Apontamentos da disciplina de:

Álgebra I

Licenciatura em Matemática

Docente responsável: Assis Azevedo

Capítulo 1

Teoria de Grupos

1.1 Grupos

Uma **operação binária** definida num conjunto não vazio A é uma aplicação de $A \times A$ em A. Note-se que, se A tem n elementos então existem n^{n^2} operações binárias sobre A, uma vez que A^2 tem n^2 elementos.

Em geral, se $\cdot$ é uma operação binária sobre A e a, b pertencem a A, denotamos por $a \cdot b$ a imagem do par (a, b) pela aplicação $\cdot$. Temos assim

$$\begin{array}{cccc} \cdot & A \times A & \longrightarrow & A \\ & (a,b) & \mapsto & a \cdot b \end{array}$$

Se $A = \{a_1, a_2, \ldots, a_n\}$ e $\cdot$ é uma operação binária sobre A, então $\cdot$ pode ser representada por uma "tabela" (dita Tabela de Cayley) do tipo

$\cdot$	a_1	a_2	$\cdots$	a_n
a_1				
a_2				
$\vdots$				
a_n				

em que na "casa" relativa à linha i e à coluna j colocamos o elemento $a_i \cdot a_j$. Convém frisar que qualquer preenchimento desta tabela com elementos de A define um grupóide.

Definição 1.1.1. *Um grupóide é um par ordenado $< A, \cdot >$, em que A é um conjunto não vazio (dito* **conjunto suporte** *do grupóide) e $\cdot$ é uma operação binária sobre A.*

Quando não houver confusão quanto à operação binária em questão, diremos **o grupóide** A em vez de o grupóide $< A, \cdot >$. Um grupóide $< A, \cdot >$ diz-se **finito**, se o seu conjunto suporte for finito.

Exemplos 1.1.2. *Os seguintes são alguns exemplos de grupóides "já conhecidos":*

a) $< \mathbb{Q}, \cdot >$;	f) $< \mathbb{N}, + >$;	k) $< \mathcal{F}(\mathbb{R}, \mathbb{R}), \cdot >$;
b) $< \mathbb{Z}, \cdot >$;	g) $< \mathbb{Q}, - >$;	l) $< \mathcal{M}_{n\times n}(\mathbb{R}), \cdot >$;
c) $< \mathbb{N}, \cdot >$;	h) $< \mathbb{Z}, - >$;	m) $< \mathbb{Z}_n, +_n >$;
d) $< \mathbb{Q}, + >$;	i) $< \mathbb{Q} \setminus \{0\}, \div >$;	n) $< \mathbb{Z}_n, \cdot_n >$;
e) $< \mathbb{Z}, + >$;	j) $< \mathcal{F}(\mathbb{R}, \mathbb{R}), \circ >$;	o) $< \mathbb{R}^3, \wedge >$.

Aqui: $\cdot$ representa o produto (de números reais, de funções ou de matrizes, conforme o caso); $+$, $-$ e $\div$ representam a soma, subtracção e divisão de números reais; $\circ$ representa a composição de funções; $\mathbb{Z}_n = \{a \in \mathbb{N}_0 : a < n\}$; $+_n$ e $\cdot_n$ representam a soma e o produto, módulo n; $\wedge$ representa o produto externo.

Um grupóide $< A, \cdot >$ diz-se **comutativo** ou **abeliano** se

$$\forall a, b \in A \quad a \cdot b = b \cdot a,$$

e diz-se **associativo** se

$$\forall a, b, c \in A \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

Se um grupóide $< A, \cdot >$ for associativo e $a, b, c \in A$ escreveremos $a \cdot b \cdot c$ em vez de $a \cdot (b \cdot c)$ ou de $(a \cdot b) \cdot c$. Do mesmo modo, se $n \in \mathbb{N}$ e $a_1, a_2, \ldots, a_n \in A$, tem sentido falar em $a_1 \cdot a_2 \cdot \cdots \cdot a_n$.

Dos exemplos acima: os grupóides a), b), c), d), e), f), k), m) e n) são associativos e comutativos; os grupóides g), h) e i) não são comutativos nem associativos; os grupóides j) e l) são associativos e não são comutativos.

Se a operação for dada por uma tabela de Cayley então a simetria dessa tabela em relação à "diagonal principal" traduz a comutatividade do grupóide. Deste modo, definir uma operação comutativa sobre A equivale a preencher, com elementos de A e de forma arbitrária, a "diagonal principal" e os elementos abaixo dela, num total de $\frac{n(n+1)}{2}$ casas, se $|A| = n$. Temos assim que existem $n^{\frac{n(n+1)}{2}}$ grupóides comutativos cujo conjunto suporte é A.

Definição 1.1.3. *Um* **semigrupo** $< A, \cdot >$ *é um grupóide associativo.*

Um elemento e de um grupóide $< A, \cdot >$ diz-se um **elemento neutro à esquerda** de A se

$$\forall a \in A \quad e \cdot a = a.$$

De modo dual se define elemento neutro à direita. Um elemento diz-se um **elemento neutro** de A se for simultaneamente elemento neutro à esquerda e à direita. É claro que, num grupóide comutativo, as noções de elemento neutro à esquerda e de elemento neutro à direita coincidem.

Seja A um grupóide finito cuja operação binária é dada por uma tabela de Cayley e seja a pertencente a A. Qual a interpretação na tabela do facto de a ser ou não um elemento neutro à esquerda? E à direita?

Lema 1.1.4. *Sejam $< A, \cdot >$ um grupóide e $e, f \in A$. Se e é elemento neutro à esquerda de A e f é elemento neutro à direita de A, então $e = f$. Em particular A admite no máximo um elemento neutro.*

Demonstração. Note-se que

$$e \cdot f = \begin{cases} f & \text{porque } e \text{ é elemento neutro à esquerda} \\ e & \text{porque } f \text{ é elemento neutro à direita.} \end{cases}$$

Deste modo $e = f$. □

Definição 1.1.5. *Um semigrupo com elemento neutro diz-se um* **monóide**.

Em Exemplos 1.1.2 só os grupóides f), g), h), i) e o) é que não são monóides. Note-se que os grupóides g), h) e i) admitem elemento neutro à direita.

Seja $< A, \cdot >$ um grupóide com elemento neutro e (que já sabemos ser único). Dizemos que um elemento a de A é **invertível à esquerda** se existir a' em A, que se diz **inverso esquerdo de** a, tal que $a' \cdot a = e$. De modo dual se define elemento invertível à direita e inverso direito. Dizemos ainda que um elemento a em A é **invertível** se existir a' em A, que designamos por **inverso** de a, que é simultaneamente inverso esquerdo e direito de a.

Lema 1.1.6. *Se $< A, \cdot >$ é um monóide e $a \in A$ admite um inverso à esquerda a' e um inverso à direita a^* então $a' = a^*$. Em particular, todo o elemento invertível admite um e um só inverso.*

Demonstração. Basta notar que $a' = a' \cdot (a \cdot a^*) = (a' \cdot a) \cdot a^* = a^*$. □

Definição 1.1.7. *Um grupóide diz-se um* **grupo** *se for um monóide e todo o seu elemento admitir inverso.*

De entre os monóides de Exemplos 1.1.2, apenas $< \mathbb{Q}, + >$, $< \mathbb{Z}, + >$ e $< \mathbb{Z}_n, +_n >$ são grupos (para além de $< \mathbb{Z}_1, \cdot_1 >$). Temos ainda que:

- 0 é o único elemento sem inverso em $< \mathbb{Q}, \cdot >$;
- apenas 1 e -1 são invertíveis em $< \mathbb{Z}, \cdot >$;
- apenas 1 é invertível em $< \mathbb{N}, \cdot >$;
- em $< \mathcal{F}(\mathbb{R}, \mathbb{R}), \circ >$ os invertíveis são as funções bijectivas;
- em $< \mathcal{F}(\mathbb{R}, \mathbb{R}), \cdot >$ os invertíveis são as funções que nunca se anulam;
- a é invertível em $< \mathbb{Z}_n, \cdot_n >$ se e so se a é primo com n.

Note-se também que $< \mathbb{Q} \setminus \{0\}, \cdot >$ é um grupo. É também claro que o conjunto das funções bijectivas de $\mathbb{R}$ em $\mathbb{R}$ munido da operação binária de composição é um grupo. O mesmo acontece se considerar o conjunto das matrizes invertíveis n por n com a operação produto de matrizes. Este grupo será denotado por $GL(n, \mathbb{R})$.

Exemplo 1.1.8 (Grupo dos invertíveis de $\mathbb{Z}_n$)**.** *Para $n \in \mathbb{N}$ seja*

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \ a \text{ é primo com } n\}.$$

Recorde-se que:

- *se a, b são primos com n então ab é primo com n;*
- *se $k \in \mathbb{Z}$ e r é o resto da divisão de k por n então o máximo divisor entre k e n é igual ao máximo divisor entre r e n.*

Deste modo, se $a, b \in \mathbb{Z}_n^*$ então $a \cdot_n b \in \mathbb{Z}_n^*$ pois $a \cdot_n b$ é igual ao resto da divisão de ab por n. Assim $< \mathbb{Z}_n^*, \cdot_n >$ é um grupóide, que é associativo e que admite 1 como elemento neutro. Por outro lado, pelo que vimos acima, todo o elemento de $\mathbb{Z}_n^*$ é invertível e por isso $< \mathbb{Z}_n^*, \cdot_n >$ é um grupo.

Além disso, $\mathbb{Z}_n^*$ tem $\varphi(n)$ elementos (sendo φ a função de Euler). Note-se ainda que, se $p \in \mathbb{P}$ então $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

Lema 1.1.9 (Lei do corte à direita)**.** *Sejam $< A, \cdot >$ é um monóide, $a, b, c \in A$ tais que $a \cdot c = b \cdot c$. Se c admite inverso à direita então $a, b \in A$.*

Demonstração. Seja e o elemento neutro de A e c' um inverso à direita de c. Então

$$\begin{aligned} a \cdot c = b \cdot c &\Rightarrow (a \cdot c) \cdot c' = (b \cdot c) \cdot c' \\ &\Rightarrow a \cdot (c \cdot c') = b \cdot (c \cdot c') \\ &\Rightarrow a \cdot e = b \cdot e \\ &\Rightarrow a = b. \end{aligned}$$

□

No monóide $< \mathbb{Z}_6, \cdot_6 >$ temos a igualdade $2 \cdot_6 3 = 2 \cdot_6 0$ apesar de $3 \neq 0$. Deste modo a lei do corte não é válida em $< \mathbb{Z}_6, \cdot_6 >$. De facto a lei do corte não é válida em $< \mathbb{Z}_n, \cdot_n >$ se n não é primo.

Corolário 1.1.10. *Num grupo $< G, \cdot >$ são válidas a* **lei do corte***, à esquerda e à direita, isto é,*

$$\begin{aligned} a \cdot c = b \cdot c &\Rightarrow a = b \quad \textit{(lei do corte à direita)} \\ c \cdot a = c \cdot b &\Rightarrow a = b \quad \textit{(lei do corte à esquerda).} \end{aligned}$$

Demonstração. Basta usar o lema anterior e o seu dual. □

Definição 1.1.11. *Um elemento a de um grupóide $< A, \cdot >$ diz-se* **idempotente** *se $a \cdot a = a$.*

Num monóide, o elemento neutro é um idempotente, mas podem existir mais. Por exemplo: as funções constantes de $\mathbb{R}$ em $\mathbb{R}$ são idempotentes de $\mathcal{F}(\mathbb{R}, \mathbb{R})$; os elementos 0 e 1 são idempotentes de $< \mathbb{Z}_n, \cdot_n >$ qualquer que seja n; 0, 1, 9 e 16 são idempotentes de $< \mathbb{Z}_n, \cdot_{24} >$: os idempotentes de $\mathcal{M}_{n \times n}(\mathbb{R})$ são as matrizes da forma $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tais que ($a = b = c = d = 0$) ou ($a = d = 1$ e $b = c = 0$) ou ($a = 1$, $c = d = 0$ e b qualquer) ou ($c \neq 0$, d qualquer, $a = -d + 1$ e $b = \frac{d(1-d)}{c}$).

Proposição 1.1.12. *Um grupo admite apenas um idempotente, o seu elemento neutro.*

Demonstração. Se $< G, \cdot >$ é um grupo, e o seu elemento neutro e se a é um idempotente, então $\underbrace{a \cdot a}_{=a} = \underbrace{a \cdot e}_{=a}$ e por conseguinte, atendendo à lei do corte, $a = e$. □

Teorema 1.1.13. *Seja $< G, \cdot >$ um semigrupo admitindo elemento neutro à esquerda e tal que, todo o seu elemento admite inverso esquerdo relativamente a esse elemento neutro, ou seja*

$$(\exists e \in G \;\; \forall a \in G \quad e \cdot a = a) \qquad e \qquad \left(\forall a \in G \;\; \exists a' \in G \quad a' \cdot a = e\right).$$

Então $< G, \cdot >$ é um grupo.

Demonstração. Seja e um elemento neutro à esquerda de G. Mostremos que e é o único idempotente de G. Suponhamos que f é um idempotente de G e seja f' um seu inverso esquerdo relativamente a e. Assim,

$$f = e \cdot f = (f' \cdot f) \cdot f = f' \cdot (f \cdot f) = f' \cdot f = e.$$

Se a pertence a G vejamos que o seu inverso esquerdo a' é também inverso direito. Para isso precisamos de mostrar que $a \cdot a' = e$ ou, pelo que vimos acima, que $a \cdot a'$ é um idempotente. Mas

$$(a \cdot a') \cdot (a \cdot a') = \left[(a \cdot a') \cdot a\right] \cdot a' = \left[a \cdot (a' \cdot a)\right] \cdot a' = (a \cdot e) \cdot a' = a \cdot (e \cdot a') = a \cdot a'.$$

Mostremos agora que e é elemento neutro à direita, ou seja, para todo a em G $a \cdot e = a$. Seja a' um inverso (à esquerda e à direita) de a. Então

$$a \cdot e = a \cdot (a' \cdot a) = (a \cdot a') \cdot a = e \cdot a = a.$$

Conclui-se assim que $< G, \cdot >$ é um grupo. □

Obviamente, o dual deste teorema também é válido.

Exemplo 1.1.14. $G = \left\{ \begin{pmatrix} a & b \\ a & b \end{pmatrix} : a, b \in \mathbb{R},\ a + b \neq 0 \right\}$ *munido do produto de matrizes é um grupóide. Para ver isso basta notar que*

$$\begin{pmatrix} a & b \\ a & b \end{pmatrix} \begin{pmatrix} c & d \\ c & d \end{pmatrix} = \begin{pmatrix} ac + bc & ad + bd \\ ac + bc & ad + bd \end{pmatrix}.$$

Em particular $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ *é um elemento neutro à esquerda. Além disso todo o elemento* $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$ *pertencente a G tem inverso à direita relativamente a* $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$, *pois*

$$\begin{pmatrix} a & b \\ a & b \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{a+b} \\ 0 & \frac{1}{a+b} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

No entanto não estamos na presença de um grupo, uma vez que

$$\begin{pmatrix} a & b \\ a & b \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & a+b \\ 0 & a+b \end{pmatrix} \neq \begin{pmatrix} a & b \\ a & b \end{pmatrix} \quad \text{se } a \neq 0.$$

Pelo teorema anterior (versão dual) podemos concluir que G não admite elemento neutro à direita.

Note-se ainda que G admite uma infinidade de elementos neutros à esquerda. Para ver isso basta considerar os elementos $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$ *com* $a+b=1$.

Notação: Usaremos dois tipos de notação para semigrupos: a multiplicativa e a aditiva. No segundo caso denotaremos a operação binária por $+$. Em notação aditiva, diremos o **simétrico de** a em vez de o inverso de a. Na seguinte tabela explicitamos as convenções para a notação.

Notação multiplicativa		Notação aditiva	
escreveremos	para representar	escreveremos	para representar
ab	$a \cdot b$		
e ou 1	elemento neutro	0	elemento neutro
a^2	$a \cdot a$	$2a$	$a+a$
a^n	$\underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ factores}}$	na	$\underbrace{a+a+\cdots+a}_{n \text{ parcelas}}$
a^{-1}	inverso de a	$-a$	simétrico de a
a^{-n}	$(a^n)^{-1}$	$-na$	$-(na)$
a^0	e	$0a$	0

Quando não se disser nada em contrário supõe-se que estamos a usar notação multiplicativa.

A "álgebra" das potências e da inversão porta-se da maneira como era de esperar, tendo em atenção que a operação binária pode não ser comutativa.

Lema 1.1.15. *Seja G um grupo e $a, b, a_1, \ldots, a_k \in G$ ($k \in \mathbb{N}$ e $m, n \in \mathbb{Z}$). Então:*

a) $\left(a^{-1}\right)^{-1} = a$;

b) $(ab)^{-1} = b^{-1}a^{-1}$;

c) $(a_1 a_2 \cdots a_k)^{-1} = a_k^{-1} \cdots a_2^{-1} a_1^{-1}$;

d) $\left(aba^{-1}\right)^n = ab^n a^{-1}$;

e) $\left(a^{-1}ba\right)^n = a^{-1}b^n a$;

f) $(a^n)^{-1} = (a^{-1})^n$;

g) $a^n a^m = a^{n+m}$;

h) $(a^n)^m = a^{nm}$.

Demonstração. Recorde-se que x é o inverso de y se e só se $xy = e$.

a) Pela observação acima a é o inverso de a^{-1} se e só se $aa^{-1} = e$. Mas $aa^{-1} = e$ por definição de a^{-1}.

b) Novamente pela observação acima basta mostrar que $b^{-1}a^{-1}ab = e$. Mas $b^{-1}a^{-1}ab = b^{-1}\underbrace{a^{-1}a}_{=e}b = b^{-1}b = e$.

c) Basta usar a alínea anterior e um raciocínio de indução sobre k, notando que, se $k > 1$ então

$$a_1 a_2 \cdots \underbrace{a_k a_k^{-1}}_{=e} \cdots a_2^{-1} a_1^{-1} = a_1 a_2 \cdots a_{k-1} a_{k-1}^{-1} \cdots a_2^{-1} a_1^{-1}$$

d) (apenas o passo de indução) Para $n > 1$,

$$\begin{aligned} \left(aba^{-1}\right)^n &= \left(aba^{-1}\right)^{n-1} \left(aba^{-1}\right) \\ &= ab^{n-1}a^{-1}aba^{-1} \quad \text{por hipótese de indução} \\ &= ab^{n-1}eba^{-1} = ab^n a^{-1}. \end{aligned}$$

e) Análogo à alínea anterior.

f) Caso particular de b), em que $k = n$ e $a_i = a$ para todo i.

g) e h) Basta simplesmente usar a definição de potência. □

Corolário 1.1.16. *Um grupo no qual todo o elemento é igual ao seu inverso (ou seja, cujo quadrado é o elemento neutro) é necessariamente abeliano.*

Demonstração. Sejam G um grupo e $a, b \in G$. Então, usando a hipótese e a alínea b) do Lema anterior, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. □

Seja $< S, \cdot >$ um semigrupo e sejam $a, b \in S$. Considere a equação

$$a\,x = b, \qquad \text{com } x \in S.$$

Quantas soluções tem? depende de a e de b? Por exemplo, em $< \mathbb{Z}_6, \cdot_6 >$ a equação $2x = 4$ tem duas soluções (2 e 4), a equação $4x = 3$ não tem solução e a equação $5x = 2$ tem uma só solução (4). No caso dos grupos a resposta é simples: há sempre uma e uma só solução.

Teorema 1.1.17. *As seguintes condições sobre um semigrupo G são equivalentes:*

a) *G é um grupo;*

b) $\forall a, b \in G,\ \exists! x \in G, \exists! y \in G : \quad ax = b, \quad ya = b;$

c) $\forall a, b \in G,\ \exists x \in G, \exists y \in G : \quad ax = b, \quad ya = b.$

Demonstração.

a) ⇒ b) Se $a, b \in G$ então

$$\begin{aligned} ax = b &\Leftrightarrow x = a^{-1}b, \quad \text{multiplicando à esquerda por } a^{-1}, \\ ya = b &\Leftrightarrow y = ba^{-1}, \quad \text{multiplicando à direita por } a^{-1}. \end{aligned}$$

b) ⇒ c) Trivial.

c) ⇒ a) Vamos usar o Teorema 1.1.13 para mostrar que G é um grupo. Seja $a \in G$ e consideremos e uma solução da equação $ya = a$. Mostremos que e é elemento neutro à esquerda de G ou seja, que $ec = c$ para qualquer $c \in G$. Se $c \in G$ consideremos d uma solução da equação $ax = c$. Então $ec = e(ad) = (ea)d = ad = c$. Para concluir que G é um grupo basta mostrar que existe $c' \in G$ tal que $c'c = e$, o que é óbvio, pois basta considerar c' uma solução da equação $yc = e$. □

Note-se que a associatividade é necessária para mostrar a equivalência. Por exemplo, o grupóide $< \mathbb{R} \setminus \{0\}, \div >$ não é um grupo mas para todo $a, b \in \mathbb{R} \setminus \{0\}$ as equações $a \div x = b$ e $y \div a = b$ têm uma e uma só solução ($x = \frac{a}{b}$, $y = ab$).

Nota 1.1.18. *Se tivermos um grupo finito dado por uma tabela então, atendendo ao teorema anterior, em cada linha (resp. coluna) tabela aparecem todos os elementos do grupo, sem repetições. Além disso a linha (resp. coluna) do elemento neutro é "igual" à primeira linha (resp. coluna).*

Daqui se concluiu que é fácil encontrar todos os grupos cujos conjuntos suporte sejam um dado conjunto finito (pequeno). Por exemplo, se o grupo tiver apenas dois elementos e e a e e for o elemento neutro então é fácil de ver que $a^2 = e$. Se tivermos um grupo com 3 elementos e, a e b, sendo e o elemento neutro então a tabela de Cayley do grupo terá de ser

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

É necessário verificar que a operação é associativa para sabermos que estamos de facto na presença de um grupo. Note-se que o grupo $< \mathbb{Z}_3, +_3 >$ tem esta tabela de Cayley, se considerarmos $e = 0$, $a = 1$ e $b = 2$. Deste modo, a associatividade da operação está garantida.

Suponhamos que temos um grupo com 4 elementos, e, a, b e c, sendo e o elemento neutro.

- *Se $a^2 = b$ então $a \cdot c = e$ atendendo ao que é dito acima (não há repetições nas linhas e nas colunas). Repetindo este argumento obtemos*

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

  O grupo $\mathbb{Z}_4$ tem esta tabela de Cayley ($e = 0$, $a = 1$, $b = 2$ e $c = 3$).

- *Se $a^2 = c$ o raciocínio é semelhante e a tabela que obtemos é obtida da anterior trocando os elementos b e c.*

- *Se $a^2 = b^2 = c^2 = e$ então com o mesmo tipo de raciocínio obtemos*

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

  Um grupo com esta tabela de Cayley é o grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$

Mas nem todas os grupóides cuja tabela tem estas propriedades são grupos, como podemos ver pelo exemplo,

$\cdot$	0	1	2	3	4
0	0	1	2	3	4
1	1	0	3	4	2
2	2	4	1	0	3
3	3	2	4	1	0
4	4	3	0	2	1

O grupóide $< \{0,1,2,3,4\}, \cdot >$ *não é um grupo pois* $(2 \cdot 3) \cdot 4 = 4$ *e* $2 \cdot (3 \cdot 4) = 2$.

Corolário 1.1.19. *Um semigrupo finito que satisfaça as leis do corte é um grupo*

Demonstração. Sejam $< A, \cdot >$ um semigrupo nas condições referidas e $a, b \in A$. Como A é finito existem $n, m \in \mathbb{N}$ tais que $a^{n+m} = a^n$. Aplicando a lei do corte temos que $a^s = a$ para $s = m + 1$. Vamos mostrar que existe $x \in A$ tal que $ax = b$. Mas

$$\begin{aligned} ax = b &\Leftrightarrow a^2x = ab \quad \text{pela lei do corte} \\ &\Leftrightarrow a^2x = a^sb \\ &\Leftrightarrow x = \begin{cases} b & \text{se } s = 2 \\ a^{s-2}b & \text{se } s > 2. \end{cases} \end{aligned}$$

De modulo análogo se mostra que existe $y \in A$ tal que $ya = b$. Usando o teorema anterior concluímos que $< A, \cdot >$ é um grupo. □

Vamos agora definir o produto de grupóides.

Definição 1.1.20. *Define-se o* **produto directo** *de n grupóides* $< G_1, \cdot_1 >, < G_1, \cdot_1 > , \ldots, < G_n, \cdot_n >$*, como sendo o grupóide cujo conjunto suporte é* $G_1 \times G_2 \cdots \times G_n$ *e a operação é*

$$\begin{array}{ccc} (G_1 \times G_2 \cdots \times G_n) \times (G_1 \times G_2 \cdots \times G_n) & \longrightarrow & (G_1 \times G_2 \cdots \times G_n) \\ ((g_1, g_2, \ldots, g_n), (h_1, h_2, \ldots, h_n)) & \mapsto & (g_1 \cdot_1 h_1, g_2 \cdot_2 h_2 \ldots, g_n \cdot_n h_n) \end{array}$$

No fundo, a operação no produto é feita coordenada a coordenada.

Proposição 1.1.21. *O produto directo de semigrupos, monóides ou grupos é um semigrupo, monóide ou grupo, respectivamente.*

Demonstração. Basta notar que:

- se e_i é o elemento neutro de G_i $(i = 1, 2, \ldots, n)$ então $(e_1, e_2, \ldots, e_n)$ é o elemento neutro de $G_1 \times G_2 \cdots \times G_n$;
- se $g_i \in G_i$ e g_i^{-1} é o inverso de g_i $(i = 1, 2, \ldots, n)$ então $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$ é o inverso de $(g_1, g_2, \ldots, g_n)$ em $G_1 \times G_2 \cdots \times G_n$.

A associatividade da operação no produto é também trivial de verificar. □

1.1.1 Exercícios

Exercício 1. Verifique as afirmações feitas sobre os grupóides apresentados na página 2.

Exercício 2. Seja $A = \{a, b, c\}$. Verifique se é comutativa ou associativa a operação $\cdot$ definida por

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

Exercício 3. Quais dos seguintes grupóides são semigrupos? Quais admitem elementos neutros à esquerda? e à direita? quais os elementos invertíveis dos grupóides que admitem elemento neutro? quais são grupos?

a) $< \mathbb{R}, \circ >$ em que $a \circ b = a + b + ab$.

b) $< \mathbb{Z}, \otimes >$ em que $a \otimes b = a + b - 3$.

c) $< \mathbb{N}, \circ >$ em que $a \circ b = a^b$.

d) $< \mathcal{F}(X, X) >, \circ >$, em que X é um conjunto não vazio e $\circ$ é composição de funções.

e) $< X, \circ >$, em que X é um conjunto não vazio e $\circ$ é a operação definida por

$$\forall a, b \in X, \quad a \circ b = a.$$

f) $< G, \circ >$, em que $G = \left\{ \begin{pmatrix} a & b \\ 0 & \frac{1}{a} \end{pmatrix} : a \in \mathbb{R} - \{0\},\ b \in \mathbb{R} \right\}$ e $\circ$ representa o produto de matrizes.

Exercício 4. Construa um grupóide com dois elementos neutros à direita.

Exercício 5. Para cada um dos casos seguintes, verifique se $< \mathbb{R}, \circ >$ é um semigrupo e se tem elemento neutro.

a) $x \circ y = x - y$;

b) $x \circ y = |x - y|$;

c) $x \circ y = x + y + xy$;

d) $x \circ y = \sqrt[3]{x^3 + y^3}$;

e) $x \circ y = [x + y]$;

f) $x \circ y = \frac{x+y}{2}$;

g) $x \circ y = (1 - x)(1 - y)$;

h) $x \circ y = |x + y|$.

Exercício 6. Seja X um conjunto não vazio. Sobre conjunto $\mathcal{P}(X)$ considere as operações de união e de intersecção. Quais das operações: são associativas, são comutativas, admitem elemento neutro?

Exercício 7. Quantas operações binárias comutativas e com elemento um é possível definir sobre um conjunto com n elementos?

Exercício 8. Mostre que o conjunto $\{(x,y,z) \in \mathbb{R}^3 : x+y+z=1\}$ munido da operação binária definida por

$$(x,y,z) \circ (a,b,c) = (xa, b+ya, c+za)$$

é um monóide. Quais são os seus elementos invertíveis?

Exercício 9. Verifique se os seguintes grupóides são grupos:

a) $< \mathbb{Q}, \circ >$, em que $a \circ b = ab + a + b + 1$;

b) $< \mathbb{Z}, \circ >$, em que $a \circ b = 2^{ab}$;

c) $< \mathbb{Z}, \circ >$, em que $a \circ b = 2a + b + 5$;

d) $< \mathbb{R} \times (\mathbb{R} \setminus \{0\}), \circ >$, em que $(a,b) \circ (c,d) = (ab + c, bd)$;

e) $< \{5, 10, 15, 20, 25, 30\}, .{}_{35} >$.

Exercício 10. Seja $< \{e,a,b,c\}, \cdot >$ um grupo tal que e é o elemento neutro com $a^2 = b^2 = e$. Mostre que $c^2 = e$.

Exercício 11. Seja $< \{e,a,b,c,d\}, \cdot >$ um grupo tal que e é o elemento neutro, $bc = e$ e $ab = c$. Construa a tabela de Cayley do grupo. Comece por notar que $cb = e$.

Exercício 12. Complete as demonstrações dos resultados apresentados na Nota 1.1.18.

Exercício 13. Seja $< G, \cdot >$ um grupo e $g \in G$. Considere $\bigodot : \begin{array}{ccc} G \times G & \longrightarrow & G \\ (x,y) & \mapsto & xgy \end{array}$.

Mostre que $< G, \bigodot >$ é um grupo.

Exercício 14. Sobre o conjunto $\{1, -1, i, -i, j, -j, k, -k\}$ considere a operação associativa definida por

$$\begin{cases} i^2 = j^2 = k^2 = -1, \\ (-1)(-1) = 1,\ (-1)i = -i,\ (-1)j = -j,\ (-1)k = -k, \\ ij = (-j)i = k,\ jk = (-k)j = i,\ ki = (-i)k = j. \end{cases}$$

Verifique se estamos na presença de um grupo.

Exercício 15. Seja X um conjunto não vazio. Mostre que $< \mathcal{P}(X), \triangle >$ é um grupo abeliano, em que $\triangle$ é a chamada *diferença simétrica* (definida por $A \triangle B = (A \cup B) \setminus (A \cap B)$).

Exercício 16. Seja G um grupo e $a \in G$. Mostre que $< G, \star >$ é um grupo, sendo $\star$ definida por $x \star y = xay$.

Exercício 17. Mostre que $< \mathbb{Z}, \star >$ é um grupo não abeliano, sendo $\star$ definida por $m \star n = m + (-1)^m n$.

Exercício 18. Mostre que $<]1, +\infty[, \star >$ é um grupo abeliano, sendo $\star$ definida por $x \star y = xy - x - y + 2$.

Exercício 19. Verifique que $< G, * >$ é um grupo, onde $G = (\mathbb{Q} - \{0\}) \times \mathbb{Q}$ e

$$\forall (a,b),(c,d) \in G,\ (a,b) * (c,d) = (2ac, 2bc - \frac{2c-d}{2a}).$$

Seja H o conjunto dos elementos de G que comutam com todos os elementos de G, isto é $H = \{x \in G : \forall y \in G,\ x * y = y * x\}$. Calcule explicitamente H. Quais os elementos de G cujo quadrado pertence a H?

Exercício 20. Seja $< G, \cdot >$ um grupo e e o seu elemento neutro. Mostre que, se $xyz = e$ então $yzx = zxy = e$. Dê um exemplo em que $yxz \neq e$. No sentido de generalizar este resultado, que conclusão pode tirar se $x_1 x_2 \cdots x_n = e$, sendo $n \in \mathbb{N}$ e $x_1, x_2, \ldots, x_n \in G$?

Exercício 21. Seja $< S, * >$ um grupóide com elemento neutro tal que

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

Mostre que S é um monóide comutativo.

Exercício 22. Mostre que o grupóide $< \mathbb{R}, * >$ em que $*$ é definida por $x * y = 2x + 3y$ para $x, y \in \mathbb{R}$, não é associativo nem tem elemento neutro mas para quaisquer $a, b \in \mathbb{R}$ as equações $a * x = b$ e $y * a = b$ admitem uma e uma só solução.

Exercício 23. Enuncie o Teorema 1.1.13 e o Lema 1.1.15 em notação aditiva.

Exercício 24. Mostre que um semigrupo que contém um idempotente cancelável é um monóide.

Exercício 25. Mostre que o produto cartesiano de grupos é abeliano se e só se cada um dos grupos o for.

Exercício 26. Sejam G um grupo e $S = \{x : x^2 = e\}$. Quais das seguintes hipóteses são possíveis?

a) $|S| = 0$;
b) $|S| = 1$;
c) $|S| = 2$;
d) $S = G$;
e) $|S| > 2$;
f) S infinito.

Exercício 27. Seja G um grupo. Mostre que, se G satisfaz **qualquer uma** das seguintes condições, então G é abeliano:

a) $\forall a, b \in G$, $bab = a$;
b) $\forall a, b \in G$, $(ab)^2 = a^2 b^2$;
c) $\forall a, b \in G$, $(ab)^{-1} = a^{-1} b^{-1}$.

Exercício 28. Sejam G um grupo e $a, b \in G$. Mostre que:

a) se $a^5 b^3 = a^8 b^5 = e$ então $a = b = e$;
b) se $a^5 = e$ e $aba^{-1} = b^2$ então $b^{31} = e$;
c) se $n \in \mathbb{N}$, $a^n = e$ e $aba^{-1} = b^s$ então $b^{s^n - 1} = e$;
d) se $b^6 = e$ e $ab = b^4 a$ então $b^3 = e$ e $ab = ba$;
e) se $a^{-1}ba = b^{-1}$ e $b^{-1}ab = a^{-1}$. então $a^4 = b^4 = e$.

1.2 Subgrupos

Seja $< S, \cdot >$ um grupóide e $A, B \subseteq S$. Escrevemos AB para denotar o conjunto $\{ab : a \in A,\ b \in B\}$. Note-se que em geral AB e BA são conjunto diferentes. Se $a \in S$, usaremos a notação aA e Aa para denotar $\{a\}A$ e $A\{a\}$, respectivamente. Se estivermos na presença de um grupo, escreveremos A^{-1} para denotar o conjunto formado pelos inversos de elementos de A.

Diz-se que A é estável para a operação do grupóide se $AA \subseteq A$, ou seja, se

$$\forall a, b \in A, \quad ab \in A.$$

Por exemplo, o conjunto formado pelos inteiros ímpares é um subconjunto de $\mathbb{Z}$ estável para a operação produto mas não para a operação soma e $\mathbb{Z}$ é um subconjunto de $\mathbb{R}$ estável para as operações soma e produto.

Se $< G, \cdot >$ é um semigrupo e A é um subconjunto de G não vazio e estável para a operação $\cdot$, então $< A, \cdot >$ é um semigrupo. Mas se G é um grupo, $< A, \cdot >$ pode não ser um grupo, nem mesmo um monóide: por exemplo, $< \mathbb{N}, + >$ não é um monóide, apesar de $< \mathbb{Z}, + >$ ser um grupo e $\mathbb{N}$ ser um subconjunto de $\mathbb{Z}$ estável para a operação $+$. Veremos que um exemplo nestas condições não existe se A for finito.

Definição 1.2.1. *Seja $< G, \cdot >$ um grupo e H um subconjunto de G. Dizemos que H é um* **subgrupo** *de G, e notamos $H \leq G$, se:*

a) *o elemento neutro de G pertence a H;*

b) *$\forall a, b \in H,\ ab \in H$ (ou seja $HH \subseteq H$);*

c) *$\forall a \in H,\ a^{-1} \in H$ (ou seja $H^{-1} \subseteq H$).*

Na presença da segunda e terceira condição na definição de subgrupo, a primeira condição é equivalente a "H é não vazio". A terceira condição é equivalente a $H^{-1} = H$ e, na presença da primeira condição, a segunda é equivalente a $HH = H$, uma vez que $H = eH \subseteq HH \subseteq H$. Quando à segunda e a terceira condição, elas podem ser substituídas por uma só. Temos assim o seguinte resultado.

Teorema 1.2.2 (Critério de subgrupo)**.** *Seja $< G, \cdot >$ um grupo e H um subconjunto de G. Então H é um subgrupo de G se e só se satisfaz as condições:*

a) *$H \neq \emptyset$;*

b) *$\forall a, b \in H,\ ab^{-1} \in H$.*

Demonstração. Seja e o elemento neutro de G. É claro que, se H é um subgrupo de G então H é não vazio pois $e \in H$. Por outro lado, se a e b são elementos de H então $b^{-1} \in H$ porque H é fechado para a "inversão" e $ab^{-1} \in H$ porque H é fechado para o produto.

Inversamente, seja H um subconjunto não vazio de G satisfazendo as condições a) e b) deste teorema e seja $a \in H$. Por b) concluímos que $e \in H$ pois $e = aa^{-1}$ e que $a^{-1} \in H$ porque $a^{-1} = ea^{-1}$. Usando este resultado e novamente b) podemos concluir que, se $a, b \in H$, então ab pertence a H pois $ab = a\left(b^{-1}\right)^{-1}$. □

Se G é um grupo e e é o seu elemento neutro, então $\{e\}$ e G são subgrupos de G, que se dizem **subgrupos triviais**.

O seguinte lema é uma consequência imediata da definição de subgrupo.

Lema 1.2.3. *Se G é um grupo e $(S_i)_{i\in I}$ é uma família não vazia (isto é $I \neq \emptyset$) de subgrupos de G então $\bigcap_{i\in I} S_i$ é um subgrupo de G.* □

Temos então que, se G é um grupo e A é um subconjunto de G, a intersecção de todos os subgrupos que contêm A é o menor subgrupo contendo A.

Definição 1.2.4. *Se G é um grupo e A é um subconjunto de G define-se* **subgrupo gerado por** *A, e denota-se por $< A >$, como sendo o menor subgrupo de G contendo A. Diz-se que G (ou um subgrupo de G) é* **cíclico** *se for gerado por um só elemento.*

Se $A = \{a\}$ e escreveremos $< a >$ em vez de $< \{a\} >$. A primeira questão que se coloca é a de saber como calcular $< a >$. Note-se que $< a >=< a^{-1} >$, uma vez que qualquer subgrupo que contenha a contem necessariamente a^{-1} e vice-versa.

Proposição 1.2.5. *Se a é um elemento de um grupo $< G, \cdot >$, então*

$$< a >= \{a^n : n \in \mathbb{Z}\}.$$

Demonstração. Como $a \in < a >$ e $< a >$ que é fechado para o "produto" e a "inversão", então $< a >$ contem todas as potências positivas e negativas de a. Por outro lado, facilmente se mostra que o conjunto $\{a^n : n \in \mathbb{Z}\}$ é um subgrupo de G que contem a e, portanto $< a > \subseteq \{a^n : n \in \mathbb{Z}\}$ (por definição de $< a >$). □

Definição 1.2.6. *Chamamos* **ordem** *de um grupo $< G, \cdot >$ ao cardinal de G. Se a é um elemento de um grupo, chamamos ordem de a à ordem de $< a >$ e denotá-la-emos por* $\operatorname{ord} a$.

Note-se que o elemento neutro de um grupo tem ordem 1. Por outro lado um grupo finito G é cíclico se e só se existir $a \in G$ tal que $\operatorname{ord} a = |G|$.

Exemplos 1.2.7. *$< \mathbb{Z}, + >$ é um grupo cíclico infinito e gerado por 1 (ou por -1). Se $n \in \mathbb{N}$ $< \mathbb{Z}_n, +_n >$ é um grupo cíclico gerado por 1 (ou por $n-1$) e com n elementos. Veremos mais tarde que estes são "essencialmente" os únicos grupos cíclicos.*

Os grupos $\mathbb{Z}_n^*$ não são em geral cíclicos. Por exemplo $\mathbb{Z}_8^*$ é um grupo com 4 elementos, 1, 3, 5 e 7 sendo que 1 tem ordem 1 e os outros têm ordem 2. Por outro lado $\mathbb{Z}_5^*$ é um grupo cíclico de 4 elementos e é gerado por 2, por 3 e por 4.

O Corolário 1.1.16 significa, neste contexto, que todo o grupo cujos elementos têm ordem 1 ou 2, é necessariamente abeliano.

Definição 1.2.8. *Chamamos grupo de Klein a um grupo de 4 elementos cujos elementos diferentes da identidade têm todos ordem 2.*

Da Nota 1.1.18 sabemos que a tabela de Cayley de um grupo de Klein é da forma

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

.

Note-se que o grupo não é cíclico mas todos os seus subgrupos próprios ($\{e\}$, $\{e, a\}$, $\{e, b\}$, $\{e, c\}$) são cíclicos.

Dois exemplos de grupos de Klein são os grupos $\mathbb{Z}_2 \times \mathbb{Z}_2$ e $\mathbb{Z}_8^*$ como vimos acima.

Teorema 1.2.9. *Seja G um grupo e seja a um elemento de G. As seguintes condições são equivalentes:*

a) $< a >$ *é finito;*

b) $\exists n, m \in \mathbb{Z}$ *tais que* $a^n = a^m$ *e* $n \neq m$*;*

c) $\exists n \in \mathbb{N}$ *tal que* $a^n = e$*;*

d) $\exists n \in \mathbb{N}$ *tal que* $< a >= \{e, a, \ldots, a^{n-1}\}$.

Demonstração.

a) $\Rightarrow$ b)

É uma consequência imediata da igualdade $< a >= \{a^k : k \in \mathbb{Z}\}$.

b) $\Rightarrow$ c)

Suponhamos que $a^n = a^m$ com $n > m$. Então (multiplicando por a^{-m}) $a^n a^{-m} = a^m a^{-m}$ e por conseguinte $a^{n-m} = e$.

c) $\Rightarrow$ d)

Seja $n \in \mathbb{N}$ tal que $a^n = e$. Mostremos que $< a >= \{e, a, \ldots, a^{n-1}\}$, ou seja, que

$$\forall k \in \mathbb{Z},\ \exists r \in \{0, 1, \ldots, n-1\}, a^k = a^r.$$

Seja então $k \in \mathbb{Z}$. Usando o algoritmo da divisão sabemos que

$$\exists q \in \mathbb{Z},\ \exists r \in \{0, 1, \ldots, n-1\} : k = qn + r,$$

e portanto $a^k = a^{qn+r} = a^{qn} a^r = (a^n)^q a^r = e^q a^r = e a^r = a^r$.

d) $\Rightarrow$ a) Imediato. □

Como corolário temos o seguinte resultado que "caracteriza" a ordem dos subgrupos cíclicos finitos.

Corolário 1.2.10. *Se a é um elemento de um grupo G, então a* $\operatorname{ord} a$ *é o menor inteiro positivo k tal que $a^k = e$. Além disso, se $n, m \in \mathbb{Z}$ então $a^n = a^m$ se e só se k divide $n - m$. Em particular, $a^n = e$ se e só se k divide n.*

Demonstração. Seja k o menor inteiro positivo tal que $a^k = e$. Atendendo ao lema anterior e à sua demonstração sabemos que $< a >= \{e, a, \ldots, a^{k-1}\}$. Para concluir que $| < a > | = k$ basta mostrar que

$$\forall s, t \in \{0, 1, \ldots, k-1\}, \quad \left[s \neq t \Rightarrow a^s \neq a^t\right].$$

Suponhamos que existiam s, t em $\{0, 1, \ldots, k-1\}$ com $s > t$ tais que $a^s = a^t$. Então $a^{s-t} = e$, o que é absurdo por definição de k.

Sejam agora $n, m \in \mathbb{N}$. Usando o algoritmo da divisão sejam $q \in Z$ e $r \in \mathbb{N}$ tais que $n - m = qk + r$ e $0 \leq r < k$. Assim $a^{n-m} = a^{qk+r} = \left(a^k\right)^q a^r = a^r$. Deste modo

$$a^n = a^m \quad \Leftrightarrow \quad a^{n-m} = e \ \Leftrightarrow \ a^r = e$$

Mas como $0 \leq r < k$ e atendendo à definição de k, $a^r = e$ se e só se $r = 0$ ou seja, se e só se k divide $n - m$. □

Corolário 1.2.11. *Sejam G e H grupos e $a \in G$ e $b \in H$. Se a e b têm ordens finitas então a ordem de (a, b) (no grupo $G \times H$) é igual ao mínimo múltiplo comum entre* $\operatorname{ord} a$ *e* $\operatorname{ord} b$. *Em particular, se G e H são grupos finitos então $G \times H$ é cíclico se e só se G e H são cíclicos e as suas ordens forem primas entre si.*

Além disso, se $a \in G$ e $b \in H$ são tais que $G =< a >$ e $H =< b >$ e G e H têm ordens primas entre si, então $G \times H =< (a, b) >$.

Demonstração. Atendendo ao corolário anterior, $\operatorname{ord}(a, b)$ é o menor k tal que $(a, b)^k = (e_G, e_H)$. Mas

$$\begin{aligned}(a,b)^k = (e_G, e_H) &\Leftrightarrow \left(a^k = e,\ b^k = e\right)\\ &\Leftrightarrow \operatorname{ord} a \text{ e } \operatorname{ord} b \text{ dividem } k, \quad \text{pelo corolário anterior,}\\ &\Leftrightarrow \text{o mínimo múltiplo comum entre } \operatorname{ord} a \text{ e } \operatorname{ord} b \text{ divide } k.\end{aligned}$$

Deste modo $\operatorname{ord}(a, b)$ é o menor múltiplo comum entre $\operatorname{ord} a$ e $\operatorname{ord} b$ ($mmc(\operatorname{ord} a, \operatorname{ord} b)$). Recorde-se que $mmc(\operatorname{ord} a, \operatorname{ord} b) = \frac{\operatorname{ord} a \cdot \operatorname{ord} b}{mdc(\operatorname{ord} a, \operatorname{ord} b)}$.

Além disso, se G e H são finitos,

$$\begin{aligned}G \times H \text{ é cíclico} &\Leftrightarrow \exists\,(x,y) \in G \times H : < (x,y) >= G \times H\\ &\Leftrightarrow \exists\,(x,y) \in G \times H :\ \operatorname{ord}(x,y) = |G| \cdot |H|\\ &\Leftrightarrow \exists\,(x,y) \in G \times H :\ mmc(\operatorname{ord} x, \operatorname{ord} x) = |G| \cdot |H|\\ &\Leftrightarrow \exists x \in G\ \exists y \in H :\ \frac{\operatorname{ord} x \cdot \operatorname{ord} y}{mdc(\operatorname{ord} x, \operatorname{ord} y)} = |G| \cdot |H|\\ &\Leftrightarrow \exists x \in G\ \exists y \in H :\ \operatorname{ord} x = |G|,\ \operatorname{ord} y = |H|,\\ &\qquad\qquad mdc(\operatorname{ord} x, \operatorname{ord} y) = 1\\ &\Leftrightarrow G \text{ e } H \text{ são cíclicos e as suas ordens são primas entre si.}\end{aligned}$$

A penúltima equivalência é uma consequência do facto de $\operatorname{ord} x \leq |G|$, $\operatorname{ord} y \leq |H|$ e $mdc(\operatorname{ord} x, \operatorname{ord} y) \geq 1$.

A última afirmação do enunciado é verdadeira uma vez que, nas condições referidas $|< (a, b) >|$ é igual a $|< a >| \times |< b >|$, que é igual a $|G \times H|$. □

Vamos agora definir outros subgrupos importantes na teoria de grupos.

Definição 1.2.12. *Seja G um grupo e $a \in G$. Define-se* **normalizador de** *a, e denota-se por N_a, como sendo o conjunto*

$$\{x \in G : ax = xa\}.$$

Isto é, o normalizador de a é o conjunto dos elementos de G que comutam com a.

É claro que a identidade de um grupo e todas as potências (positivas ou negativas) de um elemento a pertencem ao normalizador de a. Dito de outra forma, $< a >\subseteq N_a$.

Lema 1.2.13. *Se G é um grupo e $a \in G$, então N_a é um subgrupo de G.*

Demonstração. Como N_a é não vazio (pois $< a > \subseteq N_a$) resta-nos mostrar que, se x e y pertencem a N_a, então xy^{-1} também pertence a N_a (ver Teorema 1.2.2. Mas

$$\begin{aligned} xy^{-1}a = axy^{-1} &\Leftrightarrow xy^{-1}ay = ax \quad \text{“multiplicando” a equação por } y \\ &\Leftrightarrow xy^{-1}ya = ax \quad \text{porque } y \text{ pertence a } N_a \\ &\Leftrightarrow xa = ax \\ &\Leftrightarrow x \in N_a. \end{aligned}$$

Donde se conclui que $xy^{-1} \in N_a$. □

Num grupo abeliano o normalizador de qualquer elemento é o próprio grupo.

Definição 1.2.14. *Seja G um grupo. Define-se* **centro** *de G, e denota-se por Z_G, como sendo o conjunto*

$$\{x \in G : \forall y \in G,\ xy = yx\}.$$

Isto é, o centro de G é o conjunto dos elementos de G que comutam com todos os elementos de G.

Proposição 1.2.15. *Se G é um grupo então:*

a) *G é abeliano se e só se $G = Z_G$;*

b) *o elemento neutro de G pertence a Z_G;*

c) $Z_G = \bigcap_{a \in G} N_a$;

d) *Z_G é um subgrupo de G.*

Demonstração. As afirmações a), b) e c) são consequência imediata das definições e a d) decorre de c), do lema anterior e do do Lema 1.2.3. □

Vamos agora calcular o centro de dois grupos não abelianos.

Exemplos 1.2.16. *Consideremos o grupo $GL(n, \mathbb{R})$ (ver página 3). Vejamos que o centro deste grupo é formado pelas matrizes da forma λI_n em que em que I_n é a matriz identidade e $\lambda \in \mathbb{R} \setminus \{0\}$. Para simplificar vamos considerar o caso em que $n = 2$.*

Se $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ pertence ao centro de $GL(2, \mathbb{R})$ então comuta com as matrizes $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ e $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Feitas as contas concluímos que $a = d$ e $b = c = 0$. Por outro lado, é óbvio que as matrizes da forma λI comutam com qualquer matriz de $GL(2, \mathbb{R})$.

Vejamos agora um exemplo de um grupo cujo centro se resume ao elemento neutro. Seja G o grupo formado pelas bijecções de $\{0, 1, 2\}$ em $\{0, 1, 2\}$. É claro que a função identidade pertence ao centro de G. Seja $f \in G$ e suponhamos que $f(a) = b$ e $a \neq b$ $(a, b \in \{0, 1, 2\})$. Consideremos $g : \mathbb{R} \to \mathbb{R}$ tal que $g(a) = c$, $g(c) = a$ e $g(b) = b$, sendo $c \in \{0, 1, 2\} \setminus \{a, b\}$. Note-se que g é uma bijecção e que $f \circ g \neq g \circ f$ uma vez que $(g \circ f)(a) \neq (f \circ g)(a)$.

1.2.1 Exercícios

Exercício 1. Seja G um grupo e $A = \emptyset$. A que é igual $< A >$?

Exercício 2. Quais os subgrupos de $\mathbb{Z}_8$? Quais os elementos de $\mathbb{Z}_8$ que geram $\mathbb{Z}_8$?

Exercício 3. Sejam G um grupo, H um subgrupo de G e $a \in G$. Mostre que, aHa^{-1} e H^{-1} são subgrupos G.

Exercício 4. Sejam G um grupo abeliano e H um seu subconjunto não vazio. Mostre que $\{xy^{-1} : x, y \in H\}$ é um subgrupo de G.

Exercício 5. Sejam G um grupo, $a, b \in G$ e $H \leq G$. Mostre que $Ha = Hb$ se e só se $a^{-1}H = b^{-1}H$.

Exercício 6. Sejam G um grupo, $a \in G$ e $H, K \leq G$. Mostre que $aH \cap aK = a(H \cap K)$.

Exercício 7. Sejam G um grupo, H, K subgrupos de G. Mostre que:

a) $H \cup K$ é um subgrupo de G se e só se $K \subseteq H$ ou $H \subseteq K$;

b) HK é um subgrupo de G se e só se $HK = KH$.

Exercício 8. Seja G um grupo e H um seu subconjunto finito não vazio e fechado para o produto. Mostre que H é um subgrupo de G. De facto não é necessário exigir que H seja finito mas sim que todo o elemento de H tenha ordem finita.

Exercício 9. Sejam G um grupo e $a, x \in G$. Mostre que $\operatorname{ord} a = \operatorname{ord}(xax^{-1})$.

Exercício 10. Seja G um grupo e a um seu elemento diferente do elemento neutro. Mostre que a $\operatorname{ord} a = 2$ se e só se $a = a^{-1}$.

Exercício 11. Seja G um grupo e $a \in G$ com ordem ímpar. Mostre que a equação $x^2 = a$ admite solução.

Exercício 12. Mostre que todo o grupo de ordem 3 ou 5 é cíclico.

Exercício 13. Mostre que qualquer grupo infinito tem uma infinidade de subgrupos.

Exercício 14. Mostre que todo o subgrupo do grupo aditivo dos inteiros é cíclico.

Exercício 15. Seja G um grupo $a, b \in G$. Mostre que ab e ba têm a mesma ordem.

Exercício 16. Seja G um grupo abeliano e $T(G)$ o conjunto formado pelos elementos de G com ordem finita.

a) O que é $T(G)$, se $G = \mathbb{R} \setminus \{0\}$ ou $G = \mathbb{C} \setminus \{0\}$ (com a multiplicação usual)?

b) Mostre que $T(G)$ é um subgrupo de G.

Exercício 17. Seja G um grupo, $a \in G$ e $k \in \mathbb{Z}$. Mostre que $\operatorname{ord} a^k = \frac{\operatorname{ord} a}{mdc(\operatorname{ord} a, k)}$. Conclua que $< a >=< a^k >$ se e só se $(\operatorname{ord} a, k) = 1$.

Exercício 18. Mostre que um grupo não trivial admitindo apenas subgrupos triviais é necessariamente cíclico e de ordem prima.

Exercício 19. Mostre que se c é um elemento de um grupo abeliano com ordem nm com $mdc(n, m) = 1$ então existem elementos a e b com ordens n e m tais que $c = ab$.

Exercício 20. Seja G um grupo gerado por $\{x, y\}$ tais que $yx = xy^3$. Mostre que,

a) $G = \{x^n y^m : n, m \in \mathbb{Z}\}$;

b) Se $\operatorname{ord} x = s$ e $\operatorname{ord} y = t$ então $|G| \leq st$.

Exercício 21. Sejam a e b elementos de um grupo abeliano G.

a) Mostre que a ordem de $\operatorname{ord} ab \leq \operatorname{ord} a \cdot \operatorname{ord} b$.

b) Conclua que o conjunto formado pelos elementos de G com ordem finita é um subgrupo de G.

c) Mostre que, se $mdc(\operatorname{ord} a, \operatorname{ord} b) = 1$, então $\operatorname{ord} ab = \operatorname{ord} a \cdot \operatorname{ord} b$.

Exercício 22. Seja G um grupo abeliano finito.

a) Mostre que o produto dos elementos de G é igual ao produto dos elementos de G com ordem 1 ou 2.

b) Demonstre o Teorema de Wilson que diz que $(p-1)! \equiv -1 \pmod{p}$, se $p \in \mathbb{P}$. **Sugestão:** Considere o grupo $\mathbb{Z}_p^*$.

Exercício 23. Considere $G = \mathbb{R} \times (\mathbb{R} \setminus \{0\})$ com a operação binária definida em G por $(x, y) \circ (z, t) = (z + tx + 3t, yt)$.

a) Mostre que $< G, \circ >$ é um grupo.

b) Calcule Z_G.

c) Determine os elementos de G cujo quadrado pertence a Z_G.

d) Verifique se o conjunto $\left\{\left(z, \frac{17+4z}{5}\right) : z \in \mathbb{R} \setminus \{-\frac{17}{4}\}\right\}$ é um subgrupo de G

Exercício 24. Considere $G = (\mathbb{Q} \setminus \{0\}) \times \mathbb{Q}$ com a operação binária definida em G por $(a, b) \circ (c, d) = \left(2ac, 2bc - \frac{2c-d}{2a}\right)$.

a) Mostre que $< G, \circ >$ é um grupo.

b) Determine as soluções da equação $(4, 2) \circ (x, y) = (x, y) \circ (2, 4)$.

c) Calcule Z_G.

d) Determine os elementos de G cujo quadrado pertence a Z_G.

Exercício 25. Seja $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R}, ac \neq 0 \right\}$.

a) Determine Z_G.

b) Determine o normalizador de $\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$.

c) Resolva a equação $X^2 = I$.

d) Mostre que o produto de dois elementos de ordem 2 pode ter ordem infinita.

Exercício 26. Seja G um grupo, $H \leq G$ e g um elemento de G com ordem n. Mostre que, se $g^m \in H$ e $mdc(n, m) = 1$, então $g \in H$. (Sugestão: considere $a, b \in \mathbb{Z}$ tais que $an + bm = 1$).

Exercício 27. Seja G um grupo que admite um só elemento de ordem 2. Mostre que esse elemento pertence a Z_G.

Exercício 28. Sejam G um grupo e $a, b \in G$ tais que $ab \in Z_G$. Mostre que a e b comutam.

Exercício 29. Sejam G um grupo e $a, b \in G$ tais que a, b, ab têm ordem 2. Mostre que $ab = ba$.

Exercício 30. Seja G um grupo tal que $a^2b^2 = b^2a^2$ para todo $a, b \in G$. Mostre que: $\{x \in G : \text{ordem de } x \text{ é ímpar}\}$ é um subgrupo de G.

Exercício 31. Mostre que, se $n \in \mathbb{Z}$, $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$ é um subgrupo do grupo aditivo dos inteiros. Mostre ainda que $\mathbb{Z}$ não admite mais subgrupos não triviais.

Exercício 32. Demonstre o Lema 1.2.3.

Exercício 33. Mostre que $\{1, -1, i, -i\}$ é um subgrupo cíclico de $< \mathbb{C} - \{0\}, \cdot >$. Mostre ainda que, para todo o $n \in \mathbb{N}$, existem subgrupos (quantos?) de $\mathbb{C} - \{0\}$ com n elementos.

Exercício 34. Seja o grupo $GL(2\mathbb{R})$ (ver página 3). Calcule o normalizador de $\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$. Mostre que $Z_G = \{xI : x \in \mathbb{R} - \{0\}\}$, em que I representa a identidade de G.

Exercício 35. Considere o grupo G dado pela tabela

$\cdot$	e	a	b	c	t	x	y	z
e	e	a	b	c	t	x	y	z
a	a	b	c	e	x	y	z	t
b	b	c	e	a	y	z	t	x
c	c	e	a	b	z	t	x	y
t	t	z	y	x	b	a	e	c
x	x	t	z	y	c	b	a	e
y	y	x	t	z	e	c	b	a
z	z	y	x	t	a	e	c	b

a) Calcule o normalizador de y.

b) Calcule o centro de G.

c) A equação $aX^2x^2 = b$ tem solução em G? Justifique.

Exercício 36. Mostre que, se H é um subgrupo próprio de um grupo G, então $G \setminus H$ gera G.

Exercício 37. Seja G um grupo de ordem p^2 (com $p \in \mathbb{P}$) e sejam $a, b \in G$ elementos com ordem p. Mostre que $< a > \cap < b >= \{e\}$. Conclua que G tem no máximo $p + 1$ subgrupos de ordem p.

1.3 Homomorfismos

Os homomorfismos entre grupóides, fazem o papel das funções na teoria de conjuntos, das aplicações lineares na teoria dos espaços vectoriais, das funções contínuas em topologia, das funções integráveis na teoria da medida, etc.. Vamos restringir-nos ao caso dos grupos, embora muitos dos resultados sejam válidos em condições mais gerais.

Definição 1.3.1. *Sejam $< G, \cdot >$ e $< H, * >$ dois grupóides. Uma função $f : G \longrightarrow H$ diz-se um* **homomorfismo** *(ou um* **endomorfismo** *se $< G, \cdot >=< H, * >$) se*

$$\forall x, y \in G \quad f(x \cdot y) = f(x) * f(y)$$

isto é, se f respeita as operações dos grupóides.

Se, além disso, f é uma bijecção, f diz-se um **isomorfismo** *(ou um* **automorfismo** *no caso em que $< G, \cdot >=< H, * >$).*

Se $< G, \cdot >$ e $< H, * >$ forem isomorfos escreveremos $< G, \cdot > \cong < H, * >$ ou simplesmente $G \cong H$, se não houver dúvidas sobre as operações binárias envolvidas.

Exemplos 1.3.2.

- *Se G é um grupo, então a função identidade de G em G é um automorfismo.*
- *Se G e H são grupos, então a função que associa a cada elemento de G o elemento neutro de H é um homomorfismo.*
- *A função* $\begin{array}{rccc} f: & \mathbb{R}^+ & \to & \mathbb{R} \\ & x & \mapsto & \log x \end{array}$ *é isomorfismo entre $< \mathbb{R}^+, \cdot >$ e $\mathbb{R}, + >$.*
- *Se $n \in \mathbb{N}$ a função* $\begin{array}{rccc} f: & \mathbb{Z} & \to & \mathbb{Z}_n \\ & k & \mapsto & k(mod\ n) \end{array}$ *é um homomorfismo;*
- *Seja G um grupo, $n \in \mathbb{Z}$ e consideremos* $\begin{array}{rccc} f: & G & \to & G. \\ & x & \mapsto & x^n \end{array}$ *Então*
  - *se G é abeliano f é um homomorfismo;*
  - *se $n = 2$ e G não é abeliano então f não é um homomorfismo (ver Exercício 27 da página 12);*
  - *se $n = -1$ então f é um homomorfismo se e só se G for abeliano (ver Exercício 4 da página 25).*

Proposição 1.3.3. *A composta de homomorfismo é ainda um homomorfismo. Mais concretamente, se $< G_1, *_1 >$, $< G_2, *_2 >$ e $< G_3, *_3 >$ são grupos, $f_1 : G_1 \to G_2$ e $f_2 : G_2 \to G_3$ são homomorfismos de grupo então $f_2 \circ f_1 : G_1 \to G_3$ é um homomorfismo.*

Demonstração. Se $x, y \in G_1$ então

$$\begin{aligned} (f_2 \circ f_1)(x *_1 y) &= f_2(f_1(x *_1 y)) \\ &= f_2(f_1(x) *_2 f_1(y)) \quad \text{porque } f_1 \text{ é um homomorfismo} \\ &= f_2(f_1(x)) *_3 f_2(f_1(y)) \quad \text{porque } f_2 \text{ é um homomorfismo} \\ &= (f_2 \circ f_1)(x) *_3 (f_2 \circ f_1)(y), \end{aligned}$$

o que mostra que $f_2 \circ f_1$ é um homomorfismo. □

Proposição 1.3.4. *Se $< G, \cdot >$ e $< H, * >$ são grupos e $f : G \longrightarrow H$ é um homomorfismo então:*

a) $f(e_G) = e_H$;

b) *se* $x \in G$ *então* $f(x^{-1}) = f(x)^{-1}$;

c) *se* f *é bijectivo então* f^{-1} *é um homomorfismo (bijectivo) de* H *em* G;

d) *se* $H_1 \leq H$, *então* $f^{-1}(H_1) \leq G$;

e) *se* $G_1 \leq G$, *então* $f(G_1) \leq H$;

f) *se* $x \in G$ *tem ordem finita então a ordem de* $f(x)$ *divide a ordem de* x.

Demonstração.
a) Como f é um homomorfismo, $f(e_G) * f(e_G) = f(e_G \cdot e_G) = f(e_G)$, ou seja $f(e_G)$ é um idempotente e portanto $f(e_G) = e_H$.

b) Mostrar que o inverso de $f(x)$ é $f(x^{-1})$ equivale a mostrar que $f(x) * f(x^{-1}) = e_H$. Como f é um homomorfismo,

$$f(x) * f(x^{-1}) = f(x \cdot x^{-1}) = f(e_G) = e_H.$$

c) Sejam $a, b \in H$ e mostremos que $f^{-1}(a * b) = f^{-1}(a) \cdot f^{-1}(b)$. Consideremos $x, y \in G$ tais que $f(x) = a$ e $f(y) = b$. Então

$$\begin{aligned} f^{-1}(a * b) &= f^{-1}(f(x) * f(y)) = f^{-1}(f(x \cdot y)) \quad \text{porque } f \text{ é um homomorfismo} \\ &= x \cdot y = f^{-1}(a) \cdot f^{-1}(b). \end{aligned}$$

Poderíamos ter notado que, como f é uma bijecção, $f^{-1}(a * b) = f^{-1}(a) \cdot f^{-1}(b)$ se e só se $f\left(f^{-1}(a * b)\right) = f\left(f^{-1}(a) \cdot f^{-1}(b)\right)$.

d) Como $e_H \in H_1$ e $f(e_G) = e_H$, concluiu-se que $e_G \in f^{-1}(H_1)$. Sejam agora $x, y \in f^{-1}(H_1)$ e mostremos que $x \cdot y^{-1} \in f^{-1}(H_1)$, ou seja, que $f(x \cdot y^{-1}) \in H_1$.

$$\begin{aligned} f(x \cdot y^{-1}) &= f(x) * f(y^{-1}) \quad \text{porque } f \text{ é um homomorfismo} \\ &= f(x) * f(y)^{-1} \quad \text{por b)} \end{aligned}$$

e $f(x) * f(y)^{-1} \in H_1$ porque $f(x), f(y) \in H_1$ e H_1 é um subgrupo de H.

e) Como $e_G \in G_1$ e $f(e_G) = e_H$, então $e_H \in f(G_1)$. Mostremos agora que, se $a, b \in f(G_1)$ então $a * b^{-1} \in f(G_1)$. Sejam $x, y \in G_1$ tais que $f(x) = a$ e $f(y) = b$. Então

$$\begin{aligned} a * b^{-1} &= f(x) * f(y)^{-1} = f(x) * f(y^{-1}) \quad \text{por b)} \\ &= f(x \cdot y^{-1}) \quad \text{porque } f \text{ é um homomorfismo.} \end{aligned}$$

Como G_1 é um subgrupo de G, $x \cdot y^{-1} \in G_1$ e portanto $a * b^{-1}$, que é igual a $f(x \cdot y^{-1})$, pertence a $f(G_1)$.

f) Se $\operatorname{ord} x = n$ então $f(x)^n = f(x^n) = f(e_G) = e_H$. Para concluir basta usar o Corolário 1.2.10. □

Da última alínea da proposição anterior podemos concluir que, se $n \in \mathbb{N}$, o único homomorfismo de $\mathbb{Z}_n$ em $\mathbb{Z}$ é o homomorfismo constante e igual a 0.

Dois grupos isomorfos têm as mesmas propriedades. Vejamos alguns exemplos com demonstração simples. Seja $f : G \to H$ um isomorfismo entre dois grupos. Então,

- se G é cíclico e gerado por um elemento a então H é cíclico e gerado por $f(a)$;
- se a é um elemento de G então a e $f(a)$ têm a mesma ordem;
- a imagem por f do centro de G é o centro de H.

Podemos agora caracterizar todos os grupos cíclicos.

Proposição 1.3.5. *Todo o grupo cíclico é isomorfo a $\mathbb{Z}$, se for infinito, ou a $\mathbb{Z}_n$, se tiver ordem n ($n \in \mathbb{N}$).*

Demonstração. Seja G um grupo cíclico infinito e seja a um seu gerador, isto é, tal que $< a >= G$. Então

$$\begin{array}{rccc} f: & \mathbb{Z} & \to & G \\ & n & \mapsto & a^n \end{array}$$

é um homomorfismo bijectivo porque pelo Teorema 1.2.9, $a^n = a^m$ se e só se $n = m$.

Seja agora G um grupo cíclico de ordem n e seja a um seu gerador. Então

$$\begin{array}{rccc} f: & \mathbb{Z}_n & \to & G \\ & k & \mapsto & a^k \end{array}$$

define um homomorfismo (porquê?) bijectivo. □

Usando esta proposição e o facto de a relação de isomorfismo ser uma relação de equivalência temos o seguinte resultado.

Corolário 1.3.6. *Se G e H são grupos cíclicos com a mesma ordem, então G e H são isomorfos.* □

Suponhamos que temos dois grupos "dados" pela sua tabela de Cayley. Qual o significado, em termos dessas tabelas de esses grupos serem isomorfos? Atendendo à definição de isomorfismo, dois grupos G e H são isomorfos se e só se existir uma bijecção $f : G \to H$ de tal modo que se substituirmos na tabela de Cayley de G cada elemento de G pela sua imagem por f, as duas tabelas são iguais, a menos da ordem das linhas e das colunas.

Exemplos 1.3.7. *Já sabemos que os grupo de ordem 2 e 3 são cíclicos e portanto são isomorfos a $\mathbb{Z}_2$ e $\mathbb{Z}_3$, respectivamente. Por outro lado $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ sao dois grupos de ordem 4 que não são isomorfos (o primeiro é cíclico e o segundo não).Pode-se facilmente mostrar que qualquer grupo de ordem 4 é isomorfo a $\mathbb{Z}_4$ se for cíclico, e a $\mathbb{Z}_2 \times \mathbb{Z}_2$ (grupo de Klein), caso contrário. Por outro lado $\mathbb{Z}_5$ é o único grupo de ordem 5.*

Temos assim que, a menos de isomorfismo, há apenas 6 grupos com ordem até cinco.

Note-se ainda que $\mathbb{Z}_n \times \mathbb{Z}_m$ é cíclico se e só se n e m são primos entre si (ver Corolário 1.2.11). Em particular e usando a Proposição 1.3.5, $\mathbb{Z}_n \times \mathbb{Z}_m$ e $\mathbb{Z}_{mn}$ são isomorfos se e só se n e m forem primos entre si.

Usando o que é dito atrás mostra-se que, por exemplo, $\mathbb{Z}_{210} \times \mathbb{Z}_{1800} \cong \mathbb{Z}_{600} \times \mathbb{Z}_{630}$. A ideia é notar que $\mathbb{Z}_{210} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$, $\mathbb{Z}_{1800} \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{5^2}$, $\mathbb{Z}_{600} \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}$ e $\mathbb{Z}_{630} \cong \mathbb{Z}_2 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \times \mathbb{Z}_7$.

A seguinte definição e teorema são o análogo do que acontece quando estamos a lidar com aplicações lineares de um espaço vectorial num outro.

Definição 1.3.8. *Seja $\varphi : G \to K$ um homomorfismo de grupos. Define-se* **núcleo** *de φ e denota-se por* $\operatorname{Nuc}\varphi$*, como sendo o conjunto*

$$\varphi^{-1}(\{e_K\}) = \{a \in G : \varphi(a) = e_K\}.$$

Se olharmos para Exemplos 1.3.2 podemos notar que: o núcleo do primeiro e do terceiro homomorfismos se reduzem ao elemento neutro do domínio, uma vez que as funções consideradas são injectivas; no segundo caso o núcleo é o próprio grupo G; no quarto exemplo, o núcleo é formado pelos múltiplos de n; no último caso o núcleo é formado pelos elementos de G cuja ordem divide n (ver a parte final do Corolário 1.2.10).

Lema 1.3.9. *Se $\varphi : G \to K$ é um homomorfismo de grupos e $x, y \in G$ então $\varphi(x) = \varphi(y)$ se e só se $xy^{-1} \in \operatorname{Nuc}\varphi$.*

Demonstração. Basta notar que, se $x, y \in G$ então,

$$\begin{aligned}
\varphi(x) = \varphi(y) &\Leftrightarrow \varphi(x)\left(\varphi(y)\right)^{-1} = e_K, \quad \text{multiplicando à direita por } (\varphi(y))^{-1} \\
&\Leftrightarrow \varphi(x)\varphi(y^{-1}) = e_K, \quad \text{Pela Proposição 1.3.4, alínea b)} \\
&\Leftrightarrow \varphi(xy^{-1}) = e_K, \quad \text{porque } \varphi \text{ é um homomorfismo,}
\end{aligned}$$

o que conclui a demonstração. □

Teorema 1.3.10. *Se $\varphi : G \to K$ é um homomorfismo de grupos então* $\operatorname{Nuc}\varphi$ *é um subgrupo de G. Além disso, φ é injectivo se e só se* $\operatorname{Nuc}\varphi = \{e_G\}$.

Demonstração. Se $x, y \in \operatorname{Nuc}\varphi$ então

- $\varphi(x^{-1}) = \varphi(x)^{-1} = e_K^{-1} = e_K$ pela Proposição 1.3.4, alínea b);
- $\varphi(xy) = \varphi(x)\varphi(y) = e_K e_K = e_K$ porque φ é um homomorfismo;

Deste modo, usando ainda a alínea a) da Proposição 1.3.4, podemos concluir que $\operatorname{Nuc}\varphi \leq G$. Podíamos também ter usado a Proposição 1.3.4, alínea d), para tirar a mesma conclusão.

Por outro lado é óbvio que, se φ é injectivo e $x \in \operatorname{Nuc}\varphi$ então $x = e_G$ pois $\varphi(x) = \varphi(e_G)$. Inversamente, se $\operatorname{Nuc}\varphi = \{e_G\}$, $x, y \in G$ e $\varphi(x) = \varphi(y)$ então, pelo lema anterior, $xy^{-1} = e_G$ ou seja, multiplicando a igualdade à direita por y, $x = y$. □

1.3.1 Exercícios

Exercício 1. Sejam $< G, \cdot >$ e $< H, * >$ dois grupóides e $f : G \longrightarrow H$ homomorfismo.

a) Mostre que, se e é um idempotente de G, então $f(e)$ é um idempotente de H.

b) É verdade que, se G admite elemento neutro, então H também admite elemento neutro? E se f for sobrejectiva?

c) É verdade que, se G é um grupo e f é sobrejectiva, então H é um grupo? E se G for finito?

d) Mostre que, se G é um semigrupo e f é sobrejectiva, então H é um semigrupo.

e) Mostre que, se G é abeliano e f é sobrejectiva, então H é abeliano.

f) Mostre que se G e H são grupos, G é gerado por um conjunto A e f é sobrejectiva, então H é gerado por $f(A)$.

Exercício 2. Mostre que, se $f : G \to H$ é um isomorfismo de grupos e $x \in G$ então a ordem de x é igual à ordem de $f(x)$.

Exercício 3. Mostre que, se $< G_1, *_1 >, < G_2, *_2 >, < H_1, \circ_1 >, < H_2, \circ_2 >$ são grupóides tais que $< G_1, *_1 > \cong < H_1, \circ_1 >$ e $< G_2, *_2 > \cong < H_2, \circ_2 >$ então $< G_1, *_1 > \times < G_2, *_2 > \cong < H_1, \circ_1 > \times < H_2, \circ_2 >$. Generalize.

Exercício 4. Seja G um grupo, mostre que a função $G \to G$ que a cada elemento de G associa o seu inverso é um homomorfismo se e só se G for abeliano.

Exercício 5. Seja G um grupo e, para cada $a \in G$ considere-se $f_a : G \to G$ definida por $f_a(x) = axa^{-1}$, para $x \in G$. Mostre que:

a) se $a \in G$ então f_a é um isomorfismo;

b) se $a, b \in G$ então $f_a \circ f_b = f_{ab}$;

c) se $a \in G$ então f_a é a identidade se e so se $a \in Z_G$;

d) se $a \in G$ e $h : G \to G$ é um isomorfismo então $h \circ f_a \circ h^{-1} = f_{h(a)}$.

Exercício 6. Mostre que todo o grupo de ordem dois, três ou cinco é cíclico (e portanto, isomorfo a $\mathbb{Z}_2$, a $\mathbb{Z}_3$ ou a $\mathbb{Z}_5$).

Exercício 7. Mostre que todo o grupo de ordem quatro é isomorfo a $\mathbb{Z}_4$, se for cíclico, ou ao grupo de Klein, caso contrário.

Exercício 8. Dê um exemplo de um grupo de ordem 30 não isomorfo a $\mathbb{Z}_{30}$.

Exercício 9. Quais dos seguintes grupos são isomorfos: $\mathbb{Z}_{24}$, $\mathbb{Z}_8 \times \mathbb{Z}_3$, $\mathbb{Z}_{12} \times \mathbb{Z}_2$, $\mathbb{Z}_6 \times \mathbb{Z}_4$, $\mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_2$?

Exercício 10. Mostre que $\mathbb{Z}_{90} \times \mathbb{Z}_{84}$ e $\mathbb{Z}_6 \times \mathbb{Z}_{1260}$ são isomorfos.

Exercício 11. Sejam $n, m \in \mathbb{N}$ $d = mdc(n, m)$ e $D = mmc(n, m)$. Mostre que $\mathbb{Z}_n \times \mathbb{Z}_m$ e $\mathbb{Z}_d \times \mathbb{Z}_D$ são isomorfos.

Exercício 12. Mostre que, se φ é um homomorfismo sobrejectivo entre os grupos G e H, então $\varphi(Z_G)$ está contido em Z_H.

Exercício 13. Sejam G_1, G_2, G_3 grupos abelianos finitos tais que $G_1 \times G_2$ e $G_1 \times G_3$ são isomorfos. Mostre que G_2 e G_3 são isomorfos.

Exercício 14. Considere $\mathbb{R} \setminus \{-1\}$ com a operação definida por $x \circ y = x + y + xy$.

a) Mostre que $< \mathbb{R} \setminus \{-1\}, \circ >$ é um grupo.

b) Mostre que $\begin{array}{rccc} \varphi: & \mathbb{R} \setminus \{0\} & \longrightarrow & \mathbb{R} \setminus \{-1\} \\ & x & \mapsto & x-1 \end{array}$ é um isomorfismo (consideramos $\mathbb{R} \setminus \{0\}$ com a operação produto usual).

c) Resolva em $< \mathbb{R} \setminus \{-1\}, \circ >$ a equação $x^4 = 15$.

Exercício 15. Quais os homomorfismos de $\mathbb{Z}_{10}$ em $\mathbb{Z}_{15}$?

Exercício 16. Mostre que o grupo $\mathbb{Z}_{15}^*$ é isomorfo ao produto dos seus subgrupos $< 2 >$ e $< 11 >$.

Exercício 17. Mostre que os grupos multiplicativos $\mathbb{C} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ e $\mathbb{Q} \setminus \{0\}$ não são isomorfos dois a dois.

Exercício 18. Seja $G =< a >$, em que a ordem de a é 120. Encontre um homomorfismo h de G em G tal que $h(a^{22}) = a^{14}$ e $h(a^{91}) = a^{47}$. O homomorfismo h é um isomorfismo?

Exercício 19. Diga se o grupo considerado no Exercício 35 da página 20 é isomorfo a um produto de dois grupos.

Exercício 20. Considere o grupo $\mathbb{Z}^2$ com a operação de adição usual. Mostre que a função

$$\begin{array}{rccc} f: & \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}^2 \\ & (x,y) & \mapsto & (x+y, x-y) \end{array}$$

é um homomorfismo e calcule o seu núcleo.

Exercício 21. Considere os grupos $< \mathbb{R}, + >$, $< \mathbb{C} \setminus \{0\}, \cdot >$ e $< S^1, \cdot >$ (onde $S^1 = \{z \in \mathbb{C} : |z| = 1\}$). Mostre que as funções

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & S^1 \\ & x & \mapsto & e^{2\pi i x} \end{array} \qquad \begin{array}{rccc} g: \mathbb{C} \setminus \{0\} & \longrightarrow & S^1 \\ z & \mapsto & \frac{z}{|z|} \end{array}$$

são homomorfismos e calcule os seus núcleos.

Exercício 22. Encontre um homomorfismo de grupo de domínio $GL(n.\mathbb{R})$ ($n \in \mathbb{N}$) cujo núcleo seja formado pelas matrizes de determinante igual a 1.

1.4 Grupos de Permutações

Nesta secção vamos tratar de grupos cujos elementos são chamados permutações. Estes grupos são importantes uma vez que todo o grupo é isomorfo a algum grupo de permutações (Teorema de Cayley).

Historicamente estes grupos são também importantes pois foram os primeiros grupos a serem convenientemente definidos.

Definição 1.4.1. *Seja X um conjunto não vazio. Uma* **permutação** *sobre X é uma função bijectiva de X em X.*

Se X é um conjunto não vazio e S_X é o conjunto de todas as permutações sobre X, então S_X tem uma estrutura natural de grupóide $< S_X, \circ >$, onde $\circ$ denota a composição de funções. Temos assim um primeiro resultado.

Proposição 1.4.2. *Se X é um conjunto não vazio então $< S_X, \circ >$ é um grupo.*

Demonstração. É claro que $\circ$ é uma operação associativa, que 1_X (a identidade em X) é o elemento neutro de S_X e que, se $f \in S_X$ então a inversa de f é também o inverso, no grupóide $< S_X, \circ >$, de f. □

Suponhamos que $n \in \mathbb{N}$, $X = \{a_1, a_2, \ldots, a_n\}$ e f é uma permutação sobre X. Denotamos, em geral, f por uma matriz do tipo

$$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}.$$

Eventualmente, quando não houver confusão quanto ao conjunto X, e se um elemento x de X for invariante por f, omitiremos na representação "matricial" de f a coluna relativa a x.

Por exemplo, se $X = \{1, 2, 3, 4\}$ e $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$, escreveremos $f = \begin{pmatrix} 1 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix}$.

Nota 1.4.3. *Se X é um conjunto com n elementos, então $|S_X| = n!$.* □

Denotaremos por S_n ($n \in \mathbb{N}$) o grupo das permutações de $\{1, 2, \ldots, n\}$. É evidente que se X é um conjunto com n elementos, então S_X é isomorfo a S_n.

Exemplo 1.4.4. *Vamos agora fazer o estudo do grupo S_3. À esquerda apresentamos os elementos de S_3è à direita a tabela do grupo.*

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Podemos então, por análise desta tabela, concluir que o centro de S_3 se reduz ao elemento neutro (o que já sabíamos - ver Exemplos 1.2.16), e portanto S_3 não é um grupo abeliano. Facilmente se vê que os subgrupos não triviais de S_3 são

$$\{\rho_0, \mu_1\},\ \{\rho_0, \mu_2\}, \{\rho_0, \mu_3\},\ \{\rho_0, \rho_1, \rho_2\}.$$

O seguinte teorema generaliza o que foi dito para o grupo S_3.

Teorema 1.4.5. *Se X é um conjunto com mais de 2 elementos então o Z_{S_X}, o centro de S_X, reduz-se ao elemento neutro.*

Demonstração. Suponhamos que σ é um elemento de S_X que é diferente da identidade. Neste caso existe $a \in X$ tais que $\sigma(a) \neq a$. Consideremos $c \in X \setminus \{a, \sigma(a)\}$ e seja $\mu \in S_X$ tal que $\mu(a) = c$, $\mu(c) = a$ e $\mu(x) = x$ para $x \in X \setminus \{a, c\}$. Assim,

$$\sigma(\mu(a)) = \sigma(c) \quad \text{e} \quad \mu(\sigma(a)) = \sigma(a)$$

e portanto, $\sigma(\mu(a)) \neq \mu(\sigma(a))$ pois $\sigma(a) \neq \sigma(c)$ uma vez que σ é uma bijecção. Concluímos assim que σ não pertence ao centro de S_X. □

Definição 1.4.6. *Um grupo diz-se um* **grupo de permutações** *se for um subgrupo de S_X, para algum conjunto X.*

Teorema 1.4.7 (Cayley, 1854)**.** *Todo o grupo é isomorfo a um grupo de permutações.*

Demonstração. Seja $< G, \cdot >$ um grupo. Mostremos que G é isomorfo a um subgrupo de S_G. Para cada $a \in G$ considere-se $f_a : G \to G$ tal que $f_a(x) = ax$, para todo $x \in G$. Note-se que f_a é uma permutação pois $f_{a^{-1}}$ é a sua inversa. Por outro lado, se $a, b \in G$, então $f_{a \cdot b} = f_a \circ f_b$ (verifique). Estas observações mostram que

$$\begin{array}{rccc} \psi: & G & \to & S_G \\ & a & \mapsto & f_a \end{array}$$

está bem definido e é um homomorfismo.

Vejamos que ψ é injectivo. Se $a, b \in G$ e $\psi(a) = \psi(b)$, então, sendo e o elemento neutro de G, $\psi(a)(e) = \psi(b)(e)$. Mas $\psi(a)(e) = f_a(e) = a$ e $\psi(b)(e) = f_b(e) = b$.

Como ψ é injectivo, G é isomorfo a $\psi(G)$ que é um grupo de permutações. □

Exemplo 1.4.8. *Como exemplo de aplicação do Teorema de Cayley, vamos calcular, um grupo de permutações isomorfo ao grupo de Klein.*

Seja $G = \{e, a, b, c\}$ o grupo de Klein (ver tabela da página 14)). Temos então (com as notações usadas na demonstração do Teorema de Cayley)

$$f_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}, \quad f_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix},$$

$$f_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}, \quad f_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}.$$

e a tabela de $\psi(G)$ é

$\cdot$	f_e	f_a	f_b	f_c
f_e	f_e	f_a	f_b	f_c
f_a	f_a	f_e	f_c	f_b
f_b	f_b	f_c	f_e	f_a
f_c	f_c	f_b	f_a	f_e

.

1.4.1 O grupo diedral

Uma **simetria** de um n-ágono regular define-se intuitivamente como sendo um "modo de sobrepor" duas cópias desse n-ágono. Uma simetria de um n-ágono regular pode ser visto como uma permutação no conjunto dos n vértices desse n-ágono. É claro que o conjunto dessas simetrias constitui um subgrupo de $S_{\{\text{vértices do } n\text{-ágono}\}}$.

Definição 1.4.9. *Seja $n \in \mathbb{N}$. Define-se* **grupo diedral de ordem** n*, e denota-se por D_n, como sendo o grupo das simetrias de um n-ágono regular.*

Quais os elementos de D_n? Temos as rotações de 0, $\frac{2\pi}{n}$, $\frac{4\pi}{n}$, $\frac{6\pi}{n}$, $\ldots$, $\frac{2(n-1)\pi}{n}$ radianos e as reflexões relativamente aos eixos que passam pelo centro do n-ágono e por cada um dos vértices. Para n ímpar estas reflexões são em número de n, mas para n par, são $\frac{n}{2}$, porque o eixo que passa pelo vértice i e pelo centro, passa também pelo vértice $i+\frac{n}{2}$. Mas para n par temos ainda que considerar as $\frac{n}{2}$ reflexões relativas aos eixos que passam pelo centro do n-ágono e pelo ponto médio de cada lado do n-ágono.

Temos assim que, qualquer que seja n, D_n tem $2n$ elementos.

É claro que também poderíamos considerar o grupo das simetrias de polígonos não regulares, como por exemplo, o rectângulo ou o losango.

Vejamos agora os casos em que $n = 3$ e $n = 4$.

As simetrias do triângulo equilátero ($n = 3$) de vértices 1, 2 e 3 são as rotação de 0, $\frac{2\pi}{3}$ e de $\frac{4\pi}{3}$ radianos em torno do centro do triângulo e as reflexões relativamente às bissectrizes dos ângulos do triângulo. Verifica-se então que estas rotações são exactamente as permutações ρ_0, ρ_1 e ρ_2 e que as reflexões são as permutações μ_1, μ_2 e μ_3 (ver estudo do grupo S_3). Concluímos então que S_3 é isomorfo a D_3. Voltando à tabela de S_3, mas vista agora como a tabela de D_3, podemos concluir que a composta de rotações ou de reflexões é sempre uma rotação, e que a composta de uma rotação com uma reflexão e vice-versa é uma reflexão. Por análise dos subgrupos de D_3, podemos concluir que D_3 é gerado por qualquer subconjunto de D_3 que contenha pelo menos uma reflexão e uma rotação não trivial.

Consideremos agora $n = 4$. Qual o grupo D_4?

Temos as rotações em torno do centro de 0, $\frac{\pi}{2}$, π e de $\frac{3\pi}{2}$ radianos (ρ_0, ρ_1, ρ_2 e ρ_3), as reflexões relativamente às diagonais (δ_1 e δ_2) e aos bissectores de lados opostos (μ_1 e μ_2). Temos então que os 8 elementos D_4 são (chamando 1, 2, 3 e 4 aos vértices):

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \quad \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

A tabela de D_4 é em certa medida "parecida"com a de D_3.

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

Por análise à tabela podemos concluir que:

- $Z_{D_4} = \{\rho_0, \rho_2\}$;
- os subgrupos de D_4 são: $\{\rho_0\}, \{\rho_0, \mu_1\},\ \{\rho_0, \mu_2\}, \{\rho_0, \delta_1\},\ \{\rho_0, \delta_2\},\ \{\rho_0, \rho_2\},$ $\{\rho_0, \rho_1, \rho_2, \rho_3\},\ \{\rho_0, \rho_2, \mu_1, \mu_2\},\ \{\rho_0, \rho_2, \delta_1, \delta_2\},\ D_4$.

  Em particular, qualquer subconjunto de D_4 que contenha uma reflexão e uma rotação diferente de ρ_0 e de ρ_2 gera D_4.

- O produto de duas permutações do mesmo tipo (rotação ou reflexão) é uma rotação, enquanto o produto de permutações de tipo diferente é uma reflexão. Verifique que esta é uma propriedade de D_n, qualquer que seja n.

1.4.2 Ciclos

Vejamos uma outra notação muito usada para as permutações. Vamos começar por uma definição.

Definição 1.4.10. *Uma permutação σ sobre um conjunto X diz-se um* **ciclo de ordem** *n se existirem elementos distintos $a_1, a_2, \ldots, a_n \in X$, tais que*

$$\begin{cases} \sigma(a_1) = a_2,\ \sigma(a_2) = a_3,\ \ldots, \sigma(a_{n-1}) = a_n,\ \sigma(a_n) = a_1 \\ \sigma(x) = x, \quad \forall x \in X \setminus \{a_1, a_2, \ldots, a_n\}. \end{cases}$$

Um ciclo deste tipo denota-se por $\sigma = (a_1\ a_2\ \cdots\ a_n)$. No caso de $n = 1$, escreveremos (a_1) ou, simplesmente $(\ )$, que representa a permutação identidade.

Esta notação só pode ser usada quando não houver dúvidas quanto ao conjunto X.

Se $\sigma = (a_1\ a_2\ \cdots\ a_n)$, então, para todo o $i \in \{1, 2, \ldots, n\}$ e $j \in \mathbb{Z}$

$$\sigma^j(a_i) = a_r, \quad \text{em que } r \in \{1, 2, \ldots, n\} \text{ e } r \equiv i + j \ (\bmod\ n).$$

Por exemplo, se $n = 5$ e $\sigma = (a_1\ a_2\ a_3\ a_4\ a_5)$ então $\sigma^2 = (a_1\ a_3\ a_5\ a_4\ a_2)$, $\sigma^3 = (a_1\ a_4\ a_2\ a_5\ a_3)$, $\sigma^4 = (a_1\ a_5\ a_4\ a_3\ a_2)$ σ^5, $\sigma^{-1} = (a_1\ a_5\ a_4\ a_3\ a_2) = (a_5\ a_4\ a_3\ a_2\ a_1)$.

Concluímos então que a ordem de σ é n (o comprimento de σ). Por outro lado, $(a_1\ a_2\ \cdots\ a_n)^{-1} = (a_n\ a_{n-1}\ \cdots\ a_1)$.

Exemplo 1.4.11. *Se* $X = \{1, 2, 3, 4, 5, 6\}$*, então*

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

O produto de dois ciclos pode não ser um ciclo, como se vê pelo exemplo seguinte.

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

e

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

No entanto, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix}$ e $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$ não são ciclos. Note-se ainda que este exemplo mostra que o produto de ciclos pode não ser comutativo.

Definição 1.4.12. *Duas permutações* σ_1 *e* σ_2 *sobre um conjunto* X *dizem-se disjuntas se todo o elemento de* x *for invariante por uma das permutações, isto é, se*

$$\forall x \in X,\ \exists i \in \{1, 2\} \quad \sigma_i(x) = x.$$

Note-se que, se σ é uma permutação sobre X e $a \in X$ não é invariante por σ então $\sigma(a)$ também não é invariante por σ. Isto é uma consequência da injectividade de σ.

Lema 1.4.13. *Se* σ_1, σ_2 *são duas permutações disjuntas sobre um conjunto* X *então* $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$*.*

Demonstração. Seja $a \in X$. Se a é invariante por σ_1 e por σ_2 então $(\sigma_1 \circ \sigma_2)(a) = (\sigma_2 \circ \sigma_1)(a) = a$. Se a não é invariante por σ_1 (o outro caso tem tratamento igual) então $\sigma_1(a)$ também não é invariante por σ_1. Como σ_1 e σ_2 são disjuntos podemos concluir que a e $\sigma_1(a)$ são invariantes por σ_2. Deste modo $(\sigma_1 \circ \sigma_2)(a) = (\sigma_2 \circ \sigma_1)(a) = \sigma_1(a)$. □

Vejamos um exemplo para ilustrar a demonstração que toda a permutação sobre um conjunto finito é o produto (comutativo) de ciclos disjuntos.

Exemplo 1.4.14. *Considere-se a permutação* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix}$*. Note-se que* $\sigma(1) = 4$*,* $\sigma(4) = 2$ *e* $\sigma(2) = 1$*, fechando um ciclo. Escolhemos agora um elemento de* $\{1, 2, 3, 4, 5, 6\}$ *não pertencente a* $\{1, 4, 2\}$*, por exemplo o* 3*. Como* $\sigma(3) = 3$ *está fechado o ciclo. Finalmente* $\sigma(5) = 6$ *e* $\sigma(6) = 5$*. Conclui-se assim que*

$$\sigma = (1\ 4\ 2)(3)(5\ 6) = (1\ 4\ 2)(5\ 6) = (5\ 6)(1\ 4\ 2).$$

Seguindo o que foi feito para este exemplo, pode-se demonstrar o seguinte resultado.

Teorema 1.4.15. *Toda a permutação sobre um conjunto finito* X *é o produto (comutativo) de ciclos disjuntos.* □

Definição 1.4.16. *Um ciclo de comprimento* 2 *diz-se uma* **transposição**.

Uma transposição deixa todos os elementos invariantes, com excepção de dois que são enviados um no outro. Por este motivo o inverso de uma transposição é a própria transposição. Um cálculo simples mostra que

$$(a_1\ a_2\ \cdots\ a_n) = (a_1\ a_n)\cdots(a_1\ a_3)(a_1\ a_2).$$

E portanto, todo o ciclo é um produto de transposições. Usando este resultado e o Teorema 1.4.15 podemos então concluir o seguinte corolário.

Corolário 1.4.17. *Toda a permutação sobre um conjunto finito é um produto de transposições (não necessariamente disjuntas).* □

É claro que uma permutação sobre um conjunto finito, se pode escrever de muitas maneiras como um produto de transposições. Por exemplo, podemos sempre escrever a meio de uma qualquer decomposição de uma permutação sobre um conjunto X como produto de transposições, o produto $(a\ b)(b\ a)$ sem alterarmos o valor desse produto $(a, b \in X)$. Outro exemplo mais interessante é dado por

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

O que é verdade é que o número de transposições usadas numa decomposição desse tipo, é sempre par ou sempre ímpar.

Teorema 1.4.18. *Nenhuma permutação sobre um conjunto finito pode ser expresso simultaneamente como produto de um número par de transposições e como produto de um número ímpar de transposições.*

Demonstração. Sem perda de generalidade vamos supor que estamos a trabalhar com transposições sobre $\{1, 2, \ldots, n\}$ e que $n \geq 2$.

Primeiro passo. Vamos começar por mostrar que, se a permutação identidade $(\triangle)$ é um produto de k transposições, então k é par. Suponhamos então que

$$\triangle = \tau_1\tau_2\cdots\tau_k, \quad \text{onde cada } \tau_i \text{ é uma transposição.}$$

Escolha-se um inteiro m que aparece numa das transposições e seja τ_j a primeira transposição, contando da direita para a esquerda, na qual m aparece. É claro que j não pode ser 1, pois nesse caso, $\triangle(m) \neq m$. Temos então as seguintes hipóteses para $\tau_{j-1}\tau_j$

$$\tau_{j-1}\tau_j \quad = \quad \begin{cases} (m\ x)(m\ x) & = & \triangle & \text{ou} \\ (m\ y)(m\ x) & = & (m\ x)(x\ y) & \text{ou} \\ (x\ y)(m\ x) & = & (m\ y)(x\ y) & \text{ou} \\ (y\ z)(m\ x) & = & (m\ x)(y\ z) & \end{cases}$$

Se substituirmos $\tau_{j-1}\tau_j$ pelo valor encontrado, na factorização inicial de $\triangle$, reduzimos o número k de transposições em duas unidades (o que não muda a paridade), **ou** "empurramos" para a esquerda a primeira ocorrência de m. Repetimos este processo

até m ser eliminado da factorização (recordar que m não pode aparecer pela primeira vez na primeira transposição, e portanto a hipótese "$(m,x)(m,x)$" tem de ocorrer até fazer desaparecer m). Seguindo este processo para cada inteiro que apareça em alguma transposição, ao fim de um número finito de passos eliminamos todas as transposições. Uma vez que em cada passo do processo mantivemos o mesmo número de transposições ou diminuí-mo-lo em duas unidades, podemos concluir que k é par.

Segundo passo. Seja agora σ uma permutação qualquer sobre X. Suponhamos que

$$\sigma = \sigma_1\sigma_2\cdots\sigma_r = \delta_1\delta_2\cdots\delta_s,$$

em que $\sigma_1,\ldots,\sigma_r,\delta_1,\cdots,\delta_s$ são transposições. Queremos concluir que r e s têm a mesma paridade, ou seja, que $r+s$ é par.

Uma vez que toda a transposição é inversa dela própria, temos,

$$\begin{aligned}\triangle &= \sigma\sigma^{-1}\\ &= \sigma_1\sigma_2\cdots\sigma_r(\delta_1\delta_2\cdots\delta_s)^{-1}\\ &= \sigma_1\sigma_2\cdots\sigma_r(\delta_s)^{-1}\cdots(\delta_2)^{-1}(\delta_1)^{-1}\\ &= \sigma_1\sigma_2\cdots\sigma_r\delta_s\cdots\delta_2\delta_1.\end{aligned}$$

Assim $\triangle$ é o produto de $r+s$ transposições, e pelo que mostramos acima, $r+s$ é necessariamente par. □

Chamamos **par** (respectivamente **ímpar**) a uma permutação que se escreve como o produto de um número par (respectivamente ímpar) de transposições. Atendendo ao teorema anterior esta definição tem sentido. Note-se que o produto de permutações pares é ainda uma permutação par e que o inverso de uma permutação par é também uma permutação par.

Corolário 1.4.19. *Se $n\in\mathbb{N}$ e $\mathbb{Z}_2$ é o grupo aditivo dos inteiros módulo 2 então*

$$\begin{array}{rccc}\Phi: & S_n & \longrightarrow & \mathbb{Z}_2\\ & \sigma & \mapsto & \begin{cases}0 & \text{se } \sigma \text{ e par}\\ 1 & \text{se } \sigma \text{ e ímpar}\end{cases}\end{array}$$

é um homomorfismo de grupo. Em particular $\Phi^{-1}(\{0\})$ é um subgrupo de S_n.

O que o corolário diz é que: o produto de duas permutações é par se e só se tiverem a mesma paridade. Uma vez que o inverso de uma transposição é a própria transposição podemos concluir que o inverso de um produto de transposições é o produto dessas transposições pela ordem inversa. Em particular uma permutação tem a mesma paridade que o seu inverso. Daqui concluímos que a seguinte definição tem sentido.

Definição 1.4.20. *Chama-se* **grupo alterno** *com n elementos e denota-se por A_n ao grupo formado pelas permutações pares de S_n.*

Note-se que a função, se $n\geq 2$, $\Phi: A_n\to S_n\setminus A_n$ definida por $\Phi(\sigma)=\sigma\circ(1\ 2)$ é uma bijecção cuja inversa é definida por $\Phi^{-1}(\mu)=\mu\circ(1\ 2)$. Em particular o grupo A_n tem $\frac{n!}{2}$ elementos.

1.4.3 Exercícios

Exercício 1. Considere

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 2 & 1 & 8 & 5 & 7 & 6 \end{pmatrix}, \quad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 2 & 8 & 7 & 4 & 6 \end{pmatrix}.$$

Calcule:

a) σ^{-1} e μ^{-1}
b) $\sigma \circ \mu$;
c) $\mu \circ \sigma$;
d) $\mu \circ \sigma \circ \mu^{-1} \circ \sigma^{-1}$;
e) $\mu^2 \circ \sigma^2$;
f) $(\mu \circ \sigma)^{-2}$;
g) a ordem de σ e de μ;
h) σ^{23}.

Exercício 2. Exprima como produto de ciclos disjuntos:

a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 4 & 2 & 1 & 10 & 5 & 7 & 9 & 8 & 11 & 12 & 6 \end{pmatrix}$
b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 7 & 4 & 6 & 2 & 3 \end{pmatrix}$
c) $\sigma = (a\ b\ c\ d\ e)(a\ f)$;
d) $\sigma = (a\ d)(a\ b\ c\ d\ e\ f)$;
e) $\sigma = (a\ b\ c)(a\ b\ d)(a\ b\ e)(c\ d\ e)$.

Para cada uma das alíneas encontre a ordem de σ e calcule σ^{345}.

Exercício 3. Seja $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 6 & 3 \end{pmatrix}$. Escreva σ como produto de transposições. Encontre uma permutação de $\{1, 2, 3, 4, 5, 6\}$ que não comute com σ.

Exercício 4. Calcule $\sigma\alpha\sigma^{-1}$ em cada um dos seguintes casos:

a) $\sigma = (1\ 3\ 5)(1\ 2)$ e $\alpha = (1\ 5\ 7\ 9)$;
b) $\sigma = (5\ 7\ 9)$ e $\alpha = (1\ 2\ 3)(3\ 4)$;
c) $\sigma = (3\ 5\ 1\ 9)$ e $\alpha = (1\ 2\ 3)(3\ 4\ 1)(7\ 9)$;
d) $\sigma = (1\ 2)(3\ 4)$ e $\alpha = (1\ 2\ 3)(4\ 5)$.

Exercício 5. Encontre σ tal que $\sigma(1\ 2)(3\ 4)\sigma^{-1} = (5\ 6)(1\ 3)$.

Exercício 6. Mostre que não existe σ tal que $\sigma(1\ 2\ 3)\sigma^{-1} = (1\ 3)(5\ 7\ 8)$.

Exercício 7. Calcule os elementos do subgrupo de S_4 gerado por $\{(1\ 2\ 3), (1\ 2)(3\ 4)\}$.

Exercício 8. Seja $\sigma = (1\ 2)(3\ 4)\delta$ um elemento de S_7, em que $\delta = \delta^{-1}$ e δ mantém fixos os elementos $1, 2, 3$ e 4. Mostre que

$$\sigma^{-1}(2\ 3\ 4)\sigma(2\ 3\ 4)^{-1}(1\ 4\ 5)^{-1}\sigma^{-1}(2\ 3\ 4)\sigma(2\ 3\ 4)^{-1}(1\ 4\ 5)$$

é um ciclo de ordem 3.

Exercício 9. Quais das seguintes permutações são pares?

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 3 & 2 & 1 & 5 & 12 & 7 & 9 & 8 & 11 & 4 & 6 \end{pmatrix}$;

b) $(1\ 2)(1\ 3)(1\ 4)(1\ 5)$;

c) $(1\ 2\ 3)(1\ 2)$;

d) $(1\ 2\ 3\ 4\ 5)(1\ 2\ 3)(4\ 5)$;

e) $(1\ 2\ 3\ 4\ 5\ 6\ 7)(1\ 2)(2\ 3\ 4)$.

Determine a ordem de cada uma das permutações.

Exercício 10. Mostre que o grupo S_9 admite um elemento de ordem 20 e nenhum elemento de ordem 18.

Exercício 11. Mostre que o grupo S_7 não admite elementos de ordem maior que 12.

Exercício 12. Mostre que S_{10} tem elementos de ordem 10, 12 e 14 mas não de ordem 11 e 13.

Exercício 13. Dê um exemplo de um elemento de S_{13} com ordem 21 e que não deixe nenhum elemento invariante.

Exercício 14. Considere em S_6 o elemento $\sigma = (1\ 3\ 2\ 4)(5\ 6)$.

a) Encontre $\rho \in S_6$ tal que $\rho \circ \sigma \neq \sigma \circ \rho$.

b) Calcule σ^{413}.

Exercício 15. Qual o subgrupo de S_4 gerado por $\{(2\ 3\ 4), (1\ 4)(2\ 3)\}$? E por $\{(1\ 3), (1\ 2\ 3\ 4)\}$?

Exercício 16. Seja $n \in M$ com $n \geq 3$. Mostre que

a) o produto de duas transposições é igual à identidade, a um ciclo de comprimento 3 ou a um produto de dois ciclos de comprimento 3.

b) A_n é gerado pelo conjunto formado pelos ciclos de comprimento 3.

Exercício 17. Sejam $n, i, j \in \mathbb{N}$. Mostre que:

a) se $j - i \geq 2$ então $(i\ j) = (j-1\ j)(i\ j-1)(j-1\ j)$;

b) se $i \geq 2$ então $(i\ i+1) = (1\ 2\ 3\ \cdots\ n)^{i-1}(1\ 2)(1\ 2\ 3\ \cdots\ n)^{-i+1}$.

Exercício 18. Mostre (usando o exercício anterior) que, se $n \in \mathbb{N}$ então S_n é gerado por:

a) $\{(1\ 2), (2\ 3) \cdots\ (n-1, n)\}$;

b) por $\{(1\ 2), (1\ 2\ 3\ \ldots\ n)\}$.

Exercício 19. Quais os homomorfismos de:

a) S_3 em $10\mathbb{Z}$; b) S_3 em S_3; c) S_4 em $\mathbb{Z}_2 \times \mathbb{Z}_2$;

1.5 Divisores Normais

Seja G um grupo e $H \leq G$. Comecemos por notar que $HH = H$ uma vez que

$$\begin{array}{rcll} H = & eH & (e \text{ é o elemento neutro de } G) \\ \subseteq & HH & (e \in H) \\ \subseteq & H & (H \leq G). \end{array}$$

De seguida vamos encontrar condições necessárias e suficientes para que conjuntos do tipo aH e bH sejam iguais.

Proposição 1.5.1. *Se G é um grupo e $H \leq G$ a relação binária sobre G definida por*

$$\forall a, b \in G: \quad \left(a \,\lambda_H\, b \Leftrightarrow a^{-1}b \in H\right)$$

é uma relação de equivalência sobre G. Além disso, se $a \in G$ a classe de equivalência de a módulo λ_H é o conjunto aH.

Em particular, se $a, b \in G$ então aH e bH são iguais ou disjuntos e são iguais se e só se $a^{-1}b \in H$ (ou equivalentemente, $b^{-1}a \in H$).

Demonstração. Para mostrar que λ_H é uma relação de equivalência basta usar o facto de H ser um subgrupo e notar que, se $a, b, c \in G$ então:

- $a \,\lambda_H\, a$ pois $a^{-1}a = e \in H$;
- se $a \,\lambda_H\, b$ então $b \,\lambda_H\, a$ pois $b^{-1}a = \left(a^{-1}b\right)^{-1}$;
- e $a \,\lambda_H\, b$ e $b \,\lambda_H\, c$ então $a \,\lambda_H\, c$ pois $a^{-1}c = \left(a^{-1}b\right)\left(b^{-1}c\right)$.

Para a segunda parte basta notar que

$$\begin{array}{rcl} \{x \in G : a \,\lambda_H\, x\} & = & \{x \in G : a^{-1}x \in H\} \;=\; \{x \in G : \exists h \in H,\ a^{-1}x = h\} \\ & = & \{x \in G : \exists h \in H,\ x = ah\} = aH. \end{array}$$

O restante é uma consequência do facto de λ_H ser uma relação de equivalência. □

Nas condições acima, λ_H diz-se a relação de equivalência sobre G **associada à esquerda** a H e as suas classes dizem-se **classes laterais esquerdas** de H.

Tudo isto tem uma versão *dual*. Chama-se ρ_H à relação binária sobre G, que se diz **associada à direita** ao subgrupo H , definida por

$$\forall x, y \in G: \quad \left(x \rho_H y \Leftrightarrow xy^{-1} \in H\right).$$

É claro que as classes (laterais direitas) de G são agora os conjuntos da forma Ha, com $a \in H$.

Temos então que G é uma união disjunta de classes esquerdas (direitas) de G relativamente a H, e que duas classes aH e bH (respectivamente, Ha e Hb) são iguais se e só se $a^{-1}b \in H$ (respectivamente, $ab^{-1} \in H$). Além disso, se $b \in aH$ (respectivamente, $b \in Ha$) então $aH = bH$ (respectivamente, $Ha = Hb$).

Se tivermos um grupo finito e um seu subgrupo H para calcular as classes laterais esquerdas (por exemplo) de G relativamente a H: começamos por considerar a classe H; escolhemos um elemento $a \in G \setminus H$ e calculamos aH; escolhemos de seguida um elemento $b \in G \setminus (H \cup aH)$ e calculamos bH, etc..

Exemplo 1.5.2. *Consideremos S_3, o grupo das permutações de um conjunto de três elementos cuja tabela é (ver Exemplo 1.4.4)*

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Seja $H = \{\rho_0, \rho_1, \rho_2\}$. Por análise da tabela, podemos concluir que

$$H = \rho_0 H = \rho_1 H = \rho_2 H, \quad \mu_1 H = \mu_2 H = \mu_3 H = \{\mu_1, \mu_2, \mu_3\},$$
$$H = H\rho_0 = H\rho_1 = H\rho_2, \quad H\mu_1 = H\mu_2 = H\mu_3 = \{\mu_1, \mu_2, \mu_3\}.$$

Em particular, qualquer que seja x em S_3, $xH = Hx$. Note que não é verdade que os elementos de H comutam com todos os elementos de G.

Considere agora o subgrupo $T = \{\rho_0, \mu_1\}$. As classes laterais são

$$T, \quad \rho_1 T = \{\rho_0, \mu_3\}, \quad \rho_2 T = \{\rho_0, \mu_2\}$$
$$T, \quad T\rho_1 = \{\rho_0, \mu_2\}, \quad T\rho_2 = \{\rho_0, \mu_3\}.$$

Note que $\rho_1 T \neq T\rho_1$ e que $\rho_2 T \neq T\rho_2$.

Lema 1.5.3. *Seja G um grupo e H um seu subgrupo. Então, qualquer classe esquerda ou direita tem o mesmo cardinal que H.*

Demonstração. Seja $a \in G$. Mostremos que H e aH (ou Ha) têm o mesmo cardinal. Para isso considere-se a função de H em aH (ou Ha) que associa a cada elemento x de H o elemento ax de aH (ou xa de Ha). Por definição de aH (ou Ha) a função é sobrejectiva e, pela lei do corte, é injectiva. □

Atendendo a este lema, a seguinte definição tem sentido.

Definição 1.5.4. *Se H é um subgrupo de um grupo G, define-se* **índice de H em G,** *e denota-se por $(H : G)$, como sendo o cardinal do conjunto das classes esquerdas ou das classes direitas de H relativamente a G.*

Podemos então concluir que G é a união disjunta de $(H : G)$ classes esquerdas (ou direitas), todas elas com o cardinal de H. Temos assim o seguinte corolário.

Corolário 1.5.5 (Teorema de Lagrange)**.** *Se G é um grupo e H um seu subgrupo, então*

$$|G| = |H| \times (H : G).$$

Em particular, se G é um grupo finito, a ordem de H divide a ordem de G. □

Como consequência do Teorema de Lagrange, se G é um grupo de ordem n ($n \in \mathbb{N}$) e $a \in G$, então a^n é o elemento neutro de G e portanto $\operatorname{ord} a$ divide n.

Se aplicarmos o Teorema de Lagrange ao grupo $\mathbb{Z}_n^*$ (ver Exemplo 1.1.8) obtemos o seguinte resultado, que é uma generalização do chamado Pequeno Teorema de Fermat.

Corolário 1.5.6. *Se n e a são inteiros positivos primos entre si, então*

$$a^{\varphi(n)} \equiv 1 (mod\ n).$$

Em particular, se n é primo $a^{n-1} \equiv 1 (mod\ n)$.

Demonstração. Seja r o resto da divisão de a por n. Note-se que, se $k \in \mathbb{N}$ então $a^k \equiv r^k$ e que dizer que $a^k \equiv 1 (mod\ n)$ é o mesmo que dizer, no grupo $\mathbb{Z}_n^*$, $a^k = 1$. □

Teorema 1.5.7. *Todo o grupo de ordem prima é cíclico e é gerado por qualquer elemento diferente do elemento neutro.*

Demonstração. Seja G um grupo de ordem prima e seja a um elemento de G diferente do elemento neutro de G. Como $| < a > |$ é diferente de 1 e divide $|G|$, que é um número primo, então $| < a > | = |G|$ e portanto $< a >= G$. □

Concluímos ainda, usando a Proposição 1.3.5, que todo o grupo de ordem p (com p primo) é isomorfo a $\mathbb{Z}_p$.

O Teorema de Lagrange simplifica muito a procura dos subgrupos de um grupo. Por exemplo, usando usando este teorema é muito fácil encontrar os subgrupos próprios de S_3 pois todos eles são cíclicos.

Definição 1.5.8. *Seja G um grupo e H um seu subgrupo. Diz-se que H é um* **divisor normal** *(***subgrupo invariante***,* **subgrupo normal** *ou* **subgrupo auto-conjugado***) de G, e notamos $H \trianglelefteq G$, se*

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

As seguintes são observações muito simples. Se G é um grupo então:

- $\{e_G\}$ e G são divisores normais de G (ditos divisores normais triviais);
- se G é abeliano então todo o seu subgrupo é um divisor normal normal de G;
- todo o subgrupo de G contido em Z_G é um divisor normal de G.

A igualdade $xH = Hx$ não significa que os elementos de H comutem com x, como vimos no Exemplo 1.5.2. O mesmo acontece com todos os subgrupos de ordem 4 do grupo D_4. A igualdade $xH = Hx$ significa que

$$\forall h \in H\ \exists h_1, h_2 \in H :\ hx = xh_1 \ \text{ e } \ xh = h_2 x.$$

O seguinte é um resultado muito simples mas que será usado frequentemente.

Proposição 1.5.9. *Se G é um grupo e H um seu subgrupo de índice dois, então H é um divisor normal de G.*

Demonstração. Seja $a \in G \setminus H$. Como $G = H \cup aH$, sendo esta união disjunta temos $aH = G \setminus H$. Do mesmo modo $Ha = G \setminus H$. Daqui concluímos que $aH = Ha$. □

Deste resultado podemos concluir que o grupo alterno A_n é um divisor normal de S_n. Este resultado é também fácil de mostrar directamente uma vez que, se $\mu \in S_n$ e $\rho \in S_n$ então $\mu\rho\mu^{-1}$ é uma permutação par e por isso pertence a A_n.

Temos agora uma proposição que nos dá uma caracterização ligeiramente mais simples dos divisores normais de um grupo.

Proposição 1.5.10. *Seja G um grupo e H um seu subgrupo. As condições seguintes são equivalentes:*

a) $\forall x \in G \quad xH = Hx;$

b) $\forall x \in G \quad xHx^{-1} = H;$

c) $\forall x \in G \quad xH \subseteq Hx;$

d) $\forall x \in G \quad xHx^{-1} \subseteq H.$

Demonstração. As condições a) e b) bem como as condições c) e d) são trivialmente equivalentes. Como c) é uma condição "mais fraca" que a), para concluir a proposição, basta mostrar que a condição c) implica a condição a).

Suponhamos que H satisfaz c). Se $x \in G$ então

$$\begin{aligned} Hx &= xx^{-1}Hx \\ &\subseteq xHx^{-1}x, \quad \text{porque } x^{-1}H \subseteq Hx^{-1} \\ &= xH. \end{aligned}$$

o que completa a demonstração. □

Teorema 1.5.11. *Se H, K são divisores normais de um grupo G então $H \cap K$ e HK são divisores normais de G.*

Demonstração. Já sabemos que $H \cap K$ é um subgrupo de G. Seja agora $x \in G$ e $y \in H \cap K$. Então existem $h \in K$ e $k \in K$ tais que $xy = hx$ e $xy = kx$, porque $xH = Hx$ e $xK = Kx$. Da igualdade $hx = kx$ concluímos, usando a lei do corte, que $h = k$ e portanto $h \in H \cap K$. Isto mostra que $x\,(H \cap K) \subseteq (H \cap K)\,x$. Fica assim mostrado, usando a proposição anterior, que $H \cap K$ é um divisor normal de G.

Para mostrar que HK é um subgrupo de G só é necessário usar o facto de H e K serem subgrupos de G e um deles ser divisor normal (verifique!).

Para $x \in G$ temos

$$xHK = HxK = HKx, \quad \text{porque } H, K \trianglelefteq G,$$

e portanto $HK \trianglelefteq G$. □

Usando o mesmo raciocínio que acima, mostra-se que a intersecção qualquer de divisores normais de um grupo é ainda um divisor normal. Deste modo, dado um grupo G e um seu subgrupo (que pode não ser um divisor normal) tem sentido falar no menor divisor normal de G que contem H. Obviamente esse divisor normal terá de conter todos os conjuntos da forma xHx^{-1}, com $x \in G$. Por exemplo, se considerarmos o grupo S_3 e $H = \{\rho_0, \mu_1\}$ então $\bigcup_{x \in S_3} xHx^{-1} = \{\rho_0, \mu_1, \mu_2, \mu_3\}$. Note-se que esta união não é um subgrupo de S_3 e o menor subgrupo que a contem é o próprio S_3.

Por outro lado, se G for um grupo e H um seu subgrupo, então $\bigcup_{x \in S_3} xHx^{-1}$ é um subgrupo de G (pois é uma intersecção de subgrupos) que está contido em H (que é igual a eHe^{-1}). De facto mostra-se que esta intersecção é o maior divisor normal que está contido em H (ver Exercício 29).

O seguinte resultado será crucial em muito do que segue.

Teorema 1.5.12. *Sejam G um grupo e H e K divisores normais de G tais que $H \cap K = \{e\}$. Então*

a) *os elementos de H comutam com os elementos de K;*

b) *HK é isomorfo a $H \times K$;*

c) *se H e K são finitos $|HK| = |H||K|$.*

Demonstração.

a) Sejam $h \in H$ e $k \in K$. Mostrar que $hk = kh$ é o mesmo que mostrar que $hkh^{-1}k^{-1} = e$. Para isso basta mostrar que $hkh^{-1}k^{-1} \in H \cap K$.

Como $K \trianglelefteq G$ e $k \in K$ então $hkh^{-1} \in K$ e $k^{-1} \in K$ e portanto $hkh^{-1}k^{-1} \in K$. De modo análogo se mostra que $hkh^{-1}k^{-1} \in H$.

b) Considere-se a função

$$\begin{array}{rccc} \Psi: & H \times K & \to & HK. \\ & (h,k) & \mapsto & hk \end{array}$$

Ψ é sobrejectiva, por definição de HK, é um homomorfismo uma vez que, se $(h,k),(h_1,k_1) \in H \times K$ então

$$\begin{aligned} \Psi(h,k)\ \Psi(h_1,k_1) &= hkh_1k_1 \\ &= hh_1kk_1 \quad \text{pela alínea b)} \\ &= \Psi(hh_1, kk_1). \end{aligned}$$

Finalmente, Ψ é injectiva porque, se $(h,k),(h_1,k_1) \in H \times K$, então

$$\begin{aligned} \Psi(h,k) = \Psi(h_1,k_1) &\Rightarrow hk = h_1k_1 \\ &\Rightarrow h_1^{-1}h = k_1k^{-1} \\ &\Rightarrow \underbrace{h_1^{-1}h}_{\in H} = \underbrace{k_1k^{-1}}_{\in K} = e \quad \text{porque } H \cap K = \{e\} \\ &\Rightarrow h_1 = h,\ k_1 = k. \end{aligned}$$

□

Vamos agora mostrar que o conjunto formado pelas classes laterais esquerdas (ou direitas) de um grupo relativamente a um seu divisor normal tem uma estrutura natural de grupo.

Lema 1.5.13. *Seja G um grupo e H um seu subgrupo. Então*

$$\forall a, b \in G \; aH\, bH = abH.$$

Como consequência, se $a, b, x, y \in G$, $xH = aH$ e $yH = bH$, então $xyH = abH$.

Demonstração. Se $a, b \in G$ então

$$\begin{aligned} abH &= aebH \\ &\subseteq aHbH \quad \text{porque } e \in H \\ &= abHH \quad \text{porque } Hb = bH \\ &= abH \quad \text{porque } H \leq G. \end{aligned}$$

Daqui se conclui que $aH\, bH = abH$. □

De facto, um subgrupo que satisfaça a condição do lema ($\forall a, b \in G \; aH \cdot bH = abH$) é necessariamente um divisor normal. Isto acontece porque, se $x \in G$ então

$$\begin{aligned} xHx^{-1} &\subseteq xHx^{-1}H \quad \text{por que } e \in H \\ &= xx^{-1}H \quad \text{pela hipótese considerada} \\ &= H. \end{aligned}$$

Denotemos por G/H o conjunto das classes laterais esquerdas (ou direitas) de um grupo G relativamente a um seu divisor normal H, isto é

$$G/H = \{aH : a \in G\}.$$

Teorema 1.5.14. *Se G é um grupo e $H \trianglelefteq G$, então $< G/H, \cdot >$ em que,*

$$\forall a, b \in G \; aH \cdot bH = abH,$$

é um grupo. Além disso a função (dita função de projecção) de G em G/H que associa a cada elemento de G a sua classe lateral módulo H, é um homomorfismo.

Demonstração. A associatividade da operação sobre G/H é uma consequência da associatividade da operação sobre G. O elemento neutro de G/H é H (a classe de qualquer elemento de H) e o inverso de um elemento aH de G/H é $a^{-1}H$. □

Como consequência do Teorema de Lagrange, podemos concluir que, se G é um grupo finito e H é um divisor normal de G, então

$$|G/H| = (H : G) = \frac{|G|}{|H|}.$$

Vimos no Teorema 1.3.10 que o núcleo de um homomorfismo $\varphi : G \to K$ era um subgrupo de G. De facto esse núcleo é um divisor normal e temos mais: todo o divisor normal de G é o núcleo de algum homomorfismo cujo domínio é G.

Teorema 1.5.15. *Um subconjunto H de um grupo G é um divisor normal de G se e só se é o núcleo de um homomorfismo definido em G.*

Demonstração. Se H é um divisor normal de G então a função projecção de G em G/H é um homomorfismo cujo núcleo é H.

Inversamente, seja $\varphi : G \to K$ um homomorfismo de grupos. Note-se que

- $\varphi(e_G) = e_H$;
- se $a, b \in \operatorname{Nuc}\varphi$ então $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e_H e_H^{-1} = e_H$;
- se $a \in \operatorname{Nuc}\varphi$ e $x \in G$ então $\varphi(xax^{-1}) = \varphi(x)\varphi(a)\varphi(x^{-1}) = \varphi(x)e_H\varphi(x)^{-1} = \varphi(x)\varphi(x)^{-1} = e_H$ e, portanto $xax^{-1} \in \operatorname{Nuc}\varphi$.

Mostramos assim que $\operatorname{Nuc}\varphi$ é um divisor normal de G. □

Obtemos assim, dado um homomorfismo $\varphi : G \to K$, um grupo quociente $G/\operatorname{Nuc}\varphi$.

Lema 1.5.16. *Se $\varphi : G \to K$ é um homomorfismo de grupos e $a, b \in G$ então $\varphi(a) = \varphi(b)$ se e só se $ab^{-1} \in \operatorname{Nuc}\varphi$. Em particular φ é injectivo se e só se o seu núcleo se reduz ao elemento neutro de G.*

Demonstração. Note-se que

$$\begin{aligned} \varphi(a) = \varphi(b) &\Leftrightarrow \varphi(a)\varphi(b)^{-1} = e_K \\ &\Leftrightarrow \varphi(a)\varphi(b^{-1}) = e_K \\ &\Leftrightarrow \varphi(ab^{-1}) = e_K \\ &\Leftrightarrow ab^{-1} \in \operatorname{Nuc}\varphi \end{aligned}$$

É claro que se φ é injectivo, então nenhum elemento diferente de e_G pode ter imagem e_K e portanto o núcleo de φ reduz-se ao elemento neutro de G.

Inversamente, se $\operatorname{Nuc}\varphi = \{e_G\}$ e $a, b \in G$, então

$$\begin{aligned} \varphi(a) = \varphi(b) &\Leftrightarrow ab^{-1} \in \operatorname{Nuc}\varphi \\ &\Leftrightarrow ab^{-1} = e_G \quad \text{porque } \operatorname{Nuc}\varphi = \{e_G\} \\ &\Leftrightarrow a = b. \end{aligned}$$

Daqui se conclui que φ é injectivo. □

Temos agora o chamado Teorema Fundamental do Homomorfismo, que relaciona as imagens homomorfas de um grupo com os seus grupos quocientes.

Teorema 1.5.17 (Teorema Fundamental do Homomorfismo)**.** *Se $\varphi : G \to K$ é um homomorfismo sobrejectivo entre os grupos G e K, então $G/\operatorname{Nuc}\varphi$ é isomorfo a K.*

Demonstração. Notemos que, se $a, b \in G$, então

$$\begin{aligned} \varphi(a) = \varphi(b) &\Leftrightarrow ab^{-1} \in \operatorname{Nuc}\varphi \quad \text{pelo lema anterior} \\ &\Leftrightarrow a\operatorname{Nuc}\varphi = b\operatorname{Nuc}\varphi. \end{aligned}$$

O que mostra (porquê?) que a função ψ, de $G/\operatorname{Nuc}\varphi$ em K que associa ao elemento $a\operatorname{Nuc}\varphi$ o elemento $\varphi(a)$, está bem definida e é injectiva. Como φ é sobrejectiva, então ψ é sobrejectiva. Por outro lado, facilmente se vê que ψ é um homomorfismo.

Concluímos então que ψ é um isomorfismo. □

Se no enunciado do teorema anterior não exigirmos a sobrejectividade de φ, podemos concluir que $G/\text{Nuc}\,\varphi$ é isomorfo a $\varphi(G)$.

Usando o teorema fundamental do homomorfismo, mostrar que um certo grupo quociente G/H é isomorfo a um grupo K equivale a definir um homomorfismo sobrejectivo de G em K cujo núcleo seja H. Vejamos alguns exemplos.

Exemplos 1.5.18.

1. *Seja $m \in \mathbb{N}$ e considere-se o homomorfismo de $< \mathbb{Z}, + >$ em $< \mathbb{Z}_m, +_m >$ que associa a cada elemento $a \in \mathbb{Z}$ o resto da divisão de a por m. Este homomorfismo (sobrejectivo) tem $m\mathbb{Z}$ por núcleo, e portanto $\mathbb{Z}/m\mathbb{Z}$ é isomorfo a $\mathbb{Z}_m$.*

2. *Seja $n \in \mathbb{N}$ e seja A_n o conjunto das permutações pares de $\{1, 2, \ldots, n\}$. Então A_n é o núcleo do homomorfismo de S_n em $\mathbb{Z}_2$ que associa a cada permutação a sua paridade (isto é: 0 se for par e 1 se for ímpar). Concluímos então que A_n é um divisor normal de S_n e que $S_n/A_n \cong \mathbb{Z}_2$.*

3. *Consideremos o grupo aditivo $\mathbb{R}\setminus\{0\}$ e o seu subgrupo $\mathbb{R}^+$. A função f de $\mathbb{R}\setminus\{0\}$ em $\mathbb{Z}_2$ tal que $f(x)$ é igual a 0 se x é positivo e igual a 1, caso contrário, é um homomorfismo cujo núcleo é $\mathbb{R}^+$. Deste modo e que $\mathbb{R}\setminus\{0\}/\mathbb{R}^+ \cong \mathbb{Z}_2$.*

Teorema 1.5.19. *Se G é um grupo e H e K são divisores normais de G então*

$$(HK)/K \;\cong\; H/(H \cap K).$$

Em particular, se H e K são finitos, então $|HK| = \frac{|H||K|}{|H\cap K|}$.

Demonstração. Consideremos a função

$$\begin{array}{rccc} \Psi: & H & \to & HK/K \\ & h & \mapsto & hK \end{array}$$

Note-se que Ψ é um homomorfismo uma vez que, se $h_1, h_2 \in H$ então

$$\begin{aligned} \Psi(h_1)\psi(h_2) &= h_1Kh_2K \\ &= h_1h_2KK \quad \text{porque } K \trianglelefteq G \\ &= h_1h_2K \quad \text{porque } K \leq G \\ &= \Psi(h_1h_2). \end{aligned}$$

Vejamos que Ψ é sobrejectivo. Seja $xK \in HK/K$. Então existem $h \in H$ e $k \in K$ tais que $x = hk$. Deste modo $xK = hkK = hK$, porque $K \leq G$, e portanto $xK = \Psi(h)$.

Finalmente,

$$\text{Nuc}\,\Psi = \{h \in H :\; hK = K\} = \{h \in H : h \in K\} = H \cap K.$$

Usando o Teorema Fundamental do Homomorfismo concluímos que $(HK)/K$ e $H/(H \cap K)$ são isomorfos.

Para a segunda parte basta recordar que, no caso em que os grupos envolvidos são finitos, $|(HK)/K| = \frac{|HK|}{|K|}$ e $|H/(H \cap K)| = \frac{|H|}{|H\cap K|}$. □

1.5.1 Exercícios

Exercício 1. Mostre que, se um grupo admite apenas um subgrupo de uma certa ordem então esse subgrupo é um divisor normal.

Exercício 2. Escolha um subgrupo de ordem dois do grupo de Klein e faça a tabela do respectivo grupo quociente. Mostre que esse grupo é isomorfo a $\mathbb{Z}_2$.

Exercício 3. Sejam G um grupo, $a, b \in G$ e $H, K \leq G$. Mostre que:

a) $aH \cap aK = a(H \cap K)$;

b) se $aH \cap bK \neq \emptyset$ então $aH \cap bK$ é uma classe lateral esquerda do subgrupo $H \cap K$.

Exercício 4. Sejam G um grupo e $a, g, h \in G$. Mostre que: $gN_a = hN_a$ se e só se $gag^{-1} = hah^{-1}$.

Exercício 5. Sejam G um grupo, $H, K \leq G$. Mostre que, se uma classe esquerda de H é igual a uma classe esquerda de K então $H = K$.

Exercício 6. Quais os divisores normais do grupo S_3.

Exercício 7. Seja $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b \in \mathbb{Q},\ ac \neq 0 \right\}$ munido do produto de matrizes. Mostre que $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Q} \right\}$ é um divisor normal de G.

Exercício 8. Sejam H e K dois subgrupos de um grupo finito G tais que $|H|, |K| > \sqrt{|G|}$. Mostre que $|H \cap K| > 1$.

Exercício 9. Seja G um grupo e $H = \{(g, g) : g \in G\}$. Mostre que $H \leq G \times G$ e que $H \trianglelefteq G \times G$ se e só se G for abeliano.

Exercício 10. Sejam G um grupo e H um divisor normal de G com 2 elementos. Mostre que $H \subseteq Z_G$.

Exercício 11. Sejam G um grupo e $H \trianglelefteq G$. Prove que G/H é abeliano se e só se $aba^{-1}b^{-1} \in H$ para quaisquer $a, b \in G$.

Exercício 12. Mostre que $Z_{18}/ < 3 > \cong \mathbb{Z}_3$.

Exercício 13. Prove que $H = \{(\ ), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ é um subgrupo normal de S_4. Indique um grupo isomorfo a S_4/H.

Exercício 14. Sejam G um grupo, $K \leq G$ e $H \trianglelefteq G$ tais que $H \cap K = \{e\}$ e $H \cup K = G$. Mostre que $G/H \cong K$.

Exercício 15. Sejam G um grupo H um seu subgrupo. Considere $N_G(H) = \{x \in G : xHx^{-1} = H\}$. Mostre que:

a) $H \subseteq N_G(H) \leq G$;

b) H é um divisor normal de $N_G(H)$;

c) $N_G(H)$ é o maior subgrupo de G onde H é um divisor normal.

Exercício 16. Seja G um grupo e H um divisor normal de G de índice n ($n \in \mathbb{N}$). Mostre que;

a) se $g \in G$ então $g^n \in H$;

b) se $g \in G$, $g^m \in H$ e $(n, m) = 1$ então $g \in H$.

Exercício 17. Seja G um grupo abeliano de ordem p^2, com p primo. Suponha que G não é cíclico e sejam $a, b \in G \setminus \{e_G\}$. Mostre que se $b \notin < a >$, então

$$G =< a >< b > \cong < a > \times < b > \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

Exercício 18. Sejam $G_1, \ldots, G_n$ grupos e $H_1, \ldots, H_n$ divisores normais de $G_1, \ldots, G_n$, respectivamente. Mostre que $H_1 \times \cdots \times H_n \trianglelefteq G_1 \times \cdots \times G_n$ e

$$(G_1 \times \cdots \times G_n) / (H_1 \times \cdots \times H_n) \cong G_1/H_1 \times \cdots \times G_n/H_n$$

Exercício 19. Sejam G um grupo e $H, K \trianglelefteq G$ com $K \subseteq H$.

a) Mostre que $H/K \trianglelefteq G/K$;

b) Mostre que $G/H \cong (G/K) / (H/K)$.
Sugestão: Considere a projecção natural de G em $(G/K) / (H/K)$.

Exercício 20. Considere o grupo $< \mathbb{Z}, + >$. Mostre que $\mathbb{Z}/H$ é finito qualquer que seja o subgrupo não trivial H (ver Exercício 31 da página 20). Conclua que $\mathbb{Z}$ não é isomorfo a um produto de grupos não triviais.

Exercício 21. Sejam G, K grupos, sendo H abeliano, e $\varphi : G \to K$ um homomorfismo. Mostre que todo o subgrupo de G que contém o núcleo de φ é um divisor normal.

Exercício 22. Mostre que todo o subgrupo finito de $\mathbb{Q}/\mathbb{Z}$ é cíclico.

Exercício 23. Considere o grupo G considerado no Exercício 35 da página 20. Verifique se G/Z_G é isomorfo ao grupo de Klein.

Exercício 24. Seja $S^1 = \{z \in \mathbb{C} : |z| = 1\}$, com a operação de multiplicação usual. Mostre que $\mathbb{R}/\mathbb{Z}$ é isomorfo a S^1 (use o Exercício 21 da página 21). Mostre ainda que $\mathbb{R}/a\mathbb{Z}$ é isomorfo a S^1, qualquer que seja $a \in \mathbb{R}$.

Exercício 25. Mostre que:

a) $(\mathbb{R} - \{0\})/\mathbb{R}^+ \cong \mathbb{Z}_2$;

b) $(\mathbb{C} - \{0\})/\mathbb{R}^+ \cong S^1$;

c) $(\mathbb{C} - \{0\})/(\mathbb{R} - \{0\}) \cong S^1/\{1, -1\}$;

d) $(\mathbb{C} - \{0\})/S^1 \cong \mathbb{R}^+$.

Exercício 26. Seja $G = \{(a, b) \in \mathbb{R}^2 : a \neq 0\}$. Defina a seguinte operação sobre G:

$$\forall (a, b), (x, y) \in G : \quad (a, b) \cdot (x, y) = (ax, ay + b).$$

Mostre que:

a) $< G, \cdot >$ é um grupo não abeliano;

b) $K = \{(1, b) : b \in \mathbb{R}\}$ é um divisor normal de G;

c) G/K é isomorfo a $\mathbb{R} \setminus \{0\}$ com a operação de multiplicação usual.

Exercício 27. Seja $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$.

a) Mostre que G é um subgrupo do grupo $GL(n, \mathbb{R})$.

b) Mostre que $Z_G = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}$ e que Z_G é isomorfo ao grupo aditivo dos números reais.

c) Mostre que G/Z_G é isomorfo ao grupo aditivo $\mathbb{R}^2$.

Exercício 28. Sejam G um grupo e $a_1, a_2, \ldots, a_n \in G$ ($n \in \mathbb{N}$) tais que $a_i a_j = a_j a_i$ para todo o $i, j \in \{1, 2, \ldots, n\}$. Mostre que, se $G/Z_G = \{a_1 Z_G, a_2 Z_G, \ldots, a_n Z_G\}$, então G é abeliano.

Exercício 29. Seja G um grupo finito e H um seu subgrupo próprio. Mostre que:

a) $\bigcap_{x \in G} xHx^{-1}$ é o maior divisor normal de G contido em H;

b) $\bigcup_{x \in G} xHx^{-1}$ é diferente de G.

Exercício 30. Seja $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : \det(A) = 1\}$.

a) Mostre que $SL(n, \mathbb{R})$ é um divisor normal de $GL(n, \mathbb{R})$.

b) Mostre que ainda $GL(n, \mathbb{R})/SL(n, \mathbb{R})$ é isomorfo ao grupo multiplicativo $\mathbb{R} \setminus \{0\}$.

Exercício 31. Considere o grupo $GL(2, \mathbb{R})$.

a) Mostre que $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ tem ordem 4, $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ tem ordem 3 e que ab tem ordem infinita.

b) Mostre que $\{A \in GL(2, \mathbb{R}) : A^t = A^{-1}\}$ é um subgrupo de $GL(2, \mathbb{R})$.

c) Verifique se H é um divisor normal de $GL(2, \mathbb{R})$.

d) Encontre um epimorfismo de G sobre um grupo abeliano.

Exercício 32. Considere $G = (\mathbb{R} \setminus \{0\}) \times \mathbb{R}$ com a operação binária definida em G por $(a, b) \circ (c, d) = (ac, ad + b)$.

a) Mostre que $< G, \circ >$ é um grupo.

b) Calcule Z_G.

c) Seja $K = \{(1, b) \in G\}$. Mostre que $K \trianglelefteq G$ e que G/K é isomorfo ao grupo multiplicativo $\mathbb{R} \setminus \{0\}$.

1.6 Classificação dos grupos de ordem menor ou igual a 8

Sabemos que todo o grupo de ordem p (p primo) é isomorfo a $\mathbb{Z}_p$, que todo o grupo de ordem 4 é isomorfo a $\mathbb{Z}_4$ (se for cíclico) ou a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Vejamos o que acontece relativamente aos grupos de ordem 6 e 8.

Teorema 1.6.1. *Todo o grupo de ordem* 6 *é isomorfo a* $\mathbb{Z}_6$ *ou a* S_3.

Demonstração. Vamos separar a demonstração em vários casos. Pelo teorema de Lagrange sabemos que a ordem dos elementos de G é $1, 2, 3$ ou 6.

Caso 1. Existe um elemento a de ordem 6. Então a gera G e portanto $G \cong \mathbb{Z}_6$.

Caso 1. Todo o elemento de $G \setminus \{e\}$ tem ordem dois. Neste caso, pelo Corolário 1.1.16, G é abeliano. Sejam $a \in G \setminus \{e\}$ e $b \in G \setminus < a >$. Pelo Teorema 1.5.19 e), o subgrupo $< a >< b >$ tem quatro elementos, o que contraria o Teorema de Lagrange.

Caso 2. Existe um elemento a de ordem 3. Pela Proposição 1.5.9, $< a >$ é um divisor normal. Seja $b \in b \in G \setminus < a >$. Então b tem ordem 2, pois se tivesse ordem 3 então, usando o Teorema 1.5.19 e), $< a >< b >$ teria 9 elementos.

Consideremos o conjunto $S = \{e, a, a^2, b, ba, ba^2\}$. Os elementos e, a, a^2 e b são todos diferentes, por hipótese. O elemento ba é diferente de e, de a, de a^2, de b (pois caso contrário teríamos $b = a^2$, $b = e$, $b = a$ ou $a = e$). De modo semelhante mostraríamos que ba^2 é diferente de e, de a, de a^2, de b e de ba. Concluímos assim que $S = G$. Em particular $ab \in S$. Por exclusão de partes podemos concluir que $ab = ba$ ou $ab = ba^2$.

Em cada um dos casos podemos facilmente completar a tabela do grupo e verificar que o grupo que obtemos é isomorfo a $\mathbb{Z}_6$ no primeiro caso e a S_3 no segundo caso. □

Vamos agora estudar os grupos de ordem 8. Já conhecemos os grupos $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ e o grupo diedral D_4. Estes grupos não são isomorfos pois: D_4 não é abeliano e os outros são; $\mathbb{Z}_8$ é cíclico e os outros não; $\mathbb{Z}_2 \times \mathbb{Z}_4$ tem elementos de ordem 4 e $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ não.

Vamos agora definir um outro grupo de ordem 8 que não é isomorfo a nenhum dos definidos até agora.

Sejam $A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ elementos de $GL(2, \mathbb{C})$, o grupo das matrizes 2×2 invertíveis de entradas complexas.

O subgrupo de $GL(2, \mathbb{C})$ gerado por A e B é um grupo com os seguintes oito elementos:

$$\{I, A, A^2, A^3, B, AB, A^2B, A^3B\}.$$

Chamemos Q_3 a este grupo. Q_3 não é isomorfo a nenhum outro dos grupos de ordem 8 listados acima (porquê?).

Os seguintes lemas caracterizam os grupos D_4 e Q_3.

Lema 1.6.2. *Se* G *é um grupo com* 8 *elementos e se* a, b *são elementos de* G *tais que* $a^4 = e$, $b^2 = e$, $ba = a^3b$ *e*

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\},$$

então G *é isomorfo a* D_4. □

Lema 1.6.3. *Se G é um grupo com 8 elementos e se a, b são elementos de G tais que $a^4 = e$, $b^2 = a^2$, $ba = a^3b$ e*

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\},$$

então G é isomorfo a Q_3. □

As demonstrações destes dois lemas exigem apenas que se complete a tabela dos grupos e verificar que esses grupos são isomorfos aos pretendidos.

Como exercício pode demonstrar que todos os subgrupos de Q_3 são normais.

Teorema 1.6.4. *Todo o grupo de ordem oito é isomorfo a $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, D_4 ou Q_3*

Demonstração. Seja G um grupo de ordem oito. Se G admite algum elemento de ordem oito, então G é cíclico, e portanto isomorfo a $\mathbb{Z}_8$.

Se G não admite elementos de ordem oito nem elementos de ordem quatro, então

$$\forall x \in G,\ x^2 = e,$$

e portanto G é abeliano.

Sejam a um elemento de $G \setminus \{e\}$ e $b \in G \setminus < a >$. Então, como $< a > \cap < b >= \{e\}$, $< a >< b >$ é um subgrupo de G isomorfo a $< a > \times < b >$ que por sua vez é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Se c é um elemento de $G \setminus < a >< b >$, então $< c > \cap < a >< b >= \{e\}$ e, portanto $< c >< a >< b >$ é isomorfo a $< c > \times < a >< b >$, que por sua vez é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Suponhamos agora que G não admite elementos de ordem oito, mas admite elementos de ordem quatro.

Seja $a \in G$ um elemento de ordem quatro. Então, como o índice de $< a >$ é dois, $< a >$ é um divisor normal de G. Consideremos um elemento b de $G \setminus < a >$.

Facilmente se mostra que os elementos

$$e, a, a^2, a^3, b, ab, a^2b, a^3b$$

são todos distintos. Como $|G| = 8$, estes são todos os elementos de G. Em particular um deles é igual a b^2. Qual? Por exclusão de partes, mostra-se que b^2 só pode ser e ou a^2. De modo análogo se mostra que ba é igual a ab ou a a^3b.

Temos então quatro casos a considerar:

Caso um: $b^2 = e$ e $ab = ba$. Então G é abeliano e $G \cong < a > \times < b > \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Caso dois: $b^2 = a^2$ e $ab = ba$. Então G é abeliano, ab tem ordem dois e $G \cong < a > \times < ab > \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Caso três: $b^2 = e$ e $ba = a^3b$. Então, pelo Lema 1.6.2, $G \cong D_4$.

Caso quatro: $b^2 = a^2$ e $ba = a^3b$. Então, pelo Lema 1.6.3, $G \cong Q_3$.

Analogamente ao que foi dito acima, a verificação do que é dito acima pode ser feita, completando a tabela do grupo com os dados já conhecidos. □

1.7 Automorfismos internos

Seja G um grupo. Para $a \in G$ consideremos $\begin{array}{rccc} h_a: & G & \to & G. \\ & x & \mapsto & axa^{-1} \end{array}$

Então, se $a, b \in G$:

a) h_a é um homomorfismo pois, se $x, y \in G$, $h_a(x)h_a(y) = axa^{-1}aya^{-1} = axya^{-1} = h_a(xy)$;

b) $h_a \circ h_b = h_{ab}$ pois, se $x \in G$, $h_a(h_b(x)) = h_a(bxb^{-1}) = abxb^{-1}a^{-1} = abx(ab)^{-1} = h_{ab}(x)$;

c) de b), temos que $h_a \circ h_{a^{-1}} = h_e =$ identidade, e portanto h_a é um isomorfismo com inverso $h_{a^{-1}}$;

d) $\begin{array}{lll} h_a \text{ é a identidade} & \Leftrightarrow & \forall x \in G, axa^{-1} = x \\ & \Leftrightarrow & \forall x \in G, ax = xa \\ & \Leftrightarrow & a \in Z_G. \end{array}$

Aos automorfismo de G da forma h_a, chamamos **automorfismos internos**, e denotamos por $Int\, G$ o conjunto dos automorfismos internos de G.

Pelas considerações acima temos que $Int\, G$ é um subgrupo de $Aut\, G$ (o grupo dos automorfismos de G).

Teorema 1.7.1. *Se G é um grupo, então $Int\, G$ é um divisor normal de $Aut\, G$ e é isomorfo ao grupo quociente G/Z_G.*

Demonstração. Para a primeira parte do teorema basta notar que, se $f \in Aut\, G$ e $a \in G$ então

$$\forall x \in G \quad (f \circ h_a \circ f^{-1})(x) = f(af^{-1}(x)a^{-1}) = f(a)f(f^{-1}(x))f(a^{-1}) = f(a)xf(a)^{-1}.$$

Concluímos assim que $f \circ h_a \circ f^{-1} = h_{f(a)}$ e portanto $f \circ h_a \circ f^{-1}$ pertence a $Int\, G$.

Consideremos agora a função

$$\begin{array}{rccc} \Psi: & G & \to & Int\, G. \\ & a & \mapsto & h_a \end{array}$$

Pelas considerações feitas acima, Ψ é um homomorfismo sobrejectivo cujo núcleo é Z_G. Pelo Teorema Fundamental do Homomorfismo concluímos que $G/Z_G \cong Int\, G$. □

Como exemplo, uma vez que o centro de S_3 é trivial, podemos concluir que S_3 tem 6 automorfismos internos.

Teorema 1.7.2. *Se G é um grupo então G é abeliano ou então G/Z_G não é cíclico.*

Demonstração. Suponhamos que G/Z_G é cíclico e seja aZ_G um seu gerador. Então

$$G = \bigcup \{a^n Z_G : n \in \mathbb{Z}\}. \tag{1.1}$$

Mostremos que neste caso G é abeliano.

Para $x, y \in G$ sejam, usando (1.1) $r, s \in \mathbb{Z}$ e $z, w \in Z_G$ tais que $x = a^r z$ e $y = a^s w$. Então

$$\begin{aligned} xy &= a^r z a^s w = a^r a^s z w = a^{r+s} z w \quad \text{porque } z \in Z_G \\ yx &= a^s w a^r z = a^s a^r w z = a^{s+r} w z = a^{r+s} z w \quad \text{porque } w \in Z_G \end{aligned}$$

Donde se conclui que G é abeliano. □

Este teorema diz que o grupo quociente G/Z_G é cíclico se e só se for trivial (isto é $G = Z_G$).

Exemplos 1.7.3.

1. *Todo o grupo de ordem* 600 *cujo centro tem mais do que* 151 *elementos é abeliano. Basta notar que a ordem de* Z_G*, que divide* 600 *e é maior que* 150*, não pode ser* 200 *nem* 300 *pois nesse caso* G/Z_G *seria cíclico e não trivial.*

2. *Não existe um grupo* G *com um número primo de automorfismos internos, pois nesse caso* $Int\, G$ *seria um grupo cíclico não trivial o que é absurdo pois* $Int\, G$ *é isomorfo a* G/Z_G*.*

1.8 Teorema de Cauchy

Temos agora o chamado Teorema de Cauchy, que em certa medida é um recíproco parcial do Teorema de Lagrange. O recíproco do Teorema de Lagrange seria:

> *"Se* G *é um grupo de ordem* n *e* k *é um inteiro que divide* n *então* G *admite um subgrupo cuja ordem é* k*."*

Este resultado não é válido em geral, embora seja válido para grupos abelianos. Por exemplo, existe um grupo de ordem 30 (A_5, grupo formado pelas permutações pares de um conjunto com 5 elementos) que não admite subgrupos de ordem 15 (ver Teorema 1.8.6).

> *De seguida é apresentado o Teorema de Cauchy, que foi referido nas aulas mas cuja demonstração só foi feita no caso abeliano. No Apêndice que segue é apresentada a continuação da demonstração que é baseada essencialmente no Teorema 1.8.2, que também está no Apêndice.*

Teorema 1.8.1 (Teorema de Cauchy, 1844)**.** *Se* G *é um grupo finito e* p *é um primo que divide a ordem de* G*, então existe um elemento, e portanto um subgrupo, de* G *com ordem* p*.*

Demonstração. A demonstração será feita por indução sobre $|G|$. Para grupos de ordem $1, 2$ e 3 o resultado é óbvio.

Suponhamos que o teorema é válido para grupos de ordem menor do que n e mostremos que o teorema vale para grupos de ordem n.

Seja G um grupo de ordem n e p um número primo que divide n.

Consideremos a, um elemento qualquer de $G \setminus \{e\}$ e sejam $A =< a >$ e $m = |A|$. Vamos separar a demonstração em dois casos.

$\boxed{G \text{ é abeliano}}$ Neste caso $A \trianglelefteq G$. Como p divide $|G|$, $|G| = |A|\,|G/A|$ e p é primo, então p divide $|A|$ $(= m)$ ou $|G/A|$ $(= \frac{n}{m} < n)$.

- Se p divide m, então $a^{\frac{m}{p}}$ tem ordem p e a demonstração está terminada.
- Se p não divide m então p divide $|G/A|$ que é menor do que n. Usando a hipótese de indução existe em G/A um elemento xA de ordem p. Deste modo $(xA)^p = x^pA = A$. Assim $x^p \in A$, e portanto $(x^p)^m = e$, pois a ordem de A é m.

  Mas como $(x^p)^m = (x^m)^p$ concluímos que a ordem de x^m é 1 ou p. Se a ordem de x^m fosse 1, então $x^m = e$, e portanto $(xA)^m = x^mA = A$, o que implicava que a ordem de xA, que é p, dividia m, o que é absurdo. Concluímos assim que x^m tem ordem p.

$\boxed{G \text{ é abeliano}}$ Ver página 52, no Apêndice que segue. □

Apêndice

Dado um grupo G definimos uma relação de equivalência γ sobre ele a que chamamos **equivalência de conjugação**,

$$\forall a, b \in G \quad \left[a\gamma b \iff \exists\, x \in G : a = xbx^{-1}\right].$$

Dito de outro modo, $a\gamma b$ se e só se a é imagem de b por algum automorfismo interno (ver página 49). Note-se que no caso em que G é abeliano a relação γ é a identidade.

A relação de equivalência γ induz uma partição em G. Seja I um conjunto formado por um representante de cada uma das classes de equivalência. Representemos por $[a]_\gamma$ a classe de equivalência de a. Note-se que

$$\begin{cases} [a]_\gamma = \{xax^{-1} : x \in G\}, \\ [a]_\gamma = \{a\} \;\Leftrightarrow\; a \in Z_G \\ |G| = \displaystyle\sum_{a \in I} |[a]_\gamma| \end{cases}$$

Teorema 1.8.2. *Seja G um grupo finito e I um conjunto de representantes das classes de conjugação de G. Então*

$$|G| = |Z_G| + \sum_{a \in I \setminus Z_G} (N_a : G).$$

Demonstração. Para cada $a \in G$, consideremos a função

$$\begin{array}{rccc} f: & [a]_\gamma & \longrightarrow & \{\text{classes esquerdas de } G \text{ relativamente a } N_a\}. \\ & xax^{-1} & \mapsto & xN_a \end{array}$$

f está bem definida e é bijectiva (verifique). Deste modo $|[a]_\gamma| = (N_a : G)$. Assim

$$\begin{aligned} |G| &= \sum_{a\in I} |[a]_\gamma| = \sum_{a\in I} (N_a : G) = \sum_{a\in Z_G} (N_a : G) + \sum_{a\in I\setminus Z_G} (N_a : G) \\ &= \sum_{a\in Z_G} 1 + \sum_{a\in I\setminus Z_G} (N_a : G) \\ &= |Z_G| + \sum_{a\in I\setminus Z_G} (N_a : G), \end{aligned}$$

o que termina a demonstração. □

Conclusão da demonstração do Teorema de Cauchy. Suponhamos que existe $a \in G \setminus Z_G$ tal que p divide N_a. Neste caso, podemos aplicar a hipótese de indução (note-se $|N_a| < |G|$) para concluir que existe em N_a, e portanto em G, um elemento de ordem p, terminando assim a demonstração do teorema.

Se p não divide a ordem de N_a para nenhum $a \in G \setminus Z_G$, então p divide $(N_a : G)$ para todo o $a \in G \setminus Z_G$ pois $|G| = |N_a|\,(N_a : G)$. Pela igualdade dada pelo Teorema 1.8.2

$$\underbrace{|G|}_{p|} = |Z_G| + \underbrace{\sum_{a\in I\setminus Z_G} (N_a : G)}_{p|}.$$

Daqui concluímos que p divide $|Z_G|$. Como G não é abeliano $|Z_G| < |G|$. Usando a hipótese de indução existe em Z_G, e portanto em G, um elemento de ordem p. □

Apresento, apenas a nível de curiosidade/(informação extra) um teorema que não foi referido nas aulas nem faz parte do programa da disciplina, que generaliza o Teorema de Cauchy.

Teorema 1.8.3 (Teorema de Sylow)**.** *Se G é um grupo de ordem n, $n = p^m k$, em que $p, m, k \in \mathbb{N}$, p é um número primo que não divide k então*

$$\forall i \in \{1, \ldots, m\} \quad \exists\, H \leq G \ \text{ tal que } \ |H| = p^i.$$

Além disso, se n_p for o número de subgrupos de ordem p^m, então:

a) $n_p \equiv 1 \ (mod\ p)$;

b) n_p *divide* k.

Vejamos algumas aplicações deste teorema.

Proposição 1.8.4. *Sejam p um número primo e $n \in N$. Se G é um grupo de ordem $2p^n$ ou de ordem kp^n, em que $k \in \mathbb{N}$, $k \leq p$ e $(k, p) = 1$, então G tem um divisor normal não trivial (isto é, diferente de G e de $\{e\}$)*

Corolário 1.8.5. *Se G é um grupo de ordem menor que 60 então G admite um divisor normal não trivial se e só se a sua ordem for prima.*

Teorema 1.8.6. *Se n é um número inteiro maior que 4, então A_n não admite nenhum divisor normal não trivial.*

Em particular A_n, que tem ordem $\frac{n!}{2}$, não tem nenhum subgrupo de ordem $\frac{n!}{4}$.

Capítulo 2

Teoria de Anéis

2.1 Preliminares

Um bigrupóide é um tripleto $< A, +, \cdot >$ em que A é um conjunto não vazio (dito conjunto suporte do bigrupóide) e $+$ e $\cdot$ são operações binárias sobre A, isto é, $< A, + >$ e $< A, \cdot >$ são grupóides.

Definição 2.1.1. *Um bigrupóide $< A, +, \cdot >$ diz-se um anel se:*

a) $< A, + >$ *é um grupo abeliano;*

b) $< A, \cdot >$ *é um semigrupo;*

c) *a operação $\cdot$ é distributiva à esquerda e à direita relativamente a $+$, isto é,*

$$\forall a, b, c \in A \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad (b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

Seja $< A, +, \cdot >$ um anel. Como temos dois grupóides associados a $< A, +, \cdot >$, e para evitar confusões relativamente a propriedades de cada um desses grupóides, vamos fazer algumas convenções que serão usadas daqui em diante, sempre que daí não advenham confusões (ver tabela da página 5).

- ⋆ Chamaremos adição à operação $+$ e multiplicação à operação $\cdot$, e usaremos expressões do tipo "a soma de a por b", "o produto de a por b", para significar $a+b$ e $a \cdot b$ respectivamente.
- ⋆ O elemento neutro de $< A, + >$ diz-se o **zero** do anel e será denotado por 0.
- ⋆ Se $a \in A$, denotaremos por $-a$ o elemento de A que somado a a dá 0, isto é $a + (-a) = 0$. Chamaremos a $-a$ o **simétrico** de a.
- ⋆ Dados $a, b \in A$, escreveremos $a - b$ em vez de $a + (-b)$ e ab em vez de $a \cdot b$.
- ⋆ Se $a, b, c, d \in A$, escreveremos $ab+cd$ em vez de $(ab)+(cd)$, isto é, a multiplicação tem prioridade relativamente à adição.

- ⋆ Se $a \in A$, e $n \in \mathbb{N}$, então na denota a soma de n parcelas iguais a a e a^n denota o produto de n factores iguais a a. Formalmente teremos: $(n+1)a = na + a$ e $a^{n+1} = a^n a$, para $n \in \mathbb{N}$.

- ⋆ Se o grupóide $< A, \cdot >$ tiver elemento neutro, a esse elemento chamaremos **elemento um** do anel, e denotá-lo-emos por $\mathbb{1}$ ou por e. Neste caso, se $a \in A$ for invertível em $< A, \cdot >$ chamaremos **inverso** de a e denotá-lo-emos por a^{-1} ao elemento de A que multiplicado por a dá e.

- ⋆ Diremos que o anel $< A, +, \cdot >$ é comutativo se $< A, \cdot >$ for comutativo.

- ⋆ Sempre que daí não advier confusão, diremos "o anel A" em vez de "o anel $< A, +, \cdot >$".

Exemplos 2.1.2. *Muitos dos exemplos de anéis mencionados de seguida são já conhecidos. Verifique que se trata realmente de anéis. No que segue,* $n \in \mathbb{N}$.

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *e* $\mathbb{C}$, *munidos da adição e multiplicação usual.*

- $< \{0, 1, 2, \ldots, n-1\}, +_n, \cdot_n >$, *em que* $+_n$ *e* $\cdot_n$ *denotam a soma e o produto módulo* n. *Este anel diz-se o anel dos inteiros módulo* n *e denota-se por* $\mathbb{Z}_n$.

- $\{f : \mathbb{R} \to \mathbb{R}\}$, $\{f : \mathbb{R} \to \mathbb{R} : \ f$ *é de classe* $C^n\}$ *ou* $\{f : \mathbb{R} \to \mathbb{R} : \ f$ *é um polinómio*$\}$ *munidos da soma e da multiplicação de funções.*

- $\{f : \mathbb{R} \to \mathbb{R}\}$, $\{f : \mathbb{R} \to \mathbb{R} : \ f$ *é de classe* $C^n\}$ *ou* $\{f : \mathbb{R} \to \mathbb{R} : \ f$ *é um polinómio*$\}$ *munidos da soma e da composição de funções.*

- $< G, +, \cdot >$*em que* G *é um grupo abeliano e, para* $a, b \in G$, $a \cdot b = 0$.

Chamaremos **anel zero** ou **anel trivial** a um anel só com um elemento (necessariamente o elemento zero). Temos agora um outro exemplo de anel, que generaliza um dos exemplos dados acima.

Teorema 2.1.3. *Se* $< G, + >$ *é um grupo abeliano, então o conjunto dos endomorfismos de* G, *que denotamos por* $\operatorname{End} G$, *munido da adição e da composição de funções é um anel, que se diz anel dos endomorfismos de* $< G, + >$.

Demonstração. É imediato verificar que $< \operatorname{End} G, + >$ é um grupo abeliano, em que o elemento neutro é a função $\begin{array}{ccc} G & \to & G \\ x & \mapsto & e_G \end{array}$ (sendo e_G o elementos neutro de G) e o simétrico de um elemento $\alpha \in \operatorname{End} G$ é a função $-\alpha$, que associa a cada $x \in$G o simétrico de $\alpha(x)$ em G.

Para mostrar que, se $\alpha, \beta, \gamma \in \operatorname{End} G$ então $\alpha \circ (\beta + \gamma) = \alpha \circ \beta + \alpha \circ \gamma$ basta notar que, para $x \in G$

$$\begin{aligned} [\alpha \circ (\beta + \gamma)](x) &= \alpha((\beta + \gamma)(x)) \ = \ \alpha(\beta(x) + \gamma(x)) \\ &= \alpha(\beta(x)) + \alpha(\gamma(x)) \ = \ (\alpha \circ \beta)(x) + (\alpha \circ \gamma)(x) \\ &= [(\alpha \circ \beta) + (\alpha \circ \gamma)](x) \end{aligned}$$

Fica como exercício completar a demonstração do teorema. □

Como exemplo de aplicação deste teorema pode calcular o anel dos endomorfismos do grupo de Klein.

Definição 2.1.4. *Um anel* $< A, +, \cdot >$ *diz-se um* **anel com elemento um** *se* $< A, \cdot >$ *for um monóide.*

Dos exemplos dados até agora quais os que têm elemento um?

Vejamos agora algumas propriedades simples dos anéis.

Lema 2.1.5. *Se* $< A, +, \cdot >$ *é um anel e* $a, b, c \in A$ *então:*

a) $a\,0 = 0\,a = 0$*;*

b) $a(-b) = (-a)b = -(ab)$ *e* $(-a)(-b) = ab$*;*

c) *se* $m \in \mathbb{Z}$ *então* $a(mb) = (ma)b = m(ab)$*;*

d) $a(b - c) = ab - ac$*;*

e) *se* $|A| > 1$ *e* A *tem elemento um, então esse elemento um é diferente de* 0*.*

Demonstração. Para as alíneas a), b), c) e d), vamos apenas verificar algumas das igualdades enunciadas. As outras provam-se de modo análogo.

a) Basta mostrar que $0a$ e $a0$ são idempotentes, o que é verdade pois

$$0\,a = (0 + 0)a = 0\,a + 0\,a, \qquad a\,0 = a\,(0 + 0) = a\,0 + a\,0.$$

b) Para mostrar que $a(-b)$ é o simétrico de ab, ou seja que $a(-b) = -(ab)$, basta mostrar que $a(-b) + ab = 0$. Mas,

$$\begin{aligned} a(-b) + ab &= a((-b) + b) \quad \text{pela distributividade} \\ &= a\,0 \\ &= 0 \quad \text{usando a alínea anterior.} \end{aligned}$$

c) A demonstração pode ser feita por indução sobre m, para $m \in \mathbb{N}$. Vejamos o passo de indução:

$$\begin{aligned} a((m+1)b) &= a(mb + b) \\ &= a(mb) + ab \quad \text{pela distributividade} \\ &= m(ab) + ab \quad \text{por hipótese de indução} \\ &= (m+1)(ab). \end{aligned}$$

Se m é negativo então $k = -m$ é positivo e pelo que foi feito $a(kb) = k(ab)$. Daqui resulta, usando a alínea b), o pretendido. Verifique os detalhes.

d) Usando a distributividade e a alínea b) obtemos $a(b - c) = a(b + (-c)) = ab + a(-c) = ab - ac$.

e) Seja $a \in A \setminus \{0\}$. Como $ea = a$ e $0\,a = 0$ podemos concluir que $e \neq 0$. □

Vamos agora mostrar que muitos dos cálculos que se fazem no anel dos números reais, em particular, o desenvolvimento do chamado binómio de Newton, são válidos em qualquer anel comutativo. Comecemos com um pequeno lema.

Lema 2.1.6. *Se $< A, +, \cdot >$ é um anel então as condições seguintes são equivalentes:*

a) *A é um anel comutativo:*

b) $\forall a, b \in A \quad (a+b)^2 = a^2 + 2ab + b^2$*;*

c) $\forall a, b \in A \quad (a+b)(a-b) = a^2 - b^2$.

Demonstração. Se $a, b \in A$ então, usando a distributividade temos

$$(a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2.$$

Deste modo, se $a, b \in A$,

$$\begin{aligned} (a+b)^2 = a^2 + 2ab + b^2 \quad &\iff \quad a^2 + 2ab + b^2 = a^2 + ab + ba + b^2 \\ &\iff \quad ab = ba \quad \text{usando a lei do corte,} \end{aligned}$$

o que mostra que a) e b) são condições equivalentes. Do mesmo modo se prova a equivalência entre a) e c). □

Usando este lema e copiando a demonstração feita para o anel dos números reais podemos concluir que, se $< A, +, \cdot >$ é um anel comutativo então

$$\forall n \in \mathbb{N} \;\; \forall a, b \in A \;\; (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

Definição 2.1.7. *Seja $< A, +, \cdot >$ um anel e $B \subseteq A$. B diz-se um subanel de A se satisfaz as seguintes condições:*

a) $B \neq \emptyset$*;*

b) $a \in B \;\Rightarrow\; -a \in B$*;*

c) $a, b \in B \;\Rightarrow\; a + b \in B$*;*

d) $a, b \in B \;\Rightarrow\; a \cdot b \in B$.

As condições a), b) e c) significam que B é um subgrupo do grupo $< A, + >$ e as condições a) e d) que B é um subgrupóide de $< B, \cdot >$.

Escreveremos $B \leq A$ para significar que B é um subanel do anel A. É claro que, se B é um subanel de um anel A, então B, com as operações induzidas de A é um anel.

Exemplos 2.1.8. *Vejamos alguns exemplos simples.*

1. *Se A é um anel, então $\{0\}$ e A são subanéis de A.*

2. *Se A é um anel e $a \in A$, então $Aa = \{xa : x \in A\}$ e aA são subanéis de A.*

3. *O anel dos inteiros é subanel do anel dos racionais que por sua vez é subanel do anel dos reais.*

4. *Dado $n \in \mathbb{N}$, o conjunto das matrizes triangulares superiores $n \times n$ de entradas num corpo $\mathbb{K}$ é um subanel de $\mathcal{M}_{n\times n}(\mathbb{K})$.*

5. *Um subanel de um anel com elemento um pode não ter elemento um (por exemplo $2\,\mathbb{Z} \leq \mathbb{Z}$).*

6. *Um subanel de um anel pode ter elemento um diferente do elemento um do anel (por exemplo $4\,\mathbb{Z}_{12} \leq \mathbb{Z}_{12}$).*

7. *Um subanel de um anel sem elemento um, pode ter elemento um (por exemplo $4\mathbb{Z}_{12} \leq 2\,\mathbb{Z}_{12}$).*

Definição 2.1.9. *Sejam $(< A_i, +_i, \cdot_i)_{iI}$ anéis. Define-se o produto (directo ou cartesiano) desta família de anéis como sendo $< A, +, \cdot >$ em que*

$$A = \prod_{i\in I} A_i \quad \forall (a_i)_{i\in I}, (b_i)_{i\in I} \in A \quad \begin{cases} (a_i)_{i\in I} + (b_i)_{i\in I} &= (a_i +_i b_i)_{i\in I} \\ (a_i)_{i\in I} \cdot (b_i)_{i\in I} &= (a_i \cdot_i b_i)_{i\in I}. \end{cases}$$

O que a definição acima diz, é que as operações no anel produto são feitas coordenada a coordenada. No caso do produto de n anéis, $A_1, \ldots, A_n$ escreveremos $A_1 \times \cdots \times A_n$ para designar o anel produto pela ordem referida. Note-se que o anel produto tem elemento um se e só se todos os anéis "componentes" tiverem elemento um.

Definição 2.1.10. *Um anel $< D, +, \cdot >$ com mais que um elemento diz-se um* **domínio de integridade** *se tiver elemento um, for comutativo e satisfizer a condição*

$$\forall a, b \in D \quad \big[ab = 0 \;\Rightarrow\; (a = 0 \text{ ou } b = 0)\big]. \tag{2.1}$$

A condição (2.1) significa que $< D \setminus \{0\}, \cdot >$ é um grupóide. Apenas com o intuito de simplificar a escrita diremos que D é um DI para significar que D é um domínio de integridade.

Como exemplos de domínios de integridade temos os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. É obvio que se um anel satisfaz a condição (2.1) então qualquer seu subanel também satisfaz. Um DI que será muito usado é o chamado anel dos inteiros gaussianos $\mathbb{Z}[i] = \{a + b\,i : a, b \in \mathbb{Z}\}$ (com a soma e o produto usuais em $\mathbb{C}$).

Definição 2.1.11. *Um anel $< A, +, \cdot >$ diz-se um* **anel de divisão** *se $< A \setminus \{0\}, \cdot >$ for um grupo. A um anel de divisão abeliano chamámos* **corpo**.

Note-se que todo o anel de divisão comutativo é um DI. O anel dos quaterniões é um anel de divisão que não é um corpo (ver Exercício 4, página 68). $\mathbb{Z}$ é um DI que não é um corpo. $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$, com a soma e o produto usuais é um corpo (verifique!).

Lema 2.1.12. *Um anel comutativo D com elemento um diferente do elemento zero, é um DI se e só se satisfaz a lei do corte, isto é,*

$$\forall a, b, c \in D \quad \big[ab = ac \;\Rightarrow\; (a = 0 \text{ ou } b = c)\big]$$

Demonstração. A condição que aparece na definição de DI é um caso particular da lei do corte (basta considerar $c = 0$). Por outro lado a lei do corte pode ser escrita na forma

$$\forall a, b, c \in D \quad \big[a(b-c) = 0 \;\Rightarrow\; (a = 0 \text{ ou } b - c = 0)\,\big],$$

o que completa a demonstração. □

Como consequência deste lema temos o seguinte resultado.

Lema 2.1.13. *Todo o DI finito é um corpo.*

Demonstração. Resta-nos mostrar que, se $< D.+, \cdot >$ um DI finito e $a \in D \setminus \{0\}$ então existe $b \in D \setminus \{0\}$ tal que $ab = e$. Como D é finito, existem $n, k \in \mathbb{N}$ tais que $a^{n+k} = a^n$ ou seja $a^n a^k = a^n e$. Pela lei do corte, $a^k = e$ e portanto $a^{k-1}a = e$ (convencionamos que $a^0 = e$). □

Temos agora uma caracterização dos domínios de integridade da forma $\mathbb{Z}_n$.

Teorema 2.1.14. *Se $n \in \mathbb{N} \setminus \{1\}$ então $\mathbb{Z}_n$ é um DI (ou seja um corpo, uma vez que $\mathbb{Z}_n$ é finito,) se e só se n é primo.*

Demonstração. Se $n = a \cdot b$ com $1 < a, b < n$ então a e b são elementos não nulos de $\mathbb{Z}_n$ cujo produto é nulo. Em particular $\mathbb{Z}_n$ não é um DI.

Suponhamos agora que n é primo e sejam $a, b \in \mathbb{Z}_n$ tais que $a \cdot_n b = 0$ ou equivalentemente n divide ab. Nestas condições, como n é primo, n divide a ou n divide b. Concluímos assim que a ou b é o elemento zero de $\mathbb{Z}_n$. □

Proposição 2.1.15. *O produto de dois (ou mais) domínios de integridade* **nunca** *é um domínio de integridade. O mesmo acontece com anéis de divisão ou corpos.*

Demonstração. Para simplificar a escrita vamos considerar dois domínios de integridade D_1 e D_2. Sejam $a \in D_1 \setminus \{0\}$ e $b \in D_2 \setminus \{0\}$. Neste caso $(a, 0)$ e $(0, b)$ são dois elementos não nulos no anel produto $D_1 \times D_2$ cujo produto é o elemento zero. □

2.2 Teorema fundamental do homomorfismo

Vamos agora dar algumas definições que nos levarão ao Teorema Fundamental do Homomorfismo para anéis. O caminho a seguir é análogo ao que foi feito para grupos.

Definição 2.2.1. *Sejam $< A, +, \cdot >$ e $< B, +, \cdot >$ anéis (representamos as operações nos dois anéis com os mesmos símbolos por simplicidade de escrita).*

Uma função $f : A \longrightarrow B$ diz-se um **homomorfismo de anel** *se:*

a) $\forall a, b \in A, \quad f(a+b) = f(a) + f(b)$, *isto é, f é um homomorfismo de grupo de $< A, + >$ para $< B, + >$;*

b) $\forall a, b \in A, \quad f(a \cdot b) = f(a) \cdot f(b)$, *isto é, f é um homomorfismo de grupóide de $< A, \cdot >$ para $< B, \cdot >$;*

Se f for bijectiva e a inversa for um homomorfismo então, f diz-se um **isomorfismo**.

As condições a) e b) acima, significam que f "preserva" a soma e o produto. À imagem do que acontece no caso dos grupos, se f for uma homomorfismo bijectivo então é necessariamente um isomorfismo. É também claro (ver o caso dos grupos) que $f(0_A) = 0_B$ e que $f(-a) = -f(a)$ para todo $a \in A$.

Definição 2.2.2. *Seja $f : A \longrightarrow B$ um homomorfismo de anel. Define-se* **núcleo de** *f e denota-se por* $\operatorname{Nuc} f$ *como sendo o conjunto*

$$\{a \in A : f(a) = 0\}.$$

Sejam $< A, +, \cdot >$ e $< B, +, \cdot >$ anéis e $f : A \longrightarrow B$ um homomorfismo de anel. Então f é também um homomorfismo de grupo entre $< A, + >$ e $< B, + >$. Notemos agora que a definição de núcleo de f, visto como um homomorfismo de anel coincide com a definição de núcleo de f, visto como um homomorfismo de grupo. Como consequência desta observação, podemos concluir que um homomorfismo de anel é injectivo se e só se o seu núcleo se reduz ao elemento zero.

Vamos agora definir o que se entende por ideal de um anel. Os ideais têm, em teoria de anéis, um papel análogo ao dos divisores normais em teoria de grupos. Em particular, todo o ideal pode ser visto como o núcleo de algum homomorfismo.

Definição 2.2.3. *Seja $< A, +, \cdot >$ um anel e I um subconjunto de A. Diz-se que I é:*

- *um* **ideal esquerdo** *de A se for um subgrupo de $< A, + >$ e*

$$\forall a \in I \ \forall x \in A \quad xa \in I \qquad \textit{(lei da absorção à esquerda).}$$

- *um* **ideal direito** *de A se for um subgrupo de $< A, + >$ e*

$$\forall a \in I \ \forall x \in A \quad ax \in I \qquad \textit{(lei da absorção à direita).}$$

- *um* **ideal bilateral** *ou simplesmente um* **ideal** *se for simultaneamente ideal esquerdo e direito. Escreveremos $I \trianglelefteq A$ para significar que I é um ideal de A.*

Notar que a intersecção de ideais é um ideal. É claro que para anéis comutativos, as noções de ideal esquerdo e de ideal direito coincidem.

Exemplos 2.2.4.

1. *Se A é um anel, então $\{0\}$ e A são ideais de A.*
2. *Se $n \in \mathbb{Z}$ então $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$.*
3. *Como todo o ideal de qualquer anel é um subgrupo do grupo aditivo associado a esse anel, como os únicos subgrupos de $< \mathbb{Z}, + >$ são os da forma $n\mathbb{Z}$, com $n \in \mathbb{N}$ concluímos que os ideais do anel dos inteiros são os subconjuntos da forma $n\mathbb{Z}$ com $n \in \mathbb{N}$.*
4. *Seja $A = \mathcal{M}_{2\times 2}(\mathbb{Z})$. Então*

$$B = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

é um ideal esquerdo de A que não é um ideal direito (verifique).

Proposição 2.2.5. *Se* $< A, +, \cdot >$ *e* $< B, +, \cdot >$ *são anéis e* $f : A \longrightarrow B$ *é um homomorfismo de anel, então* $\operatorname{Nuc} f$ *é um ideal de* A.

Demonstração. Já sabemos que $\operatorname{Nuc} f$ é um subgrupo do grupo $< A, + >$. Por outro lado, se $a \in \operatorname{Nuc} f$ e $x \in A$, então

$$\begin{aligned} f(ax) &= f(a)f(x) = 0f(x) = 0 \\ f(xa) &= f(x)f(a) = f(x)0 = 0, \end{aligned}$$

e portanto $ax, xa \in \operatorname{Nuc} f$. □

Proposição 2.2.6. *Se* A *é um anel com elemento um e se* I *é um ideal de* A *contendo algum elemento invertível, então* $I = A$

Demonstração. Sejam e, o elemento um de A, i um elemento invertível de I e $j \in A$ tal que $ij = e$. Deste modo $e \in I$, usando a lei da absorção à direita.

Mostremos que todo o elemento de A pertence a I. Se $a \in A$ então $a = e \cdot a$ e portanto $a \in I$, usando novamente a lei da absorção (à direita). □

Note-se que na demonstração só foi usado o facto de o elemento i ser invertível à direita. É claro que puder-se-ia fazer uma demonstração análoga usando o facto de i ser invertível à esquerda.

Corolário 2.2.7. *Se* $\mathbb{K}$ *é um anel de divisão então* $\{0\}$ *e* $\mathbb{K}$ *são os seus únicos ideais.*

Demonstração. Se I é um ideal de A diferente de $\{0\}$, então I tem algum elemento diferente de 0. Como A é um anel de divisão, esse elemento é necessariamente invertível. Pela proposição anterior $I = A$. □

Corolário 2.2.8. *Seja* $f : A \longrightarrow B$ *um homomorfismo de anel e suponhamos que* A *é um anel de divisão. Então* f *ou é injectiva ou é constante.*

Demonstração. Como $\operatorname{Nuc} f$ é um ideal de A, que é um anel de divisão, então, pelo corolário anterior, $\operatorname{Nuc} f = \{0\}$ ou $\operatorname{Nuc} f = A$. No primeiro caso f é injectiva e no segundo caso f é constante e igual a 0. □

Seja $< A, +, \cdot >$ um anel e I um ideal de A. Como $< A, + >$ é um grupo do qual I é um subgrupo, sabemos que a relação

$$\forall a, b \in A,\ [a \rho b \ \Leftrightarrow\ a - b \in I],$$

é uma relação de equivalência cujas classes, ditas classes de equivalência de A módulo I, são os subconjuntos de A da forma $a + I$, em que $a \in A$. Como $< A, + >$ é um grupo abeliano, o conjunto A/I das classes de equivalência de A módulo I tem uma estrutura de grupo (abeliano) de tal modo que a função

$$\begin{array}{rccc} p: & A & \longrightarrow & A/I \\ & a & \mapsto & a + I \end{array}$$

é um homomorfismo (de grupo) sobrejectivo.

Até aqui só usamos o que já sabíamos, pois I é um divisor normal de $< A, + >$.

Vejamos que A/I tem uma estrutura de anel de tal modo que a função p é um homomorfismo de anel.

Proposição 2.2.9. *Seja $< A, +, \cdot >$ um anel e I um seu ideal. Para todo o $a, b \in A$ defina-se*

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+I\\ (a+I)\cdot(b+I) &= ab+I.\end{aligned}$$

Então $+$ e $\cdot$ são operações binárias sobre A/I tais que $< A/I, +, \cdot >$ é um anel e

$$\begin{array}{rccc} p: & A & \longrightarrow & A/I \\ & a & \mapsto & a+I \end{array}$$

é um homomorfismo (de anel) sobrejectivo cujo núcleo é I.

Demonstração. Já sabemos que $< A/I, + >$ é um grupo abeliano e que p é um homomorfismo de grupo sobrejectivo. Vejamos que a operação $\cdot$ sobre A/I está bem definida. Sejam então $a, b, c, d \in A$ tais que $a + I = c + I$ e $b + I = d + I$ (ou equivalentemente $a - c, b - d \in I$). Mostremos que $ab + I = cd + I$, ou seja que $ab - cd \in I$. Para isso note-se que

$$ab - cd = a\underbrace{(b-d)}_{\in I} + \underbrace{(a-c)}_{\in I} d \in I \quad \text{porque } I \text{ é um ideal de } A.$$

É também óbvio que p preserva o produto. □

Chamamos ao anel A/I o **anel quociente** de A por I. Nas notações desta proposição o elemento zero de A/I é $0 + I$. Se A tem elemento um (e) então $e + I$ é o elemento um de A/I. Se além disso um elemento $a \in A$ tem inverso b, então $b + I$ é o inverso de $a + I$ em A/I. Em termos gerais o anel A/I "não perde" as propriedades do anel A. Mais precisamente, se A for um anel de divisão, ou um corpo, ou um domínio de integridade então também o é A/I.

Como corolário desta proposição e da Proposição 2.2.5, podemos concluir que os ideais de um anel A são precisamente os núcleos dos homomorfismos cujo domínio é A.

Temos agora o Teorema Fundamental do Homomorfismo para anéis, cuja demonstração segue os passos de teorema análogo para grupos e que, por essa razão, é deixada como exercício.

Teorema 2.2.10 (Teorema Fundamental do Homomorfismo)**.** *Toda a imagem homomorfa de um anel A é isomorfa a um anel quociente de A.* □

Exemplos 2.2.11.

1. *Se $n \in \mathbb{N}$, a função*

$$\begin{array}{rcl} \mathbb{Z} & \longrightarrow & \mathbb{Z}_n \\ a & \mapsto & a(mod\ n) \end{array}$$

é um homomorfismo (de anel) sobrejectivo cujo núcleo é $n\mathbb{Z}$ e, portanto $\mathbb{Z}/n\mathbb{Z}$ é isomorfo a $\mathbb{Z}_n$.

2. *Sejam I e J ideais de um anel A. Usando o mesmo tipo de demonstração feita em teoria de grupos, pode-se mostrar que:*

   a) $I + J$ *é um ideal de* A;

   b) J *é um ideal de* $I + J$;

   c) $I \cap J$ *é um ideal de* I *e de* J;

   d) $(I + J)/J$ *é isomorfo a* $I/I \cap J$.

2.3 Idempotentes, nilpotentes e divisores de zero

Definição 2.3.1. *Um elemento a de um anel A diz-se:*

- ⋆ **nilpotente**, *se existir* $n \in \mathbb{N}$ *tal que* $a^n = 0$;
- ⋆ **idempotente**, *se* $a^2 = a$;
- ⋆ **divisor esquerdo de zero**, *se existir* $b \in A \setminus \{0\}$ *tal que* $ab = 0$;
- ⋆ **divisor direito de zero**, *se existir* $b \in A \setminus \{0\}$ *tal que* $ba = 0$;
- ⋆ **divisor de zero**, *se existir* $b \in A \setminus \{0\}$ *tal que* $ab = 0$ *ou* $ba = 0$;
- ⋆ **divisor próprio de zero**, *se for um divisor de zero diferente de* 0.

Vejamos alguns exemplos e resultados sobre idempotentes, nilpotentes e divisores de zero, cuja verificação é deixada como exercício.

Exemplos 2.3.2.

1. *Num anel A qualquer, o elemento zero é sempre nilpotente, idempotente e, no caso de A ter mais do que um elemento, divisor de zero (esquerdo e direito).*

2. *Em $\mathbb{Z}$ só o 0 é nilpotente e divisor de zero, e só o 0 e o 1 são idempotentes.*

3. *Em $\mathbb{Z}_{72}$ os nilpotentes são os múltiplos de 6 (verifique), os divisores de zero são os não primos com 72. Quais os idempotentes?*

4. *Num anel com elemento um diferente do elemento zero, os elementos invertíveis não são nilpotentes.*

5. *Num DI, só o elemento zero é nilpotente e divisor de zero e só o 0 e o 1 são idempotentes.*

6. *Se a é idempotente de um anel A, então o subanel de A gerado por a é um anel cujo elemento um é o a.*

7. *Se A é o anel das funções de $\mathbb{R}$ em $\mathbb{R}$ e $f \in A$ é uma função que se anula em algum ponto, então f é um divisor de zero de A.*

8. *Se $n \in \mathbb{N}$, os divisores de zero de $\mathbb{Z}_n$ são os inteiros que não são primos com n.*

Num anel com elemento um, os idempotentes aparecem sempre "aos pares".

Proposição 2.3.3. *Sejam A um anel com elemento um (e) e $a \in A$. Então a é um idempotente se e só se $e-a$ é idempotente. Além disso, se $|A| > 1$ então $a \neq e-a$.*

Demonstração. Note.se que

$$(e-a)^2 = e-a \Leftrightarrow e-2a+a^2 = e-a \Leftrightarrow a^2 = a.$$

Por outro lado, se $a^2 = a$ e $a = e-a$ então $a^2 = a-a$ e portanto $a = 0 = e$. □

2.3.1 Idempotentes e nilpotentes de $\mathbb{Z}_n$

Vejamos agora como calcular os idempotentes e os nilpotentes do anel dos inteiros módulo n ($n \in \mathbb{N}$).

Proposição 2.3.4. *Seja $n \in \mathbb{N}$ e suponhamos que $n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$, em que $s \in \mathbb{N}$, $p_1, p_2, \ldots, p_s$ são primos distintos e $n_1, n_2, \ldots, n_s \in \mathbb{N}$. Então os nilpotentes de $\mathbb{Z}_n$ são os múltiplos de $p_1 p_2 \ldots p_k$. Em particular $\mathbb{Z}_n$ admite $\frac{n}{p_1 p_2 \cdots p_k}$ nilpotentes.*

Demonstração. Seja $a \in \mathbb{Z}_n$ um nilpotente. Então $k \in \mathbb{N}$ tal que n divide a^k. Em particular $p_1, p_2, \ldots, p_s$ dividem a^k e, como $p_1, p_2, \ldots, p_s$ são números primos, $p_1, p_2, \ldots, p_s$ dividem a ou equivalentemente $p_1 p_2 \ldots p_k$ divide a.

Inversamente se existe $m \in \mathbb{N}$ tal que $a = m p_1 p_2 \ldots p_s$ então, se $t \geq n_1, n_2, \ldots, n_s$, a^t é um múltiplo de n e portanto é igual a 0 em $\mathbb{Z}_n$. □

Note-se que se n é livre de quadrados (isto é, não admite nenhum divisor diferente de 1 que seja um quadrado perfeito) então 0 é o único nilpotente de $\mathbb{Z}_n$.

Para o cálculo dos idempotentes de $\mathbb{Z}_n$ precisamos de alguns preliminares.

Definição 2.3.5. *Seja n um inteiro positivo e d um seu divisor. Diz-se que d é um divisor unitário de n se d e $\frac{n}{d}$ são primos entre si.*

Se d é um divisor unitário de n escrevemos $d|^* n$.

O cálculo dos divisores unitários de n é extremamente simples. Seja $n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$, em que os p_i's são primos distintos e $s, n_1, \ldots, n_s \in \mathbb{N}$. Os divisores unitários de n podem ser encontrados do seguinte modo. Escolha-se $k \in \{1, \ldots, s\}$ e $p_{i_1}, p_{i_2}, \ldots, p_{i_k}$, k dos primos $p_1, p_2, \ldots, p_s$. Então

$$p_{i_1}^{n_{i_1}} p_{i_2}^{n_{i_2}} \cdots p_{i_k}^{n_{i_k}}$$

é um divisor unitário de n. Por exemplo, os divisores unitários de $600 = 2^3 \times 3 \times 5^2$ são: 1, 2^3, 3, 5^2, $2^3 \times 3$, $2^3 \times 5^2$, 3×5^2, $2^3 \times 3 \times 5$.

Como consequência existem tantos divisores unitários de n como subconjuntos de $\{p_1, p_2, \ldots, p_s\}$, ou seja existem 2^s divisores unitários de n.

Temos assim o seguinte resultado que relaciona os divisores unitários de n e os idempotentes de $\mathbb{Z}_n$. O teorema é "construtivo", isto é, dá-nos uma maneira de encontrar todos os idempotentes de $\mathbb{Z}_n$ resolvendo 2^s sistemas de congruências ou, que podem ser reduzidos a metade se usarmos a Proposição 2.3.3.

Teorema 2.3.6. *Se $n \in \mathbb{N}$ então há tantos idempotentes no anel $\mathbb{Z}_n$ como divisores unitários de n. Mais concretamente:*

a) *se d é um divisor unitário de n, então o sistema* $\left\{ \begin{array}{rcl} a & \equiv & 0 \pmod{d} \\ a & \equiv & 1 \pmod{\frac{n}{d}} \end{array} \right.$ *admite uma e uma só solução, módulo n.*

b) *se $a \in \mathbb{N}$ então a é um idempotente em $\mathbb{Z}_n$ se e só se existe d, divisor unitário de n, tal que* $\left\{ \begin{array}{rcl} a & \equiv & 0 \pmod{d} \\ a & \equiv & 1 \pmod{\frac{n}{d}} \end{array} \right.$ *;*

c) *se a é um idempotente associado (segundo a alínea anterior) a um divisor unitário d então $b = 1 - a$ é um idempotente associado ao divisor unitário de $\frac{n}{d}$.*

d) *se a é um idempotente de $\mathbb{Z}_n$ então a está associado a um só divisor unitário de n;*

e) *se a é idempotente então o divisor unitário de n associado a a é (n, a);*

f) *a função*

$$\begin{array}{rccc} \Phi: & \{a \in \mathbb{Z}_n : \ a = a^2\} & \longrightarrow & \{d \in \mathbb{N} : \ d|^* n\} \\ & a & \mapsto & (n, a) \end{array}$$

é uma bijecção, cuja inversa é

$$\begin{array}{rccc} \Psi: & \{d \in \mathbb{N} : \ d|^* n\} & \longrightarrow & \{a \in \mathbb{Z}_n : \ a = a^2\} \\ & d & \mapsto & \textit{idempotente associado a } d \end{array}$$

g) *existem em $\mathbb{Z}_n$, 2^s idempotentes, se s for o número de primos (distintos) que divide n.*

Demonstração.

a) Basta usar o teorema chinês dos restos.

b) Note-se que

$$a \text{ é um idempotente de } \mathbb{Z}_n \ \Leftrightarrow \ n|(a^2 - a) \ \Leftrightarrow n|a(a-1).$$

Como $(a, a-1) = 1$ então

$$n|a(a-1) \ \Leftrightarrow \ \exists d|^* n : d|a, \ \frac{n}{d}|(a-1).$$

c) Se a é um idempotente de $\mathbb{Z}_n$ então temos $b^2 = (1-a)^2 = 1 - 2a + a^2$ que é congruente módulo n com $1 - 2a + a = 1 - a = b$. Além disso $b = 1 - a \equiv 1 - 0 = 1 \pmod{d}$ e $b = 1 - a \equiv 1 - 1 = 0 \pmod{\frac{n}{d}}$.

d) Suponhamos que a é um idempotente de $\mathbb{Z}_n$ associado a dois divisores unitários d_1 e d_2 diferentes. Como d_1 e d_2 são divisores unitários então existe $p \in \mathbb{P}$ que divide um deles e não divide o outro. Suponhamos que $p|d_1$ e $p \not| d_2$. Neste caso $p|\frac{n}{d_2}$. Como $a \equiv 0 \pmod{d_1}$ e $a \equiv 1 \pmod{\frac{n}{d_2}}$ então $a \equiv 0 \pmod{p}$ e $a \equiv 1 \pmod{p}$, o que é absurdo.

e) Basta notar que, (n, a) divide a e que

$$\begin{aligned} n \text{ divide } a(a-1) &\Rightarrow \tfrac{n}{(n,a)} \text{ divide } \tfrac{a}{(n,a)}\,(a-1) \\ &\Rightarrow \tfrac{n}{(n,a)} \text{ divide } (a-1), \text{ pois } \tfrac{n}{(n,a)} \text{ e } \tfrac{a}{(n,a)} \text{ são primos entre si} \end{aligned}$$

As alíneas f) e g) são uma consequência das alíneas anteriores. □

Note-se que para qualquer n, os idempotentes 0 e 1 estão associados aos divisores unitários 1 e n.

Vejamos um exemplo: $n = 60$, cujos divisores unitários são: 1 e 60, 4 e 15, 3 e 20, 5 e 12. Pelo teorema anterior a cada um destes divisores unitários está associado um idempotente de $\mathbb{Z}_{60}$. Para além disso basta-nos calcular os idempotentes associados a 4, 3 e 5 pois os outros resultam da alínea c) do teorema anterior e da observação acima. Vamos assim resolver os sistemas

$$\left\{\begin{array}{rcl} a & \equiv & 0 \ (\bmod 4) \\ a & \equiv & 1 \ (\bmod 15) \end{array}\right. \quad \left\{\begin{array}{rcl} a & \equiv & 0 \ (\bmod 3) \\ a & \equiv & 1 \ (\bmod 20) \end{array}\right. \quad \left\{\begin{array}{rcl} a & \equiv & 0 \ (\bmod 5) \\ a & \equiv & 1 \ (\bmod 12) \end{array}\right.$$

Vamos resolver apenas o primeiro sistema. A primeira congruência diz que $4 = 4k$ para algum $k \in \mathbb{N}$. Ficamos assim sucessivamente com

$$\left\{\begin{array}{rcl} a & = & 4k \\ 4k & \equiv & 1 \ (\bmod 15) \end{array}\right. \quad \left\{\begin{array}{rcl} a & = & 4k \\ k & \equiv & 4 \ (\bmod 15) \end{array}\right.$$

o que diz que $a = 16$. O idempotente associado a 15 é 45.

Repetindo o mesmo tipo de argumentação concluímos que os idempotentes de $\mathbb{Z}_{60}$ são: 0, 1, 16, 45, 21, 40, 25 e 36.

2.4 Característica de um anel

Definição 2.4.1. *Seja A um anel. Define-se* **característica** *de A como sendo o menor inteiro positivo n, caso exista, tal que*

$$\forall a \in A \quad na = 0.$$

Se um tal inteiro não existir, dizemos que a característica do anel é zero.
Denotamos a característica de A por $\mathrm{car}(A)$

A característica de um anel A tem apenas que ver com a sua estrutura aditiva. Dizer que $na = 0$ para $a \in A$ e $n \in \mathbb{N}$ equivale a dizer que a ordem em a no grupo $< A, + >$ divide n. Em particular:

- $\mathrm{car}(A)$ é o mínimo múltiplo comum, se existir, das ordens dos elementos do grupo $< A, + >$, e é igual a 0 se esse mínimo múltiplo comum não existir;
- se A for finito então $\mathrm{car}(A)$ divide $|A|$ (pelo teorema de Lagrange).

Facilmente se mostra que $\text{car}(\mathbb{Z}) = \text{car}(\mathbb{Q}) = \text{car}(\mathbb{R}) = \text{car}(\mathbb{C}) = 0$, $\text{car}(\mathbb{Z}_n) = n$, $\text{car}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots) = 2$, $\text{car}(A \times B) = [\text{car}(A), \text{car}(B)]$, se A e B são anéis.

O cálculo da característica de um anel simplifica-se bastante se ele tiver elemento um.

Proposição 2.4.2. *Se $< A, +, \cdot >$ é um anel com elemento um (e) então*

$$\text{car}(A) = \begin{cases} 0 & \text{se } ne \neq 0 \text{ para todo } n \in \mathbb{N} \\ \text{menor } n \in \mathbb{N} \text{ tal que } ne = 0 & \text{caso contrário.} \end{cases}$$

Demonstração. Basta notar que, se $n \in \mathbb{N}$ é tal que $ne = 0$ e $a \in A$ então $na = n(ea) = (ne)a = 0a = 0$. □

Este resultado diz que a característica de um anel com elemento um (e) é a ordem de e no grupo aditivo $(A, +)$.

Corolário 2.4.3. *A característica de um DI é 0 ou é um número primo.*

Demonstração. Seja e o elemento um do DI. Note-se que a característica não pode ser 1 pois nesse caso $e = 1e = 0$. Suponhamos que a característica de D é igual a rs em que $1 < r, s$. Então

$$(re)(se) = (rs)(ee) = (rs)e = 0,$$

e portanto, como D é um DI, $re = 0$ ou $se = 0$, o que contradiz a proposição anterior. □

Vamos fazer agora duas demonstrações do teorema seguinte. Uma usando o Teorema de Cauchy para grupos e outra usando resultados básicos de álgebra linear.

Teorema 2.4.4. *Se $\mathbb{K}$ é um corpo finito e $p \in \mathbb{P}$ é a sua característica então existe $r \in \mathbb{N}$ tal que $\mathbb{K}$ tem p^r elementos.*

Demonstração. (usando o Teorema de Cauchy)

Note-se que a ordem de qualquer elemento não nulo no grupo aditivo $(\mathbb{K}, +)$ é p, uma vez que $px = 0$ para todo $x \in \mathbb{K}$. Se a ordem de $\mathbb{K}$ não fosse uma potência de p então existia um primo q, diferente de p, que dividia a ordem de $\mathbb{K}$. Como $(\mathbb{K}+)$ é um grupo então pelo Teorema de Cauchy (página 44) (versão abeliana) existe um elemento em $(\mathbb{K}, +)$ com ordem q, o que é absurdo.

Demonstração. (usando o Álgebra Linear)

Seja $A = \{ke : k = 0, 1, \ldots, p-1\}$. É fácil de mostrar que $(A, +, \cdot)$ é um corpo (subcorpo de $(\mathbb{K}, +, \cdot)$). Note-se que, se $k \in \{1, \ldots, p-1\}$ então o inverso de ke é se em que s é solução da congruência $kx \equiv 1 \pmod{p}$, que tem solução porque $(k, p) = 1$.

Deste modo $\mathbb{K}$ é um espaço vectorial sobre o corpo A com dimensão finita (pois $\mathbb{K}$ é finito). Seja $\{a_1, a_2, \ldots, a_n\}$ uma base de K sobre A. Deste modo todo o elemento de $\mathbb{K}$ se escreve de maneira única na forma $\lambda_1 a_1 + \cdots + \lambda_n a_n$, o que mostra que $\mathbb{K}$ tem p^n elementos. □

2.5 Imersão de um DI num corpo

Diz-se que um anel A está mergulhado num anel B se A for isomorfo a um subanel de B, isto é, se existir um homomorfismo injectivo de A em B.

Em vista desta definição, o anel $2\mathbb{Z}$, que não tem elemento um, está mergulhado em $\mathbb{Z}$ que tem elemento um. É fácil de mostrar que este resultado é geral.

Seja A um anel e consideremos $B = A \times \mathbb{Z}$. Vamos munir B de uma estrutura de anel, definindo para $(a, m), (b, n) \in B$,

$$(a, m) + (b, n) = (a + b, m + n), \quad (a, m) \cdot (b, n) = (ab + na + mb, mn).$$

É simples verificar que $< B, +, \cdot >$ é um anel, que $(0, 1)$ é o seu elemento um e que a função que associa a cada elemento a de A o elemento $(a, 0)$ é um homomorfismo injectivo.

Seja D um DI e vamos construir um corpo $\mathbb{K}$ de tal modo que D está mergulhado em $\mathbb{K}$. A ideia da construção é sugerida pela construção dos números racionais a partir dos números inteiros.

Seja $A = D \times (D \setminus \{0\})$. Defina-se sobre A seguinte relação ρ,

$$\forall (a, b), (c, d) \in A \quad \big[(a, b) \, \rho \, (c, d) \;\Leftrightarrow\; ad = bc \big].$$

Note-se que ρ é uma relação de equivalência sobre A. Denote-se por $[(a, b)]$ a classe de equivalência de (a, b). Observe-se que:

- para $(a, b) \in A$, $[(a, b)] = \{(xa, xb) : x \in D \setminus \{0\}\}$;
- $[(0, 1)] = \{(0, x) : x \in D \setminus \{0\}\}$;
- $[(1, 1)] = \{(x, x) : x \in D \setminus \{0\}\}$;
- se $(a, b), (c, d), (x, y), (z, t) \in A$ então

$$(ad + bc, bd) \, \rho \, (xt + yz, yt) \;\text{ e }\; (ac, bd) \, \rho \, (xz, yt).$$

Seja $\mathbb{K} = A/\rho$. Pela última observação, as seguintes funções estão bem definidas.

$$\begin{array}{rccc} \oplus : & \mathbb{K} \times \mathbb{K} & \longrightarrow & \mathbb{K} \\ & \big([(a,b)], [(c,d)]\big) & \mapsto & [(ad + bc, bd)] \end{array} \qquad \begin{array}{rccc} \odot : & \mathbb{K} \times \mathbb{K} & \longrightarrow & \mathbb{K} \\ & \big([(a,b)], [(c,d)]\big) & \mapsto & [(ac, bd)] \end{array}$$

Facilmente se mostra que $< \mathbb{K}, \oplus, \odot >$ é um corpo tal que:

- o elemento zero é $[(0, 1)]$;
- o elemento um é $[(1, 1)]$;
- o inverso de um elemento não nulo, isto é, da forma $[(a, b)]$ com $a, b \neq 0$ é o elementos $[(b, a)]$.

Para concluir basta notar que a função de D em $\mathbb{K}$ que associa a cada $a \in D$ o elemento $[(a, 1)]$ é um homomorfismo injectivo.

2.6 Exercícios

Exercício 1. Mostre que a intersecção de subanéis de um anel é um subanel.

Exercício 2. Mostre que $< \mathbb{Z}, *, \diamondsuit >$ em que

$$\forall m, n \in \mathbb{Z} \quad m * n = m + n - 1,\ m \diamondsuit n = m + n - mn$$

é um anel comutativo com elementos um. O anel é um domínio de integridade?

Exercício 3. Seja $(A, +, \cdot)$ um anel com elemento um e U o subconjunto de A formado pelos invertíveis de A. Mostre que:

a) $(U, \cdot)$ é um grupo;
b) se $n \in \mathbb{N}$, $a \in A$ e $a^n \in U$ então $a^n \in U$;
c) se $a, b \in A$ e $ab \in U$ então $a, b \in U$.

Exercício 4. (Uma apresentação do anel dos quaterniões) Mostre que $< \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} : \ a, b \in \mathbb{C} \right\}, +, \cdot >$ é um anel de divisão que não é um corpo.

Exercício 5. Sejam $p \in \mathbb{P}$ e $D = \{\frac{a}{p^k} : \ a \in \mathbb{Z},\ k \in \mathbb{N}_0,\ p \nmid a\}$. Mostre que $< D, +, \cdot >$ (em que $+$ e $\cdot$ são a soma e multiplicação usual em $\mathbb{R}$) é um domínio de integridade.

Exercício 6. Seja m um inteiro que não é um quadrado perfeito.

a) Mostre que $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$ é um domínio de integridade (com a soma e o produto usuais em $\mathbb{C}$) cujos invertíveis são os elementos $a + b\sqrt{m}$ tais que $|a^2 - mb^2| = 1$. Faça $m = -5$ e calcule explicitamente os invertíveis de $\mathbb{Z}[\sqrt{m}]$.
b) Mostre que $\mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m} : a, b \in \mathbb{Q}\}$ é um corpo (com a soma e o produto usuais em $\mathbb{C}$).

Exercício 7. Mostre que, se A é um anel com elemento um (e) e $a \in A$ admite um só inverso à esquerda a', então a' é inverso de a. Sugestão: Calcule $(a' + aa' - e)a$.

Exercício 8. Seja A um anel com elemento um (e) e $a, b \in A$ tais que $e - ab$ é invertível. Mostre que $e - ba$ é invertível. Sugestão: Calcule $(e - ba)\left(e + b(1 - ab)^{-1}a\right)$.

Exercício 9. Mostre que o anel $< \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : \ a, b \in \mathbb{R} \right\}, +, \cdot >$ tem uma infinidade de elementos um à esquerda e não tem elemento um.

Exercício 10. Mostre que, se num anel com elemento um, um elemento tem dois inversos esquerdos então tem uma infinidade de inversos esquerdos.

Exercício 11. Sejam A um domínio de integridade e $a, b \in A$ tais que $3a = 3b$ e $a \neq b$. Mostre que $3x = 0$ para todo $x \in A$. E se no lugar de 3 estiver 6?

Exercício 12. Seja A um anel. Para $x, y \in A$ defina-se $[x, y] = xy - yx$. Demonstre a chamada *igualdade de Jacobi*

$$\forall x, y, z \in A \quad [x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0.$$

Exercício 13. Resolva os sistemas:

a) $\begin{cases} 3x+4y &= 5 \\ 4x+5y &= 3 \end{cases}$ em $\mathbb{Z}_{20}$;

b) $\begin{cases} 4x+6y &= 8 \\ 10x+8y &= 4 \end{cases}$ em $\mathbb{Z}_{24}$;

c) $\begin{cases} 2x+ay &= b \\ ax+5y &= 2b+1 \end{cases}$ em $\mathbb{Z}_{14}$, para os diversos valores de a e b.

Exercício 14. Seja A um anel no qual todo o elemento é idempotente. Mostre que A é comutativo (comece por mostrar que $a = -a$ para todo $a \in A$).

Exercício 15. Seja A um anel tal que, se $x \in A$ então $x^2 - x$ comuta com qualquer elemento de A. Mostre que, se $x, y \in A$ então:

a) $xy + yx$ comuta com todos os elementos de A;

b) $yx^2 = x^2y$;

c) $xy = yx$.

Conclua que A é um anel comutativo.

Exercício 16. Quais os elementos idempotentes do anel $\mathcal{M}_{2\times 2}(\mathbb{Z})$?

Exercício 17. Mostre que $4\,\mathbb{Z}_{84}$ tem elemento um. Verifique se 76 tem inverso.

Exercício 18. Mostre que anel $< \left\{ \begin{pmatrix} n & 0 \\ 2n & 0 \end{pmatrix} : \ n \in \mathbb{N} \right\}, +, \cdot >$ é isomorfo ao anel dos números reais.

Exercício 19. Seja A um anel tal que $a^3 = a$ para todo $a \in A$. Considere $Z = \{a \in A : ax = xa, \ \forall x \in A\}$. Mostre que

a) se $ab = 0$ então $ba = 0$. Sug: desenvolva $(ba)^3$.

b) $a^2 \in Z$ para todo $a \in A$. Sug: desenvolva $a^2(x - a^2x)$ e $(x - xa^2)a^2$.

c) $a + a^2 \in Z$. Sug: verifique que $(a + a^2)^3 = 2(a + a^2)^2$.

d) A é comutativo, ou seja $A = Z$.

Exercício 20. Mostre que um idempotente não nulo de um anel nunca é um nilpotente.

Exercício 21. Seja A um anel admitindo com mais que um elemento um à direita. Mostre que o anel admite divisores próprios de zero.

Exercício 22. Seja A um anel sem elemento propriamente nilpotentes. Mostre que, se $a, b \in A$, n, m são inteiros positivos primos entre si e $a^m = b^m$ e $a^n = b^n$ então $a = b$.

Exercício 23. Seja X um conjunto não vazio. Mostre que $< \mathcal{P}(X), \triangle, \cap >$ em que

$$\forall A, B \in \mathcal{P}(X) \quad A \triangle B = (A \cup B) \setminus (A \cap B),$$

é um anel comutativo com elemento um. Quais os elementos invertíveis do anel? E os nilpotentes? E os divisores de zero? E os idempotentes?

Exercício 24. Suponha que X é infinito e considere $T = \{A \in \mathcal{P}(X) : A \text{ é finito}\}$. Mostre que:

a) T é um subanel do anel $< \mathcal{P}(X), \triangle, \cap >$;

b) T não tem elemento um;

c) todo o elemento de T é um divisor de zero (em T).

Exercício 25. Seja A um anel, $a \in A$ e $\begin{array}{rccc} f_a : & A & \longrightarrow & A \\ & x & \mapsto & ax \end{array}$.

a) Mostre que f_a é injectiva se e só se a não é divisor de zero.

b) Dê um exemplo em que f_a seja injectiva e não seja bijectiva.

c) Mostre que, se A for finito e a não é divisor de zero então f_a é sobrejectiva.

d) Mostre que, se A for finito, a não é divisor de zero e $f_a(b) = a$ então A tem elemento um e os seus elementos não invertíveis são os divisores de zero.

Exercício 26. Sejam a, b dois divisores de zero de um anel. Mostre que $a + a$ é um divisor de zero mas que $a + b$ pode não ser. O que acontece com ab?

Exercício 27. Sejam A um anel com elemento um (e) e $b \in A$. Mostre que, se b é nilpotente então $e + b$ é invertível. Generalize o resultado considerando em vez de e um qualquer invertível a que comute com b.

Exercício 28. Seja A um anel em que 0 é o único elemento nilpotente. Mostre que, se $e, x \in A$ e $e = e^2$ então $ex = xe$ (comece por calcular $(ex - exe)^2$).

Exercício 29. Seja A um anel não trivial com elemento identidade e. Mostre que, se r é um idempotente de A então $e - r$ é idempotente e r ou $e - r$ é um divisor de zero.

Exercício 30. Seja A um anel não trivial tal que para todo $a \in A \setminus \{0\}$ existe um e e um só $b \in A$ tal que $a = aba$. Mostre que:

a) A não tem divisores próprios de zero;

b) A tem elemento um;

c) se $a, b \in A$, $aba = a$ e $a \neq 0$ então $bab = b$;

d) A é um anel de divisão.

Exercício 31. Mostre que no anel $\mathcal{M}_{2\times 2}(\mathbb{Z})$ os elementos $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ e $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ são nilpotentes e a sua soma e o seu produto não é nilpotente.

Exercício 32. Mostre que num um anel comutativo, o conjunto formado pelos elementos nilpotentes é um ideal.

Exercício 33. Determine todos os elementos nilpotentes do anel $\mathcal{M}_{2\times 2}(\mathbb{Z})$.

Exercício 34. Determine os idempotentes e os nilpotentes de $\mathbb{Z}_{900}$ e de $\mathbb{Z}_{136}$.

Exercício 35. Quais os inteiros $n \in \mathbb{N}$ tais que $\mathbb{Z}_n$ não tem elementos propriamente nilpotentes.

Exercício 36. Para que inteiros n o anel $\mathbb{Z}_n$ tem 8 idempotentes e 100 nilpotentes? E 8 idempotentes e 20 nilpotentes?

Exercício 37. Determine $m \in \mathbb{Z}_{880}$ tal que $f_m : \begin{array}{ccc} \mathbb{Z}_{880} & \longrightarrow & \mathbb{Z}_{880} \\ x & \mapsto & mx \end{array}$ seja um endomorfismo não nulo. Para cada um dos valores de m encontrados calcule $\mathrm{Nuc} f_m$.

Exercício 38.

a) Calcule os idempotentes de $\mathbb{Z}_{144}$.

b) Quais os elementos de $\mathbb{Z}_{144}$ que são iguais ao seu inverso?

c) Mostre que o anel $12\mathbb{Z}_{144}$ não tem elemento 1.

d) Mostre que o anel $9\mathbb{Z}_{144}$ tem elemento 1.

e) Resolva a equação $16\,X = 48$ no anel $12\mathbb{Z}_{144}$

Exercício 39. Considere o anel $3\,\mathbb{Z}$ e o seu ideal $1800\,\mathbb{Z}$.

a) Calcule os idempotentes de $\mathbb{Z}_{1800}$.

b) Resolva a equação $(3a + 1800\,\mathbb{Z})(3 + 1800\,\mathbb{Z}) = (3 + 1800\,\mathbb{Z})$.

c) Conclua que o anel $3\mathbb{Z}/1800\mathbb{Z}$ não tem elemento um.

Exercício 40. Quais os inteiros n tais que $\mathbb{Z}_n$ admite:

a) apenas os idempotentes 0 e 1?

b) admite apenas os idempotentes 0, 1, 49 e 344?

c) os idempotentes 0, 1, 3025 e 5929?

Exercício 41. Sejam $n \in \mathbb{N}$ e s o número de primos ímpares que dividem n. Usando um raciocínio análogo ao que foi utilizado no Teorema 2.3.6 pretendemos calcular o número de elementos de ordem 2. Mostre que:

a) a tem ordem 2 se e só se n divide $(a-1)(a+1)$;

b) se $a \in \mathbb{Z}$ então $(a-1, a+1) \in \{1, 2\}$;

c) se n é ímpar ou o dobro de um número ímpar, então a tem ordem 2 se e só se existe um divisor unitário d tal que d divide $a-1$ e $\frac{n}{d}$ divide $(a+1)$;

d) se n é ímpar ou o dobro de um número ímpar então existem 2^s elementos de $\mathbb{Z}_n$ com ordem 2;

e) se n é o quadruplo de um número ímpar então existem 2^{s+1} elementos de $\mathbb{Z}_n$ com ordem 2;

f) se n não está nas condições das duas alíneas anteriores então existem 2^{s+2} elementos de $\mathbb{Z}_n$ com ordem 2.

Exercício 42. Seja A um anel e $a \in A$. Mostre que o conjunto $\{x \in A : ax = 0\}$ é um ideal direito de A.

Exercício 43. Sejam A um anel comutativo com elemento um e $a, b \in A$. Mostre que $\{ax + by : x, y \in A\}$ é o ideal gerado por $\{a, \}$ (menor ideal de A contendo $\{a.b\}$). O que muda se o anel não tiver elemento um? E se não for comutativo?

Exercício 44. Seja $\mathbb{K}$ um corpo com característica p ($p \in \mathbb{P}$). Mostre, por indução sobre r, que:

$$\forall x, y \in \mathbb{K} \;\; \forall r \in \mathbb{N} \quad (x + y)^{p^r} = x^{p^r} + y^{p^r}$$

Exercício 45. Seja A um anel comutativo e $I \trianglelefteq A$. Mostre que $\{x \in A : \exists n \in \mathbb{N},\ x^n \in I\} \trianglelefteq A$.

Exercício 46. Mostre que todo o anel comutativo com elemento um admitindo apenas ideias triviais é um corpo.

Exercício 47. Determine os endomorfismos de $\mathbb{Z}$ e de $\mathbb{Z}_{180}$.

Exercício 48. Sejam A um anel e $I, J \trianglelefteq A$. Mostre que $I + J \trianglelefteq A$ e $(I + J)/J \cong I/(I \cap J)$.

Exercício 49. Sejam A um anel e $I, J \trianglelefteq A$. Mostre que $\{x \in A : x\, I \subseteq J\} \trianglelefteq A$.

Exercício 50. Considere o anel $\mathbb{Z}_{160}$ e o subanel $5\,\mathbb{Z}_{160}$.

a) Verifique se $5\,\mathbb{Z}_{160}$. tem elemento um e, em caso afirmativo, determine os invertíveis de $5\,\mathbb{Z}_{160}$.

b) Verifique se existe algum epimorfismo de $\mathbb{Z}_{160}$ em $5\,\mathbb{Z}_{160}$ e, em caso afirmativo calcule o seu núcleo.

Exercício 51. Considere o anel $\mathbb{Z}_{540}$ e o subanel $2\,\mathbb{Z}_{540}$.

a) Verifique se $2\,\mathbb{Z}_{540}$ tem elemento um e, em caso afirmativo, verifique se 162 é invertível.

b) Mostre que existe um epimorfismo de $\mathbb{Z}_{540}$ em $2\,\mathbb{Z}_{540}$ e determine o seu núcleo.

c) Resolva em $2\,\mathbb{Z}_{540}$ a equação $140\,x = 36$.

Exercício 52. Quais das seguintes afirmações são verdadeiras?

a) $\mathbb{Z}_{320} \leq \mathbb{Z}_{640}$.

b) Se A é um anel e $I \leq A$ então $\{x \in A : x^2 \in I\} \leq A$.

c) Se D é um domínio de integridade, $a \in D \setminus \{0\}$ e $a^2 = 2a$ então $ab = 2b$ para todo $b \in D$.

d) Se $f : A \to B$ é um homomorfismo de anel e $I \trianglelefteq A$ então $f(I) \trianglelefteq B$.

e) O anel $3\mathbb{Z}/210\mathbb{Z}$ não tem elementos propriamente nilpotentes.

f) Se A é um anel e $a \in A$ tal que $18\,a = 23\,a$ então $a = 0$.

Capítulo 3

Divisibilidade

3.1 Preliminares

Vamos agora, dado um anel A, definir o que se entende por divisibilidade. O nosso modelo será o anel dos inteiros no qual temos a relação de divisão usual. Naturalmente, dados dois elementos a e b de A, dizemos que a divide b se e só se a "vezes" algum elemento de A é igual a b. Aqui surge-nos o primeiro problema: se o a anel A não for comutativo teremos de definir duas divisões, a esquerda e a direita, ou optar por uma delas. Por exemplo, se considerarmos o anel $\mathcal{M}_{2\times 2}(\mathbb{Z})$, o anel das matrizes 2×2 de entradas inteiras e

$$a = \begin{pmatrix} 2 & 1 \\ 0 & 4 \end{pmatrix}, \quad b = \begin{pmatrix} 2 & 4 \\ 0 & 8 \end{pmatrix}$$

então a é um "divisor esquerdo" e não é um "direito direito" de b.

A solução que adoptaremos aqui é a de considerar apenas anéis comutativos.

Queremos também que a relação "divide" seja, como em $\mathbb{Z}$, uma relação reflexiva e transitiva. A transitividade não levanta problemas, mas o mesmo não acontece com a reflexividade. Por exemplo: no anel $2\mathbb{Z}$ apenas o elemento 0 divide ele próprio. Um modo de "resolver este problema" é trabalhar apenas com anéis com elemento um.

Queremos ainda, dados elementos a e b tais que a divide b, "poder falar" no quociente de b por a. Ou seja, se x é tal que $b = ax$, queremos definir x como o quociente de b por a. Para isso é preciso garantir a unicidade de x. Queremos então que A tenha a propriedade

$$\forall a, b, x, y \in A, \ [ax = b, ay = b, a \neq 0 \ \Rightarrow x = y].$$

Ou seja, queremos que A seja um DI.

A partir daqui, e em tudo o que diga respeito a divisibilidade num anel, suporemos que o anel é um DI.

Definição 3.1.1. *Seja D um DI e $a, b \in D$. Dizemos que:*

a) *a* **divide** *b, e notaremos $a|b$, se existir $x \in D$ tal que $ax = b$;*

b) *a é* **associado** *a b, e notaremos $a \sim b$, se $a|b$ e $b|a$.*

Vejamos algumas propriedades elementares cuja demonstração é deixada como exercício.

Lema 3.1.2. *Sejam D um domínio de integridade e $a, b, c, d, \mu \in D$, com μ invertível. Então:*

a) *se $a|b$ então $a|bc$;*

b) *$\mu|a$;*

c) *$a|b$ se e só se $\mu a|b$;*

d) *se $a|b$ e $c|d$ então $ac|bd$;*

e) *se $a|b$ e $a|c$ então $a|(b+c)$.*

Nota 3.1.3. *Se D é um DI e $a \in D$ então $a \sim 1$ se e só se a é invertível.*

Em $\mathbb{Z}$ dois elementos são associados se e só se um deles é o produto do outro por 1 ou -1. Notar que 1 e -1 são os únicos invertíveis de $\mathbb{Z}$.

Resultado análogo é válido para qualquer DI.

Proposição 3.1.4. *Seja D um DI e $a, b \in D$. Então $a \sim b$ se e só se existe x, elemento invertível de D tal que $ax = b$.*

Demonstração.

$\Rightarrow$

Sejam x e y tais que $ax = b$ e $by = a$. Se $a = 0$ então $b = 0$ e portanto $a1 = b$. Se $a \neq 0$ então $a = axy$ e, pela lei do corte, $xy = 1$ e portanto x e y são invertíveis.

$\Leftarrow$

Suponhamos que $ax = b$ com x invertível. Se y é o inverso de x então $a = axy = by$, o que mostra que a e b são associados. □

Vamos agora introduzir os conceitos de *primo* e de *irredutível*, conceitos esses que, como sabemos, são equivalentes em $\mathbb{Z}$. Veremos que tais conceitos são equivalentes numa classe relativamente grande de domínios de integridade.

Definição 3.1.5. *Seja D um domínio de integridade. Um elemento a de D diz-se* **irredutível** *se:*

a) *$a \neq 0$;*

b) *a não é invertível ($a \not\sim 1$);*

c) *$\forall x, y \in D \ \big[a = xy \ \Rightarrow \ a \sim x \ ou \ a \sim y\big]$.*

Atendendo à Proposição 3.1.4, a última condição é equivalente a cada uma das seguintes

c') $\forall x, y \in D \ \big[a = xy \ \Rightarrow \ x \sim 1 \ ou \ y \sim 1\big]$,

c") $\forall x, y \in D \ \big[a = xy \ \Rightarrow \ (x \sim 1 \ e \ y \sim a) \ \ ou \ \ (x \sim a \ e \ y \sim 1)\big]$.

Chamamos **redutível** a um elemento não nulo nem invertível que não seja irredutível. Temos assim D escrito como uma união disjunta

$$D = \{0\} \cup \{\text{invertíveis de } D\} \cup \{\text{irredutíveis de } D\} \cup \{\text{redutíveis de } D\}.$$

Definição 3.1.6. *Um elemento a de um domínio de integridade D diz-se* **primo** *se:*

a) $a \neq 0$;

b) *a não é invertível;*

c) $\forall x, y \in D \ \big[a|xy \ \Rightarrow \ a|x \text{ ou } a|y\big]$.

Proposição 3.1.7. *Seja D um DI e $a \in D$. Se a é primo então a é irredutível.*

Demonstração. Suponhamos que existiam $x, y \in D$ tais que $a = xy$. Então a divide xy e, como a é primo, a divide x ou a divide y. Como x e y dividem a, concluímos que a é associado ou x ou a y. □

É claro que se D é um domínio de integridade, p é um primo então

$$\forall n \in \mathbb{N} \ \forall a_1, \ldots, a_n \in D \ \ \Big[p|a_1 \cdots a_n \implies \exists i \leq n \ \ p|a_i\Big].$$

Na secção seguinte são dados exemplos de domínios de integridade admitindo elementos irredutíveis que não são primos.

3.2 Anéis $\mathbb{Z}[\sqrt{d}]$ e $\mathbb{Z}[i\sqrt{d}]$, com $d \in \mathbb{N}$

Dado $d \in \mathbb{N}$ denotemos por $\mathbb{Z}[\sqrt{d}]$ o menor subanel de $\mathbb{R}$ que contém $\mathbb{Z}$ e $\sqrt{d}$ e por $\mathbb{Z}[i\sqrt{d}]$ o menor subanel de $\mathbb{C}$ que contém $\mathbb{Z}$ e $i\sqrt{d}$. É claro que, se d for um quadrado perfeito então $\mathbb{Z}[\sqrt{d}] = \mathbb{Z}$. Por esse motivo, sempre que falarmos no anel $\mathbb{Z}[\sqrt{d}]$ estaremos a supor que $\boxed{d \text{ não é um quadrado perfeito}}$. No caso do anel $\mathbb{Z}[i\sqrt{d}]$, d pode ser um inteiro positivo qualquer. É imediato ver que

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}, \quad \mathbb{Z}[i\sqrt{d}] = \{a + bi\sqrt{d} : a, b \in \mathbb{Z}\}.$$

Nas condições referidas consideremos as funções

$$\begin{array}{ccc} \mathbb{Z}[\sqrt{d}] & \longrightarrow & \mathbb{N}_0 \\ a + b\sqrt{d} & \mapsto & \left|a^2 - db^2\right| \end{array} \qquad \begin{array}{ccc} \mathbb{Z}[i\sqrt{d}] & \longrightarrow & \mathbb{N}_0 \\ a + bi\sqrt{d} & \mapsto & a^2 + db^2 \end{array} \tag{3.1}$$

Facilmente se mostra que estas funções preservam o produto ou seja

$$\forall a, b, x, y \in \mathbb{Z} \quad \begin{cases} \left|(ax + byd)^2 - d(ay + bx)^2\right| = \left|a^2 - db^2\right| \ \left|x^2 - dy^2\right| \\ (ax - byd)^2 + d(ay + bx)^2 = \left(a^2 + db^2\right)\left(x^2 + dy^2\right) \end{cases}$$

Como consequência temos os seguintes resultados apresentados em separados para os anéis $\mathbb{Z}[\sqrt{d}]$ e $\mathbb{Z}[i\sqrt{d}]$.

Proposição 3.2.1. *Seja d um inteiro positivo que não é quadrado perfeito e $a+b\sqrt{d}, x+y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Então,*

a) *se* $a+b\sqrt{d}$ *divide* $x+y\sqrt{d}$ *então* $\left|a^2-db^2\right|$ *divide* $\left|x^2-dy^2\right|$;

b) $a+b\sqrt{d}$ *é invertível se e só se* $a^2-db^2=\pm 1$;

c) *há uma infinidade de elementos invertíveis.*

Demonstração.

a) Se existe $r+s\sqrt{d}\in\mathbb{Z}[\sqrt{d}]$ tal que $(a+b\sqrt{d})(r+s\sqrt{d})=x+y\sqrt{d}$ então, pela observação acima, $\left|a^2-db^2\right|\cdot\left|r^2-ds^2\right|=\left|x^2-dy^2\right|$ e portanto $\left|a^2-db^2\right|$ divide $\left|x^2-dy^2\right|$.

b) Se $a+b\sqrt{d}$ é invertível então divide 1 e portanto, pela alínea anterior, $a^2-db^2=\pm 1$. Para mostrar o inverso basta notar que $(a+b\sqrt{d})(a-b\sqrt{d})=a^2-db^2$.

c) Do estudo das equações de Pell (não são resultados triviais) há sempre inteiros positivos a e b tais que $a^2-db^2=1$. Deste modo $a+b\sqrt{d}$ e qualquer das suas potências positivas (que são todas diferentes) são elementos invertíveis de $\mathbb{Z}[\sqrt{d}]$. □

Em $\mathbb{Z}[\sqrt{2}]$, $1+\sqrt{2}$ e $3+2\sqrt{2}$ são invertíveis pois $1^2-2\cdot 1^2=-1$ e $3^2-2\cdot 2^2=1$. Deste modo qualquer potência destes números é invertível. Por exemplo, $41+29\sqrt{2}, 99+70\sqrt{2}, 665857+470832\sqrt{2}$ são invertíveis de $\mathbb{Z}[\sqrt{2}]$.

Do mesmo modo, $2+\sqrt{3}, 97+56\sqrt{3}, 26650854921601+15386878263120\sqrt{3}$ são invertíveis de $\mathbb{Z}[\sqrt{3}]$. Note-se que a equação $x^2-3y^2=-1$ não tem solução (faça as contas "módulo 3").

Proposição 3.2.2. *Seja* $d\in\mathbb{N}$ *e* $a+ib\sqrt{d}, x+yi\sqrt{d}\in\mathbb{Z}[i\sqrt{d}]$. *Então,*

a) *se* $a+bi\sqrt{d}$ *divide* $x+yi\sqrt{d}$ *então* a^2+db^2 *divide* x^2+dy^2;

b) *os invertíveis de* $\mathbb{Z}[i]$ *são* 1, -1, i *e* -1 *(sendo* 1 *e* -1 *inversos deles próprios e* i *e* $-i$ *inversos um do outro);*

c) *se* $d>1$ *os invertíveis de* $\mathbb{Z}[i\sqrt{d}]$ *com* $d>1$ *são* 1 *e* -1.

Demonstração. A demonstração segue os passos da demonstração da proposição anterior. A situação aqui é mais simples uma vez que a equação $a^2+db^2=1$ tem resolução trivial. □

Vejamos que nestes anéis as noções de *primo* e de *irredutível* nem sempre coincidem.

Corolário 3.2.3. *Se* $d\in\mathbb{N}$ *e* $d\geq 3$ *então* 2 *é um irredutível de* $\mathbb{Z}[i\sqrt{d}]$ *que não é primo.*

Demonstração. Note-se que 2 é irredutível em $\mathbb{Z}[i\sqrt{d}]$. De facto, se $2=(a+bi\sqrt{d})(x+yi\sqrt{d})$ com $a+bi\sqrt{d}, x+yi\sqrt{d}$ elementos não invertíveis de $\mathbb{Z}[i\sqrt{d}]$ então atendendo às alíneas a) e b) da proposição anterior, teríamos $a^2+db^2=x^2+dy^2=2$, o que é impossível com $d\geq 3$. Vejamos que 2 não é primo em $\mathbb{Z}[i\sqrt{d}]$.

• Se d é ímpar então 2 divide $d+1$ e $d+1=(1+i\sqrt{d})(1-i\sqrt{d})$. Se 2 fosse primo então 2 dividiria $1+i\sqrt{d}$ ou $1-i\sqrt{d}$, o que não acontece.

• Se d é par então 2 divide $d+4$ e $d+4=(2+i\sqrt{d})(2-i\sqrt{d})$. Se 2 fosse primo então 2 dividiria $2+i\sqrt{d}$ ou $2-i\sqrt{d}$, o que não acontece. □

Note-se que, fazendo (por exemplo) $d = 5$, $d = 3$ e $d = 6$, obtemos

$$\begin{cases} 6 = 2 \times 3 = & (1 + i\sqrt{5})(1 - i\sqrt{5}) \text{ e } 2,\ 3,\ 1 + i\sqrt{5} \text{ e } 1 - i\sqrt{5} \\ & \text{são todos irredutíveis e não primos de } \mathbb{Z}[i\sqrt{5}]. \\ 4 = 2 \times 2 = & (1 + i\sqrt{3})(1 - i\sqrt{3}) \text{ e } 2,\ 1 + i\sqrt{3} \text{ e } 1 - i\sqrt{3} \\ & \text{são todos irredutíveis e não primos de } \mathbb{Z}[i\sqrt{3}]. \\ 10 = 2 \times 5 = & (2 + i\sqrt{6})(2 - i\sqrt{6}) \text{ e } 2,\ 5,\ 2 + i\sqrt{6} \text{ e } 2 - i\sqrt{6} \\ & \text{são todos irredutíveis e não primos de } \mathbb{Z}[i\sqrt{6}]. \end{cases}$$

No caso dos anéis $\mathbb{Z}[\sqrt{d}]$ a situação é mais complicada. Apresentamos aqui a situação mais simples.

Corolário 3.2.4. *Se d é um inteiro positivo maior que 1, que não é um quadrado perfeito e é congruente com 1 módulo 4 então 2 é um irredutível de $\mathbb{Z}[\sqrt{d}]$ que não é primo.*

Demonstração. A ideia é semelhante à do corolário anterior. Note-se que 2 divide $d-1$, que $d-1 = (1+\sqrt{d})(-1+\sqrt{d})$ e que 2 não divide $1+\sqrt{d}$ nem $-1+\sqrt{d}$. Resta mostrar que 2 é irredutível. Se 2 fosse redutível então (com os mesmos argumentos que acima) existiriam $a + b\sqrt{d}, x + y\sqrt{d}$ não invertíveis tais que $2 = (a + b\sqrt{d})(x + y\sqrt{d})$. Em particular $4 = |a^2 - db^2|\,|x^2 - dy^2|$ e portanto $a^2 - db^2 = \pm 2$. Trabalhando agora módulo 4 temos $a^2 - db^2 \equiv a^2 - b^2 \pmod 4$, pela hipótese sobre d. Mas

$$\begin{cases} a^2 - b^2 \equiv 0 \pmod 4 & \text{se } a, b \text{ forem pares} \\ a^2 - b^2 \equiv 0 \pmod 4 & \text{se } a, b \text{ forem ímpares} \\ a^2 - b^2 \equiv 1 \pmod 4 & \text{se } a \text{ for par e } b \text{ ímpar} \\ a^2 - b^2 \equiv 3 \pmod 4 & \text{se } a \text{ for ímpar e } b \text{ par.} \end{cases}$$

Chegamos assim a um absurdo. □

O raciocínio referido acima não funciona por exemplo se $d = 7$. Uma vez que $2 = (3 - \sqrt{7})(3 + \sqrt{7})$ e nem $3 - \sqrt{7}$ nem $3 + \sqrt{7}$ são invertíveis, concluímos que 2 é redutível em $\mathbb{Z}[\sqrt{7}]$. Note-se que $3 - \sqrt{7}$ e $3 + \sqrt{7}$ são irredutíveis.

Na secção seguinte veremos que em $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}[\sqrt{2}]$ e $\mathbb{Z}[\sqrt{3}]$ as noções de primo e de invertível são equivalentes.

3.3 Domínios euclideanos

Voltemos ao nosso "modelo", o anel $\mathbb{Z}$. A existência de máximo divisor comum e de mínimo múltiplo comum é demonstrada, por vezes, usando o chamado "algoritmo da divisão".

Vejamos que "esse" algoritmo funciona em vários outros DI's e com propriedades análogas. É claro que o algoritmo da divisão em $\mathbb{Z}$ usa a sua ordem natural. Vejamos como se pode fugir a esta questão sem perder as propriedades desejadas.

Definição 3.3.1. *Seja* $< D, +, \cdot >$ *um DI e* $v : D \setminus \{0\} \longrightarrow \mathbb{N}_0$ *uma função. Diz-se que* $< D, +, \cdot, v >$ *é um domínio euclideano se:*

a) $\forall a, b \in D \setminus \{0\} \;\; v(a) \leq v(ab)$*;*

b) $\forall a \in D \;\; \forall b \in D \setminus \{0\} \;\; \exists q, r \in D\text{:} \;\; a = bq + r$*, com* $r = 0$ *ou* $v(r) < v(b)$*.*

A condição a) é equivalente a

$$\forall a, b \in D \setminus \{0\} \;\; [a|b \;\Rightarrow\; v(a) \leq v(b)].$$

Chamamos à condição b), o **algoritmo da divisão**. Por simplicidade de escrita, escreveremos "D é um DE" em vez de "D é um domínio euclideano".

Dado um DE $< D, +, \cdot, v >$, chamaremos a v a **função valorização** de D.

Um primeiro exemplo de um DE é dado pelo anel dos inteiros juntamente com a função "módulo de". A verificação de $< \mathbb{Z}, +, \cdot, |.| >$ é um DE é deixada como exercício. Note-se que no algoritmo da divisão deste DE não há unicidade se a divisão não for "exacta". De facto se $a = bq + r$ com $0 < |r| < |b$ então $a = b(q + 1) + (r - b)$ e $0 < |r - b| < |b$.

Notar que, dados dois inteiros a e b, $|ab| = |a| \cdot |b|$, condição esta que é mais forte do que a condição a) da definição de DE.

Um outro exemplo que será muito usado é o DE associado ao anel $\mathbb{Z}[i]$, o anel dos inteiros de Gauss.

Teorema 3.3.2. *Os anéis* $\mathbb{Z}[i]$*,* $\mathbb{Z}[i\sqrt{2}]$*,* $\mathbb{Z}[\sqrt{2}]$ *e* $\mathbb{Z}[\sqrt{3}]$*, com as funções (de valorização) definidas em (3.1) da página 75 são domínios euclideanos.*

Demonstração. Comecemos por notar que as funções definidas em (3.1) da página 75 podem ser prolongadas aos anéis $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ (a da esquerda) e a $\mathbb{Q}[i\sqrt{d}] = \{a + bi\sqrt{d} : a, b \in \mathbb{Q}\}$ (a da direita) continuando em ambos os casos a preservar o produto.

Em todos os casos, a condição a) da definição já foi "essencialmente" demonstrada.

Vejamos agora a condição b). Comecemos com o caso do anel $\mathbb{Z}[i]$.

Sejam $\alpha, \beta \in \mathbb{Z}[i]$, com $\beta \neq 0$. Consideremos o número complexo $\frac{\alpha}{\beta}$ que se escreve na forma $x + iy$ com $x, y \in \mathbb{Q}$. Deste modo $\alpha = \beta(x + yi)$. Consideremos $a, b \in \mathbb{Z}$ tais que $|x - a|, |y - b| \leq \frac{1}{2}$. Então

$$\alpha \;\; = \;\; \beta(x + iy) \;\; = \;\; \beta(a + bi) + \beta\big[(x - a) + i(y - b)\big].$$

Note-se que $\beta\big[(x - a) + i(y - b)\big] \in \mathbb{Z}[i]$ uma vez que é igual a $\alpha - \beta(a + ib)$ que pertence a $\mathbb{Z}[i]$. Para concluir a demonstração resta mostrar que $\beta\big[(x - a) + i(y - b)\big]$ tem valorização menor que a valorização de β ou seja, que $(x - a)^2 + (y - b)^2 < 1$. Mas

$$(x - a)^2 + (y - b)^2 \leq \frac{1}{4} + \frac{1}{4} < 1, \quad \text{pela escolha de } a \text{ e } b.$$

Se repetirmos os mesmos argumentos em relação aos outros anéis teremos de mostrar que, se $|x - a|, |y - a| < \frac{1}{2}$ então

$$\begin{aligned} (x - a)^2 + 2(y - b)^2 &< 1 \qquad \text{no caso do anel } \mathbb{Z}[i\sqrt{2}] \\ \big|(x - a)^2 - 2(y - b)^2\big| &< 1 \qquad \text{no caso do anel } \mathbb{Z}[\sqrt{2}] \\ \big|(x - a)^2 - 3(y - b)^2\big| &< 1 \qquad \text{no caso do anel } \mathbb{Z}[\sqrt{3}]. \end{aligned}$$

Mas estas desigualdades são triviais. Nos dois últimos casos use as desigualdades $|A-B| \leq \max\{A,B\}$, se $A, B \in \mathbb{R}^+$. □

Note que a demonstração do teorema é construtiva. Para além disso nada garante a unicidade. O que é essencial é que, no caso de $\mathbb{Z}[i]$, tenhamos $(x-a)^2+(y-b)^2<1$ (e o análogo nos outros casos).

Exemplos 3.3.3. *Vamos ver um exemplo em $\mathbb{Z}[i]$ e em $\mathbb{Z}[\sqrt{2}]$.*

a) *Em $\mathbb{Z}[i]$ se considerarmos $\alpha = 17+8i$ e $\beta = 5+9i$ obtemos $\frac{\alpha}{\beta} = \frac{157}{106} + \frac{-113}{106}$. Utilizando o teorema temos*

$$\alpha = \beta \underbrace{(1-i)}_{quociente} + \underbrace{(3+4i)}_{resto}.$$

Mas poderíamos ter também escolhido para quociente $2-i$ (e o correspondente resto, $-2-5i$)) uma vez que $\left(\frac{157}{106}-2\right)^2 + \left(-\frac{113}{106}+1\right)^2 = \frac{29}{106} < 1$.

b) *Em $\mathbb{Z}[\sqrt{2}]$ se considerarmos $\alpha = 17-8\sqrt{2}$ e $\beta = 5+3\sqrt{2}$ obtemos $\frac{\alpha}{\beta} = \frac{37}{7} + \frac{11}{7}\sqrt{2}$. Utilizando o teorema temos*

$$\alpha = \beta \underbrace{(5+2\sqrt{2})}_{quociente} + \underbrace{(4-3\sqrt{2})}_{resto}.$$

Mas poderíamos ter também escolhido para quociente:

- $5+\sqrt{2}$ *(e o resto, $-2+2\sqrt{2}$) porque* $\left|\left(\frac{37}{7}-5\right)^2 - 2\left(\frac{11}{7}-\right)^2\right| = \frac{4}{7} < 1$;
- $6+2\sqrt{2}$ *(e o resto, -1) porque* $\left|\left(\frac{37}{7}-6\right)^2 - 2\left(\frac{11}{7}-2\right)^2\right| = \frac{1}{7} < 1$.

Nota 3.3.4. *Suponhamos que $< D, +, \cdot, v >$ é um domínio euclideano em que v satisfaz a condição: $v(ab) = v(a)v(b)$ para todo $a, b \in D \setminus \{0\}$. Se pretendermos factorizar um dado elemento x então podemos usar o método de tentativas procurando elementos y cuja valorização divide a valorização de x.*

Por exemplo, se pretendermos factorizar em $\mathbb{Z}[i]$ o elemento $7+i$, que tem valorização 50, vamos procurar elementos com valorização 2 ou 5 (10 ou 25 não é necessário (porquê?)). Os elementos com valorização 2 são $\pm 1 + \pm i$ que são todos associados. Deste modo basta experimentar um deles. Obtemos $7+i = (1+i)(4-3i)$. De seguida vamos experimentar dividir $4-3i$ por elementos com valorização 5 (que são $1+2i$, $2+i$ e seus associados). Obtemos $4-3i = (2+i)(1-2i)$ e $2+i$ e $1-2i$ são irredutíveis (porquê?).

O seguinte resultado é deixado como exercício.

Lema 3.3.5. *Se D é um DE então:*

a) *$v(1) \leq v(a)$ para todo o $a \in D$;*

b) *para $a \in D$, $v(a) = v(1)$ se e só se a é invertível;*

c) *para $a, b \in D$, se $a|b$ e a não é associado a b, então $v(a) < v(b)$;*

d) *v é constante se e só se D é um corpo.* □

3.4 Máximo divisor comum

Definição 3.4.1. *Sejam a, b e d elementos de domínio de integridade D. Diz-se que d é um* **máximo divisor comum** *de a e b e escrevemos $d \sim (a, b)$ ou $d \sim mdc(a, b)$ se:*

a) $d|a$ *e* $d|b$;

b) $\forall d' \in D \quad \left[d'|a,\ d'|b \Rightarrow\ d'|d\right]$.

Escreveremos em geral mdc para significar máximo divisor comum. Vejamos algumas consequências (imediatas) da definição.

Proposição 3.4.2. *Sejam D um domínio de integridade e $a, b, d, a', b', d' \in D$. Então:*

a) *se $d \sim (a, b)$ então $d' \sim (a, b)$ se e só se $d \sim d'$;*

b) *se a divide b então $a \sim (a, b)$;*

c) $a \sim (a, 0)$;

d) *se $a \sim b$ então $a \sim (a, b)$;*

e) *se a é irredutível e não divide b então $1 \sim (a, b)$;*

f) *se a é invertível então $1 \sim (a, b)$;*

g) *se $a \sim a'$ e $b \sim b'$ então $(a, b) \sim (a', b')$.* □

Nem sempre existe máximo divisor comum entre dois elementos de um domínio de integridade. Por exemplo, em $\mathbb{Z}[i\sqrt{5}]$ não existe máximo divisor comum entre 6 e $2 + 2i\sqrt{5}$. Neste caso é fácil encontrar todos os divisores comuns a 6 e $2 + 2i\sqrt{5}$ e verificar se algum deles é múltiplo dos outros. Se $a + bi\sqrt{5}$ dividir 6 então $a^2 + 5b^2$ terá de dividir 36. Analisando os vários casos obtemos os seguintes divisores de 6: ± 1, ± 2, ± 3, ± 6, $\pm(1 + i\sqrt{5})$, $\pm(1 - i\sqrt{5})$. Destes elementos apenas ± 1, ± 2, $\pm(1 + i\sqrt{5})$, $\pm(1 - i\sqrt{5})$ dividem $2+2\sqrt{5}$. De entre estes elementos não há nenhum que seja múltiplo de todos os outros.

Mais geralmente temos.

Proposição 3.4.3. *Se d é um inteiro maior que 2 então em $\mathbb{Z}[i\sqrt{d}]$ nem sempre há máximo divisor comum entre dois elementos. Mais concretamente isso acontece (por exemplo) com os elementos $d+1$ e $2+i2\sqrt{d}$, se d é ímpar, e com d e $2i\sqrt{d}$, se d é par.*

Demonstração. Poderemos fazer demonstrações idênticas nos dois casos mas vamos optar por usar em cada caso um raciocínio diferente.

Suponhamos que d é ímpar e que $D = (d + 1, 2 + i2\sqrt{d})$.

Seja $a + bi\sqrt{d} \in \mathbb{Z}[i\sqrt{d}]$. Note-se que $a + bi\sqrt{d}$ divide $d + 1$ e $2 + i2\sqrt{d}$ se e só se:

$$\frac{2a + 2bd}{a^2 + db^2},\ \frac{2a - 2b}{a^2 + db^2},\ \frac{a(d + 1)}{a^2 + db^2},\ \frac{b(d + 1)}{a^2 + db^2} \in \mathbb{Z}.$$

Se $b = 0$ então, substituindo na primeira fracção obtemos: $a = \pm 1$ ou $a = \pm 2$.

Se $|b| \geq 2$ então o quarto número não é inteiro pois é diferente de zero e pertence ao intervalo $]-1, 1[$.

Se $|b| = 1$ então o quarto número é inteiro se e só se $|a| = 1$.

Obtemos assim os números 1, 2, $1+i\sqrt{d}$, $1-i\sqrt{d}$ e seus associados, que de facto são divisores de $d+1$ e de $2+i2\sqrt{d}$. Para concluir resta notar que nenhum destes números é múltiplo de todos os outros.

Suponhamos que d é par e que $D \sim (d, 2i\sqrt{d})$.

Uma vez que $i\sqrt{d}$ divide d (pois $d = i\sqrt{d} \cdot (-i\sqrt{d})$) e divide $2i\sqrt{d}$ então, pela definição de máximo divisor comum, $i\sqrt{d}$ divide D. Do mesmo modo se pode concluir que 2 divide D. Por outro lado D divide $2i\sqrt{d}$. Deste modo existem $E, F \in \mathbb{Z}[i\sqrt{d}]$ tal que $D = i\sqrt{d}\,E$ e $2i\sqrt{d} = DF$. Em particular $2i\sqrt{d} = EFi\sqrt{d}$ e portanto $2 = EF$. Uma vez que 2 é irredutível (ver Corolário 3.2.3), $E \sim 1$ ou $F \sim 1$. No primeiro caso $D \sim i\sqrt{d}$ que não é um múltiplo de 2 e no segundo caso $D \sim 2i\sqrt{d}$, o que é impossível pois $2i\sqrt{d}$ não divide d. □

Teorema 3.4.4. *Se D é um DE e $a, b \in D$ então existe mdc entre a e b. Além disso, se $d \sim (a, b)$, existem $x, y \in D$ tais que $d = ax + by$.*

Demonstração. Atendendo ao que foi dito acima posso supor $a \neq 0$ e $b \neq 0$. Sejam $B = \{z \in D \setminus \{0\} : \exists x, y \in D \ z = ax + by\}$ e $A = \{v(z) : z \in B\}$. Como A é um subconjunto de $\mathbb{N}_0$ não vazio (pois $a, b \in B$) existe $d \in B$ tal que

$$\forall z \in B, \ v(d) \leq v(z).$$

Mostremos que $d \sim (a, b)$. Vejamos que d divide a. Sejam $x, y \in D$ tais que $d = ax + by$ e, aplicando o algoritmo da divisão, $q, r \in D$ tais que $a = dq + r$ com $r = 0$ ou $v(r) < v(d)$. Como $r = a - dq = a(1 - xq) + (-yq)b$, r tem de ser igual a zero, pois caso contrário, r pertenceria a B e tinha valorização menor do que d, o que é absurdo por definição de d. Concluímos assim que $r = 0$ e portanto d divide a. De modo análogo se mostra que d divide b.

Suponhamos agora que d' é um divisor de a e de b. Como $d = ax + by$, então d' divide d. Fica assim mostrado que $d \sim (a, b)$.

Vamos agora fazer uma outra demonstração deste teorema. Demonstração essa que tem a vantagem de ser construtiva. Este método é o chamado método das divisões sucessivas.

Novamente supomos que a e b são diferentes de 0, pois nesse caso a situação é trivial.

Sejam $q, r \in D$ tais que

$$a = bq + r, \quad \text{com } r = 0 \text{ ou } v(r) < v(b).$$

Observe-se que os divisores comuns de a e de b são os mesmos que os divisores comuns de b e de r. Em particular os mdc's entre a e b são os mesmos que os mdc's entre b e r.

Se $r = 0$, então $b \sim (r, b)$ e portanto $r \sim (a, b)$. Se $r \neq 0$, sejam q_1 e r_1 tais que

$$b = rq_1 + r_1, \quad \text{com } r_1 = 0 \text{ ou } v(r_1) < v(q_1).$$

Pelo mesmo motivo que acima, os mdc's entre b e r são os mesmos que os mdc's entre r e r_1 e portanto são os mesmos que os mdc's entre a e b.

Se $r_1 = 0$, então $r \sim (r, r_1)$ e portanto $r \sim (a, b)$.

Se $r_1 \neq 0$, sejam q_2 e r_2 tais que

$$r = r_1 q_2 + r_2, \quad \text{com } r_2 = 0 \text{ ou } v(r_2) < v(r_1).$$

Continuando este processo, como

$$v(b) > v(r) > v(r_1) > v(r_2) \cdots,$$

existe i tal que $r_i = 0$ e portanto $r_{i-1} \sim (a, b)$.

Como $r, r_1, r_2, \ldots$ se escrevem da forma $ax+by$, temos demonstrada a segunda parte do teorema. □

Corolário 3.4.5. *Se D é um domínio euclidiano, $a, b, c \in D$ e $d \sim (a, b)$ então a equação (diofantina) $ax + by = c$ tem solução se e só se $d|c$.* □

Como aplicação vamos calcular os mdc's entre $2+11i$ e $15+5i$, em $\mathbb{Z}[i]$. Utilizando o método do Teorema 3.3.2, obtemos, sucessivamente

$$\begin{array}{lcll} 15+5i & = & (2+11i)(2-i)+(2-4i) & \therefore \quad (15+5i, 2+11i) = (2+11i, 2-4i) \\ 2+11i & = & (2-4i)(-2+i)+(2+i) & \therefore \quad (2+11i, 2-4i) = (2-4i, 2+i) \\ (2-4i) & = & (2+i)(-2i)+0 & \therefore \quad (2-4i, 2+i) = (2+i, 0) \sim 2+i \end{array}$$

Concluímos assim que $2+i \sim (2+11i, 15+5i)$. Como os mdc's entre $2+11i$ e $15+5i$ são os associados a $2+i$, e os elementos invertíveis de $\mathbb{Z}[i]$ são $1, -1, i, -i$, concluímos que os mdc's entre $2+11i$ e $15+5i$ são

$$2+i, -2-i, -1+2i, 1-2i.$$

Nota 3.4.6. *Note-se que, se D é um domínio de integridade qualquer (não necessariamente domínio euclideano), $a, b, q, r \in D$ e $a = bq + r$ então $(a, b) = (b, r)$ independentemente de estarmos ou não num domínio euclideano. Entendendo-se a igualdade acima como: se um dos máximos divisores comum existir então o outro também existe e são iguais. Isto acontece porque $\{$divisores de a e $b\} = \{$divisores de b e $r\}$.*

Definição 3.4.7. *Seja D um DI e $a, b \in D$. Dizemos que a e b são primos entre si se $(a, b) \sim 1$.*

Lema 3.4.8. *Se D é um domínio euclideano então*

$$\forall a, b, c \in D \quad \big[a|bc, \quad (a, b) \sim 1 \implies a|c\big].$$

Demonstração. Sejam $x, y \in D$ tais que $ax + by = 1$. Multiplicando a igualdade por c obtemos $acx + bcy = c$. Como a divide acx e bc então a divide $acx + bcy = c$. □

Teorema 3.4.9. *Num domínio euclideano D os conceitos de primo e de irredutível são equivalentes.*

Demonstração. Basta verificar que, se a é um irredutível de D então a é primo.

Suponhamos que $x, y \in D$ e $a|xy$ e mostremos que $a|x$ ou $a|y$. Seja $d \sim (a, x)$. Como a é irredutível então, pela Proposição 3.4.2, d é invertível ou é associado a a. Se d é invertível, então $1 \sim d \sim (a, x)$ e, pelo lema anterior $a|y$. Se d é associado a a então $a|d$ e, como $d|x$, $a|x$. □

Como consequência do Lama 3.4.8 temos o seguinte resultado cuja demonstração é deixada como exercício.

Lema 3.4.10. *Se D é um domínio euclideano então*

$$\forall a,b,c \in D \ \big[(a,b) \sim 1, \ \ (a,c) \sim 1 \implies (a,bc) \sim 1\big].$$

Chegamos agora ao Teorema da Factorização Única que generaliza o que já conhecemos do anel dos inteiros.

Teorema 3.4.11 (Teorema da factorização única)**.** *Se D é um DE e $a \in D - \{0\}$ então existem $k \in \mathbb{N}_0$, $p_1, \ldots, p_k$ elementos irredutíveis de D não associados dois a dois, ε elemento invertível de D e $n_1, \ldots, n_k \in \mathbb{N}$ tais que*

$$a = \varepsilon p_1^{n_1} \cdots p_k^{n_k}.$$

Além disso, esta factorização é única no seguinte sentido: se $s \in \mathbb{N}_0$, $q_1, \ldots, q_s$ são elementos irredutíveis de D não associados dois a dois, μ é um elemento invertível de D e $m_1, \ldots, m_s \in \mathbb{N}$ são tais que tais que

$$a = \mu q_1^{m_1} \cdots q_k^{m_s},$$

então $k = s$, e para todo o $i \in \{1, \ldots, k\}$ existe $j \in \{1, \ldots, k\}$ tal que $p_i \sim q_j$ e $n_i = m_j$.

Demonstração. Para a primeira parte do teorema vamos fazer uma demonstração por indução sobre a valorização de a. Notemos que a menor valorização possível para a é $v(1)$, situação que acontece apenas no caso em que a é invertível.

Seja $n \in \mathbb{N}$ e suponhamos agora que a primeira parte do teorema é válida para elementos com valorização menor que n e mostremos que o resultado é válido se $v(a) = n$.

Se a é irredutível então não há nada a demonstrar. Se a é redutível, sejam $b, c \in D$ tais que $a = bc$ e a não é associado nem a b nem a c. Pelo Lema 3.3.5, $v(b) < v(a)$ e $v(c) < v(a)$. Posso então aplicar a hipótese de indução a b e a c. Temos então que b e c se factorizam da maneira pretendida. Usando o facto de o produto de invertíveis ser ainda um invertível posso então escrever

$$a = bc = \varepsilon p_1^{n_1} \cdots p_k^{n_k}$$

para alguns irredutíveis $p_1, \ldots, p_k$, ε invertível e $k, n_1, \ldots, n_k \in \mathbb{N}$. Se para alguns $i, j \in \{1, \ldots, k\}$ $p_i \sim p_j$, então existe δ invertível tal que $p_i = \delta p_j$ e portanto $p_i^{n_i} = (\delta p_j)^{n_i} = \delta^{n_i} p_j^{n_i}$. Como δ^{n_i} é ainda um invertível temos uma factorização de a como um produto de um invertível por um produto de potências dos irredutíveis $p_1, \ldots, p_{i-1}, p_{i+1}, \ldots p_k$. Repetindo, se necessário o processo, ao fim de um número finito de passos escreveríamos a como um produto de um invertível por um produto de potências de irredutíveis não associados.

Para a segunda parte do teorema vamos novamente fazer uma demonstração por indução sobre $v(a)$. Como acima, seja $n \in \mathbb{N}$ e suponhamos que o resultado é válido para os elementos com valorização menor do que n. Mostremos então que, se $v(a) = n$ e a "admite" duas factorizações, então essas factorizações são essencialmente as mesmas no sentido enunciado acima.

Suponhamos então que tínhamos duas factorizações de a naquelas condições:

$$a = \varepsilon p_1^{n_1} \cdots p_k^{n_k}, \qquad a = \mu q_1^{m_1} \cdots q_s^{m_s}.$$

Como p_1 é irredutível (ou equivalentemente, primo), divide $\mu q_1^{m_1} \cdots q_s^{m_s}$, não divide μ, então existe $j \in \{1, \ldots, s\}$ tal que p_1 divide q_j. Como q_j é irredutível, p_1 é associado a q_j. Seja γ um invertível tal que $p_1 = \gamma q_j$. Substituindo nas duas factorizações de a e usando a lei do corte obtemos

$$\varepsilon\gamma p_1^{n_1-1} \cdots p_k^{n_k} = \mu q_1^{m_1} \cdots q_j^{m_j-1} q_s^{m_s}.$$

Aplique-se a hipótese de indução a $b = \varepsilon\gamma p_1^{n_1-1} \cdots p_k^{n_k}$ (notar que, b divide a e b não é associado a a e que, portanto $v(b) < v(a)$) para concluir o resultado pretendido. □

A factorização de um elemento de um DE na forma enunciada pelo teorema acima, é em geral muito difícil e por vezes **impossível**.

Como procurar os invertíveis que dividem um certo elemento a? O método sugerido pela demonstração do teorema é começar por procurar todos os elementos do DE com valorização menor que a e verificar se esses elementos dividem ou não a. Este método exaustivo em geral não leva a lado nenhum a não ser em alguns casos muito particulares.

A situação em alguns DE's é um pouco mais simples. Temos assim o seguinte resultado cuja demonstração já está "essencialmente feita".

Lema 3.4.12. *Se $< D, +, \cdot, v >$ é um DE tal que*

$$\forall a, b \in D,\ v(ab) = v(a)v(b),$$

então, para $x, y \in D$,

a) *se x divide y então $v(x)$ divide $v(y)$;*

b) *se $v(x)$ é um número primo então x é um primo (ou irredutível) de D;*

c) *$v(1) = 1$ ou então v é constante e igual a 0.* □

Em DE's satisfazendo a condição enunciada no lema, a procura de elementos que dividam um certo elemento a é relativamente mais simples, pois só temos como "candidatos" os elementos cuja valorização divide $v(a)$.

Isto acontece com os domínios $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}[\sqrt{2}]$ e $\mathbb{Z}[\sqrt{3}]$. No caso dos dois primeiros a situação é muito mais simples pois dado $r \in \mathbb{N}_0$ há apenas um número finito de elementos com valorização igual a r, que são em geral fáceis de encontrar.

Vejamos um exemplo: Como factorizar $3 + i$? Começamos por calcular a sua valorização (10). Em seguida, notamos que, se $3 + i$ é irredutível, ele é um produto de um elemento de valorização 2 por um de valorização 5 (porquê?).

Vamos então, de entre todos os elementos de valorização 2 (ou de entre os de valorização 5) procurar quais os que dividem $3 + i$. Os elementos de valorização 2 são $1 + i, 1 - i, -1 + i, -1 - i$. Como estes quatro elementos são todos associados, se um deles dividir $3 + i$ então todos eles dividem $3 + i$. Verifiquemos então se $1 + i$ divide $3 + 1$. Para isso, vamos calcular em $\mathbb{C}$ a divisão de $3 + i$ por $1 + i$.

$$\frac{3+i}{1+i} = \frac{(3+i)(1-i)}{(1+i)(1-i)} = \frac{4-2i}{2} = 2 - i.$$

Temos assim que $3+i = (1+i)(2-i)$. O passo seguinte é factorizar $1+i$ e $2-i$. Como ambos têm valorização prima, eles são irredutíveis, e como têm valorização diferente, eles não são associados.

Chama-se a atenção para o facto de um elemento poder ser primo e não ter valorização prima, como acontece para o elemento 7 de $\mathbb{Z}[i]$. Por outro lado 2, 13, 17, 29 e 37 (por exemplo) são primos em $\mathbb{Z}$ e não são primos em $\mathbb{Z}[i]$.

Veremos mais tarde (Teorema 3.6.10) que o método usado em $\mathbb{Z}$ para calcular o máximo divisor comum entre dois números já factorizados como produto de potências de primos também vale numa classe mais geral de domínios de integridade, que inclui os domínios euclideanos.

3.5 Ideais primos, ideais maximais e ideais principais

Seja A um anel comutativo e com elemento um. Existirá alguma imagem homomorfa de A que seja um DI? E que seja um corpo? Pelo teorema fundamental do homomorfismo, a questão que se coloca é a de encontrar um ideal I de A tal que A/I é um DI, no primeiro caso, ou um corpo, no segundo.

Temos a seguinte caracterização dos ideais que respondem afirmativamente a cada uma destas perguntas. Comecemos por duas definições.

Definição 3.5.1. *Seja A um anel comutativo e com elemento um e I um ideal de A.*

- *I diz-se um ideal* **primo** *se satisfaz a condição*

$$\forall a, b \in A \quad \big[ab \in I \Rightarrow a \in I \text{ ou } b \in I\big].$$

- *I diz-se um ideal* **maximal** *se for próprio e não estiver contido propriamente num outro ideal próprio.*

Teorema 3.5.2. *Seja A um anel comutativo e com elemento um e I um ideal próprio de A. Então:*

a) *A/I é um DI se e só se I é um ideal primo.*

b) *A/I é um corpo se e só se I é um ideal maximal.*

Demonstração. Note-se que A/I é um anel comutativo e com elemento um.

a) Nas condições referidas, dizer que A/I é um domínio de integridade é o mesmo que dizer que

$$\forall a, b \in A \ \Big[(a+I)(b+I) = I \Rightarrow a+I = I \text{ ou } b+I = I\Big],$$

ou seja

$$\forall a, b \in A \ \big[ab+I = I \Rightarrow a+I = I \text{ ou } b+I = I\big],$$

que é o mesmo que dizer que

$$\forall a, b \in A \ \big[ab \in I \ \Rightarrow \ a \in I \text{ ou } b \in I\big].$$

Fica assim demonstrada a alínea a).

b) ($\Rightarrow$)

Seja J um ideal de A tal que $I \subseteq J \subseteq A$ e $I \neq J$. Mostremos que $J = A$. Seja $a \in J \setminus I$ e consideremos, usando o facto de A/I ser um corpo, $b \in A$ tal que $(a+I)(b+I) = 1+I$. Deste modo $ab - 1 \in I \subseteq J$. Note-se que $ab \in J$ (pois $a \in J$) e portanto $1 \in J$ pois $1 = -[(ab-1) - ab]$. Pelo Proposição 2.2.6, $J = A$.

($\Leftarrow$)

Atendendo a que A é um anel comutativo e com elemento um, basta-nos mostrar que para todo $a \in A$, se $a+I \neq I$ (ou seja $a \notin I$) existe $b \in A$ tal que $(a+I)(b+I) = 1+I$.

Seja então $a \in A \setminus I$ e $J = I + < a >$. J é um ideal contendo propriamente I, pois $a \notin I$. Como I é maximal, $J = A$. Em particular $1 \in J$, e portanto existe $b \in A$ e $i \in I$ tal que $1 = i + ab$. Daqui se conclui que $(a+I)(b+I) = ab + I = 1 + I$. □

Corolário 3.5.3. *Todo o ideal maximal de um anel comutativo e com elemento um é um ideal primo.*

Demonstração. Basta usar o teorema anterior e o facto de todo o corpo ser um DI. □

Definição 3.5.4. *Seja A um anel e I um seu ideal. I diz-se um* **ideal principal** *se existe $a \in I$ tal que I é o menor ideal de A contendo a. Neste caso, diz-se que I é o ideal principal gerado por a e denota-se, $I =< a >$.*

É claro que o ideal principal gerado por um elemento a tem de conter os elementos da forma na, com $n \in \mathbb{Z}$, da forma xa, ay e xay com $x, y \in I$. Além disso tem de conter somas finitas de elementos do tipo dos anteriores.

Lema 3.5.5. *Seja A um anel comutativo e $a \in A$. Então:*

a) $< a >= \{na + ax : n \in \mathbb{Z}, x \in A\}$;

b) *se A tem elemento um,* $< a >= \{ax : x \in A\}$.

Demonstração.

a) Pelo que foi dito atrás basta mostrar que $H = \{na + ax : n \in \mathbb{Z}, x \in A\}$ é um ideal. É claro que $0 = 0a + a0 \in H$. Vejamos que H é fechado para a soma e o produto e que satisfaz a lei da absorção. Sejam então $n, m \in \mathbb{Z}$, $x, y, z \in A$.

$$(na + ax) + (ma + ay) = (n+m)a + a(x+y) \in H,$$

$$(na + ax)(ma + ay) = a[(nm)a + nay + max + axy],$$

$$(na + ax)z = a(nz + xz) \in H.$$

b) Seja e é o elemento um de A e $n \in \mathbb{Z}$. Então $na = n(ea) = (ne)a = a(ne)$ e $ne \in A$. Para concluir basta usar a alínea anterior. □

Corolário 3.5.6. *Se D é um domínio de integridade e $a, b \in D$ então o ideal gerado por $\{a, b\}$ é igual $a < a > + < b >$ que por sua vez é igual a $\{ax + by : x, y \in D\}$.*

Demonstração. É óbvio que $\{a, b\} \subseteq \{ax + by : x, y \in D\} \subseteq < a > + < b >$ e que $\{ax + by : x, y \in D\}$ está contido em qualquer ideal que contem $\{a, b\}$. Por outro lado $\{ax + by : x, y \in D\}$ é um ideal de D. □

3.6 Domínios de ideais principais e domínios de factorização única

Vamos agora considerar duas classes de domínios de integridade onde é válido muito do que foi dito para domínios euclideanos.

Definição 3.6.1. *Um domínio de integridade onde todo o ideal é principal, diz-se um* **domínio de ideais principais**.

Definição 3.6.2. *Um domínio de integridade onde "é válida" a tese do Teorema 3.4.11 diz-se um* **domínio de factorização única**.

Em vez de escrevermos "D é um domínio de ideais principais" e 'D é um domínio de factorização única" escrevemos "D é um DIP" e "D é um DFU".

Num domínio de factorização única é fácil encontrar os divisores de um elemento do qual conheçamos a factorização como produto de potências de irredutíveis.

Proposição 3.6.3. *Se D é um DFU e $a = \varepsilon p_1^{n_1} \cdots p_k^{n_k}$, em que $k \in \mathbb{N}$, ε é invertível, $p_1, \ldots, p_k$ são irredutíveis não associados e $n_1, \ldots, n_k \in \mathbb{N}_0$, então os divisores de a são os elementos que são associados a elementos da forma $p_1^{s_1} \cdots p_k^{s_k}$, em que $s_1, \ldots, s_k \in \mathbb{N}_0$ e $s_i \leq n_i$. Em particular há $(n_1 + 1) \cdots (n_k + 1)$ divisores de a não associados dois a dois.*

Demonstração. É obvio que os elementos referidos são divisores de a. Por outro lado, se d é um divisor de a então existe $x \in D$ tal que $a = dx$. Factorizando d e x, usando a igualdade $a = dx$ e a unicidade de factorização de a obtemos o resultado pretendido. □

Seja D um domínio euclideano. Pelo Teorema 3.4.11 D é um domínio de factorização única. Vejamos que D também é um domínio de ideias principais.

Teorema 3.6.4. *Todo o domínio euclideano é um domínio de ideais principais.*

Demonstração. Seja $< D, +, \cdot, v >$ um DE e seja I um seu ideal. Se $I = \{0\}$, então $I =< 0 >$. Se $I \neq \{0\}$, seja $B = \{v(x) : x \in I \setminus \{0\}\}$. Como B é um subconjunto de $\mathbb{N}_0$ então B tem um primeiro elemento. Consideremos então $a \in I \setminus \{0\}$ tal que $v(a) \leq v(b)$ para todo o $b \in I \setminus \{0\}$ e mostremos que $< a >= I$. É claro que $< a > \subseteq I$. Inversamente, seja $b \in I$, e sejam $q, r \in D$ tais que

$$b = aq + r \text{ e } r = 0 \text{ ou } v(r) < v(a).$$

Então $r = b - aq \in I$, e portanto $v(r)$ não pode ser menor que $v(a)$, por definição de a. Assim $r = 0$ e portanto $b \in < a >$. □

Vejamos agora uma caracterização dos ideais maximais em DIP. Comecemos por uma observação. Seja A um anel comutativo e com elemento um e $a, b \in A$. Então $< a > \subseteq < b >$ se e só se $a \in < b >$ se e só se existe $x \in A$ tal que $a = bx$ se e só se b divide a. Em particular a e b geram o mesmo ideal se e só se são associados.

Proposição 3.6.5. *Seja D um DIP e I um ideal de D. Então I é um ideal maximal se e só se I é gerado por um irredutível.*

Demonstração. Seja a um irredutível de D. Mostremos que $< a >$ é maximal. Seja J um ideal contendo I e seja $b \in J$ tal que $J =< b >$. Então, como $I \subseteq J$, b divide a. Como a é irredutível b é associado a a, e portanto $I = J$, ou b é invertível, e portanto $J = A$.

Inversamente, suponhamos que $< a >$ é um ideal maximal. Vejamos que a é irredutível. Seja $b \in A$ tal que b divide a. Vejamos que b é associado a a ou b é invertível. Como b divide a, $< a > \subseteq < b >$. Como $< a >$ é maximal, $< a >=< b >$, e portanto a e b são associados, ou $< b >= A$ e portanto b é invertível. □

Nesta demonstração, a hipótese de A ser um DIP só foi precisa para mostrar que, se I é gerado por um irredutível então I é maximal. Assim, num anel comutativo e com elemento um, se um elemento a gera um ideal maximal então esse elemento é irredutível.

Para concluir o diagrama da inclusão destas classes de anéis falta a prova de que todo o DIP é um DFU. Mas antes vamos ver alguns resultados.

Proposição 3.6.6. *Se D é um DIP, então todo o par de elementos de D admite máximo divisor comum que se escreve como uma combinação linear dos dois elementos.*

Demonstração. Sejam $a, b \in D$. Como D é um DIP existe $d \in D$ tal que $< a > + < b >=< d >$. Vejamos que $d \sim (a, b)$. Como $a, b \in < d >$ então d divide a e b. Por outro lado, se $d' \in D$ e d' divide a e divide b então $a, b \in < d' >$ e portanto $< a > + < b > \subseteq < d' >$. Como $< a > + < b >=< d >$ temos $d \in < d' >$ ou seja d' divide d. □

Proposição 3.6.7. *Num DIP as noções de primo e de irredutível são equivalentes.*

Demonstração. Basta notar que a demonstração do Teorema 3.4.9 e do Lema 3.4.8 continuam válidas para D atendendo à proposição anterior. □

Proposição 3.6.8. *Sejam D um DIP e $(a_n)_{n\in\mathbb{N}}$ uma sucessão de elementos de D tais que a_{k+1} divide a_k para todo $k \in \mathbb{N}$. Então existe k_0 tal que $a_{k_0} = a_n$ para todo $n \geq k_0$.*

Demonstração. Para $n \in \mathbb{N}$ seja $I_n =< a_n >$ e consideremos $I = \bigcup_{n\in\mathbb{N}} I_n$. Como I é um ideal (verifique) e D é um DIP então existe $a \in I$ tal que $I =< a >$. Seja $k_0 \in \mathbb{N}$ tal que $a \in I_{k_0}$. Deste modo $< a > \subseteq I_{k_0}$ e portanto, pela definição de I, $I = I_{l_0}$ e a conclusão segue imediatamente. □

Teorema 3.6.9. *Todo o domínio de ideais principais é um domínio de factorização única.*

Demonstração. Sejam D um DIP e vejamos que todo o seu elemento não nulo nem invertível se pode escrever como produto de irredutíveis.

Seja $F = \{a \in D : a$ é redutível mas não é um produto de irredutíveis$\}$ e suponhamos que $F \neq \emptyset$ e seja $a \in F$. Como a é redutível então existem $x, y \in D$ tais que $a = xy$ e x e y não são associados a a nem são invertíveis. É claro que $x \in F$ ou $y \in F$ pois caso contrário $a \notin F$. Suponhamos que $x \in F$ e sejam x_1, y_i tais que $x = x_1 y_1$ e x_1 e y_1 não são associados a x nem invertíveis. Da mesma maneira que acima, x_1 ou y_1 terá de pertencer a F. Repetimos assim indefinidamente o processo e obtemos uma

sucessão $(x_n)_{n\in\mathbb{N}}$ de elementos de D tais que x_{k+1} divide x_k para todo $k \in \mathbb{N}$, o que contradiz a proposição anterior.

Mostramos assim que todo o elemento de D não nulo nem invertível é um produto de irredutíveis. Podemos de seguida juntar irredutíveis associados e obter o resultado pretendido.

Suponhamos agora que $a \in D$ e $a = p_1 \cdots p_k = q_1 \cdots q_s$ em que $k, s \in \mathbb{N}$ e $p_1, \ldots p_k, q_1, \ldots q_s$ são irredutíveis de D. Como p_1 é primo (ver Proposição 3.6.8) existe j tal que p_1 divide q_j. Trocando a ordem dos factores, se necessário, podemos supor que $j = 1$. Como q_1 é irredutível então $p_1 \sim q_1$ e portanto existe μ invertível tal que $p_1 = \mu q_1$. Substituindo na igualdade $p_1 \cdots p_k = q_1 \cdots q_s$ e simplificando obtemos $(\mu p_2) \cdots p_k = q_2 \cdots q_s$. Usando um processo de indução sobre o número de invertíveis envolvidos tiramos a conclusão final. □

Um método de encontrar máximo divisor comum entre dois elementos de um DFU (e portanto de um DE ou de um DIP) é dado pelo seguinte resultado.

Teorema 3.6.10. *Num domínio de factorização única existe sempre máximo divisor comum entre dois elementos.*

Demonstração. Basta analisar o caso em que os dois elementos não são 0 nem invertíveis pois nesse caso existe sempre máximo divisor comum (ver Proposição 3.4.2). Sejam a, b elementos de D nas condições referidas. Podemos sempre escrever a e b na forma

$$a = \varepsilon p_1^{n_1} \cdots p_k^{n_k} \quad \text{e} \quad b = p_1^{m_1} \cdots p_k^{m_k}$$

em que $k \in \mathbb{N}$, $p_1, \ldots, p_k$ são irredutíveis e $n_1, \ldots, n_k, m_1, \ldots, m_k \in \mathbb{N}_0$ e ε é invertível (note-se que alguns expoentes podem ser nulos).

Atendendo à Proposição 3.6.3 os divisores de a e de b são os elementos de D que são associados aos elementos da forma $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ em que $0 \leq \alpha_i \leq \min\{n_i, m_i\}$, para $i = 1, \ldots, k$. Todos estes elementos dividem $p_1^{\min\{n_1,m_1\}} \cdots p_k^{\min\{n_k,m_k\}}$ e portanto este último elemento é um máximo divisor comum entre a e b. □

É claro que esta proposição pressupõe o conhecimento da factorização de a e de b, que já sabemos ser em geral muito difícil ou até mesmo impossível.

Nota 3.6.11. *Já vimos que todo o DE é um DIP e que todo DIP é um DFU. Estas inclusões são estritas.*

- *Consideremos $\mathbb{Z}[x]$ o anel dos polinómios de coeficientes inteiros e seja I o conjunto formado por todos os polinómios cujo termo independente é par. É claro que I é um ideal de $\mathbb{Z}[x]$. Por outro lado, se I fosse um ideal principal então existia $f(x)$ tal que $I =< f(x) >$. Como o polinómio constante e igual a 2 pertence a I então $f(x)$ divide 2 e portanto $f(x) = \pm 1$ ou $f(x) = \pm 2$. No primeiro caso I seria igual a $\mathbb{Z}[x]$ e no segundo caso os elementos de I seriam os polinómios cujos coeficientes eram todos pares. Em qualquer dos casos chegamos a uma contradição que decorreu do facto de termos suposto que I era um ideal principal.*

  Concluímos assim que $\mathbb{Z}[x]$ não é um DIP. Veremos em Algebra II que este anel é um DFU.

- *Pode-se mostrar (não é simples) que o anel* $\mathbb{Z}[(1+i\sqrt{19})/2]$ *é um DIP que não é um DE.*

A noção de máximo divisor comum em DI pode ser generalizada à imagem do que acontece com o anel dos inteiros.

Definição 3.6.12. *Sejam* D *um DI,* $n \in \mathbb{N}$ *e* $a_1, \ldots, a_n, d \in D$*. Diz-se que* d *é um* **máximo divisor comum** *de* $a_1, \ldots, a_n$ *e escrevemos* $d \sim (a_1, \ldots, a_n)$ *ou* $d \sim mdc(a_1, \ldots, a_n)$ *se:*

a) $d|a_1, \ldots, d|a_n$*;*

b) $\forall d' \in D \quad \left[d'|a_1, \ldots, d'|a_n \Rightarrow \ d'|d\right]$.

Essencialmente "tudo" o que foi dito para o máximo divisor comum de dois elementos pode ser generalizado. Essencialmente o que é relevante é que, se D é um domínio de integridade e $a, b, c \in D$ então $(a, b, c) = (a, (b, c))$, no sentido em que, se um dos "lados" da igualdade existir então o outro também existe e são iguais.

A noção de mínimo múltiplo comum também pode ser dada em domínios de integridade quaisquer.

Definição 3.6.13. *Sejam* D *um DI,* $n \in \mathbb{N}$ *e* $a_1, \ldots, a_n, d^* \in D$*. Diz-se que* d^* *é um* **mínimo múltiplo comum** *de* $a_1, \ldots, a_n$ *e escrevemos* $d \sim [a_1, \ldots, a_n]$ *ou* $d \sim mmc(a_1, \ldots, a_n)$ *se:*

a) $a_1|d^*, \ldots, a_n|d^*$*;*

b) $\forall d' \in D \quad \left[a_1|d', \ldots, a_n|d' \Rightarrow \ d^*|d'\right]$.

Em domínios de factorização única o mínimo múltiplo comum pode ser encontrado como no Teorema 3.6.10, substituindo "$\min\{n_i, m_i\}$" por "$\max\{n_i, m_i\}$". Daqui resulta que o mínimo múltiplo comum existe sempre e que, se a, b são elementos de um DFU então $[a, b](a, b) = ab$. Por este motivo o estudo do mínimo múltiplo comum não traz nada de novo!

Em jeito de conclusão.

- Se $\mathbb{K}$ é um corpo então $\mathbb{K}$ é um domínio euclideano (com função de valorização constante). O inverso não é verdadeiro.
- Se $\mathbb{K}$ é um domínio euclideano então $\mathbb{K}$ é um domínio de ideais principais (um ideal é gerado por um seu elemento com a menor valorização possível). O inverso não é verdadeiro.
- Se $\mathbb{K}$ é um domínio de ideais principais então $\mathbb{K}$ é um domínio de factorização única (dado um elemento, vamos factorizando até não ser possível continuar). O inverso não é verdadeiro.
- Se $\mathbb{K}$ é um domínio de factorização única então dois quaisquer elementos admitem máximo divisor comum.

3.7 Exercícios

Exercício 1. Considere o anel $\mathbb{Z}[i]$.

a) Mostre que a valorização de qualquer elemento de $\mathbb{Z}[i]$ é congruente com 0 ou com 1, módulo 4.

b) Calcule todos os elementos de $\mathbb{Z}[i]$ com valorização igual a 0, 1, 4, 5, 8, 9, 12, 13, 16, 17, ..., 52 e 53.

Exercício 2. Faça "qualquer coisa de semelhante" ao exercício anterior relativamente aos anéis $\mathbb{Z}[i\sqrt{2}]$ e $\mathbb{Z}[i\sqrt{3}]$.

Exercício 3. Quais os divisores não invertíveis de 16 no anel $\mathbb{Z}[i\sqrt{7}]$? Factorizando 16 de "duas maneiras diferentes", mostre que $\mathbb{Z}[i\sqrt{7}]$ não é um DFU.

Exercício 4. Considere um anel do tipo $\mathbb{Z}[i\sqrt{d}]$ ou $\mathbb{Z}[\sqrt{d}]$, dois elementos a e b desse anel e $d \sim (a, b)$. Mostre que a valorização de (a, b) divide o máximo divisor comum das valorizações de a e de b.

Exercício 5. Mostre que todo o elemento em $\mathbb{Z}[\sqrt{d}]$ ou em $\mathbb{Z}[i\sqrt{d}]$ com valorização prima é irredutível.

Exercício 6. Calcule a valorização de $11 + 2i$ e de $7 + 3i$ no anel $\mathbb{Z}[i]$. Conclua que os dois elementos são primos entre si.

Exercício 7. Sejam $\alpha, \beta \in \mathbb{Z}[i\sqrt{5}]$ tais que a "valorização" de α é igual a 644 e a de β é igual a 69. Mostre que α e β são primos entre si.

Exercício 8. Quantos divisores de 845 existem em $\mathbb{Z}[i]$? E de 1105? E de $15(2 + 3i)^2$?

Exercício 9. Seja $d \in \mathbb{N}$ mostre que $i\sqrt{d}$ é irredutível em $\mathbb{Z}[i\sqrt{d}]$.

Exercício 10. Mostre que, se $n > 1$ então $6^n + 1$ não é um primo em $\mathbb{Z}[i]$.

Exercício 11. Considere o anel dos inteiros de Gauss $\mathbb{Z}[i]$.

a) Seja r tal que existem $n, m \in \mathbb{Z}$ tais que $r = n^2 + m^2$. Mostre que r é redutível em $\mathbb{Z}[i]$.

b) Mostre que r, elemento de $\mathbb{N}$, pode ser redutível em $\mathbb{Z}[i]$ e não existirem $n, m \in \mathbb{Z}$ tais que $r = n^2 + m^2$.

c) Mostre que se p é um primo de $\mathbb{Z}$ então p é um primo de $\mathbb{Z}[i]$ se e só se não existem $n, m \in \mathbb{Z}$ tais que $p = n^2 + m^2$.

d) Mostre que se p um número primo de $\mathbb{Z}$ tal que $p \equiv 3 \pmod 4$ então p é um primo de $\mathbb{Z}[i]$.

e) Seja p um primo (de $\mathbb{Z}$) e suponha que $n, m \in \mathbb{Z}$ são tais que $p = n^2 + m^2$. Mostre que $n + mi$ é um irredutível de $\mathbb{Z}[i]$.

Exercício 12. Justifique a afirmação: se d é um inteiro maior que 2 então $\mathbb{Z}[i\sqrt{d}]$ não é um DFU.

Exercício 13. Seja D um DIP e $a, b \in D$. Mostre que $< (a,b) >=< a > + < b >$ e $< [a,b] >=< a > \cap < b >$.

Exercício 14. Mostre que, se D é um DIP e $a, b, c \in D$ com $(a,b) \sim 1$ então $(a, bc) \sim (a, c)$.

Exercício 15. Calcule, sem usar o algoritmo da divisão o máximo divisor comum e o mínimo múltiplo comum entre:

a) $55 + 10i$ e $-18 + 26i$;

b) $31 + 53i$ e $33 + 19i$;

c) $23 + 89i$ e $146 - 57i$;

d) $(12 - 5i)(3 + 4i)(3 - i)^2$ e $232 - 1674i$.

Exercício 16. Seja I um ideal não nulo de $\mathbb{Z}[i]$. Mostre que $I \cap \mathbb{Z}$ é um conjunto infinito.

Exercício 17. Seja D um domínio de integridade e I um seu ideal. Mostre que I é maximal se e só se para qualquer $a \in D \setminus I$ existir $b \in D$ tal que $1 - ab \in I$.

Exercício 18. Considere o anel $\mathbb{Z}$ e os ideais $I =< 24 >$ e $J =< 36 >$

a) Quais são os elementos de $I \setminus J$?

b) Encontre a e b tais que $I \cap J =< a >$ e $I + J =< b >$.

c) Encontre uma cadeia de ideais $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$ começando em I e acabando em $\mathbb{Z}$ e de tal forma que para $i = \ldots, n - a$, não exista nenhum ideal K tal que $I_i \subsetneqq K \subsetneqq I_{i+1}$.

Exercício 19. Considere o anel $\mathbb{Z}[i\sqrt{d}]$ em que d é um inteiro ímpar maior que 1. Mostre que $(2, 1 + i\sqrt{d}) \sim 1$ mas não existem $x, y \in \mathbb{Z}[i\sqrt{d}]$ tais que $2x + (1 + i\sqrt{d})y = 1$ (compare com a Proposição 3.6.6).

Exercício 20. Considere o anel $\mathbb{Z}[i\sqrt{6}]$. Mostre que $(5, 2 + i\sqrt{6}) \sim 1$ mas não existem $x, y \in \mathbb{Z}[i\sqrt{d}]$ tais que $5x + (2 + i\sqrt{6})y = 1$ (compare com a Proposição 3.6.6).

Exercício 21. Considere o anel $\mathbb{Z}[i\sqrt{d}]$ em que d é um inteiro positivo maior que 1. Generalize o exercício anterior:

a) supondo $d \equiv 1 \pmod 5$ e escolhendo os elementos 5 e $2 + i\sqrt{d}$;

b) escolhendo os elementos $d - 1$ e $a + i\sqrt{d}$, supondo a um inteiro tal que $d - 1$ e $a^2 + 1$ não sejam primos entre si (em $\mathbb{Z}$).

Exercício 22. Conclua que os anéis considerados nos Exercícios 19 e 21 não são DIP's.

Exercício 23. Seja D um DE e I um ideal. Mostre que

$$D/I = \{a + I : \ a \in D, \, a = 0 \text{ ou } v(a) < v(\alpha)\} \quad \text{em que } \alpha \text{ é tal que } I =< \alpha >.$$

Exercício 24. Calcule todos os ideais maximais de $\mathbb{Z}[i]$ que contêm o ideal gerado por $(12 - 5i)(3 + 4i)(3 - i)^2$. Para cada um desses ideais J calcule o inverso de $111 + 123i + J$ no corpo $\mathbb{Z}[i]/J$. Quantos elementos tem cada um desses corpos?

Exercício 25. Considere o ideal I de $\mathbb{Z}[i]$ gerado por $\{61-23i, 142+44i\}$.

a) Encontre $\alpha \in \mathbb{Z}[i]$ tal que $I =< \alpha >$.

b) Determine os ideais maximais de $\mathbb{Z}[i]$ que contêm I.

c) Se K é um dos ideais encontrados na alínea anterior calcule o inverso de $2+7i+K$ em $\mathbb{Z}[i]/K$.

d) Para K nas condições acima, quantos elementos tem $\mathbb{Z}[i]/K$?

Exercício 26. Considere os ideais de $\mathbb{Z}[i]$, $I =< 85-51i >$, $J =< -18+106i >$ e $L = I + J$.

a) Encontre $\alpha \in \mathbb{Z}[i]$ tal que $L =< \alpha >$.

b) Verifique se $\mathbb{Z}[i]/I$ e $\mathbb{Z}[i]/J$ são corpos.

c) Determine os ideais maximais de $\mathbb{Z}[i]$ que contêm I.

d) Se K é um dos ideais encontrados na alínea anterior calcule o inverso de $2+7i+K$ em $\mathbb{Z}[i]/K$.

e) Para K nas condições acima, quantos elementos tem $\mathbb{Z}[i]/K$?

Exercício 27. Considere o ideal I de $\mathbb{Z}[i]$ gerado por $\{32+43i, 1+4i, 6-61i\}$.

a) Encontre $\alpha \in \mathbb{Z}[i]$ tal que $I =< \alpha >$.

b) Determine os ideais maximais de $\mathbb{Z}[i]$ que contêm I.

c) Se K é um dos ideais encontrados na alínea anterior calcule o inverso de $2+7i+K$ em $\mathbb{Z}[i]/K$.

d) Para K nas condições acima, quantos elementos tem $\mathbb{Z}[i]/K$?

Exercício 28. Verifique que $\mathbb{Z}[i]/ < 4+i >$ é um corpo e calcule o inverso de $2+i+ < 4+i >$. Quantos elementos tem o corpo $\mathbb{Z}[i]/ < 4+i >$?

a) Seja $I = \{2x+23y+(23x-2y)i : x, y \in \mathbb{Z}\}$.

b) Mostre que I é u ideal de $\mathbb{Z}[i]$.

c) Calcule $\alpha \in \mathbb{Z}[i]$ tal que $I =< \alpha >$.

d) Verifique se $\mathbb{Z}[i]/I$ é um corpo e, em hipótese negativa, calcule um ideal J contendo I tal que $\mathbb{Z}[i]/J$ seja um corpo.

e) Quantos elementos tem $\mathbb{Z}[i]/J$ em que J foi calculado na alínea anterior?

Exercício 29. Sejam D é um domínio de integridade, $a, b, d, k, r \in D$ tais que $d \sim (a, b)$ e $r \sim (ka, kb)$. Pretende-se provar que $r \sim k\, d$. Mostre que:

a) $dk|r$ e portanto existe $t \in D$ tal que $r = dkt$;

b) existem $q, s \in D$ tais que $a = dtq$ e $b = dts$ (note que r divide ak e bk);

c) t é invertível;

d) $(ka, kb) \sim k\,(a, b)$.

Exercício 30. Mostre que em $\mathbb{Z}[i\sqrt{3}]$ existe $(2, 1+i\sqrt{3})$ mas não existe $[2, 1+i\sqrt{3}]$. Compare com o Exercício 32

Exercício 31. Seja D um domínio de integridade e $a, b \in D$ tais que existe $[a, b]$ (mínimo múltiplo comum entre a e b).

a) Conclua da definição de mínimo múltiplo comum que existe $d \in D$ tal que $[a, b]\, d = ab$.

b) Mostre que d divide a e b. **Sugestão:** Escreva $[a, b] = an = bm$, calcule $[ab] \times [a, b]$ e use a alínea anterior.

c) Se $s = ax$ e $s = by$, com $x, y \in D$, mostre que $[a, b] \big| sxy$ e $[a, b]s \big| ab$.

d) Conclua que o elemento d encontrado na alínea anterior é um máximo divisor comum entre a e b.

Exercício 32. Seja D um domínio de integridade tais que existe máximo divisor comum de entre dois quaisquer dos seus elementos. Vejamos que existe mínimo múltiplo comum entre dois quaisquer dos seus elementos. Sejam $a, b \in D$, $d \sim (a, b)$ e $m, n \in D$ tais que $a = md$ e $b = nd$.

a) Considere $r = mnd$ e mostre que a e b dividem r.

b) Se s é um múltiplo de a e de b mostre que ab divide sa e sb.

c) Conclua do Exercício 29 que ab divide sd.

d) Mostre que r divide s e portanto $r = [a, b]$.