1 + A_2$ ,

$$(a_1 + a_2)(b_1 + b_2) = a_1b_1 + a_2b_1 + a_1b_2 + a_2b_2$$

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

## 4.4 ideais e relações de congruência num anel

**Definição 4.50.** *Seja  $A$  um anel. Uma parte  $I$  de  $A$  diz-se um ideal direito (respetivamente, ideal esquerdo) de  $A$  se:*

$$(i) (I, +) < (A, +);$$

$$(ii) (\forall a \in A) (\forall x \in I) \quad xa \in I \text{ (respetivamente, } ax \in I)$$

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

**Exemplo 4.51.** *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 4.52.** *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

$$\bar{0} \cdot \bar{0} = \bar{0} \cdot \bar{1} = \bar{0} \cdot \bar{2} = \bar{0} \cdot \bar{3} = \bar{0} \in \{\bar{0}, \bar{2}\}$$

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

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

**Exemplo 4.53.** *Seja  $A$  um anel. Então,  $\{0_A\}$  é um ideal de  $A$  (ao qual se chama ideal trivial de  $A$ ).*

**Exemplo 4.54.** *Um anel  $A$  é um ideal de si próprio (ao qual se chama ideal impróprio de  $A$ ).*

Resulta imediatamente do critério de subanel (ver Proposição 4.47) e da definição de subanel que:

**Proposição 4.55.** *Todo o ideal de um anel  $A$  é um subanel de  $A$ .* □

Apresentamos de seguida algumas proposições envolvendo ideais.

**Proposição 4.56.** *A intersecção de uma família de ideais de um anel  $A$  é um ideal de  $A$ .*

**Demonstração:** Exercício. □

**Proposição 4.57.** *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,

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

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

**Proposição 4.58.** *Num anel de divisão existem apenas dois ideais: o trivial e o impróprio.*

**Demonstração:** Vimos já nos Exemplos 4.53 e 4.54 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. □

Novamente à semelhança do caso dos grupos, podemos ter ideais de um anel  $A$  que sejam gerados por um elemento de  $a$ .

**Definição 4.59.** *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 4.60.** 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 vice-versa, 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

$$\begin{aligned}(\bar{0}) &= \{\bar{0}\}, \\(\bar{2}) &= \{\bar{0}, \bar{2}\}, \\(\bar{1}) &= (\bar{3}) = \mathbb{Z}_4\end{aligned}$$

Os resultados que de seguida apresentamos, caracterizam os ideais principais esquerdos, ideais principais direitos e ideais principais de um anel, de um anel com identidade e de um anel comutativo com identidade.

**Proposição 4.61.** Sejam  $A$  um anel e  $a \in A$ . Então,

- (i)  $(a)_d$  é a intersecção de todos os ideais direitos de  $A$  que contêm  $a$ .
- (ii)  $(a)_e$  é a intersecção de todos os ideais esquerdos de  $A$  que contêm  $a$ .
- (iii)  $(a)$  é a intersecção de todos os ideais de  $A$  que contêm  $a$ .

**Demonstração:** Imediata, tendo em conta a Proposição 4.56. □

**Proposição 4.62.** 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)  $ax, ay \in aA \Rightarrow ax - ay = a(x - y) \in aA$ ;

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,

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

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

**Corolário 4.63.** *Sejam  $A$  um anel comutativo com identidade e  $a \in A$ . Então,  $(a) = Aa = aA$ .*  $\square$

Estudadas que estão algumas propriedades de ideais de um anel, vamos ver qual a sua relação com as relações de congruência nesse mesmo anel. Começamos por apresentar a definição de relação de congruência num anel.

**Definição 4.64.** *Seja  $A$  um anel. Uma relação de equivalência  $\rho$  definida em  $A$  diz-se uma relação de congruência se, para todos  $x, x', y, y' \in A$ ,*

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

**Exemplo 4.65.** *Considere-se em  $\mathbb{Z}$  a relação*

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

*Então, a relação  $\rho$  é de equivalência e é tal que*

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

*pelo que  $\rho$  é uma relação de equivalência.*

A proposição seguinte generaliza o exemplo anterior.

**Proposição 4.66.** *Sejam  $A$  um anel e  $I$  um ideal de  $A$ . Então, a relação definida em  $A$  por*

$$a \rho b \iff a - b \in I$$

*é uma relação de congruência.*

**Demonstração:** Começemos por provar que  $\rho$  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,  $\rho$  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  $\rho$  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  $\rho$  é transitiva.

Assim,  $\rho$  é uma relação de equivalência. Para concluir que  $\rho$  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  $A$ ,

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

□

**Proposição 4.67.** *Seja  $\rho$  uma relação de congruência definida num anel  $A$ . Então:*

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

**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,  $ax \rho 0_Ax$  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,

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

□

#### 4.4.1 anel quociente

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

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

Neste conjunto, definem-se duas operações binárias:

(i) uma adição de classes: para  $a, b \in A$ ,

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

(ii) uma multiplicação de classes: para  $a, b \in A$ ,

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

Sendo  $\rho$  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

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

e, portanto,

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

**Teorema 4.68.** *Sejam  $A$  um anel e  $\rho$  uma relação de congruência definida em  $A$ . Então, considerando a adição e a multiplicação acima definidas,  $(A/\rho, +, \cdot)$  é um anel.*

**Demonstração:** Exercício. □

**Observação.** Pelas Proposições 4.66 e 4.67, 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 falar no anel quociente

$$A/I = \{x + I : x \in A\}$$

e escreve-se

$$y \in x + I \iff y - x \in I.$$

Mais ainda, as operações são definidas por, para todos  $x, y \in A$ ,

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

e

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

Resulta de imediato que a comutatividade e a existência da identidade se mantêm quando passamos ao anel quociente. De facto, tem-se que:

**Proposição 4.69.** *Sejam  $A$  um anel e  $I$  um ideal de  $A$ .*

(i) *Se  $A$  é um anel comutativo, então  $A/I$  é um anel comutativo;*

(ii) *Se  $A$  é um anel com identidade  $1_A$ , então  $A/I$  é um anel com identidade  $1_A + I$ . □*

#### 4.4.2 ideais primos e ideais maximais

**Definição 4.70.** *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*

$$I \subsetneq K \subsetneq A.$$

**Exemplo 4.71.** *O ideal  $2\mathbb{Z}$  do anel  $\mathbb{Z}$  é maximal. O ideal  $4\mathbb{Z}$  não é maximal pois*

$$4\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}.$$

**Definição 4.72.** *Seja  $A$  um anel comutativo com identidade. Um ideal  $I$  de  $A$  diz-se primo se  $A \setminus I \neq \emptyset$  e  $A \setminus I$  é fechado para o produto.*



**Exemplo 4.73.** O ideal  $2\mathbb{Z}$  do anel  $\mathbb{Z}$  é primo. De facto,  $\mathbb{Z} \setminus 2\mathbb{Z} = 2\mathbb{Z} + 1$  é fechado para o produto, já que

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

para todos  $n, m \in \mathbb{Z}$ .

**Teorema 4.74.** Sejam  $A$  um anel comutativo com identidade e  $I$  um ideal de  $A$ . Então, são equivalentes as seguintes afirmações:

- (i)  $I$  é maximal;
- (ii)  $A/I$  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,

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

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  $I \subsetneq K \subseteq A$ . De  $I \subsetneq K$ , concluímos que

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

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

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

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

**Exemplo 4.75.** 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 4.76.** Sejam  $A$  um anel comutativo com identidade e  $I$  um ideal de  $A$ . Então, são equivalentes as seguintes afirmações:

- (i)  $I$  é ideal primo;
- (ii)  $A/I$  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,  $A \setminus I \neq \emptyset$ , pelo que  $A/I \neq \{I\}$ . Para provar que  $A/I$  é um domínio de integridade, falta então provar que

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

De facto,

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

[(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  $A \setminus I \neq \emptyset$ .

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

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

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

o que contradiz a hipótese de  $a, b \in A \setminus I$ . □

Como consequência dos dois últimos teoremas, temos que

**Corolário 4.77.** *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,

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

□

## 4.5 morfismos

**Definição 4.78.** *Sejam  $A$  e  $A'$  dois anéis. Uma aplicação  $\varphi : A \rightarrow A'$  diz-se um morfismo (ou homomorfismo) se satisfaz as seguintes condições:*

$$\begin{aligned}
 (i) \quad (\forall a, b \in A) \quad &\varphi(a + b) = \varphi(a) + \varphi(b); \\
 (ii) \quad (\forall a, b \in A) \quad &\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).
 \end{aligned}$$

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

**Exemplo 4.80.** Seja  $A$  um anel. Então, a aplicação identidade em  $A$  é um automorfismo, ao qual chamamos morfismo identidade.

**Proposição 4.81.** Sejam  $A$  e  $A'$  dois anéis e  $\varphi : A \rightarrow A'$  um morfismo. Então:

- (i)  $\varphi(0_A) = 0_{A'}$ ;
- (ii)  $(\forall a \in A) \quad \varphi(-a) = -\varphi(a)$ ;
- (iii)  $(\forall a \in A) (\forall k \in \mathbb{Z}) \quad \varphi(ka) = k\varphi(a)$ .

**Demonstração:** (i) De

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

concluimos, pela lei do corte, que

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

(ii) Seja  $a \in A$ . Como

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

temos que

$$-\varphi(a) = \varphi(-a);$$

(iii) Sejam  $a \in A$  e  $k = 0$ . Então,

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

Sejam  $a \in A$  e  $k \in \mathbb{Z}^+$ . Então, como

$$\varphi(1a) = \varphi(a) = 1\varphi(a)$$

e, sempre que  $\varphi(na) = n\varphi(a)$ , temos que

$$\varphi((n+1)a) = \varphi(na + a) = \varphi(na) + \varphi(a) = n\varphi(a) + \varphi(a) = (n+1)\varphi(a),$$

concluimos, por indução, que

$$\varphi(ka) = k\varphi(a).$$

Sejam  $a \in A$  e  $k \in \mathbb{Z}^-$ . Então,

$$\varphi(ka) = \varphi(-(-k)a) = -\varphi((-k)a) = -(-k)\varphi(a) = k\varphi(a).$$

□

De modo análogo ao efetuado já no caso dos grupos, as seguintes proposições caracterizam as imagens e as imagens inversas de subanéis e de ideais de anéis por morfismos.

**Proposição 4.82.** *Sejam  $\varphi : A \rightarrow A'$  um morfismo de anéis e  $B$  um subanel de  $A$ . Então,  $\varphi(B)$  é um subanel de  $A'$ .*

**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 4.83.** *Sejam  $\varphi : A \rightarrow A'$  um epimorfismo de anéis e  $I$  um ideal de  $A$ . Então,  $\varphi(I)$  é um ideal de  $A'$ .*

**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  $A'$ .

□

**Proposição 4.84.** *Sejam  $\varphi : A \rightarrow A'$  um morfismo de anéis e  $B'$  um subanel de  $A'$ . Então,*

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

*é um subanel de  $A$ .*

**Demonstração:** Seja  $B'$  um subanel de  $A'$ . Então,

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

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

$$\varphi(x - y) = \varphi(x) - \varphi(y) \in B',$$

pelo que  $x - y \in \varphi^{-1}(B')$ ;

(iii) dados  $x, y \in \varphi^{-1}(B')$ , temos que  $\varphi(x), \varphi(y) \in B'$  e, portanto,

$$\varphi(xy) = \varphi(x)\varphi(y) \in B',$$

pelo que  $xy \in \varphi^{-1}(B')$ .

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

**Proposição 4.85.** *Sejam  $\varphi : A \rightarrow A'$  um morfismo de anéis e  $I'$  um ideal de  $A'$ . Então,*

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

*é um ideal de  $A$ .*

**Demonstração:** Seja  $I'$  um ideal de  $A'$ . Então, pela proposição anterior,  $\varphi^{-1}(I')$  é um subanel de  $A$ . Por outro lado, seja  $a \in A$  e  $x \in \varphi^{-1}(I')$ . Então,  $\varphi(x) \in I'$  e, portanto,

$$\varphi(ax) = \varphi(a)\varphi(x) \in I',$$

pelo que  $ax \in \varphi^{-1}(I')$ . De modo análogo, temos  $xa \in \varphi^{-1}(I')$  e, portanto,  $\varphi^{-1}(I')$  é um ideal de  $A$ . □

Dado um qualquer morfismo entre dois anéis, destacam-se os seguintes subconjuntos do domínio e do conjunto de chegada desse mesmo morfismo.

**Definição 4.86.** *Seja  $\varphi : A \rightarrow A'$  um morfismo de anéis.*

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

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

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

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

**Proposição 4.87.** *Seja  $\varphi : A \rightarrow A'$  um morfismo de anéis. Então,*

- (i)  $\text{Nuc}\varphi$  é um ideal de  $A$ ;
- (ii)  $\text{Im}\varphi$  é um subanel de  $A'$ .

**Demonstração:** (i) Trivial, tendo em conta que  $\text{Nuc}\varphi = \varphi^{-1}\{0_{A'}\}$  e  $\{0_{A'}\}$  é um ideal de  $A'$  e aplicando a Proposição 4.85.

(ii) Trivial, tendo em conta que  $A$  é um subanel de  $A$  e aplicando a Proposição 4.82.  $\square$

#### 4.5.1 teorema fundamental do homomorfismo

**Proposição 4.88.** *Sejam  $A$  um anel e  $I$  um seu ideal. Então, a aplicação  $\pi : A \rightarrow A/I$  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  $\pi$  é tal que

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

e

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

pelo que  $\pi$  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  $\pi$  é uma aplicação sobrejetiva.  $\square$

**Teorema 4.89. (fundamental do homomorfismo)** *Seja  $\varphi : A \rightarrow A'$  um morfismo de anéis. Então, existe um ideal  $I$  de  $A$  tal que*

$$A/I \cong \varphi(A).$$

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

- (i)  $\theta$  é uma aplicação injetiva, pois

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

e

$$\begin{aligned}
 x + \text{Nuc}\varphi = y + \text{Nuc}\varphi &\iff x - y \in \text{Nuc}\varphi \\
 &\iff \varphi(x - y) = 0_{A'} \\
 &\iff \varphi(x) - \varphi(y) = 0_{A'} \\
 &\iff \varphi(x) = \varphi(y).
 \end{aligned}$$

(ii)  $\theta$  é um morfismo, pois

$$\begin{aligned}
 \theta((x + \text{Nuc}\varphi) + (y + \text{Nuc}\varphi)) &= \theta((x + y) + (\text{Nuc}\varphi)) \\
 &= \varphi(x + y) \\
 &= \varphi(x) + \varphi(y) \\
 &= \theta(x + \text{Nuc}\varphi) + \theta(y + \text{Nuc}\varphi)
 \end{aligned}$$

e

$$\begin{aligned}
 \theta((x + \text{Nuc}\varphi) \cdot (y + \text{Nuc}\varphi)) &= \theta((x \cdot y) + (\text{Nuc}\varphi)) \\
 &= \varphi(x \cdot y) \\
 &= \varphi(x) \cdot \varphi(y) \\
 &= \theta(x + \text{Nuc}\varphi) \cdot \theta(y + \text{Nuc}\varphi).
 \end{aligned}$$

(iii)  $\theta(A/\text{Nuc}\varphi) = \text{Im}\varphi$ , porque

$$\begin{aligned}
 y \in \theta(A/\text{Nuc}\varphi) &\iff (\exists x \in A) \quad y = \theta(x + \text{Nuc}\varphi) \\
 &\iff (\exists x \in A) \quad y = \varphi(x) \\
 &\iff y \in \text{Im}\varphi.
 \end{aligned}$$

Logo, concluímos que

$$A/\text{Nuc}\varphi \cong \text{Im}\varphi.$$

□

#### 4.5.2 teoremas do isomorfismo

Mais uma vez fazendo o paralelismo com a Teoria de Grupos, apresentamos aqui dois teoremas envolvendo isomorfismos entre anéis, teoremas esses que são conhecidos como teoremas de isomorfismo.



**Teorema 4.90. (1º Teorema do Isomorfismo)** Seja  $\varphi : A \rightarrow A'$  um epimorfismo de anéis. Se  $I$  é um ideal de  $A$  tal que  $\text{Nuc}\varphi \subseteq I$ , então,

$$A/I \cong A'/\varphi(I).$$

**Demonstração:** Começamos por observar que, sendo  $\varphi$  um epimorfismo, então,  $\varphi(I)$  é um ideal de  $A'$ , pelo que faz sentido falar no anel quociente  $A'/\varphi(I)$ .

Seja  $\theta$  a relação que, dado  $x \in A$ , faz corresponder a classe  $x + I$  de  $A/I$  na classe  $\varphi(x) + \varphi(I)$  do anel  $A'/\varphi(I)$ . Então,

(i)  $\theta$  é uma aplicação, pois

$$(\forall a + I \in A/I) (\exists y = \varphi(a) \in A') \quad \theta(a + I) = \varphi(a) + \varphi(I) \in A'/\varphi(I)$$

e

$$\begin{aligned} a + I = b + I &\iff a - b \in I \\ &\Rightarrow \varphi(a - b) \in \varphi(I) \\ &\iff \varphi(a) - \varphi(b) \in \varphi(I) \\ &\iff \varphi(a) + \varphi(I) = \varphi(b) + \varphi(I) \\ &\iff \theta(a + I) = \theta(b + I). \end{aligned}$$

(ii)  $\theta$  é injetiva, pois

$$\begin{aligned} \theta(a + I) = \theta(b + I) &\iff \varphi(a) + \varphi(I) = \varphi(b) + \varphi(I) \\ &\iff \varphi(a - b) \in \varphi(I) \\ &\Rightarrow a - b \in \varphi^{-1}(\varphi(I)) = I \quad (\text{porque } \text{Nuc}\varphi \subseteq I) \\ &\iff a + I = b + I. \end{aligned}$$

e  $\theta$  é sobrejetiva porque  $\varphi$  é sobrejetiva.

(iii)  $\theta$  é um morfismo, porque

$$\begin{aligned} \theta((x + I) + (y + I)) &= \theta((x + y) + I) \\ &= \varphi(x + y) + \varphi(I) \\ &= (\varphi(x) + \varphi(y)) + \varphi(I) \\ &= (\varphi(x) + \varphi(I)) + (\varphi(y) + \varphi(I)) \\ &= \theta(x + I) + \theta(y + I) \end{aligned}$$

e

$$\begin{aligned}
 \theta((x+I) \cdot (y+I)) &= \theta(xy+I) \\
 &= \varphi(xy) + \varphi(I) \\
 &= \varphi(x)\varphi(y) + \varphi(I) \\
 &= (\varphi(x) + \varphi(I)) \cdot (\varphi(y) + \varphi(I)) \\
 &= \theta(x+I) \cdot \theta(y+I).
 \end{aligned}$$

Logo,  $\theta$  é um isomorfismo, pelo que

$$A/I \cong A'/\varphi(I).$$

□

**Teorema 4.91. (2º Teorema do Isomorfismo)** *Sejam  $A$  um anel e  $A_1$  e  $A_2$  subanéis de  $A$ . Se  $A_2$  é um ideal de  $A$ , então,*

$$(A_1 + A_2)/A_2 \cong A_1/(A_1 \cap A_2).$$

**Demonstração:** Começamos por observar que:

(i)  $A_1 + A_2$  é um subanel de  $A$  que contém  $A_2$  (assim sendo,  $A_2$  é ideal de  $A_1 + A_2$ ). De facto,

$$0_A = 0_A + 0_A \in A_1 + A_2,$$

pelo que  $A_1 + A_2 \neq \emptyset$ . Mais ainda, se  $x = a_1 + a_2, y = b_1 + b_2 \in A_1 + A_2$ , temos que

$$x + y = (a_1 + b_1) + (a_2 + b_2) \in A_1 + A_2$$

e, porque  $A_2$  é ideal de  $A$ ,

$$\begin{aligned}
 xy &= a_1b_1 + a_1b_2 + a_2b_1 + b_1b_2 \\
 &= a_1b_1 + (a_1b_2 + a_2b_1 + b_1b_2) \in A_1 + A_2.
 \end{aligned}$$

Finalmente, como

$$a_2 \in A_2 \Rightarrow a_2 = 0_A + a_2 \in A_1 + A_2,$$

temos que  $A_1 + A_2$  é um subanel de  $A$  tal que  $A_2 \subseteq A_1 + A_2$ .

(ii)  $A_1 \cap A_2$  é um ideal de  $A_1$ . De facto,  $A_1 \cap A_2 \subseteq A_1$  e, dados  $x \in A_1$  e  $i \in A_1 \cap A_2$ , temos que  $xi \in A_1$ , porque  $A_1$  é subanel de  $A$ , e  $xi \in A_2$ , porque  $A_2$  é ideal de  $A$ .

Faz, então, sentido falar nos dois anéis quociente. Consideremos a restrição do epimorfismo

$$\begin{aligned}\pi : A_1 + A_2 &\longrightarrow (A_1 + A_2) / A_2 \\ x &\longmapsto x + A_2,\end{aligned}$$

ao subconjunto  $A_1$  de  $A_1 + A_2$  ( $a \in A_1 \Rightarrow a = a + 0_A \in A_1 + A_2$ ). Temos, portanto, o morfismo

$$\begin{aligned}\pi|_{A_1} : A_1 &\longrightarrow (A_1 + A_2) / A_2 \\ a_1 &\longmapsto a_1 + A_2.\end{aligned}$$

Este morfismo  $\pi|_{A_1}$  é, na verdade, um epimorfismo tal que  $\text{Nuc}\pi|_{A_1} = A_1 \cap A_2$ . De facto, para todo  $x = a_1 + a_2 \in A_1 + A_2$ ,

$$x + A_2 = a_1 + A_2,$$

pelo que, para todo  $x + A_2 \in (A_1 + A_2) / A_2$ , existe  $a_1 \in A_1$  tal que

$$x + A_2 = \pi|_{A_1}(a_1).$$

Por outro lado,

$$\begin{aligned}a \in \text{Nuc}\pi|_{A_1} &\iff a \in A_1 \text{ e } \pi|_{A_1}(a) = A_2 \\ &\iff a \in A_1 \text{ e } a + A_2 = A_2 \\ &\iff a \in A_1 \text{ e } a \in A_2 \\ &\iff a \in A_1 \cap A_2.\end{aligned}$$

Logo, pelo teorema fundamental do homomorfismo,

$$A_1 / (A_1 \cap A_2) = A_1 / \text{Nuc}\pi|_{A_1} \cong \pi|_{A_1}(A_1) = (A_1 + A_2) / A_2.$$

□



## 5 divisibilidade em domínios de integridade

### 5.1 definições básicas

Ao longo deste capítulo,  $D$  é um domínio de integridade, i.e., um anel comutativo com identidade no qual  $0_D$  é o único divisor de zero. Recordamos também que  $\mathcal{U}_D$  representa o conjunto das unidades de  $D$ , i.e., o conjunto dos elementos  $u \in D$  para os quais existe  $u^{-1} \in D$ . Como  $1_D \in D$ , temos que  $\mathcal{U}_D \neq \emptyset$ .

**Definição 5.1.** Dados  $x, y \in D$ , diz-se que  $x$  divide  $y$  (ou que  $x$  é fator de  $y$  ou que  $y$  é divisível por  $x$ ) se

$$\exists t \in D : y = tx.$$

Neste caso, diz-se também que  $tx$  é uma fatorização (ou decomposição em fatores) de  $y$ .

**Exemplo 5.2.** No domínio de integridade  $\mathbb{Z}$ , temos que  $-2 \mid 4$ , mas  $2 \nmid 3$ .

Como consequência da definição, provam-se algumas propriedades básicas que agrupamos na seguinte proposição:

**Proposição 5.3.** Sejam  $x, y \in D$ . Então,

- (i)  $x \mid 0_D$ ;
- (ii)  $1_D \mid x$ ;
- (iii)  $\forall u \in \mathcal{U}_D \quad u \mid x$ ;
- (iv)  $x \mid y$  e  $y \mid x$  se e só se  $y = ux$  para algum  $u \in \mathcal{U}_D$  (e, consequentemente,  $x = u^{-1}y$ ).

**Demonstração:** (i) Seja  $x \in D$ . Então,  $0_D = 0_D x$ , pelo que podemos afirmar que  $x \mid 0_D$ .

(ii) Seja  $x \in D$ . Como  $x = 1_D x$ , temos que  $1_D \mid x$ .

(iii) Sejam  $x \in D$  e  $u$  uma unidade de  $D$ . Como

$$x = 1_D x = u(u^{-1}x),$$

concluimos que  $u \mid x$ .

(iv) Sejam  $x, y \in D$  tais que  $y = ux$  e  $x = u^{-1}y$  para algum  $u \in \mathcal{U}_D$ . Então, obviamente, temos que  $x \mid y$  e  $y \mid x$ .

Reciprocamente, suponhamos que  $x \mid y$  e  $y \mid x$ . Então, existem  $t, s \in D$  tais que

$$y = tx \text{ e } x = sy. \quad (*)$$

Temos que considerar 2 casos:

Caso 1:  $x = 0_D$  ou  $y = 0_D$ . Neste caso, concluimos que  $x = y = 0_D$  e, como  $0_D = 1_D 0_D$ , temos que  $x = uy$  para  $u = 1_D \in \mathcal{U}_D$ ;

Caso 2:  $x \neq 0_D$  e  $y \neq 0_D$ . Neste caso, por  $(*)$ , temos que

$$1_D x = x = sy = stx.$$

Aplicando a lei do corte (pois  $x \neq 0_D$ ), temos que

$$st = 1_D.$$

Assim,  $s = t^{-1}$  e  $t = s^{-1}$ , pelo que  $s, t \in \mathcal{U}_D$ . □

**Exemplo 5.4.** No anel dos inteiros relativos, se  $x, y \in \mathbb{Z}$  são tais que  $x \mid y$  e  $y \mid x$ , então,  $x = \pm y$ . De facto, sabemos que  $\mathcal{U}_{\mathbb{Z}} = \{-1, 1\}$ .

Na sequência da propriedade (iv) da última proposição, surge a seguinte definição:

**Definição 5.5.** Dois elementos  $x$  e  $y$  de um domínio de integridade  $D$  dizem-se associados se  $x \mid y$  e  $y \mid x$ .

**Proposição 5.6.** Sejam  $x, y \in D$ . Então, são equivalentes as seguintes afirmações:

- (i)  $x$  e  $y$  são associados;
- (ii)  $x \in y\mathcal{U}_D$ ;
- (iii)  $y \in x\mathcal{U}_D$ .

**Demonstração:** Trivial, tendo em conta a Proposição 5.3(iv).  $\square$

**Definição 5.7.** Um elemento  $p \in D$  diz-se irredutível em  $D$  se

- (i)  $p \neq 0_D$  e  $p \notin \mathcal{U}_D$ ;
- (ii)  $p = ab \Rightarrow a \in \mathcal{U}_D$  ou  $b \in \mathcal{U}_D$ .

O elemento  $p$  diz-se redutível em  $D$  se não for irredutível em  $D$ .

**Exemplo 5.8.** Em  $\mathbb{Z}$ , os elementos irredutíveis são os números primos e os seus simétricos.

**Definição 5.9.** Um elemento  $p \in D$  diz-se primo se

- (i)  $p \neq 0_D$  e  $p \notin \mathcal{U}_D$ ;
- (ii)  $p \mid ab \Rightarrow p \mid a$  ou  $p \mid b$ .

**Proposição 5.10.** Seja  $p$  um elemento não nulo de  $D$ . Então,

- (i)  $p$  é primo se e só se  $(p)$  é ideal primo de  $D$ ;
- (ii)  $p$  é irredutível se e só se  $(p)$  é ideal maximal na classe dos ideais principais de  $D$ .

**Demonstração:** (i) Como  $D$  é um anel comutativo com identidade, temos, pelo Corolário 4.63, que  $(p) = pD$ . Suponhamos, então, que  $p$  é primo. Como  $p \notin \mathcal{U}_D$ ,  $1_D \notin pD$ , pelo que  $D \setminus (p) \neq \emptyset$ . Sejam  $a, b \in D$  tais que  $ab \in pD$ . Então,  $p \mid ab$ . Como  $p$  é primo, temos que  $p \mid a$  ou  $p \mid b$  e, portanto,  $a \in pD$  ou  $b \in pD$ . Estamos em condições de concluir que  $pD$  é ideal primo de  $D$ .

Reciprocamente, suponhamos que  $(p) = pD$  é um ideal primo. Então,  $pD \neq D$  pelo que, pela Proposição 2.17,  $1_D \notin pD$  e, portanto,  $p$  não é unidade de  $D$ . Sejam  $a, b \in D$  tais que  $p \mid ab$ . Então,  $ab \in (p)$ . Como  $(p)$  é ideal primo, concluímos que  $a \in (p)$  ou  $b \in (p)$ . Assim, temos que  $p \mid a$  ou  $p \mid b$ . Logo,  $p$  é primo.

(ii) Exercício.  $\square$

**Proposição 5.11.** Todo o elemento primo de  $D$  é um elemento irredutível.

**Demonstração:** Sejam  $p$  um elemento primo e  $a, b \in D$  tais que  $p = ab$ . Então,  $p \notin \mathcal{U}_D \cup \{0_D\}$  é tal que  $p \mid ab$  e, portanto,  $p \mid a$  ou  $p \mid b$ . Se  $p \mid a$ , temos que  $a = px$ , para algum  $x \in D$ . Logo,

$$p = ab = pxb.$$

Assim, pela lei de corte,

$$1_D = xb,$$

o que nos leva a concluir que  $b \in \mathcal{U}_D$ . Analogamente, ao supor que  $p \mid b$ , concluíamos que  $a \in \mathcal{U}_D$ . Logo,  $p$  é irredutível  $\square$

O recíproco deste corolário não é verdadeiro, como o demonstra o seguinte exemplo.

**Exemplo 5.12.** Considere-se o conjunto  $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$ , algebrizado com duas operações definidas por, para todos  $a, b, c, d \in \mathbb{Z}$ :

$$(a + b\sqrt{-3}) + (c + d\sqrt{-3}) = (a + c) + (b + d)\sqrt{-3},$$

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = (ac - 3bd) + (ad + bc)\sqrt{-3}.$$

Então,  $\mathbb{Z}[\sqrt{-3}]$  é um domínio de integridade. Para provarmos este facto, basta observarmos que  $\mathbb{Z}[\sqrt{-3}]$  é um subdomínio de integridade de  $\mathbb{C}$ , munido das operações usuais de adição e multiplicação de números complexos. De facto, tendo em conta que

$$a + b\sqrt{-3} = a + 3bi,$$

verificamos que a adição e multiplicação definidas no enunciado não são mais do que restrições das operações usuais de números complexos ao subconjunto  $\mathbb{Z}[\sqrt{-3}]$  de  $\mathbb{C}$ . Mais ainda, temos que  $1 = 1 + 0\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$  e a soma e o produto de dois elementos de  $\mathbb{Z}[\sqrt{-3}]$  são ainda elementos de  $\mathbb{Z}[\sqrt{-3}]$ . Logo, pela Proposição 2.13,  $\mathbb{Z}[\sqrt{-3}]$  é um subdomínio de integridade de  $\mathbb{C}$ .

Neste domínio, o elemento  $x = 1 + \sqrt{-3}$  é irredutível, mas não é primo.

Determinemos primeiro o conjunto das unidades de  $\mathbb{Z}[\sqrt{-3}]$ : Seja  $a + b\sqrt{-3}$  uma unidade de  $\mathbb{Z}[\sqrt{-3}]$ . Então, existe  $c + d\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$  tal que

$$(A) \quad (a + b\sqrt{-3})(c + d\sqrt{-3}) = 1.$$

Sendo dois números complexos iguais, também são iguais os quadrados dos seus módulos. Assim, temos que

$$(a^2 + 3b^2)(c^2 + 3d^2) = 1.$$

Como  $a, b, c, d \in \mathbb{Z}$ , concluimos que só podemos ter  $a = \pm 1, c = \pm 1$  e  $b = d = 0$ . Substituindo em (A), concluimos que só podemos ter  $a = c = \pm 1$  e  $b = d = 0$ . Assim, as únicas unidades de  $\mathbb{Z}[\sqrt{-3}]$  são 1 e -1. Logo  $\mathcal{U}_{\mathbb{Z}[\sqrt{-3}]} = \{-1, 1\}$ .



Para provarmos que  $1 + \sqrt{-3}$  é irredutível temos de escrever esse elemento como produto de dois e chegar à conclusão que um destes dois é uma unidade. Sejam  $a + b\sqrt{-3}, c + d\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$  tais que

$$1 + \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3}).$$

Sendo estes dois complexos iguais, então, também o são os quadrados dos seus módulos. Logo, temos que

$$4 = (a^2 + 3b^2)(c^2 + 3d^2).$$

Tendo em conta que os fatores são não negativos, as únicas fatorizações possíveis são, a menos da ordem dos fatores,  $2 \times 2$  e  $1 \times 4$ . Como a primeira é impossível (pois  $a^2 + 3b^2 \neq 2$ , para quaisquer inteiros  $a$  e  $b$ ), concluímos que  $a^2 + 3b^2 = 1$  ou  $c^2 + 3d^2 = 1$ . Aplicando agora o raciocínio usado anteriormente, concluímos que  $a + b\sqrt{-3}$  é uma unidade ou  $c + d\sqrt{-3}$  é uma unidade. Logo  $1 + \sqrt{-3}$  é irredutível.

Finalmente, temos que  $1 + \sqrt{-3}$  não é primo pois divide  $4 (= 2 \times 2)$  (pois  $4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ ) e não divide 2. De facto, se  $1 + \sqrt{-3} \mid 2$ , existiria  $a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$  tal que

$$2 = (1 + \sqrt{-3})(a + b\sqrt{-3}) = (a - 3b) + (b + a)\sqrt{-3},$$

ou seja, existiria  $b \in \mathbb{Z}$  tal que  $2 = -4b$ .

**Definição 5.13.** Dados  $a, b \in D$ , um elemento  $d$  de  $D$  diz-se um máximo divisor comum de  $a$  e  $b$  (abreviadamente, m.d.c.  $(a, b)$ ) se:

- (i)  $d \mid a$  e  $d \mid b$ ;
- (ii)  $(\forall c \in D) \quad c \mid a \text{ e } c \mid b \Rightarrow c \mid d$ .

**Exemplo 5.14.** No domínio de integridade dos inteiros relativos, 2 e  $-2$  são m.d.c.  $(4, 6)$ .

Observe-se que, embora no anel dos inteiros relativos qualquer par de elementos admite pelo menos um máximo divisor comum, existem anéis onde não existem máximos divisores comuns de pares de elementos. Pelo facto de estarmos a falar em anéis com identidade, temos a certeza que existem sempre divisores comuns a quaisquer dois elementos. No entanto, dois elementos podem ter dois divisores em comum que não sejam comparáveis em termos de divisibilidade. O seguinte exemplo ilustra esta situação.

**Exemplo 5.15.** Considere-se, no domínio de integridade definido no Exemplo 5.12, os elementos  $-2 + 2\sqrt{-3}$  e 8. Tirando as unidades, os divisores comuns dos dois elementos são

$$2, -2, 1 + \sqrt{-3}, -1 - \sqrt{-3}.$$

No entanto, dentro desta lista não temos nenhum elemento que seja maior do que os outros, no sentido em não há nenhum elemento que seja divisível por todos os outros (basta verificarmos que  $2 \nmid 1 + \sqrt{-3}$  e  $1 + \sqrt{-3} \nmid 2$ , todos os outros casos são iguais a este a menos de uma unidade). Concluimos, assim, que não existe máximo divisor comum destes dois elementos em  $\mathbb{Z}[\sqrt{-3}]$ .

**Proposição 5.16.** Sejam  $d$  um m.d.c.( $a, b$ ) e  $d' \in D$ . Então,

$$d' \text{ é m.d.c.}(a, b) \iff d' \in d\mathcal{U}_D.$$

**Demonstração:** Suponhamos que  $d$  e  $d'$  são m.d.c.( $a, b$ ). Então,

$$(i_d) \quad d \mid a \text{ e } d \mid b;$$

$$(ii_d) \quad c \mid a \text{ e } c \mid b \Rightarrow c \mid d;$$

$$(i_{d'}) \quad d' \mid a \text{ e } d' \mid b;$$

$$(ii_{d'}) \quad c \mid a \text{ e } c \mid b \Rightarrow c \mid d'.$$

Logo, de  $(i_d)$  e de  $(ii_{d'})$ , concluimos que  $d \mid d'$  e, de  $(i_{d'})$  e de  $(ii_d)$ , concluimos que  $d' \mid d$ .

Assim, pela Proposição 5.3(iv), obtemos o resultado.

Reciprocamente, suponhamos que  $d' \in d\mathcal{U}_D$  e que  $d$  é m.d.c.( $a, b$ ). Então:

$$(i_d) \quad d \mid a \text{ e } d \mid b;$$

$$(ii_d) \quad c \mid a \text{ e } c \mid b \Rightarrow c \mid d;$$

$$(iii) \quad \exists u_0 \in \mathcal{U}_D : \quad d' = du_0.$$

Assim,

(a) De  $(i_d)$ , temos que existem  $s, t \in D$  tais que

$$a = ds \quad e \quad b = dt.$$

Então,

$$a = (du_0)(u_0^{-1}s) \quad e \quad b = (du_0)(u_0^{-1}t).$$

Logo, por (iii), temos que  $d' \mid a$  e  $d' \mid b$ .

(b) Seja  $c \in D$  tal que  $c \mid a$  e  $c \mid b$ . Então, por  $(ii_d)$ , temos que  $c \mid d$ , pelo que existe  $r \in D$  tal que  $d = cr$ . Logo,

$$d' = du_0 = cru_0$$

e, portanto,  $c \mid d'$ .

Estamos em condições de concluir que  $d'$  é m.d.c.( $a, b$ ).  $\square$

A última proposição apresentada permite-nos afirmar que, se existe m.d.c.( $a, b$ ), ele é univocamente determinado a menos de uma unidade. Assim, representando por  $[a, b]$  o conjunto dos m.d.c.( $a, b$ ) em  $D$ , se  $d$  é m.d.c.( $a, b$ ), temos que

$$[a, b] = d\mathcal{U}_D.$$

Mais ainda, como a relação de associado é uma relação de equivalência, o conjunto  $[a, b]$  pode ser visto como uma classe de equivalência. Temos assim, o seguinte resultado.

**Corolário 5.17.** *Sejam  $a, b, c, e, d, d' \in D$  tais que  $d \in [a, b]$ ,  $d' \in [c, e]$  e  $d$  e  $d'$  são associados. Então,  $[a, b] = [c, e]$ .*  $\square$

**Proposição 5.18.** *Sejam  $a, b, p \in D$ . Então,*

(i) *se  $a \mid b$ ,  $a \in [a, b]$  e, portanto,  $[a, b] = a\mathcal{U}_D$ ;*

(ii) *se  $p$  é irredutível, existe m.d.c.( $a, p$ ) e*

$$[a, p] = \mathcal{U}_D \quad \text{ou} \quad [a, p] = p\mathcal{U}_D.$$

**Demonstração:** Exercício.  $\square$

**Proposição 5.19.** *Em  $D$ , sempre que as expressões fizerem sentido, são válidas as seguintes igualdades:*

(i)  $[ac, bc] = [a, b]c$ ;

(ii)  $[[a, b], c] = [a, [b, c]]$ .

**Demonstração:** (i) Seja  $d' \in [ac, bc]$ . Queremos provar que  $d' = d_1c$  para algum  $d_1 \in [a, b]$ . Começamos por observar que, por um lado,

$$d \in [a, b] \Rightarrow d \mid a \text{ e } d \mid b \Rightarrow dc \mid ac \text{ e } dc \mid bc \Rightarrow dc \mid d' \Rightarrow \exists t \in D : d' = tdc = dtc.$$

Por outro lado,

$$d' \mid ac \Rightarrow \exists q \in D : ac = d'q \Rightarrow \exists q \in D : ac = dtcq \Rightarrow \exists q \in D : a = dtq$$

e, de modo análogo,

$$d' \mid b \Rightarrow \exists s \in D : b = dts.$$

Logo,

$$dt \mid a \text{ e } dt \mid b,$$

pelo que  $dt \mid d$  (pois  $d \in [a, b]$ ). Assim,

$$\exists r \in D : d = dtr$$

e, portanto,

$$1_D = tr.$$

Concluimos então que  $t \in \mathcal{U}_D$  e, assim,  $dt \in [a, b]$ . Logo, existe  $d_1 = dt \in [a, b]$  tal que  $d' = d_1c$ .

Reciprocamente, seja  $d \in [a, b]$ . Queremos provar que  $dc \in [ac, bc]$ . Seja  $d' \in [ac, bc]$ . Como  $dc \mid ac$  e  $dc \mid bc$ , temos que  $dc \mid d'$ . Assim, existe  $t \in D$  tal que  $d' = dct$ . Como já provamos que existe  $d_1 \in [a, b]$  tal que  $d' = d_1c$ , concluimos que  $d_1 = dt$  e, portanto,  $t \in \mathcal{U}_D$ . Logo,  $dc \in d' \mathcal{U}_D = [ac, bc]$ .

(ii) Sejam

$$d \in [a, b], \quad d' \in [b, c],$$

$$d_1 \in [d, c], \quad d'_1 \in [a, d'].$$

Então,

(a) de  $d \mid a$ ,  $d \mid b$  e  $d_1 \mid d$ , concluimos que  $d_1 \mid a$  e  $d_1 \mid b$ ;

(b) de  $d_1 \mid b$  e  $d_1 \mid c$ , concluimos que  $d_1 \mid d'$ ;

(c) de  $d_1 \mid d'$  e  $d_1 \mid a$ , concluimos que  $d_1 \mid d'_1$ .

De igual modo,

(d) de  $d' \mid b$ ,  $d' \mid c$  e  $d'_1 \mid d'$ , concluimos que  $d'_1 \mid b$  e  $d'_1 \mid c$ ;

(e) de  $d'_1 \mid a$  e  $d'_1 \mid b$ , concluimos que  $d'_1 \mid d$ ;

(f) de  $d'_1 \mid d$  e  $d'_1 \mid c$ , concluimos que  $d'_1 \mid d_1$ .

De (c) e (f), temos que  $d_1$  e  $d'_1$  são associados e, portanto,  $[d, c] = [a, d']$ , i.e.,

$$[[a, b], c] = [a, [b, c]].$$

□

**Proposição 5.20.** *Sejam  $a, b, c \in D$ . Se existe m.d.c. de qualquer par de elementos em  $D$ , então,*

$$[a, b] = \mathcal{U}_D, \quad [a, c] = \mathcal{U}_D \Rightarrow [a, bc] = \mathcal{U}_D.$$

**Demonstração:** Seja  $d \in [a, bc]$ . Então,  $d \mid a$  e  $d \mid bc$ , pelo que  $d \mid ac$  e  $d \mid bc$ . Logo,  $d \mid d_1$  para algum  $d_1 \in [ac, bc]$ . Então, pela Proposição anterior, existe  $u \in [a, b] = \mathcal{U}_D$  tal que  $d_1 = uc$ . Logo,  $d \mid uc$ . Como  $uc \mid c$ , temos que  $d \mid c$ . Assim, de  $d \mid a$  e  $d \mid c$ , concluímos que  $d \mid u'$ , para qualquer  $u' \in \mathcal{U}_D = [a, c]$ . Logo,  $d \in \mathcal{U}_D$ . Logo,  $[a, bc] \subseteq \mathcal{U}_D$ . Como  $[a, bc]$  é uma classe de equivalência, temos que  $[a, bc] = \mathcal{U}_D$ .  $\square$

Vimos já que, num domínio de integridade, nem todo o elemento irredutível é primo. No entanto, se existir m.d.c. de dois quaisquer elementos do domínio, prova-se que todo o elemento irredutível é primo.

**Proposição 5.21.** *Se  $[a, b] \neq \emptyset$ , para todos  $a, b \in D$ , então, qualquer elemento irredutível é primo.*

**Demonstração:** Sejam  $x \in D$  um elemento irredutível e  $a, b \in D$  tais que  $x \mid ab$ . Se  $x \nmid a$  e  $x \nmid b$ , teríamos  $[x, a] = [x, b] = \mathcal{U}_D$  e, portanto, pela proposição 5.20,

$$[x, ab] = \mathcal{U}.$$

Mas, pela Proposição 5.18, como  $x \mid ab$ ,

$$[x, ab] = x\mathcal{U}_D.$$

No entanto,  $x\mathcal{U} \neq \mathcal{U}_D$ , já que  $x \notin \mathcal{U}_D$ . A contradição a que chegamos resultado do facto de supormos que  $x \nmid a$  e  $x \nmid b$ . Logo,  $x \mid a$  ou  $x \mid b$ .  $\square$

O Exemplo 5.15 permite-nos concluir que nem sempre existe m.d.c. de dois elementos quaisquer de um domínio de integridade. Nas secções seguintes vamos estudar algumas classes de domínios de integridade onde a existência de m.d.c. de dois elementos é garantida.

## 5.2 domínios de fatorização única

**Definição 5.22.** *Um domínio de fatorização única ou domínio de Gauss é um domínio de integridade  $D$  no qual todo o elemento  $x \in D \setminus (\mathcal{U}_D \cup \{0_D\})$  se escreve como produto de elementos irredutíveis, sendo essa decomposição única, a menos do produto por unidades, ou seja,*

$$\forall x \in D \setminus (\mathcal{U}_D \cup \{0_D\}) \exists p_1, p_2, \dots, p_n \text{ irredutíveis em } D : x = p_1 p_2 \cdots p_n$$

e se existem  $q_1, q_2, \dots, q_t$  irredutíveis em  $D$  tais que

$$x = q_1 q_2 \cdots q_t,$$

então,  $n = t$  e cada elemento  $p_i$  ( $i = 1, 2, \dots, n$ ) é associado a um elemento  $q_j$  ( $j = 1, 2, \dots, n$ ) e reciprocamente.

Ao número de fatores irredutíveis que aparecem na fatorização de um elemento  $x$  de  $D$  chamamos o comprimento de  $x$ .

**Exemplo 5.23.** O domínio de integridade  $\mathbb{Z}$  é um domínio de Gauss. Pelo Teorema Fundamental da Aritmética, sabemos que todo o inteiro maior que 1 se escreve como produto de primos (que, como já vimos, são os elementos irredutíveis de  $\mathbb{Z}^+$ ) de modo único, a menos da ordem dos fatores. Assim, concluímos que  $x \in \mathbb{Z} \setminus \{-1, 0, 1\}$  se escreve como produto de elementos irredutíveis de  $\mathbb{Z}$ . Essa decomposição é única a menos do produto de  $\pm 1$ . Por exemplo, as únicas fatorizações possíveis de 6 são, a menos da ordem dos fatores,  $2 \cdot 3$  e  $(-2)(-3)$ .

**Exemplo 5.24.** O domínio de integridade  $\mathbb{Z}[\sqrt{-3}]$  não é um domínio de fatorização única. De facto, temos que  $8 = 2 \times 2 \times 2 = 2(1 + \sqrt{-3})(1 - \sqrt{-3})$ .

**Teorema 5.25.** Seja  $D$  um domínio de Gauss e  $a, b \in D$ . Então, existe m.d.c.( $a, b$ ).

**Demonstração:** Se  $a = 0_D$  ou  $b = 0_D$ , temos que  $[a, b] = \{0_D\}$ . Sejam, então,  $a, b \in D \setminus \{0_D\}$ . Suponhamos primeiro que  $a \in \mathcal{U}_D$ . Então,  $a \mid b$  e, portanto, pela Proposição 5.18, existe m.d.c.( $a, b$ ) e  $[a, b] = a\mathcal{U}_D$ . A situação é análoga se supormos que  $b \in \mathcal{U}_D$ .

Suponhamos, então, que  $a, b \notin \mathcal{U}_D$ . Então, existem  $r \in \mathbb{N}$ ,  $m_1, m_2, \dots, m_r, n_1, n_2, \dots, n_r \in \mathbb{N}_0$  e  $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_r$  elementos irredutíveis em  $D$  tais que

$$a = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$$

e

$$b = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}.$$

Observe-se que temos garantia que existe pelo menos um dos fatores. Se mais não houver, consideramos expoentes nulos, que transforma o fator em  $1_D$ . Assim, nestas duas fatorizações, podemos considerar o mesmo número de fatores.

Seja  $d = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$  onde  $s_i = \min(m_i, n_i)$  para cada  $i = 1, 2, \dots, r$ . Vamos provar que  $d$  é m.d.c.( $a, b$ ). Uma vez que  $s_i \leq m_i$ , podemos escrever

$$a = (p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r})(p_1^{m_1-s_1} p_2^{m_2-s_2} \cdots p_r^{m_r-s_r}) = d(p_1^{m_1-s_1} p_2^{m_2-s_2} \cdots p_r^{m_r-s_r}),$$

pelo que  $d \mid a$ . De modo análogo, concluímos que  $d \mid b$ .

Seja  $k \in D$  tal que  $k \mid a$  e  $k \mid b$ . Se  $k \in \mathcal{U}_D$ , temos obviamente que  $k \mid d$ . Se  $k \notin \mathcal{U}_D$ , existem  $v_1, v_2, \dots, v_r \in \mathbb{N}_0$  tais que

$$u = p_1^{v_1} p_2^{v_2} \cdots p_r^{v_r} u',$$

com  $u' \in \mathcal{U}_D$  e, como  $k \mid a$  e  $k \mid b$ ,

$$v_i \leq m_i \text{ e } v_i \leq n_i \quad (i = 1, 2, \dots, r).$$

Logo, para cada  $i = 1, 2, \dots, r$ ,  $v_i \leq s_i$  e, portanto,  $k \mid d$ . Logo,  $d$  é m.d.c.( $a, b$ ).  $\square$

O Teorema que acabámos de enunciar e demonstrar permite-nos concluir que, num domínio de Gauss, são válidos todos os resultados que apresentámos que envolvem máximos divisores comuns, pois temos sempre a garantia que qualquer par de elementos admite pelo menos um m.d.c..

### 5.3 domínios de ideais principais

**Definição 5.26.** Um domínio de ideais principais é um domínio de integridade onde todos os ideais são principais.

**Exemplo 5.27.** O domínio de integridade dos inteiros é um domínio de ideais principais. De facto, sabemos que  $B$  é ideal de  $\mathbb{Z}$  se e só se existe  $n \in \mathbb{Z}$  tal que  $B = (n)$ .

A Proposição 5.10(b) pode ser reescrita no caso de um domínio de ideais principais.

**Proposição 5.28.** Se  $D$  é um domínio de ideais principais,  $p \in D \setminus \{0_D\}$  é irredutível se e só se  $(p)$  é um ideal maximal de  $D$ .  $\square$

O Teorema seguinte, cuja demonstração omitimos mas que pode ser encontrada em qualquer livro de Álgebra, permite-nos incluir a classe dos domínios de ideais principais na classe dos domínios de Gauss.

**Teorema 5.29.** Todos os domínios de ideais principais são domínios de fatorização única.  $\square$

Observemos, no entanto, que o recíproco do teorema anterior não é verdadeiro como mostra o seguinte exemplo.

**Exemplo 5.30.** *Consideremos o conjunto dos polinómios em  $x$  com coeficientes em  $\mathbb{Z}$ , o qual representamos por  $\mathbb{Z}[x]$ . Prova-se que, quando algebrizado com a adição e a multiplicação usuais de polinómios, é um domínio de fatorização única. No entanto, não é um domínio de ideais principais. Para provarmos tal afirmação basta observar que o ideal gerado pelos polinómios  $p(x) = 2$  e  $q(x) = x$ , i.e., o menor ideal que contém os dois polinómios, não é principal.*

Estamos, então, em condições de afirmar que, num domínio de ideais principais, existe m.d.c. de qualquer par de elementos de  $D$ . De facto, cada domínio de ideais principais é um domínio de Gauss e, em cada domínio de Gauss, existe m.d.c. de dois quaisquer elementos. No entanto, é só num domínio de ideais principais que podemos escrever qualquer m.d.c. de dois elementos como combinação linear desses mesmos elementos. É o resultado que enunciamos e demonstramos de seguida.

**Proposição 5.31.** *Sejam  $D$  um domínio de ideais principais e  $a, b, d \in D$ . Se  $d$  é m.d.c.  $(a, b)$ , então, existem  $\alpha, \beta \in D$  tais que  $d = \alpha a + \beta b$ .*

**Demonstração:** Seja  $I = \{xa + yb : x, y \in D\}$ . Como

- $0_D = 0_D a + 0_D b \in I$ ;
- $(x_1 a + y_1 b) - (x_2 a + y_2 b) = (x_1 - x_2)a + (y_1 - y_2)b \in I$  para todos  $x_1, x_2, y_1, y_2 \in D$ ;
- $t(xa + yb) = (tx)a + (ty)b \in I$ , para todos  $x, y, t \in D$ ,

concluimos que  $I$  é um ideal de  $D$ . Como  $D$  é um domínio de ideais principais, temos que

$$\exists d \in D : I = (d) = dD.$$

Facilmente se vê que  $d$  é m.d.c.  $(a, b)$  (porquê?). Assim, de  $d \in I$ , concluimos que

$$\exists \alpha, \beta \in D : d = \alpha a + \beta b.$$

Mais ainda, se  $d_1 \in [a, b]$ ,  $d_1 = du$  para alguma unidade  $u$  de  $D$ . Logo,

$$d_1 = (\alpha u)a + (\beta u)b.$$

□



## 5.4 domínios euclidianos

**Definição 5.32.** Um domínio de integridade diz-se um domínio euclidiano se for possível definir uma aplicação  $\delta : D \rightarrow \mathbb{N}_0$  tal que

$$(E1) \forall a, b \in D \setminus \{0_D\} \quad b \mid a \Rightarrow \delta(b) \leq \delta(a);$$

$$(E2) \text{ se } a, b \in D \text{ e } b \neq 0_D, \text{ então, existem } q, r \in D \text{ tais que } a = bq + r \text{ e } \delta(r) < \delta(b).$$

À aplicação  $\delta$  chama-se valoração em  $D$ .

**Exemplo 5.33.** O domínio de integridade  $\mathbb{Z}$  é um domínio euclidiano. Basta pensar na aplicação que a cada inteiro faz corresponder o seu valor absoluto.

**Proposição 5.34.** Seja  $D$  um domínio euclidiano. Então,

$$\forall b \in D \setminus \{0_D\} \quad \delta(0_D) < \delta(b).$$

**Demonstração:** Como  $b \neq 0_D$  e  $0_D \in D$ , temos, por (E2) da definição de domínio euclidiano, que existem  $q, r \in D$  tais que  $0_D = bq + r$  e  $\delta(r) < \delta(b)$ . Assim,  $r = -bq = b(-q)$  e, portanto,  $b \mid r$ . Se  $r \neq 0_D$ , temos, por (E1), que  $\delta(b) \leq \delta(r)$ . Logo,  $\delta(r) < \delta(r)$ , o que é um absurdo. O absurdo resulta do facto de supormos que  $r \neq 0_D$ . Concluimos, então, que  $r = 0_D$  e, portanto,  $\delta(0_D) < \delta(b)$ .  $\square$

**Exemplo 5.35.** O conjunto dos inteiros de Gauss (ou inteiros gaussianos)

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

é um domínio euclidiano quando consideradas as operações de adição e multiplicação usuais de complexos:

- $\mathbb{Z}[i]$  é um domínio de integridade. De facto, como  $1 = 1 + 0i$ , temos que  $1_{\mathbb{C}} \in \mathbb{Z}[i]$ . Dados  $a + bi$  e  $c + di$ , com  $a, b, c, d \in \mathbb{Z}$ , temos que

$$(a + bi) - (c + di) = (a - c) + (b - d)i \in \mathbb{Z}[i]$$

e

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i],$$

o que, pela Proposição 4.48, nos permite concluir que  $\mathbb{Z}[i]$  é um subdomínio de integridade de  $\mathbb{C}$  e, por isso, um domínio de integridade.

- O conjunto das unidades de  $\mathbb{Z}[i]$  é  $\mathcal{U}_{\mathbb{Z}[i]} = \{-1, 1, -i, i\}$ . De facto, se  $a + bi \in \mathcal{U}_{\mathbb{Z}[i]}$ , então, existe  $c + di \in \mathbb{Z}[i]$  tal que  $(a + bi)(c + di) = 1$ . Considerando o quadrado dos módulos dos complexos, temos que

$$\begin{aligned} (a + bi)(c + di) = 1 &\Rightarrow (a^2 + b^2)(c^2 + d^2) = 1 \\ &\Leftrightarrow a^2 + b^2 = 1 \text{ e } c^2 + d^2 = 1 \\ &\Rightarrow (a^2 = 1 \text{ e } b^2 = 0) \text{ ou } (a^2 = 0 \text{ e } b^2 = 1) \\ &\Leftrightarrow a + bi = \pm 1 \text{ ou } a + bi = \pm i. \end{aligned}$$

- A aplicação  $\delta : \mathbb{Z}[i] \rightarrow \mathbb{N}_0$ , definida por  $\delta(a + bi) = a^2 + b^2$ , é uma valoração em  $\mathbb{Z}[i]$ . Por um lado, sejam  $a + bi, x + yi \in \mathbb{Z}[i]$ . Então,

$$\begin{aligned} a + bi \mid x + yi &\Leftrightarrow (\exists m + ni \in \mathbb{Z}[i]) \ x + yi = (a + bi)(m + ni) \\ &\Rightarrow x^2 + y^2 = (a^2 + b^2)(m^2 + n^2) \\ &\Rightarrow a^2 + b^2 \leq x^2 + y^2 \Leftrightarrow \delta(a + bi) \leq \delta(x + yi) \end{aligned}$$

e, por isso, a condição (E1) é satisfeita.

Por outro lado, seja  $\alpha, \beta \in \mathbb{Z}[i]$ , com  $\beta \neq 0$ . Queremos determinar  $\sigma$  e  $\rho$  em  $\mathbb{Z}[i]$  tais que  $\alpha = \beta\sigma + \rho$ , com  $\delta(\rho) < \delta(\beta)$ . Pela divisão de complexos, sabemos que

$$\frac{\alpha}{\beta} = r + si, \quad r, s \in \mathbb{Q}.$$

Sejam  $q_1$  e  $q_2$  os inteiros mais próximos de  $r$  e  $s$ , respetivamente. Considerem-se  $\sigma = q_1 + q_2i$  e  $\rho = \alpha - \beta\sigma$ .

Se  $\rho = 0$ , pela proposição anterior,  $\delta(\rho) < \delta(\beta)$ .

Se  $\rho \neq 0$ , pela escolha de  $q_1$  e  $q_2$ , temos que  $|r - q_1| \leq \frac{1}{2}$  e  $|s - q_2| \leq \frac{1}{2}$ . Assim,

$$\begin{aligned} \delta\left(\frac{\alpha}{\beta} - \sigma\right) &= \delta((r + si) - (q_1 + q_2i)) \\ &= \delta((r - q_1) + (s - q_2)i) \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}. \end{aligned}$$

Logo,

$$\delta(\alpha - \beta\sigma) = \delta\left(\beta\left(\frac{\alpha}{\beta} - \sigma\right)\right) = \delta(\beta)\delta\left(\frac{\alpha}{\beta} - \sigma\right) \leq \frac{1}{2}\delta(\beta) < \delta(\beta),$$

o que prova a condição (E2).

O exemplo seguinte ilustra o raciocínio que acabámos de efetuar para provar que  $\mathbb{Z}[i]$  é domínio euclidiano.

**Exemplo 5.36.** Sejam  $\alpha = 7 + 2i, \beta = 3 - 4i \in \mathbb{Z}[i]$ . Queremos determinar  $\sigma\rho \in \mathbb{Z}[i]$  tais que  $\alpha = \beta\sigma + \rho$  com  $\delta(\rho) < \delta(\beta)$ :

Temos:

$$\frac{\alpha}{\beta} = \frac{7 + 2i}{3 - 4i} = \frac{(7 + 2i)(3 + 4i)}{(3 - 4i)(3 + 4i)} = \frac{13 + 34i}{25} = \frac{13}{25} + \frac{34}{25}i.$$

Como  $\frac{13}{25} = 0.52$ , consideramos  $q_1 = 1$  e como  $\frac{34}{25} = 1.36$ , consideramos  $q_2 = 1$ .

Sejam  $\sigma = 1 + i$  e  $\rho = 7 + 2i - (3 - 4i)(1 + i) = 3i$ .

Logo,

$$7 + 2i = (3 - 4i)(1 + i) + 3i \text{ com } \delta(3i) = 9 < 25 = \delta(3 - 4i).$$

**Teorema 5.37.** Todo o domínio euclidiano é um domínio de ideais principais.

**Demonstração:** Sejam  $D$  um domínio euclidiano e  $I$  um ideal de  $D$ . Se  $I = \{0_D\}$ , então,  $I = (0_D)$  e  $I$  é principal.

Suponhamos que  $I \neq \{0_D\}$ . Então, existe  $b \neq 0_D$  e, portanto, pela proposição anterior,  $\delta(b) \neq \delta(0_D)$ . Seja  $a \in I \setminus \{0_D\}$  tal que  $\delta(a) \leq \delta(x)$  para todo  $x \in I \setminus \{0_D\}$ . Vamos provar que  $I = (a)$ . Seja  $i \in I$ . Como  $a \neq 0_D$ , por (E2) existem  $q, r \in D$  tais que  $i = aq + r$  e  $\delta(r) < \delta(a)$ . Então,

$$r = i - aq \in I.$$

Como  $a$  é o elemento não nulo de  $D$  de menor valoração, concluímos que  $r = 0_D$  e, portanto,  $i = aq \in aD = (a)$ . Assim,  $I \subseteq (a)$ . Como a outra inclusão é trivial, concluímos que  $I$  é principal.  $\square$

**Corolário 5.38.** Todo o domínio euclidiano é domínio de fatorização única.

**Demonstração:** Resulta do facto de todo o domínio de ideais principais ser um domínio de fatorização única.  $\square$

Mais uma vez, estamos perante um teorema cujo recíproco é falso e, mais uma vez, apresentamos um exemplo que o demonstra.

**Exemplo 5.39.** O anel  $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \{a + b\frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z}\}$  é um domínio de ideais principais que não é euclidiano.

A importância do estudo dos domínios euclidianos prende-se com a generalização do conhecido Algoritmo de Euclides, enunciado para os inteiros (aliás, é deste facto que resulta a escolha do nome para esta classe de domínios de integridade). É esse resultado que passamos a apresentar.

**Teorema 5.40. Algoritmo de Euclides** *Sejam  $D$  um domínio euclidiano e  $a, b \in D \setminus \{0_D\}$ . Sejam  $r_1, q_1 \in D$  tais que*

$$a = bq_1 + r_1 \quad \text{onde ou } r_1 = 0_D \text{ ou } \delta(r_1) < \delta(b).$$

*Se  $r_1 \neq 0_D$ , sejam  $r_2, q_2 \in D$  tais que*

$$b = r_1q_2 + r_2 \quad \text{onde ou } r_2 = 0_D \text{ ou } \delta(r_2) < \delta(r_1).$$

*Em geral, sejam  $r_{i+1}, q_{i+1} \in D$  tais que*

$$r_{i-1} = r_iq_{i+1} + r_{i+1} \quad \text{onde ou } r_{i+1} = 0_D \text{ ou } \delta(r_{i+1}) < \delta(r_i).$$

*Então, a sequência  $r_1, r_2, \dots$  tem de terminar para algum  $r_s = 0_D$ . Se*

- $r_1 = 0_D$  então  $b \in [a, b]$ ;
- $r_1 \neq 0_D$  e  $r_s$  é o primeiro dos  $r_i$  nulo, então  $r_{s-1} \in [a, b]$ .

**Demonstração:** Como  $\delta(r_i) < \delta(r_{i-1})$  e  $\delta(r_i) \in \mathbb{N}_0$ , é óbvio que, após um número finito de passos, temos algum  $r_s = 0_D$ .

Se  $r_1 = 0_D$ , então  $a = bq_1$  e, portanto,  $b \mid a$ . Logo,  $b \in [a, b]$  (ver Proposição 5.18).

Suponhamos que  $r_1 \neq 0_D$ . Se  $d \in D$  é tal que  $d \mid a$  e  $d \mid b$ , então,  $d \mid (a - bq_1)$ , ou seja,  $d \mid r_1$ . No entanto, se  $d_1 \in D$  é tal que  $d_1 \mid r_1$  e  $d_1 \mid b$ , então,  $d_1 \mid (bq_1 + r_1)$ , i.e.,  $d_1 \mid a$ . Assim,  $[a, b] = [b, r_1]$ . Com um raciocínio análogo, se  $r_2 \neq 0_D$ , provamos que  $[b, r_1] = [r_1, r_2]$ . Continuando o processo, concluímos que  $[a, b] = [r_{s-2}, r_{s-1}]$ , onde  $r_s$  é o primeiro dos  $r_i$  nulo. Mas, como

$$r_{s-2} = r_{s-1}q_s + r_s = r_{s-1}q_s,$$

$r_{s-1} \mid r_{s-2}$ . Logo,

$$[a, b] = r_{s-1}\mathcal{U}.$$

□

**Exemplo 5.41.** *Determinemos, em  $\mathbb{Z}$ , um m.d.c.(10354, 5046). Procedendo às seguintes divisões inteiras*

$$1. 10354 = 2 \times 5046 + 262$$

$$2. 5046 = 19 \times 262 + 68$$

$$3. 262 = 3 \times 68 + 58$$

$$4. 68 = 1 \times 58 + 10$$

$$5. 58 = 5 \times 10 + 8$$

$$6. 10 = 1 \times 8 + 2$$

$$7. 8 = 4 \times 2 + 0$$

obtemos que 2 é m.d.c.(10354, 5046) e, por isso,  $[10354, 5046] = \{-2, 2\}$ .

**Exemplo 5.42.** Determinemos, em  $\mathbb{Z}[i]$ , o conjunto  $[8 + 6i, 5 - 15i]$ . Considerando que

$$\frac{8 + 6i}{5 - 15i} = \frac{(8 + 6i)(5 + 15i)}{(5 - 15i)(5 + 15i)} = \frac{-50 + 150i}{25 + 225} = -\frac{1}{5} + \frac{3}{5}i,$$

sejam  $\sigma = 0 + i$  e  $\rho = 8 + 6i - (5 - 15i)i = -7 + i$ .

Como  $\rho \neq 0$ , efetuamos nova divisão:

$$\frac{5 - 15i}{-7 + i} = \frac{(5 - 15i)(-7 - i)}{(7 - i)(-7 - i)} = \frac{-50 + 100i}{49 + 1} = -1 + 2i.$$

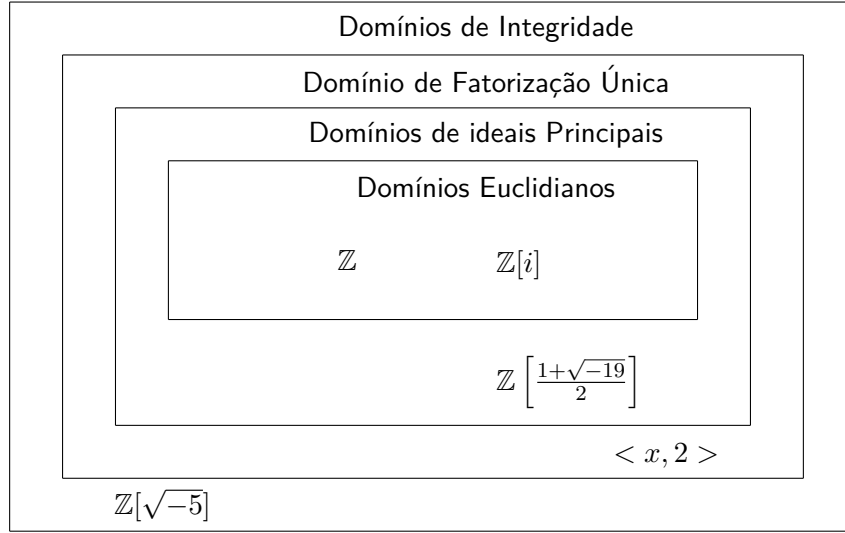
Como tanto a parte real como a imaginária são inteiros, temos que  $\sigma = -1 + 2i$  e  $\rho = 0$  e o processo termina aqui.

Assim,  $-7 + i$  é m.d.c.( $8 + 6i, 5 - 15i$ ).

Uma vez que  $\mathcal{U}_{\mathbb{Z}[i]} = \{-1, 1, -i, i\}$ , temos que

$$[8 + 6i, 5 - 15i] = \{7 - i, -7 + i, 1 + 7i, -1 - 7i, \}.$$

As quatro classes de domínios de integridade que apresentamos neste capítulo podem ser representadas no seguinte esquema



## 5.5 Corpo de frações de um domínio de integridade

Nesta secção, apresentamos um modo de construir um corpo partindo de uma domínio de integridade. Apresentado para um domínio de integridade qualquer, este processo de construção não é mais do que a teoria que permite definir o corpo dos racionais partindo dos números inteiros, processo que todos conhecemos bem.

Dado o domínio de integridade  $D$ , considere-se o conjunto

$$F = \{(a, b) \in D \times D : b \neq 0_D\}.$$

Neste conjunto considere-se a relação binária  $\theta$  definida por

$$(a, b)\theta(x, y) \Leftrightarrow ay = bx \quad (a, b), (x, y) \in S.$$

A relação  $\theta$  é uma relação de equivalência em  $S$ :

1. Para todo  $(a, b) \in S$ , temos que  $ab = ba$ , pelo que  $(a, b)\theta(a, b)$ . Logo,  $\theta$  é reflexiva;
2. Sejam  $(a, b), (x, y) \in S$ . Então,

$$(a, b)\theta(x, y) \Leftrightarrow ay = bx \Leftrightarrow xb = ya \Leftrightarrow (x, y)\theta(a, b)$$

e, por isso,  $\theta$  é simétrica;

3. Sejam  $(a, b), (x, y), (u, v) \in S$ . Então,

$$\begin{aligned} (a, b)\theta(x, y) \text{ e } (x, y)\theta(u, v) &\Leftrightarrow ay = bx \text{ e } xv = yu \\ &\Rightarrow yav = ayv = bxv = byu = ybu \\ &\Rightarrow av = bu \quad [y \text{ é simplificável}] \\ &\Leftrightarrow (a, b)\theta(u, v). \end{aligned}$$

Logo,  $\theta$  é transitiva.

Como relação de equivalência,  $\theta$  define, em  $S$ , uma partição, através do conjunto quociente

$$S/\theta = \{[(a, b)]_\theta : (a, b) \in S\}.$$

Para  $(a, b) \in S$ , representa-se por  $\frac{a}{b}$  a classe  $[(a, b)]_\theta$ . Temos então

$$S/\theta = \left\{ \frac{a}{b} : a, b \in D, b \neq 0_D \right\}.$$

Em  $S/\theta$  definem-se duas operações binárias: dados  $\frac{a}{b}, \frac{c}{d} \in S/\theta$ ,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

e

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

Para provar que estas correspondências são, de facto, operações binárias em  $S/\theta$ , começamos por observar que, para  $\frac{a}{b}, \frac{c}{d} \in S/\theta$ ,  $(a, b), (c, d) \in S$  e, portanto,  $b \neq 0_D$  e  $d \neq 0_D$ . Como  $D$  é domínio de integridade,  $bd \neq 0_D$ , pelo que  $(ad + bc, bd), (ac, bd) \in S$ .

Mais ainda, se  $\frac{a}{b} = \frac{x}{y}$  e  $\frac{c}{d} = \frac{z}{w}$ , temos que  $ay = bx$  e  $cw = dz$ . Então:

$$1. (ad + bc)(yw) = adyw + bcyw = (ay)(dw) + (cw)(by) = (bx)(dw) + (dz)(by) = bdxw + bdyz = (bd)(xw + yz), \text{ pelo que } \frac{ad + bc}{bd} = \frac{xw + yz}{yw};$$

$$2. (ac)(yw) = aycw = bxdz = (bd)(xz), \text{ pelo que } \frac{ac}{bd} = \frac{xz}{yw}.$$

**Teorema 5.43.** O conjunto  $F = S/\theta$ , munido com as operações binárias definidas por

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

e

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd},$$

para  $\frac{a}{b}, \frac{c}{d} \in S/\theta$ , é um corpo.

**Demonstração:** Pretende-se provar que:

1.  $+$  é comutativa;
2.  $+$  é associativa;
3.  $\frac{0_D}{1_D}$  é o elemento neutro da  $+$  - o zero do anel ( $\frac{a}{b} = \frac{0_D}{1_D} \Leftrightarrow a = 0_D$ );
4.  $\frac{-a}{b}$  é o simétrico de  $\frac{a}{b}$ ;
5.  $\times$  é comutativa;
6.  $\times$  é associativa;
7.  $\frac{1_D}{1_D}$  é o elemento neutro da  $\times$  - a identidade do anel ( $\frac{a}{b} = \frac{1_D}{1_D} \Leftrightarrow a = b \neq 0_D$ );
8.  $\frac{b}{a}$  é o inverso de  $\frac{a}{b}$ , para todo  $a \neq 0_D$ ;
9. A operação  $\times$  é distributiva em relação a  $+$ .

Provemos apenas (1) e (3), deixando as restantes provas como exercício.

1. Sejam  $\frac{a}{b}, \frac{c}{d} \in F$ . Pretende-se provar que  $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$ , i.e., que  $\frac{ad+bc}{bd} = \frac{cb+da}{db}$ , o que é óbvio pois, em  $D$ ,  $ad + bc = cb + da$  e  $bd = db$ .

3. Observamos primeiro que, uma vez que, em  $D$ ,  $1_D \neq 0_D$ ,  $(0_D, 1_D) \in S$  e, por isso,  $\frac{0_D}{1_D} \in F$ .  
Mais ainda, para  $\frac{a}{b} \in F$ ,

$$\frac{a}{b} + \frac{0_D}{1_D} = \frac{a1_D + b0_D}{d1_D} = \frac{a}{b}.$$

Por último, temos que

$$\frac{a}{b} = \frac{0_D}{1_D} \Leftrightarrow (a, b)\theta(0_D, 1_D) \Leftrightarrow a1_D = b0_D \Leftrightarrow a = 0_D.$$



**Definição 5.44.** Dado um domínio de integridade  $D$ , chama-se corpo das frações de  $D$  ao corpo  $F = \{\frac{a}{b} : a, b \in D, b \neq 0_D\}$  definido anteriormente.

De seguida, mostramos que o corpo de frações de um domínio de integridade contém sempre um cópia desse domínio.

**Teorema 5.45.** Sejam  $D$  um domínio de integridade e  $F$  o seu corpo de frações. Então,  $i : D \rightarrow F$ , definido por  $i(a) = \frac{a}{1_D}$ , para todo  $a \in D$ , é um monomorfismo de anéis tal que  $i(1_D) = 1_F$ .

**Demonstração:** Começamos por provar que  $i$ , assim definida, é um morfismo de anéis. De facto, dados  $a, b \in D$ , temos que

$$1. \ i(a + b) = \frac{a+b}{1_D} = \frac{a1_D + 1_D b}{1_D 1_D} = \frac{a}{1_D} + \frac{b}{1_D} = i(a) + i(b);$$

$$2. \ (i(ab)) = \frac{ab}{1_D} = \frac{ab}{1_D 1_D} = \frac{a}{1_D} \times \frac{b}{1_D}.$$

Por outro lado,

$$\text{Nuc } i = \{a \in D : i(a) = 0_F\} = \{a \in D : \frac{a}{1_D} = \frac{0_D}{1_D}\} = \{a \in D : a = 0_D\} = \{0_D\}.$$

Logo, o morfismo  $i$  é injetivo e, por isso, monomorfismo. Finalmente, temos que  $i(1_D) = \frac{1_D}{1_D} = 1_F$ .  
□

**Corolário 5.46.** Sejam  $D$  um domínio de integridade e  $F$  o seu corpo de frações. Então,  $F$  admite um subdomínio de integridade  $D'$  tal que  $D' \simeq D$ .

**Exemplo 5.47.** O corpo  $\mathbb{Q}$  é o corpo de frações do domínio de integridade  $\mathbb{Z}$ .

**Exemplo 5.48.** Determinemos o corpo de frações do domínio  $\mathbb{Z}[i]$ : Por definição, temos que

$$F = \left\{ \frac{a + bi}{c + di} : a, b, c, d \in \mathbb{Z}, c + di \neq 0 \right\}$$

Mas,

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{c^2 + d^2} = \frac{(ac + bd) + (cb - ad)i}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{cb - ad}{c^2 + d^2}i,$$

pelo que

$$F \subseteq \{q + ri : q, r \in \mathbb{Q}\}.$$

Por outro lado, se  $q, r \in \mathbb{Q}$ , então, existem  $x, y, z, w \in \mathbb{Z}$ , com  $y, w \neq 0$  tais que

$$q + ri = \frac{x}{y} + \frac{z}{w}i = \frac{xw + zy i}{yw + 0i}.$$

Logo,  $\mathbb{Q} \subseteq F$ . Estamos em condições de concluir que

$$F = \mathbb{Q}[i].$$

- [1] Durbin, J. R., *Modern Algebra, an introduction*, John Wiley (1985)
- [2] Fraleigh, J. B., *A first course in Abstract Algebra*, Addison-Wesley (1982)
- [3] Marques Smith, P., Mendes Martins, P., Roçadas, L., *Álgebra. Exercícios resolvidos e exercícios propostos*, Escolar Editora (2015),
- [4] Monteiro, A. J., Matos, I. T., *Álgebra, um primeiro curso*, Escolar Editora (1995)