

“Isto portanto é a Matemática: ela faz lembrar a forma invisível da alma, ela dá vida às suas próprias descobertas; ela desperta a mente e purifica o intelecto; ela traz luz às nossas ideias intrínsecas; ela elimina o vazio e a ignorância com que nascemos.”

Proclo (410–485)

“O conhecimento é o nosso destino.”

Carl Sagan (1934–1996)

# Notas de Álgebra II

António Machiavelo

*Com o desejo de que quem ler estas notas  
faça bom uso das suas margens...*

Departamento de Matemática Pura  
Faculdade de Ciências da Universidade do Porto  
1997/98



# Capítulo 1

## Introdução, à laia de aperitivo.

“... o tempo é o único teste decisivo para a fecundidade de novas ideias ou pontos de vista. A fecundidade mede-se pela descendência e não pelas honras.”

A. Grothendieck (Math. Intell., vol. 11, n. 1, 1989, p. 35)

Por volta de 290 A.C., Soter Ptolomeu, primeiro rei de toda uma dinastia de monarcas de origem grega que governaram o Egípto após o desmembramento do império de Alexandre Magno (356–323 A.C.), mandou construir em Alexandria, cidade fundada por aquele na costa mediterrânica do norte de África, um edifício no qual eruditos e sábios pudessem estudar e ensinar, continuando assim o plano de Alexandre (que foi educado por Aristóteles (384–322 A.C.)) de fazer daquela cidade o centro de uma cultura cosmopolita. Este edifício, dedicado às musas, ficou a ser conhecido como o Museu e nele conviviam, entre outros, poetas, filósofos, filologistas, astrónomos, geógrafos, médicos, historiadores, artistas e os mais famosos matemáticos da civilização grega do chamado período helénico, desde Euclides (~350 A.C.) a Hipácia (370–415 D.C.), e incluindo: Arquimedes (287–212 A.C.), Apolónio (~262–190 A.C.), Hiparco (m. ~125 A.C.), Menelau (~98 D.C.), Ptolomeu (m. 168 D.C.), Herão (séc. III D.C.), Pappo (fim do séc. III D.C.) e Diofanto (~250 D.C.)

Adjacente ao Museu, Ptolomeu construiu uma Biblioteca, não só para preservação de documentos importantes, mas também para uso do público em geral. O Museu e a Biblioteca de Alexandria (que se diz ter chegado a conter 750 000 livros) floresceram durante toda a dinastia ptolemaica, até 30 D.C., e mesmo durante a ocupação romana mas só até 415 D.C., data do assassinio de Hipácia e altura em que parte das obras da Biblioteca foram queimadas por cristãos fanáticos, naquele que é talvez o maior crime de sempre contra o património cultural da Humanidade.

Nada se sabe da vida de Diofanto para além do que é descrito num problema contido na *Antologia Grega* (~ 500 D.C.) de Metrodoro, o que é fraca garantia da sua autenticidade.

Esse problema descreve os seguintes factos da vida de Diofanto: foi um rapaz durante  $\frac{1}{6}$  da sua vida; após  $\frac{1}{12}$  desta já usava barba; passados mais  $\frac{1}{7}$  (da sua vida) casou, tendo

um filho 5 anos depois. Este viveu metade da vida do pai, que morreu 4 anos após a morte daquele filho.

*Exercício:* Quantos anos viveu Diofanto?

Das obras de Diofanto sobreviveram uma parte de um tratado sobre números poligonais e parte de uma obra constituída por 13 livros, intitulada *Aritmética*, uma obra que inspirou matemáticos de gerações futuras, e muito em particular alguns do século XVII, e que é assim directamente responsável por algumas das ideias e resultados que serão estudados neste curso.

A *Aritmética* de Diofanto consiste numa colecção de problemas, cujo objectivo é a resolução de certas equações indeterminadas (i.e., com várias soluções) em números racionais, e respectivas soluções. Um desses problemas, que se passa a descrever, iria ter consequências que Diofanto não podia sequer imaginar...

Problema 8, Livro II: *Dividir um número quadrado em dois quadrados.*

*Resolução de Diofanto* (em notação moderna!...): Seja 16 o quadrado que se pretende dividir em dois quadrados. Seja  $x^2$  um deles; então o outro será  $16 - x^2$ . Queremos pois que  $16 - x^2$  seja um quadrado. Tomo um quadrado da forma  $(ax - 4)^2$ ,  $a$  sendo um número qualquer e 4 a raiz de 16; por exemplo, seja o lado igual a  $2x - 4$ , sendo o quadrado igual a  $4x^2 + 16 - 16x$ . Então  $4x^2 + 16 - 16x = 16 - x^2$ . Adicione a ambos os lados os termos negativos e tire-se aqueles que são iguais. Então  $5x^2 = 16x$ , e  $x = \frac{16}{5}$ . Um dos números será pois  $\frac{256}{25}$  e o outro  $\frac{144}{25}$ .

Este e outros problemas da *Aritmética* mostram que Diofanto sabia bem como obter soluções racionais da equação  $x^2 + y^2 = z^2$ , dita pitagórica, que veremos de seguida, numa versão muito mais recente.

Solução da equação pitagórica ( $x^2 + y^2 = z^2$ ) em números inteiros:

Sejam  $a, b, c \in \mathbb{Z}$  tais que  $a^2 + b^2 = c^2$ . Tem-se que:

1. Se  $d$  divide dois dos números  $a, b, c$ , então também divide o terceiro;
2. Dividindo  $a, b, c$  pelo seu máximo divisor comum, obtém-se uma solução de  $x^2 + y^2 = z^2$  em que quaisquer dois dos três números são primos entre si;
3. Sejam então  $a, b, c \in \mathbb{Z}$  primos entre si dois a dois, e tais que  $a^2 + b^2 = c^2$ . Se  $c$  fosse par, então  $a$  e  $b$  seriam ímpares e ter-se-ia  $a^2 \equiv b^2 \equiv 1 \pmod{4}$ ,  $c^2 \equiv 0 \pmod{4}$ , o que não pode ser, pois isto implicaria  $1 + 1 \equiv 0 \pmod{4}$ . Conclui-se assim que  $c$  é ímpar (!).
4. Supondo, sem perda de generalidade, que  $a$  é par e  $b$  é ímpar, tem-se:

$$a^2 = c^2 - b^2 = (c + b)(c - b) \Rightarrow \left(\frac{a}{2}\right)^2 = \left(\frac{c + b}{2}\right)\left(\frac{c - b}{2}\right) (*),$$

sendo todos os números nesta última igualdade inteiros.

5. Os números  $\left(\frac{c+b}{2}\right)$  e  $\left(\frac{c-b}{2}\right)$  são primos entre si:

$$d \mid \frac{c+b}{2} \text{ e } d \mid \frac{c-b}{2} \Rightarrow d \mid \frac{c+b}{2} + \frac{c-b}{2} = c \text{ e } d \mid \frac{c+b}{2} - \frac{c-b}{2} = b \Rightarrow d \mid c \text{ e } d \mid b.$$

6. Resulta de (\*), pela **unicidade da decomposição em números primos**, que:

$$\left(\frac{c+b}{2}\right) = \pm u^2 \text{ e } \left(\frac{c-b}{2}\right) = \pm v^2 \text{ para alguns } u, v \in \mathbb{Z} \text{ (porquê?).}$$

7. Conclui-se que  $a = \pm 2uv$ ,  $b = \pm(u^2 - v^2)$  e  $c = \pm(u^2 + v^2)$ .

Tudo isto (quase...) prova o seguinte:

### Teorema 1.0.1 (dos ternos pitagóricos)

$$\begin{array}{l} x, y, z \in \mathbb{Z} \\ \wedge \\ x^2 + y^2 = z^2 \end{array} \Leftrightarrow \exists u, v, d \in \mathbb{Z} : \begin{cases} x = 2duv \\ y = d(u^2 - v^2) \\ z = d(u^2 + v^2) \end{cases} \vee \begin{cases} x = d(u^2 - v^2) \\ y = 2duv \\ z = d(u^2 + v^2) \end{cases}$$

*Observação:* Uma solução  $(a, b, c)$  de  $x^2 + y^2 = z^2$  em números inteiros diz-se um *terno pitagórico*. Usa-se o adjectivo *primitivo* quando  $\text{m.d.c.}(a, b, c) = 1$ .

*Exercício:* Complete os detalhes dos passos da demonstração anterior que sejam menos claros para si, e mostre “ $\Leftarrow$ ”.

*Exemplos:*  $d = 1, u = 2, v = 1 \longrightarrow (3, 4, 5)$   
 $d = 1, u = 3, v = 2 \longrightarrow (5, 12, 13)$

A obra de Diofanto, como a de vários outros matemáticos e pensadores gregos, esteve esquecida e perdida durante séculos. Foi por volta de 1570 que o matemático italiano Rafael Bombelli (1526–72) descobriu, no Vaticano, 6 dos livros da *Aritmética* de Diofanto<sup>1</sup>, e inclui todos os problemas dos primeiros 4 livros na sua *Álgebra*, publicada em 1572, intercalando com alguns originais seus. Em 1575 é publicada a primeira tradução da *Aritmética*, do grego para o latim, por Wilhelm Holtzman (1532–76).

<sup>1</sup>Em 1973 foram descobertos mais 4, no Irão, que se pensa serem os livros IV, V, VI e VII. Os seis que se conheciam até então são o I, II, III e outros 3 (ver J. Sesiano, *Books IV to VII of Diophantus' Arithmetica: in the arabic translation attributed to Qustā ibn Lūqā*, Springer-Verlag 1982).

Em 1621, Bachet de Méziriac (1581–1638)<sup>2</sup> publica o texto em grego da *Aritmética* juntamente com uma tradução para o latim e algumas notas suas sobre os problemas e soluções de Diofanto. Uma cópia desta edição que é adquirida por Pierre de Fermat (1601–65), homem de leis por profissão (foi conselheiro do tribunal superior de Toulouse), matemático por paixão.

Fermat irá anotar nas margens da sua cópia da *Aritmética* resultados sobre números naturais, inspirados sem dúvida no seu estudo e leitura desta obra, mas completamente novos e de uma beleza e profundidade impressionantes, e sem paralelo até então. Fermat limita-se a enunciar, nessas margens e em cartas a outros matemáticos, esses resultados, sendo apenas conhecido um esboço de uma prova sua em Teoria dos Números. Os melhores matemáticos do século XVII, em especial L. Euler (1707–83), trabalharam arduamente na tentativa de provar os resultados de Fermat. Um destes, que se passou a chamar “o último”, deu que fazer a muitos dos melhores matemáticos desde Fermat a 1994!

Alguns exemplos de resultados descobertos por Fermat:

- “Pequeno” Teorema de Fermat:

$$p \in \mathbb{N} \text{ primo, } a \text{ não divisível por } p \Rightarrow a^{p-1} \equiv 1 \pmod{p}.$$

[Fermat é conduzido a este resultado procurando números perfeitos<sup>3</sup>]

- $p \in \mathbb{N}$  primo,  $p \equiv 1 \pmod{4} \Rightarrow p$  é soma de dois quadrados.

[Este resultado aparece da tentativa de resposta à pergunta natural: quais os números que são hipotenusas de triângulos retângulos de lados inteiros?]

- Todo o número natural é soma de:

- não mais de 3 números triangulares (Gauss, 10/7/1796  $\rightarrow$  entrada #18 do seu diário matemático: EYPHKA! num =  $\triangle + \triangle + \triangle$ );
- não mais de 4 números quadrados (Lagrange, 1770);
- não mais de 5 números pentagonais;
- ...etc... (Cauchy, 1815).

- “Grande” ou “Último” Teorema de Fermat:

$$\text{a equação } x^n + y^n = z^n \text{ não tem soluções em } \mathbb{N}, \forall n > 2.$$

<sup>2</sup>Se lê francês, então o leitor não poderá deixar de dar uma olhada numa deliciosa obra de Bachet: *Problèmes Plaisants et Délectables qui se font par les Nombres*, (editora A. Bralchard, 1993; a primeira edição é de 1612) (Há uma cópia na biblioteca do Departamento de Matemática Pura do Porto).

<sup>3</sup>Ver: H. M. Edwards, *Fermat’s Last Theorem: a genetic introduction to algebraic number theory*, Springer–Verlag, 1977, Cap. 1.

[Este é o resultado que Fermat escreve na margem ao lado da Proposição 8 do livro II, e que só foi provado em 1994<sup>4</sup>]

- A equação  $y^3 = x^2 + 2$  tem apenas uma solução em  $\mathbb{N}$ :  $x = 5, y = 3$  !!

É o trabalho na tentativa de provar resultados do tipo dos dois últimos que irá conduzir às noções de “anel” e de “ideal” que estudaremos neste curso. Daremos aqui apenas uma muito pequena ideia dessa evolução, exibindo um método, que se deve a Euler e Lagrange, e que foi aperfeiçoado e clarificado por Gauss, para mostrar o penúltimo dos resultados de Fermat que acabamos de mencionar.

*Ideia para resolver  $y^3 = x^2 + 2$ :*

Em  $\mathbb{C}$  tem-se  $y^3 = x^2 + 2 = (x + \sqrt{2}i)(x - \sqrt{2}i)$ . Considere-se o conjunto dos números complexos da forma  $a + b\sqrt{2}i$ , com  $a, b \in \mathbb{Z}$ . Designemos tal conjunto por  $A$ . Observe-se que  $A$  é “fechado” para a soma e para a multiplicação:

$$\begin{aligned}(a + b\sqrt{2}i) + (c + d\sqrt{2}i) &= (a + c) + (b + d)\sqrt{2}i, \quad \forall a, b, c, d \in \mathbb{Z}; \\ (a + b\sqrt{2}i) \cdot (c + d\sqrt{2}i) &= (ac - 2bd) + (ad + bc)\sqrt{2}i, \quad \forall a, b, c, d \in \mathbb{Z}.\end{aligned}$$

Agora: **se**  $A$  fosse “como”  $\mathbb{Z}$ , no sentido de se poder falar em primos e **se** cada elemento de  $A$  admitisse uma única decomposição como produto de primos, então **se**  $x + \sqrt{2}i$  e  $x - \sqrt{2}i$  fossem “primos entre si”, ter-se-ia:

$$x + \sqrt{2}i = (a + b\sqrt{2}i)^3, \text{ para alguns } a, b \in \mathbb{Z} \text{ (porquê?).}$$

Mas  $x + \sqrt{2}i = (a + b\sqrt{2}i)^3 \Rightarrow x = a^3 - 6ab^2 = a(a^2 - 6b^2) \wedge 1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2) \Rightarrow b = \pm 1 \wedge 3a^2 - 2b^2 = b \Rightarrow 3a^2 - 2 = b = \pm 1 \Rightarrow b = 1 \wedge a = \pm 1$ . Resulta assim que  $x = a(a^2 - 6b^2) = \pm(1 - 6) = \mp 5$ , e portanto  $y = 3$  !!

Vislumbra-se assim a importância de estudar conjuntos de números como  $A$ , que é um exemplo daquilo a que hoje se chama um anel.

---

<sup>4</sup>Ver: A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **142** (1995) 443–551.

# Capítulo 2

## Factorização em Anéis

### 2.1 Anéis e Corpos: noções e exemplos básicos.

**Definição 2.1.1** *Um conjunto (não-vazio)  $A$  munido de duas operações,  $+$  :  $A \times A \rightarrow A$  e  $\cdot$  :  $A \times A \rightarrow A$ , diz-se um **anel** se se tiver:*

- i)  $(A, +)$  é um grupo abeliano;*
- ii)  $\cdot$  é associativa e tem elemento neutro;*
- iii)  $\forall a, b, c \in A$   $(a+b) \cdot c = a \cdot c + b \cdot c$  e  $a \cdot (b+c) = a \cdot b + a \cdot c$  (distributividade de  $\cdot$  relativamente a  $+$ ).*

*Um **subanel** de um anel é um subconjunto que é um anel para as operações induzidas e com o mesmo elemento neutro para  $\cdot$ .*

*Observação:* Em certos contextos usa-se a palavra **anel** para um conjunto munido de duas operações satisfazendo as condições contidas na definição anterior excepto a existência de elemento neutro para  $\cdot$ . Nesses contextos, um anel que tenha elemento neutro para  $\cdot$  diz-se um **anel unitário**.

*Observação:* As condições contidas na definição anterior dizem-se os axiomas de anel. Note-se que a condição i) é uma maneira resumida de expressar 4 axiomas...

*Notações:* As operações  $+$  e  $\cdot$  são usualmente designadas a adição e a multiplicação do anel (podendo obviamente nada ter a ver com as operações de  $\mathbb{R}$  e  $\mathbb{C}$  com esse nome...); o elemento neutro para  $+$  é designado por 0 e o para  $\cdot$  por 1, e dizem-se o zero e o um do anel (respectivamente).

*Observação/Exercício:* É fácil ver que um subconjunto  $S$  de um anel  $A$  é um subanel se e só se:

- i)  $1 \in S$ ;

ii)  $x, y \in S \Rightarrow x - y \in S$ ;

iii)  $x, y \in S \Rightarrow x \cdot y \in S$ .

**Definição 2.1.2** Um anel diz-se **comutativo** se  $\cdot$  for comutativa.

**CONVENÇÃO**: Como neste curso lidaremos (quase) exclusivamente com anéis comutativos, usaremos a palavra anel como sinónimo de anel comutativo. Quando, eventualmente, precisarmos de nos referir a anéis que não são comutativos isso será sempre explicitado.

**Definição 2.1.3** Um anel (comutativo) diz-se um **corpo** se  $K - \{0\}$  for não-vazio e  $(K - \{0\}, \cdot)$  for um grupo abeliano. Isto é, um corpo é um conjunto  $K$  com pelo menos dois elementos, munido de duas operações, usualmente designadas por  $+$  e  $\cdot$ , tais que  $(K, +)$  e  $(K - \{0\}, \cdot)$  são grupos abelianos (onde  $0$  designa o elemento neutro para  $+$ ) e  $\cdot$  é distributiva relativamente a  $+$ .

Um **subcorpo** de um corpo é um subconjunto que é um corpo para as operações induzidas.

*Observação/Exercício:* É fácil ver que um subconjunto  $F$  de um corpo  $K$  é um subcorpo sse:

i)  $F \neq \emptyset$ ;

ii)  $x, y \in F \Rightarrow x - y \in F$ ;

iii)  $x, y \in F - \{0\} \Rightarrow x \cdot y^{-1} \in F - \{0\}$ .

*Exemplos:*

1.  $\mathbb{Z}$  munido da adição e multiplicação usuais é um anel e não é um corpo;
2.  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  munidos da adição e multiplicação usuais são corpos, e portanto anéis;
3.  $\mathcal{M}_{n \times n}(\mathbb{R})$  ( $n \in \mathbb{N}$ ), o conjunto das matrizes  $n \times n$  com entradas reais, munido da soma e multiplicação usuais de matrizes, é um anel unitário não-comutativo para  $n \geq 2$ ;
4.  $\mathbb{Z}$  é um subanel de  $\mathbb{Q}$  (e de  $\mathbb{R}$ ; e de  $\mathbb{C}$ );
5.  $2\mathbb{Z}$  **não** é um subanel de  $\mathbb{Z}$ , uma vez que  $(2\mathbb{Z}, \cdot)$  não tem elemento neutro;
6.  $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$  é um subanel de  $\mathbb{C}$ , a que é usual chamar o anel dos inteiros de Gauss;

7.  $\mathcal{C}(I, \mathbb{R})$ , o conjunto das funções contínuas definidas num intervalo  $I$  de  $\mathbb{R}$  e com valores reais, munido das operações dadas por:  
 $(f+g)(x) := f(x) + g(x)$  e  $(f \cdot g)(x) := f(x)g(x), \forall x \in I (f, g \in \mathcal{C}(I, \mathbb{R}))$ ,  
 é um anel;
8. Para cada  $n \in \mathbb{N}$ , o conjunto  $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$  das classes de congruência módulo  $n$  (relembre que  $[a]_n := \{a + nk : k \in \mathbb{Z}\}$ ), munido das operações dadas por  $[a]_n + [b]_n := [a + b]_n$  e  $[a]_n \cdot [b]_n := [ab]_n$  é um anel, que se chama o anel dos inteiros módulo  $n$ ;
9. Se  $p \in \mathbb{N}$  é um número primo, então  $\mathbb{Z}_p$  é um corpo. Que todo o elemento de  $\mathbb{Z}_p - \{0\}$  tem inverso multiplicativo resulta de:  $0 < i < p \Rightarrow (i, p) = 1 \Rightarrow \exists x, y \in \mathbb{Z} : ix + py = 1 \Rightarrow [i]_p \cdot [x]_p = 1$ ;
10.  $B := \{[0]_6, [3]_6\}$  **não** é um subanel de  $\mathbb{Z}_6$  pois, apesar de  $(B, +) \leq (\mathbb{Z}_6, +)$  e  $(B, \cdot)$  ser associativo e ter elemento neutro ( $[3]_6$ ), este não é o elemento neutro de  $(\mathbb{Z}_6, \cdot)$ ;
11.  $\mathbb{Q}(i) := \{a + bi : a, b \in \mathbb{Q}\}$  é um subcorpo de  $\mathbb{C}$ :  $\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i, \forall a + bi \neq 0$ , mostra que o inverso de todo o elemento de  $\mathbb{Q}(i) - \{0\}$  ainda pertence a  $\mathbb{Q}(i)$ . O resto é óbvio.

*Notações:* O inverso aditivo de um elemento  $a$  de um anel é denotado por  $-a$  e designado por o simétrico de  $a$ . Caso  $a$  tenha um inverso multiplicativo (por exemplo, num corpo se  $a \neq 0$ ), então ele é único (*porquê?*) e é denotado por  $a^{-1}$ , sendo designado simplesmente por o inverso de  $a$ .

**Proposição 2.1.4** *Seja  $A$  um anel. Tem-se que:*

- i)  $0 \cdot a = 0, \forall a \in A$ ;
- ii)  $(-1) \cdot a = -a, \forall a \in A$ .

*Demonstração:*

- i)  $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \Rightarrow 0 \cdot a = 0$ .
- ii)  $0 = 0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a \Rightarrow (-1) \cdot a = -a$ .

Um conjunto com um único elemento,  $\{\spadesuit\}$ , é obviamente um anel tomando para ‘adição’ e para ‘multiplicação’ a mesma operação, que tem de ser a única operação que pode ser definida num tal conjunto:  $(\spadesuit, \spadesuit) \mapsto \spadesuit$ . “Este” anel diz-se “o” anel trivial ou anel zero, escrevendo-se  $A = 0$  quando se quer indicar que o anel  $A$  é trivial. Observe que num anel trivial  $1 = 0$ .

**Proposição 2.1.5**  $A \neq 0 \Rightarrow 1 \neq 0$ .

*Razão:*  $1 = 0 \Rightarrow a = 1 \cdot a = 0 \cdot a = 0, \forall a \in A$ .

*Observação:* Um anel trivial não é um corpo, uma vez que na definição de corpo se excluiu explicitamente tal possibilidade. Obviamente isto é uma questão de convenção, usando-se a que dá mais jeito num maior número de situações...

## 2.2 Anéis de polinômios

Dado um anel  $A$  e um *símbolo abstracto*, distinto dos elementos de  $A$ , que é usual denotar por  $x$  e chamar “uma variável” (por razões históricas...), denota-se por  $A[x]$  o conjunto das *expressões formais*  $a_0 + a_1x + \dots + a_nx^n$ , com  $n \in \mathbb{N}_0, a_i \in A (\forall 0 \leq i \leq n)$ , munido da adição dada por:

$$\begin{aligned} (a_0 + a_1x + a_2x^2 + \dots) + (b_0 + b_1x + b_2x^2 + \dots) &:= \\ &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots, \quad (a_i, b_j \in A, \forall i, j), \end{aligned}$$

e da única multiplicação tal que  $x^m \cdot x^n = x^{m+n} (\forall m, n \in \mathbb{N}_0)$  e que é distributiva relativamente à adição acabada de definir, i.e. a operação dada por:

$$\begin{aligned} (a_0 + a_1x + a_2x^2 + \dots) \cdot (b_0 + b_1x + b_2x^2 + \dots) &:= \\ &= (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \\ &\quad + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3 + \dots \quad (a_i, b_j \in A, \forall i, j), \end{aligned}$$

(onde “...” significa, como é usual, “continuando de acordo com o padrão evidenciado”).

$A[x]$  é um anel (verifique-o!), que se chama o anel dos polinômios com coeficientes em  $A$ , ou mais simplesmente o anel dos polinômios sobre  $A$ .

Trabalhar com polinômios definidos como acima tem, por vezes, inconvenientes técnicos. Por exemplo, ao somar ou multiplicar dois polinômios genéricos  $a_0 + a_1x + \dots + a_nx^n$  e  $b_0 + b_1x + \dots + b_mx^m$  é necessário saber se  $n > m$ ,  $n = m$  ou  $n < m$ , o que conduz à sempre desagradável subdivisão em casos. Na análise de problemas um pouco mais complexos esses inconvenientes podem-se revelar insuportavelmente aborrecidos. Assim, e por razões de ordem técnica, repita-se, é por vezes útil definir os polinômios com coeficientes num anel  $A$  como sendo as aplicações de  $\mathbb{N}_0$  em  $A$  com suporte finito, o que quer dizer que são não-nulas apenas para um número finito de elementos de  $\mathbb{N}_0$ . Mais precisamente: dado  $f : \mathbb{N}_0 \rightarrow A$ , o conjunto  $\{n \in \mathbb{N}_0 : f(n) \neq 0\}$  diz-se o **suporte** de  $f$ . Assim,  $A[x]$  pode ser também definido como o conjunto  $\{f : \mathbb{N}_0 \rightarrow A : f \text{ tem suporte finito}\}$ , munido das operações dadas por:

$$(f + g)(n) := f(n) + g(n) \text{ e } (f \cdot g)(n) := \sum_{i+j=n} f(i)g(j), \quad \forall n \in \mathbb{N}_0 (f, g \in A[x]).$$

*Exercício:* Mostre que:  $f$  e  $g$  têm suporte finito  $\Rightarrow f + g$  e  $f \cdot g$  têm suporte finito.

A ideia desta “construção” dos polinómios é a de que um polinómio é inteiramente determinado pelos seus coeficientes; e dar os coeficientes de um polinómio  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  é equivalente a dar uma função  $a : \mathbb{N}_0 \rightarrow A$  com suporte finito, nomeadamente  $a(0) = a_0, a(1) = a_1, a(2) = a_2, \dots, a(n) = a_n$  e  $a(k) = 0 \forall k > n$ . Isto corresponde a “ver” os polinómios como expressões infinitas da forma  $a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0x^{n+1} + 0x^{n+2} + \dots$ , com coeficientes nulos a partir de certa ordem. Deste modo podemos operar com polinómios sem nos termos de preocupar onde é que eles “acabam”.

*Exercício:* Qual é a função que corresponde ao “x”?

Esta definição tem também a vantagem de os elementos de  $A[x]$  serem definidos como entidades matemáticas genuínas e não meramente como “expressões da forma...”, usando um “símbolo abstracto”.

Mais ainda, é imediatamente generalizável a polinómios de várias variáveis, tornando o seu tratamento muito mais simpático:

**Definição 2.2.1** *Um polinómio em  $n$  variáveis com coeficientes num anel  $A$  é uma aplicação  $p : \mathbb{N}_0^n \rightarrow A$  com suporte finito, i.e. tal que o conjunto  $\{v \in \mathbb{N}_0^n : p(v) \neq 0\}$  seja finito.*

*Notação:* Um polinómio  $p$  em  $n$  variáveis com coeficientes num anel  $A$  é usualmente escrito na forma:

$$\sum_{(i_1, i_2, \dots, i_n) \in \mathbb{N}_0^n} a_{i_1 i_2 \dots i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n},$$

onde  $a_{i_1 i_2 \dots i_n} = p(i_1, i_2, \dots, i_n)$ .

Denota-se por  $A[x_1, x_2, \dots, x_n]$  o conjunto dos polinómios em  $n$  variáveis com coeficientes no anel  $A$ , munido da adição e multiplicação dadas por:

$$\begin{aligned} (f + g)(u) &= f(u) + g(u), \quad \forall u \in \mathbb{N}_0^n \\ (f \cdot g)(u) &= \sum_{v+w=u} f(v)g(w), \quad \forall u \in \mathbb{N}_0^n, \end{aligned}$$

onde  $f, g \in A[x_1, \dots, x_n]$  e a soma debaixo do somatório é a adição usual de vectores(!).

A título de exemplo, vejamos a prova da associatividade da multiplicação de  $A[x_1, x_2, \dots, x_n]$  ( $n \in \mathbb{N}$ ). Dados  $f, g, h \in A[x_1, x_2, \dots, x_n]$ , tem-se, para todo  $n \in \mathbb{N}_0^n$ :

$$\begin{aligned} ((f \cdot g) \cdot h)(n) &= \sum_{i+j=n} (f \cdot g)(i)h(j) = \sum_{i+j=n} \left( \sum_{k+l=i} f(k)g(l) \right) h(j) = \\ &= \sum_{i+j=n} \sum_{k+l=i} f(k)g(l)h(j) = (\text{porquê?}) = \sum_{k+l+j=n} f(k)g(l)h(j), \end{aligned}$$

enquanto que:

$$\begin{aligned} (f \cdot (g \cdot h))(n) &= \sum_{k+i=n} f(k)(g \cdot h)(i) = \sum_{k+i=n} f(k) \left( \sum_{l+j=i} g(l)h(j) \right) = \\ &= \sum_{k+i=n} \sum_{l+j=i} f(k)g(l)h(j) = (\text{porquê?}) = \sum_{k+l+j=n} f(k)g(l)h(j), \end{aligned}$$

o que conclui a prova.

*Exercício:* Verifique que as operações definidas em  $A[x_1, x_2, \dots, x_n]$  satisfazem todos os outros axiomas de anel.

**Definição 2.2.2** Se  $f = a_0 + a_1x + \dots + a_nx^n \in A[x]$  ( $A$  um anel qualquer) for um polinómio não-nulo com  $a_n \neq 0$ , diz-se que  $n$  é o **grau** de  $f$ , que denotaremos por  $\text{gr}(f)$ ;  $a_n$  diz-se o **coeficiente guia** de  $f$  e  $a_0$  diz-se o **termo constante** ou **independente** de  $f$ . O polinómio  $f$  diz-se **mónico** se o seu coeficiente guia for 1. Um polinómio diz-se **constante**, **linear**, **quadrático**, **cúbico**, consoante o seu grau for 0, 1, 2, 3, respectivamente.

## 2.3 Homomorfismos e Isomorfismos de Anéis

**Definição 2.3.1** Dados dois anéis  $A$  e  $B$ , uma aplicação  $\varphi : A \rightarrow B$  diz-se um **homomorfismo (de anéis)** se:

1.  $\varphi(a + b) = \varphi(a) + \varphi(b)$ ,  $\forall a, b \in A$   
(ou seja, se  $\varphi$  for um homomorfismo (de grupos) de  $(A, +)$  em  $(B, +)$ );
2.  $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ ,  $\forall a, b \in A$ ;
3.  $\varphi(1_A) = 1_B$ .

Um homomorfismo (de anéis) bijectivo diz-se um **isomorfismo (de anéis)**. Diz-se que dois anéis  $A$  e  $B$  são **isomorfos**, o que é denotado por  $A \simeq B$ , se existir pelo menos um isomorfismo  $\varphi : A \rightarrow B$ .

Um homomorfismo  $\varphi : A \rightarrow A$  diz-se um **endomorfismo** de  $A$ . Um **automorfismo** é um isomorfismo de  $A$  em  $A$ .

*Observação:*  $\simeq$  é uma relação de equivalência.

*Exemplos:*

1. A aplicação natural  $\mathbb{Z} \rightarrow \mathbb{Z}_n$  é um homomorfismo (de anéis) sobrejectivo;  
 $x \mapsto [x]_n$

2. Seja  $A$  um anel arbitrário. A aplicação  $i : A \rightarrow A[x]$  definida por  $a \mapsto a + 0x + 0x^2 + \dots$  é um homomorfismo injectivo. Uma vez que  $A \simeq i(A)$ , isto permite-nos identificar  $A$  com o subanel de  $A[x]$  constituído pelos polinómios constantes (verifique que estes formam de facto um subanel...) e justifica o ligeiro abuso de linguagem quando se diz que  $A$  é um subanel de  $A[x]$ ;
3. Se  $\varphi : A \rightarrow B$  é um homomorfismo de anéis, então a aplicação  $\tilde{\varphi} : A[x] \rightarrow B[x]$  dada por  $\sum_{i \in \mathbb{N}_0} a_i x^i \mapsto \sum_{i \in \mathbb{N}_0} \varphi(a_i) x^i$  também o é (*verifique-o!*). Mais ainda, se  $\varphi$  for um isomorfismo, então também  $\tilde{\varphi}$  o é. Em particular:  $A \simeq B \Rightarrow A[x] \simeq B[x]$ .

## 2.4 Ideais e Anéis Quociente

Seja  $A$  um anel qualquer (comutativo e unitário). Dado um subgrupo  $I$  de  $(A, +)$ , ele é automaticamente normal por  $(A, +)$  ser abeliano. Portanto, como sabemos de Álgebra I,  $A/I$ , o conjunto das classes laterais esquerdas<sup>1</sup> (= direitas, neste caso) de  $A$  módulo  $I$  é um grupo abeliano para a operação natural definida por:

$$(a + I) + (b + I) := (a + b) + I \quad (a, b \in A).$$

É assim natural considerar a questão: quando é que

$$(a + I) \cdot (b + I) := ab + I \quad (a, b \in A)$$

define uma operação em  $A/I$ ?

*Resposta:* Para  $\cdot$  estar bem definida é necessário e suficiente que se tenha (*porquê?*):

$$\begin{aligned} (a + I) \cdot (b + I) &= ((a + x) + I) \cdot ((b + y) + I), \forall a, b \in A; x, y \in I \Leftrightarrow \\ &\Leftrightarrow ab + I = (a + x)(b + y) + I, \forall a, b \in A; x, y \in I \Leftrightarrow \\ &\Leftrightarrow (a + x)(b + y) - ab = ay + xb + xy \in I, \forall a, b \in A; x, y \in I. \end{aligned}$$

Mas então ter-se-á de ter, em particular (fazendo  $y = 0$ ):

$$bx \in I \quad \forall b \in A, x \in I.$$

---

<sup>1</sup>N.B. O conceito de grupo e anel quociente é de uma importância fundamental em Álgebra. Assim deve ser aprendido com especial cuidado, de modo a se tornar um conceito completamente familiar. Ao longo dos anos, geração após geração de alunos, é sempre a mesma coisa: um medo irracional do conceito de quociente, que se evita e se deixa para “aqueles que já nasceram para perceber estas coisas”... Quanto desperdício de capacidades! Em especial quando a receita para aprender estas, bem como muitas outras coisas, é muito simples: basta um pouco de audácia para seguir o caminho dos nossos próprios passos; não ter medo de trabalhar um pouco (e de o dizer!), e de um modo contínuo; e tentar **honestamente** perceber estas coisas. Quem experimentar esta simples receita, irá surpreender-se!...

Porém, esta condição é também suficiente, pois se for satisfeita, então  $a, b \in A; x, y \in I \Rightarrow xy \in I, ay \in I, bx \in I \Rightarrow ay + xb + xy \in I$ , pois  $(I, +) \leq (A, +)$ .

Conclusão: se  $I \subseteq A$  for um subgrupo de  $(A, +)$  tal que  $a \in A, x \in I \Rightarrow ax \in I$ , então  $A/I$  fica naturalmente munido das operações dadas por:  $(a + I) + (b + I) := (a + b) + I$  e  $(a + I) \cdot (b + I) := ab + I$  ( $a, b \in A$ ).

*Exercício:* Verificar que  $A/I$  fica assim munido de uma estrutura de anel.

**Definição 2.4.1** Dado um anel  $A$ , um subconjunto não-vazio  $I$  de  $A$  diz-se um **ideal** se:

- i)  $x, y \in I \Rightarrow x - y \in I$  ( $\Leftrightarrow (I, +) \leq (A, +)$ );
- ii)  $a \in A, x \in I \Rightarrow ax \in I$ .

Se  $I$  é um ideal de  $A$ , então  $A/I$  é, como vimos, um anel de um modo natural, a que se chama o anel quociente de  $A$  por  $I$  (ou módulo)  $I$ .

*Exemplos:*

1.  $n\mathbb{Z}$  é um ideal de  $\mathbb{Z}$ , para todo  $n \in \mathbb{N}$ , e  $\mathbb{Z}_n$  é precisamente o anel quociente de  $\mathbb{Z}$  por  $n\mathbb{Z}$ , i.e.  $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ .
2. Se  $A$  for um anel qualquer, então  $\{\sum_{i \geq 0} a_i x^i \in A[x] : a_0 = 0\}$  é um ideal de  $A[x]$ .
3.  $I = \{\sum_{i \geq 0} a_i x^i \in \mathbb{Z}[x] : a_0 \text{ é par}\}$  é um ideal de  $\mathbb{Z}[x]$ .
4. Se  $A$  é um anel e  $a_1, a_2, \dots, a_n \in A$ , então  $\langle a_1, a_2, \dots, a_n \rangle := \{a_1 x_1 + a_2 x_2 + \dots + a_n x_n : x_1, x_2, \dots, x_n \in A\}$  (o conjunto de todas as “combinações lineares” de  $a_1, a_2, \dots, a_n$ ) é um ideal de  $A$ , que se diz **ideal gerado por**  $a_1, a_2, \dots, a_n$ .

*Verificação:*

$$\begin{aligned} \left( \sum_{i=1}^n a_i x_i \right) - \left( \sum_{i=1}^n a_i y_i \right) &= \\ &= \left( \sum_{i=1}^n a_i (x_i - y_i) \right) \in \langle a_1, a_2, \dots, a_n \rangle, \forall x_1, x_2, \dots, x_n; y_1, y_2, \dots, y_n \in A; \end{aligned}$$

$$a \left( \sum_{i=1}^n a_i x_i \right) = \left( \sum_{i=1}^n a_i (ax_i) \right) \in \langle a_1, a_2, \dots, a_n \rangle, \forall a; x_1, x_2, \dots, x_n \in A.$$

Trata-se de facto do menor (para a inclusão) ideal de  $A$  que contém  $a_1, a_2, \dots, a_n$ , uma vez que:  $a_1, a_2, \dots, a_n \in I$ ;  $I$  ideal de  $A \Rightarrow a_1 x_1 + a_2 x_2 + \dots + a_n x_n \in I \forall x_1, x_2, \dots, x_n \in A$ .

*Observação/Exercício:* Dado um ideal  $I$  de um anel  $A$ , tem-se:  $1 \in I \Leftrightarrow I = A$ .

**Definição 2.4.2** Dado  $\varphi : A \rightarrow B$  um homomorfismo de anéis (que é, em particular, um homomorfismo entre os respectivos grupos aditivos),  $\text{Ker } \varphi := \{a \in A : \varphi(a) = 0\}$  diz-se o núcleo de  $\varphi$  e  $\text{Im } \varphi := \{\varphi(a) : a \in A\}$  diz-se a imagem de  $\varphi$ .

**Teorema 2.4.3 (do homomorfismo)** Se  $\varphi : A \rightarrow B$  é um homomorfismo de anéis, então  $\text{Ker } \varphi$  é um ideal de  $A$ ,  $\text{Im } \varphi$  é um subanel de  $B$  e  $A/\text{Ker } \varphi \simeq \text{Im } \varphi$  (como anéis).

*Demonstração:* Que  $\text{Ker } \varphi$  é um ideal de  $A$  resulta de:  $x, y \in \text{Ker } \varphi \Rightarrow \varphi(x - y) = \varphi(x) - \varphi(y) = 0 \Rightarrow x - y \in \text{Ker } \varphi$ ;  $a \in A, x \in \text{Ker } \varphi \Rightarrow \varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)0 = 0$ .

Que  $\text{Im } \varphi$  é um subanel de  $B$  resulta de:  $b_1, b_2 \in \text{Im } \varphi \Rightarrow b_1 = \varphi(a_1), b_2 = \varphi(a_2)$ , para alguns  $a_1, a_2 \in A \Rightarrow b_1 - b_2 = \varphi(a_1 - a_2)$  e  $b_1 b_2 = \varphi(a_1 a_2) \Rightarrow b_1 - b_2, b_1 b_2 \in \text{Im } \varphi$ ; e de se ter  $1_B = \varphi(1_A) \in \text{Im } \varphi$ .

Agora, a aplicação  $\tilde{\varphi} : A/\text{Ker } \varphi \rightarrow \text{Im } \varphi$  dada por  $a + \text{Ker } \varphi \mapsto \varphi(a)$  está bem definida, pois:  $a_1 + \text{Ker } \varphi = a_2 + \text{Ker } \varphi \Leftrightarrow a_1 - a_2 \in \text{Ker } \varphi \Leftrightarrow \varphi(a_1 - a_2) = 0 \Leftrightarrow \varphi(a_1) = \varphi(a_2)$ , o que também mostra que  $\tilde{\varphi}$  é injectiva.

A sobrejectividade de  $\tilde{\varphi}$  é óbvia, assim como é imediato verificar que  $\tilde{\varphi}$  é um homomorfismo (de anéis).

*Observação:* Um homomorfismo de anéis  $\varphi : A \rightarrow B$  é injectivo se e só se  $\text{Ker } \varphi = \{0\}$ , pois:  $\varphi(x) = \varphi(y) \Leftrightarrow x - y \in \text{Ker } \varphi \dots$

## 2.5 Polinómios sobre um corpo e DIPs

Seja  $K$  um corpo qualquer.

**Teorema 2.5.1 (da divisão para polinómios)** Dados  $f, g \in K[x]$  com  $g \neq 0$ , existem  $q, r \in K[x]$  tais que  $f = gq + r$  com  $r = 0$  ou  $\text{gr}(r) < \text{gr}(g)$ . Tais polinómios  $q, r$  são únicos.

*Demonstração:* Seja  $S = \{f - gh : h \in K[x]\}$ . Se  $0 \in S$ , então  $f = gh$  para algum  $h \in K[x]$ , e basta pôr  $q = h$  e  $r = 0$ .

Se  $0 \notin S$ , seja  $r$  um dos polinómios de  $S$  com grau mínimo (existe, pois  $\{\text{gr}(p) : p \in S - \{0\}\} \subseteq \mathbb{N} \dots$ ). Suponhamos que se tinha  $\text{gr}(r) \geq \text{gr}(g)$ . Sejam  $r = r_m x^m + r_{m-1} x^{m-1} + \dots$  e  $g = g_n x^n + g_{n-1} x^{n-1} + \dots$ , com  $r_m \neq 0$  e  $g_n \neq 0$  (com  $m, n \in \mathbb{N}$  e, por hipótese,  $m \geq n$ ; observe-se que é aqui que se usa a hipótese:  $g \neq 0$ ); seja  $h \in K[x]$  tal que  $r = f - gh$ . Ter-se-ia então que o polinómio  $s = r - r_m g_n^{-1} x^{m-n} g$  seria tal que  $\text{gr}(s) < \text{gr}(r)$  (porquê?) e  $s = f - gh - r_m g_n^{-1} x^{m-n} g = f - g(h + r_m g_n^{-1} x^{m-n}) \in S$ , contradizendo a escolha de  $r$ . Resulta disto tudo que  $\text{gr}(r) < \text{gr}(g)$ .

Finalmente:  $f = gq + r$  e  $f = gq' + r'$ , com  $r = 0 \vee \text{gr}(r) < \text{gr}(g)$  e  $r' = 0 \vee \text{gr}(r') < \text{gr}(g)$ . Mas, se  $q' \neq q$ , então ter-se-ia

(porquê?)  $\text{gr}(g) \leq \text{gr}(g) + \text{gr}(q - q') = \text{gr}(r - r') < \text{gr}(g)$ , o que é absurdo. Portanto,  $q' = q$  e  $r' = r$ .

**Definição 2.5.2** *Os polinómios  $q$  e  $r$  cuja existência e unicidade são asseguradas pelo resultado anterior chamam-se, respectivamente, o **quociente** e o **resto** da divisão de  $f$  por  $g$ . Diz-se que  $g$  divide  $f$ , o que se denotará por  $g \mid f$ , quando  $r = 0$ .*

*Observação:*  $q$  e  $r$  podem ser calculados por um algoritmo em tudo análogo ao algoritmo usual da divisão de números naturais. Por exemplo (em  $\mathbb{Q}[x]$ ):

$$\begin{array}{r|l} 3x^5 + 2x^2 - 1 & 2x^2 + 1 \\ -3x^5 - \frac{3}{2}x^3 & \frac{3}{2}x^3 - \frac{3}{4}x + 1 \\ \hline -\frac{3}{2}x^3 + 2x^2 - 1 & \\ \frac{3}{2}x^3 + \frac{3}{4}x & \\ \hline 2x^2 + \frac{3}{4}x - 1 & \\ -2x^2 - 1 & \\ \hline \frac{3}{4}x - 2 & \end{array}$$

Assim:  $3x^5 + 2x^2 - 1 = (2x^2 + 1)(\frac{3}{2}x^3 - \frac{3}{4}x - 1) + (\frac{3}{4}x - 2)$ .

*Exercício:* Porque é que isto dá certo?

A resposta ao segundo “porquê?” da prova anterior passa pelo facto de num corpo se ter:  $a \neq 0$  e  $b \neq 0 \Rightarrow ab \neq 0$ , uma vez que  $a \neq 0$  e  $ab = 0 \Rightarrow b = (a^{-1}a)b = a^{-1}(ab) = a0 = 0$ .

**Definição 2.5.3** *Um anel comutativo  $A$  diz-se um **domínio de integridade** se:  $\forall a, b \in A \ ab = 0 \Rightarrow a = 0$  ou  $b = 0$ .*

*Exemplos:*

1.  $\mathbb{Z}_6$  não é um domínio de integridade:  $[2]_6 \cdot [3]_6 = 0$ .
2.  $\mathbb{Z}$  é um domínio de integridade.
3.  $\mathbb{Z}[x]$  é um domínio de integridade.
4.  $A$  domínio de integridade  $\Rightarrow A[x]$  domínio de integridade (porquê?).

*Exercício:* Analise a prova anterior e conclua que o teorema da divisão de polinómios é válido para polinómios  $f$  e  $g$  com coeficientes num domínio de integridade, desde que o coeficiente guia de  $g$  seja invertível.

**Definição 2.5.4** *Seja  $A$  um anel. Um elemento  $\alpha \in A$  diz-se uma **raiz** de  $f \in A[x]$  se o elemento de  $A$  que se obtém substituindo, em  $f$ , o “ $x$ ” por  $\alpha$ , e que é denotado por  $f(\alpha)$ , for 0.*

**Proposição 2.5.5** *Seja  $K$  um corpo,  $f \in K[x]$  e  $\alpha \in K$ . O resto da divisão de  $f(x)$  por  $x - \alpha$  é igual a  $f(\alpha)$ .*

*Demonstração:* Sejam  $q, r \in K[x]$  tais que  $f(x) = q(x)(x - \alpha) + r$ , com  $r = 0$  ou  $\text{gr}(r) < 1$ . Então  $r \in K$  e substituindo  $x$  por  $\alpha$  obtém-se  $f(\alpha) = q(\alpha)0 + r = r$ .

*Exercício:* Seja  $A$  um anel (comutativo) e  $\alpha \in A$ . Mostre que a aplicação  $A[x] \rightarrow A$  dada por  $f \mapsto f(\alpha)$  é um homomorfismo de anéis. Onde é que isto foi usado na prova anterior?

**Corolário 2.5.6** *Seja  $K$  um corpo e  $\alpha \in K$ . Então,  $\alpha$  é raiz de  $f \in K[x]$  se e só se  $x - \alpha \mid f(x)$ .*

**Proposição 2.5.7** *Um polinómio de grau  $n$  sobre um corpo tem no máximo  $n$  raízes nesse corpo.*

*Demonstração:* (indução sobre  $n$ )

Para  $n = 0$  é óbvio.

Suponhamos que a proposição foi já verificada para todos os polinómios de grau  $n$ , para um certo  $n \in \mathbb{N}_0$ , e seja  $f \in K[x]$  com  $\text{gr}(f) = n + 1$ . Se  $f$  não tiver raízes, o resultado verifica-se. Se tiver raízes, seja  $\alpha$  uma dessas raízes. Pelo resultado anterior,  $f = (x - \alpha)g$  para algum  $g \in K[x]$ , com  $\text{gr}(g) = n$  (*porquê?*). Como  $f(\beta) = 0 \Leftrightarrow \beta = \alpha$  ou  $g(\beta) = 0$  (*porquê?*), conclui-se que as raízes de  $f$  são exactamente as raízes de  $g$  e  $\alpha$ . Mas, por hipótese de indução,  $g$  tem no máximo  $n$  raízes, e portanto  $f$  tem no máximo  $n + 1$ , como queríamos concluir.

*Observações:*

1. Este último resultado é válido para domínios de integridade (*porquê?*).
2. O resultado é falso para anéis arbitrários. Por exemplo,  $x^2 - 1$  tem 4 raízes em  $\mathbb{Z}_8$ . Um exemplo surpreendente é dado pelo polinómio  $x^2 + 1 \in \mathbb{H}[x]$ , onde  $\mathbb{H}$  é o anel dos quaterniões (ver exercício #8), que satisfaz todos os axiomas de corpo menos um: a comutatividade da multiplicação. Este polinómio tem pelo menos 6 raízes:  $\pm i, \pm j, \pm k$  (*Exercício:* será que tem mais?). Isto mostra que algures na prova anterior a comutatividade foi usada de uma maneira essencial. *Exercício:* onde?

**Definição 2.5.8** *Dado um anel  $A$ , um seu ideal  $I$  diz-se **principal** se existir algum  $x \in A$  tal que  $I = \langle x \rangle (= Ax = \{ax : a \in A\}$ , ver exemplo 4, p. 15). Um domínio de integridade  $A$  é chamado um **DIP** (de **D**omínio de **I**deais **P**incipais), se todo o seu ideal for principal.*

**Teorema 2.5.9** *Se  $K$  for um corpo, então  $K[x]$  é um DIP.*

*Demonstração:* Seja  $I$  um ideal de  $K[x]$ . Se  $I = \{0\}$ , então  $I = \langle 0 \rangle$ . Se  $I \neq \{0\}$ , seja  $m(x)$  um dos polinômios de  $I - \{0\}$  de grau mínimo. Vamos ver que  $I = \langle m(x) \rangle$ .

É claro que  $\langle m(x) \rangle \subseteq I$  (*porquê?*). Para provar a inclusão oposta, seja  $f(x) \in I$ . Pelo teorema da divisão, existem  $q, r \in K[x]$  tais que  $f = qm + r$  com  $r = 0$  ou  $\text{gr}(r) < \text{gr}(m)$ . Mas então  $r = f - qm \in I$  (*porquê?*), e da minimalidade de  $m(x)$  resulta que  $r = 0$  e portanto  $m(x) \mid f(x)$ , ou seja  $f \in \langle m(x) \rangle$ . Isto mostra que  $I \subseteq \langle m(x) \rangle$ .

Conclui-se assim que todo o ideal de  $K[x]$  é principal.

*Exemplos:*

- $\mathbb{Z}$  é um DIP: a prova é inteiramente análoga à que acaba de ser feita. Aliás, a prova dada em Álgebra I de que os subgrupos de  $\mathbb{Z}$  são exactamente os subconjuntos  $n\mathbb{Z}$ ,  $n \in \mathbb{N}_0$ , resultado que mostra imediatamente que todos os ideais de  $\mathbb{Z}$  são principais, é completamente isomorfa a esta. (Repare que  $n\mathbb{Z} = \langle n \rangle$ ).
- $\mathbb{Z}[x]$  não é um DIP: o ideal  $\langle 2, x \rangle = \{2a(x) + xb(x) : a(x), b(x) \in \mathbb{Z}[x]\} = \{\sum_{i \geq 0} a_i x^i \in \mathbb{Z}[x] : a_0 \text{ é par}\}$  não é principal, pois  $\langle m(x) \rangle = \langle 2, x \rangle \Rightarrow 2 \in \langle m(x) \rangle$  e  $x \in \langle m(x) \rangle \Rightarrow \exists f(x), g(x) \in \mathbb{Z}[x] : 2 = f(x)m(x), x = g(x)m(x) \xrightarrow{\text{(porquê?)}} \text{gr}(m) = 0, m(x) = 1 \Rightarrow \langle 2, x \rangle = \mathbb{Z}[x]$ , o que é falso.

**Definição 2.5.10** *Seja  $A$  um anel. Dados  $a, b \in A$ , diz-se que  $a$  **divide**  $b$  (ou que  $b$  é **múltiplo** de  $a$ ) se existir  $q \in A$  tal que  $b = aq$ .*

*Notação:*  $a \mid b$  significa “ $a$  divide  $b$ ” e  $a \nmid b$  significa “ $a$  não divide  $b$ ”.

**Proposição 2.5.11** *Se  $A$  é um domínio de integridade e  $a, b \in A, a \neq 0$  e  $a \mid b$ , então  $\exists^1 q \in A : b = aq$  (i.e. o quociente é único, em domínios de integridade).*

*Demonstração:*  $b = aq_1$  e  $b = aq_2 \Rightarrow a(q_1 - q_2) = 0 \Rightarrow q_1 = q_2$ , por  $A$  ser um domínio de integridade e  $a \neq 0$ .

*Observação/Exercício:*  $a \mid b \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$ .

**Definição 2.5.12** *Seja  $A$  um anel. Diz-se que  $u$  é uma **unidade** de  $A$  se  $u \mid 1$  ( $\Leftrightarrow \langle u \rangle = A \Leftrightarrow u$  tem inverso (multiplicativo)).*

$A^* := \{u \in A : u \mid 1\}$ .

*Dois elementos  $a, b \in A$  dizem-se **associados** se  $a \mid b$  e  $b \mid a$ , o que é equivalente a se verificar:  $\langle a \rangle = \langle b \rangle$ .*

*Observação/Exercício:*  $u \in A^* \Leftrightarrow \forall a \in A \ u \mid a$ , ou seja, as unidades são os elementos de um anel que dividem todos os outros.

*Exemplos:*

1.  $\mathbb{Z}^* = \{-1, 1\}$ .
2.  $K$  corpo  $\Leftrightarrow K$  anel (comutativo) e  $K^* = K - \{0\}$ .
3.  $\mathbb{Z}_n^* = \{[a]_n : (a, n) = 1\}$ .
4.  $K[x]^* = K^*$ , para todo o corpo  $K$  (*Exercício:*  $A[x]^* = A^*$ , para todo o domínio de integridade  $A$ ).
5.  $m$  e  $-m$  são associados,  $\forall m \in \mathbb{Z}$ .

*Exercício:* No anel dos inteiros Gaussianos:  $\mathbb{Z}[i]^* = \{-1, 1, -i, i\}$ ;  $1+i \mid 2$ ;  $1+i$  e  $1-i$  são associados.

*Observação:* Num anel de integridade  $A$ , dois elementos  $a, b \in A$  são associados se e só se  $\exists u \in A^* : b = ua$  ( $\Leftrightarrow \exists v \in A^* : a = vb$ )

*Razão:*  $a \mid b$  e  $b \mid a \Leftrightarrow \exists u, v \in A : b = au$  e  $a = bv \Rightarrow b = bvu \Rightarrow$  (se  $b \neq 0$ )  $1 = vu \Rightarrow u, v \in A^*$ ; se  $b = 0$ , então  $a = 0$  e o resultado é obviamente verdadeiro. O recíproco é fácil.

**Definição 2.5.13** *Seja  $A$  um anel;  $a, b \in A$ . Um elemento  $d \in A$  diz-se um máximo divisor comum de  $a$  e  $b$  se:*

- i)  $d \mid a$  e  $d \mid b$  (i.e.  $d$  é um divisor comum de  $a$  e  $b$ );
- ii)  $c \mid a$  e  $c \mid b \Rightarrow c \mid d$ .

*Exemplo:*  $-3$  é um m.d.c. de 6 e 9.

*Observações:*

1. Dois máximos divisores comuns são associados (*justifique!*).
2. Existem anéis onde há elementos que não têm nenhum máximo divisor comum (mas é difícil dar um exemplo...).

*Observação/Exercício:* Em termos de ideais,  $d$  é um máximo divisor comum de  $a$  e  $b$  se:

- i)  $\langle a, b \rangle \subseteq \langle d \rangle$ ;

- ii)  $\langle a, b \rangle \subseteq \langle c \rangle \Rightarrow \langle d \rangle \subseteq \langle c \rangle$  (ou seja,  $\langle d \rangle$  é o menor (para a inclusão) ideal principal de  $A$  que contém o ideal  $\langle a, b \rangle$ ).

Resulta imediatamente que:

**Proposição 2.5.14** *Num DIP dois quaisquer elementos têm um máximo divisor comum, e qualquer máximo divisor comum de dois elementos se pode escrever como combinação linear desses elementos.*

*Demonstração:* Se  $A$  é um DIP e  $a, b \in A$ , então  $\langle a, b \rangle = \langle d \rangle$  para algum  $d \in A$ . Da observação anterior resulta imediatamente que  $d$  é um máximo divisor comum de  $a$  e  $b$ . O resto fica como exercício.

**Corolário 2.5.15** *Sejam  $f(x)$  e  $g(x)$  dois polinômios com coeficientes num corpo  $K$ . Então existem máximos divisores comuns de  $f(x)$  e  $g(x)$ . Se  $d(x)$  é um deles, então  $d(x) = a(x)f(x) + b(x)g(x)$  para alguns  $a(x), b(x) \in K[x]$  e os máximos divisores comuns de  $f(x)$  e  $g(x)$  são exactamente os polinômios  $\lambda d(x)$ ,  $\lambda \in K^*$ .*

*Observação:* Dados dois polinômios  $f, g \in K[x]$ ,  $K$  corpo, é usual chamar ao único m.d.c. de  $f$  e  $g$  que é *mónico*, o máximo divisor comum de  $f$  e  $g$ .

O m.d.c. de dois polinômios pode ser calculado, e expresso como combinação linear desses polinômios, por um processo inteiramente análogo ao de fazer o mesmo para inteiros:

**Algoritmo de Euclides:** *Seja  $K$  um corpo;  $f, g \in K[x]$ . Usando o algoritmo da divisão, obtêm-se  $r_1, r_2, r_3, \dots$ , satisfazendo:*

$$\begin{array}{rcll} f & = & gq_1 + r_1 & \text{com } \text{gr}(r_1) < \text{gr}(g) \\ g & = & r_1q_2 + r_2 & \text{com } \text{gr}(r_2) < \text{gr}(r_1) \\ r_1 & = & r_2q_3 + r_3 & \text{com } \text{gr}(r_3) < \text{gr}(r_2) \\ & \vdots & & \vdots \\ r_{n-2} & = & r_{n-1}q_n + r_n & \text{com } \text{gr}(r_n) < \text{gr}(r_{n-1}) \\ & \vdots & & \vdots \end{array} \quad (\dagger)$$

Como  $\text{gr}(g) > \text{gr}(r_1) > \text{gr}(r_2) > \dots$  é uma sequência de números inteiros não negativos enquanto  $r_i \neq 0$ , tem-se que  $\exists m \in \mathbb{N}_0 : r_{m+1} = 0$ . Então  $r_m$  é um m.d.c. de  $f$  e  $g$  (faça-se  $r_0 := g \dots$ ), e eliminando  $r_{m-1}, r_{m-2}, \dots$  das equações anteriores, obtêm-se  $r_m$  como combinação linear de  $f$  e  $g$ .

*Demonstração:* Procedendo da equação  $r_{m-2} = r_{m-1}q_m + r_m$  e ‘subindo’  $(\dagger)$  até à primeira, vê-se sucessivamente que:  $r_m \mid r_{m-1}, r_m \mid r_{m-2}, \dots, r_m \mid r_2, r_m \mid r_1, r_m \mid g, r_m \mid f$ . Logo,  $r_m$  é um divisor comum de  $f$  e  $g$ . Por outro lado, se  $c$  é um divisor comum de  $f$  e  $g$ , então, ‘descendo’ agora  $(\dagger)$ , vê-se que,

sucessivamente:  $c \mid r_1, c \mid r_2, \dots, c \mid r_m$ . Isto mostra que  $r_m$  é um m.d.c. de  $f$  e  $g$ .

Finalmente:

$$\left. \begin{array}{l} r_m = r_{m-2} - r_{m-1}q_m \\ r_{m-1} = r_{m-3} - r_{m-2}q_{m-1} \end{array} \right\} \Rightarrow \left( \begin{array}{l} \text{eliminando} \\ r_{m-1} \text{ da } 1^{\text{a}}, \\ \text{usando a } 2^{\text{a}} \end{array} \right) \Rightarrow r_m = \boxed{?}r_{m-3} + \boxed{?}r_{m-2}. \text{ Em}$$

seguida,  $\left. \begin{array}{l} r_m = \boxed{?}r_{m-3} + \boxed{?}r_{m-2} \\ r_{m-2} = r_{m-4} - r_{m-3}q_{m-2} \end{array} \right\} \xrightarrow{\text{(analogamente)}} r_m = \boxed{?}r_{m-4} + \boxed{?}r_{m-3} \dots \text{ etc.}$

... até que se obtém  $r_m = \boxed{?}f + \boxed{?}g$ .

*Exemplo:*  $f = x^5, g = x^2 + 1$  (Qual a diferença se tomar  $g = x^2 + 1, f = x^5$  ?)

$$\begin{array}{l} x^5 = (x^2 + 1) \cdot (x^3 - x) + x \\ x^2 + 1 = x \cdot x + 1 \\ x = x \cdot 1 + 0 \end{array} \quad \searrow \quad \begin{array}{l} 1 = (x^2 + 1) - x \cdot x = \\ = (x^2 + 1) - x \cdot (x^5 - (x^2 + 1) \cdot (x^3 - x)) = \\ = (x^2 + 1) \cdot (1 + x^4 - x^2) - x \cdot x^5. \end{array}$$

Resulta que 1 é um dos m.d.c. de  $x^5$  e  $x^2 + 1$ , e que  $a(x) = -x, b(x) = x^4 - x^2 + 1$  é uma solução de  $1 = a(x)x^5 + b(x)(x^2 + 1)$ .

**Definição 2.5.16** *Dois elementos  $a$  e  $b$  de um anel  $A$  dizem-se primos entre si se 1 for um dos m.d.c. de  $a$  e  $b$ .*

*Observação:* Se  $A$  for um DIP, então  $a, b \in A$  são primos entre si se e só se  $\langle a, b \rangle = \langle 1 \rangle (= A)$ .

*Exemplo:* Acabou de se ver que os polinómios  $x^5$  e  $x^2 + 1$  são primos entre si no anel  $\mathbb{Q}[x]$  (e também em  $\mathbb{R}[x]$ , e em  $\mathbb{C}[x]$ ...).

**Definição 2.5.17** *Seja  $A$  um anel. Um elemento  $a \in A - (A^* \cup \{0\})$  diz-se:*

- i) **irredutível** se:  $a = xy \Rightarrow x \in A^* \text{ ou } y \in A^*$ .
- ii) **primo** se:  $a \mid bc \Rightarrow a \mid b \text{ ou } a \mid c$ .

*Exemplo:* Seja  $A = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$ .

2 é irredutível em  $\mathbb{Z}[\sqrt{-5}]$ :  $2 = (a + b\sqrt{5}i)(c + d\sqrt{5}i) \xrightarrow{\text{(porquê?)}} 4 = (a^2 + 5b^2)(c^2 + 5d^2) \Rightarrow$  (sem perda de generalidade)  $a^2 = 4, c^2 = 1, b = d = 0 \Rightarrow c + d\sqrt{5}i = \pm 1 \in A^*$ .

2 não é primo em  $\mathbb{Z}[\sqrt{-5}]$ :  $2 \mid (1 + \sqrt{5}i)(1 - \sqrt{5}i) = 6$ , mas  $2 \nmid (1 + \sqrt{5}i)$  e  $2 \nmid (1 - \sqrt{5}i)$  (porquê?).

**Proposição 2.5.18** *Num domínio de integridade todos os primos são irredutíveis.*

*Demonstração:* Seja  $A$  um domínio de integridade e  $a \in A - (A^* \cup \{0\})$  um primo. Então:  $a = xy$  ( $x, y \in A$ )  $\Rightarrow$  (sem perda de generalidade)  $a \mid x \Rightarrow \exists z \in A : x = az$ . Donde resulta  $a = azy$ , e portanto  $a(1 - zy) = 0$ . Como  $a \neq 0$  e  $A$  é um domínio de integridade, conclui-se que  $1 = zy$ , o que mostra que  $y \in A^*$ . Isto prova que  $a$  é irredutível.

**Teorema 2.5.19** *Num DIP os irredutíveis são primos.*

*Demonstração:* Vamos começar por provar duas proposições auxiliares que vale a pena evidenciar.

**Lema 2.5.20** *Num anel qualquer, tem-se:*

*$a$  irredutível,  $d \mid a \Rightarrow \langle d \rangle = \langle 1 \rangle$  ou  $\langle d \rangle = \langle a \rangle$ .*

*Razão:*  $d \mid a \Rightarrow \exists q : a = dq \Rightarrow d \in A^*$  ou  $q \in A^* \Rightarrow \langle d \rangle = \langle 1 \rangle$  ou  $\langle d \rangle = \langle a \rangle$ , respectivamente.

**Lema 2.5.21** *Num anel qualquer, tem-se:  $a \mid bc$  e  $\langle a, b \rangle = 1 \Rightarrow a \mid c$ .*

*Razão:* Seja  $q$  tal que  $bc = aq$ . Então:  $\langle a, b \rangle = 1 \Rightarrow \exists x, y \in A : 1 = ax + by \Rightarrow c = acx + bcy = acx + aqy = a(cx + qy) \Rightarrow a \mid c$ .

*Prova do teorema:* Seja  $A$  um DIP e  $a \in A$  um irredutível. Sejam  $b, c \in A$  tais que  $a \mid bc$  e seja  $d \in A$  tal que  $\langle a, b \rangle = \langle d \rangle$ . Pelo primeiro dos lemas anteriores, resulta que  $\langle d \rangle = \langle 1 \rangle$  ou  $\langle d \rangle = \langle a \rangle$ , o que implica  $\langle a, b \rangle = \langle 1 \rangle$  ou  $a \mid b$ . Usando o segundo lema, conclui-se que  $a \mid c$  ou  $a \mid b$ .

*Observação:*

1. Em particular, se  $K$  for um corpo, então um polinómio  $f \in K[x]$  é primo se e só se for irredutível.
2. Resulta do que se viu que  $\mathbb{Z}[\sqrt{-5}]$  não é um DIP, o que pode ser verificado directamente mostrando que, por exemplo, o ideal  $\langle 2, 1 + \sqrt{5}i \rangle$  não é principal (*exercício!*).

Vamos agora ver que todo o elemento de um DIP se pode escrever como um produto de irredutíveis (= primos) e que esses irredutíveis são únicos, a menos de unidades.

**Lema 2.5.22 ( E. Noether)** *Seja  $A$  um DIP e  $a_1, a_2, a_3, \dots \in A$  tais que  $\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \langle a_3 \rangle \subseteq \dots$  é uma cadeia ascendente de ideais de  $A$ . Então  $\exists n \in \mathbb{N} \forall t \in \mathbb{N} \langle a_n \rangle = \langle a_{n+t} \rangle$ . Noutras palavras, a cadeia é “estacionária”.*

*Demonstração:* Seja  $I = \bigcup_{i \in \mathbb{N}} \langle a_i \rangle$ .  $I$  é um ideal de  $A$ , pois:  $x, y \in I \Rightarrow \exists i, j \in \mathbb{N} : x \in \langle a_i \rangle, y \in \langle a_j \rangle$ , e tomando  $k = \max\{i, j\}$  têm-se  $x, y \in \langle a_k \rangle$ , donde  $x - y \in \langle a_k \rangle \subseteq I$ ;  $a \in A, x \in I \Rightarrow a \in A, x \in \langle a_i \rangle$ , para algum  $i \in \mathbb{N} \Rightarrow ax \in \langle a_i \rangle \subseteq I$ .

Como  $A$  é um DIP,  $\exists a \in A : I = \langle a \rangle$ . Mas então  $a \in \langle a_n \rangle$ , para algum  $n \in \mathbb{N}$ , e portanto  $I = \langle a \rangle \subseteq \langle a_n \rangle$ , o que implica  $\langle a_{n+t} \rangle \subseteq \langle a_n \rangle \forall t \in \mathbb{N}$ .

**Proposição 2.5.23** *Seja  $A$  um DIP. Então, todo o elemento de  $A - (A^* \cup \{0\})$  pode ser escrito como um produto de irredutíveis.*

*Demonstração:* Seja  $a \in A - (A^* \cup \{0\})$ .

Vejamos em primeiro lugar que  $a$  é divisível por algum irredutível. Se  $a$  for irredutível, é imediato. Caso contrário,  $a = a_1 b_1$  para alguns  $a_1, b_1 \in A - (A^* \cup \{0\})$  (porquê?). Se  $a_1$  for irredutível, temos o que queríamos. Senão,  $a = a_2 b_2$  para alguns  $a_2, b_2 \in A - (A^* \cup \{0\})$ . Se  $a_2$  for irredutível...etc...

Observando que  $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \dots^2$  enquanto os  $a_i$  não forem irredutíveis (porquê?), conclui-se do lema de E. Noether que este processo termina num número finito de etapas. Logo,  $a_k$  é irredutível para algum  $k \in \mathbb{N}$ .

Vejamos agora que  $a$  é igual a um produto de irredutíveis. Se  $a$  for irredutível, é imediato. Caso contrário, seja  $p_1$  um irredutível que divide  $a$ . Então  $a = p_1 a_1$ , para algum  $a_1 \in A - (A^* \cup \{0\})$  (porquê?). Se  $a_1$  for irredutível, então temos o que queríamos. Senão, seja  $p_2$  um irredutível tal que  $p_2 \mid a_1$ . Então  $a_1 = p_2 a_2$ , para algum  $a_2 \in A - (A^* \cup \{0\})$ ...etc... Obtém-se assim uma cadeia  $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \dots$ , enquanto os  $a_i$  não forem irredutíveis. Novamente pelo lema de E. Noether, conclui-se que o processo indicado termina após de um número finito de etapas, o que significa que eventualmente  $a_n$  é irredutível, ficando nessa altura  $a$  decomposto num produto de irredutíveis.

**Lema 2.5.24** *Seja  $A$  um DIP,  $p \in A$  um primo e  $a \in A - \{0\}$ . Então,  $\exists n \in \mathbb{N}_0$  tal que  $p^n \mid a$  e  $p^{n+1} \nmid a$ .*

*Demonstração:* Se o resultado fosse falso, então para todo o  $m \in \mathbb{N}$  existiria  $b_m \in A - \{0\}$  tal que  $a = p^m b_m$ . Portanto,  $p b_{m+1} = b_m$  (porquê?)  $\forall m \in \mathbb{N}$ , o que implicaria  $\langle b_1 \rangle \subset \langle b_2 \rangle \subset \langle b_3 \rangle \subset \dots$ , contradizendo o lema de E. Noether.

**Definição 2.5.25**  $\text{ord}_p(a) = \max\{n \in \mathbb{N}_0 : p^n \mid a\}$  (cuja existência é garantida pelo lema anterior).

*Exercício:*

- i)  $p$  primo,  $u \in A^* \Rightarrow \text{ord}_p(u) = 0$ .

<sup>2</sup>Nestas notas usamos o símbolo  $\subset$  para significar “contido, mas distinto de”.

ii)  $p, q$  primos não-associados  $\Rightarrow \text{ord}_p(q) = 0$ .

**Lema 2.5.26** *Seja  $A$  um DIP;  $a, b \in A - \{0\}$ . Tem-se que  $\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b)$ .*

*Demonstração:* Sejam  $\alpha = \text{ord}_p(a), \beta = \text{ord}_p(b)$ . Então  $a = p^\alpha c, b = p^\beta d$  com  $p \nmid c$  e  $p \nmid d$ . Portanto  $ab = p^{\alpha+\beta} cd$  e, como  $p$  é primo,  $p \nmid cd$ . Consequentemente,  $\text{ord}_p(ab) = \alpha + \beta$ .

Estamos finalmente em condições de enunciar e provar o teorema da unicidade da decomposição em primos num DIP.

Seja  $A$  um DIP e  $\mathcal{P}$  um conjunto de primos (= irreduzíveis, neste caso) de  $A$  tal que:

- i) todo o primo de  $A$  é associado a algum primo de  $\mathcal{P}$ ;
- ii) nenhum primo de  $\mathcal{P}$  é associado a um outro primo de  $\mathcal{P}$ .

Para obter um tal conjunto  $\mathcal{P}$  basta escolher um elemento de cada classe de primos associados (a relação “associado a” é uma relação de equivalência...). Há obviamente uma grande dose de arbitrariedade nesta escolha. Em  $\mathbb{Z}$  e em  $K[x]$ ,  $K$  corpo, há escolhas naturais: em  $\mathbb{Z}$  é usual escolher  $\mathcal{P} = \{\text{primos positivos}\}$ ; em  $K[x]$  é usual tomar  $\mathcal{P} = \{\text{polinômios mônicos irreduzíveis}\}$ . Mas, em geral não há nenhuma maneira natural de fazer essa escolha...

**Teorema 2.5.27** *Seja  $A$  um DIP e  $\mathcal{P}$  um conjunto de primos com as propriedades atrás mencionadas. Então, todo o elemento  $a \in A - \{0\}$  pode ser escrito na forma:*

$$a = u \prod_{p \in \mathcal{P}} p^{e_p} \quad (e_p \in \mathbb{N}_0), \quad (\bullet)$$

com  $u \in A^*$  e  $e_p \neq 0$  apenas para um número finito de primos  $p$ .

A unidade  $u$  e os expoentes  $e_p$  são unicamente determinados por  $a$ . De facto,  $e_p = \text{ord}_p(a)$ .

*Demonstração:* Pela Prop. 2.5.23, p. 24, tem-se que  $a = a_1 a_2 \cdots a_n$  para alguns  $a_i$  irreduzíveis. Agora, para cada  $i = 1, \dots, n$ ,  $a_i = u_i p_i$  para alguns  $u_i \in A^*$  e  $p_i \in \mathcal{P}$  (*porquê?*). Mas então  $a = u_1 u_2 \cdots u_n p_1 p_2 \cdots p_n$  e como o produto de unidades é uma unidade (*porquê?*) (tem-se um pouco mais:  $(A^*, \cdot)$  é um grupo), fica provada a existência da decomposição  $(\bullet)$ .

Para provar a unicidade, seja  $q \in \mathcal{P}$  e aplique o lema anterior a uma decomposição de  $a$  da forma  $(\bullet)$ . Obtém-se:  $\text{ord}_q(a) = \text{ord}_q(u) + \sum_{p \in \mathcal{P}} e_p \text{ord}_q(p) = e_q$  (*porquê?*). Finalmente, como os expoentes  $e_p$  são unicamente determinados por  $a$ , resulta que  $u$  também o é.

**Corolário 2.5.28** *Todo o número inteiro não-nulo se pode escrever de modo único na forma<sup>3</sup>:*

$$\epsilon \prod_{\substack{p \text{ primo} \\ \text{positivo}}} p^{e_p}, \text{ com } \epsilon \in \{-1, 1\}, e_p \in \mathbb{N}_0, \text{ quase todos nulos.}$$

*Todo o polinómio não-nulo de  $K[x]$ ,  $K$  corpo, se pode escrever de uma só maneira na forma:*

$$\lambda \prod_{\substack{f(x) \text{ irredutível} \\ \text{mónico}}} f(x)^{e_f}, \text{ com } \lambda \in K^*, e_f \in \mathbb{N}_0, \text{ quase todos nulos.}$$

*Observações:*

1. Um domínio de integridade no qual todo o elemento se pode escrever como um produto de irredutíveis de um só maneira, *a menos de unidades* (i.e. tal que existe um conjunto de irredutíveis que satisfaz o resultado descrito no teorema anterior), diz-se um **DFU** (de **D**omínio de **F**actorização **Ú**nica). Ficou visto que todo o DIP é um DFU. O recíproco é falso: por exemplo,  $\mathbb{R}[x, y]$  não é um DIP (*fácil...*) mas é um DFU (*menos fácil...*).
2. Outros exemplos de DIPs são (ver exercício # 31):  $\mathbb{Z}[i]$  (ver próxima secção),  $\mathbb{Z}[\sqrt{2}]$ ,  $\mathbb{Z}[\sqrt{-2}]$  (o que permite resolver a equação  $y^3 = x^2 + 2$  em números inteiros, como foi esboçado na introdução, ver p. 7),  $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ .  
[**NOTA:**  $\mathbb{Z}[\alpha]$  denota o menor subanel de  $\mathbb{C}$  que contém  $\mathbb{Z}$  e  $\alpha$  (ver exercício # 17).]
3.  $\mathbb{Z}[\sqrt{-5}]$  e  $\mathbb{Z}[\sqrt{10}]$  não são DFUs (em  $\mathbb{Z}[\sqrt{10}]$  tem-se:  $3 \cdot 3 = (\sqrt{10} + 1)(\sqrt{10} - 1)$  e  $3, \sqrt{10} + 1, \sqrt{10} - 1$  são não-associados (*verifique-o!*).  
Outro exemplo é  $\mathbb{Z}[\sqrt{-23}]$ , onde  $3 \cdot 3 \cdot 3 = (2 + \sqrt{-23})(2 - \sqrt{-23})$  são duas decomposições em irredutíveis em que nem sequer o número destes é o mesmo!

## 2.6 A aritmética de $\mathbb{Z}[i]$

A aplicação

$$\begin{aligned} N : \quad \mathbb{Z}[i] &\longrightarrow \mathbb{N}_0 \\ z = x + yi &\longmapsto z\bar{z} = x^2 + y^2 \end{aligned}$$

desempenha um papel essencial no estudo da aritmética do anel dos inteiros Gausianos, ou seja, na determinação das suas unidades e dos seus primos, essencialmente por se ter:  $N(wz) = N(w)N(z) \forall w, z \in \mathbb{Z}[i]$  (*porquê?*).

<sup>3</sup>“Quase todos nulos” é uma expressão do calão matemático usual que significa “todos, menos um número finito”.

Começemos por mostrar que, usando a aplicação  $N$  para “medir” inteiros de Gauss, se tem um análogo do teorema da divisão para inteiros:

**Afirmção:**  $\forall a \in \mathbb{Z}[i], b \in \mathbb{Z}[i] - \{0\} \exists q, r \in \mathbb{Z}[i] : a = bq + r$  e  $N(r) < N(b)$ .

*Demonstração:* Tem-se:  $\frac{a}{b} = \frac{a\bar{b}}{N(b)} = \frac{Re(a\bar{b})}{N(b)} + \frac{Im(a\bar{b})}{N(b)}i$ , o que mostra que  $\frac{a}{b} = x_1 + x_2i$ , para alguns  $x_1, x_2 \in \mathbb{Q}$ . Sejam  $q_1, q_2 \in \mathbb{Z}$  ‘os’ inteiros mais perto de  $x_1, x_2$ , respectivamente (se houver ambiguidade, o que acontece se um dos  $q_i$  pertencer a  $\frac{1}{2} + \mathbb{Z}$ , escolha-se um qualquer...) Então  $\frac{a}{b} = (q_1 + q_2i) + (\epsilon_1 + \epsilon_2i)$ , com  $|\epsilon_1| \leq \frac{1}{2}$  e  $|\epsilon_2| \leq \frac{1}{2}$ . Faça-se  $q := q_1 + q_2i$ ,  $\epsilon := \epsilon_1 + \epsilon_2i$  e  $r := \epsilon b$ . Resulta que:  $r = a - bq \in \mathbb{Z}[i]$  e  $N(r) = N(\epsilon)N(b) = (\epsilon_1^2 + \epsilon_2^2)N(b) \leq \frac{1}{2}N(b) < N(b)$  (*porquê?*).

**Afirmção:**  $\mathbb{Z}[i]$  é um DIP.

*Demonstração:* Seja  $I \neq \{0\}$  um ideal de  $\mathbb{Z}[i]$  e escolha-se  $z \in I$  tal que  $N(z) = \min\{N(x) : x \in I - \{0\}\}$ . É claro que  $\langle z \rangle \subseteq I$ . Reciprocamente, se  $w \in I$ , resulta do que foi atrás visto que existem  $q, r \in \mathbb{Z}[i]$  com  $w = zq + r$  e  $N(r) < N(z)$ . Mas:  $r = w - zq \in I$  e  $N(r) < N(z) \Rightarrow r = 0$ , pela escolha de  $z$ . Donde se conclui que  $w \in \langle z \rangle$ . Por conseguinte,  $I = \langle z \rangle$ .

*Observação:* Repare na semelhança entre esta prova, a de que  $\mathbb{Z}$  é um DIP e a de que  $K[x]$  é um DIP sempre que  $K$  for um corpo.

**Afirmção:**  $u \in \mathbb{Z}[i]^* \Leftrightarrow N(u) = 1$

*Demonstração:*  $(\Rightarrow) u \in \mathbb{Z}[i]^* \Rightarrow \exists v \in \mathbb{Z}[i] : uv = 1 \Rightarrow N(u)N(v) = N(1) = 1 \xrightarrow{\text{porquê?}} N(u) = 1$ .

$(\Leftarrow) N(u) = 1 \Rightarrow 1 = u\bar{u} \Rightarrow u \in \mathbb{Z}[i]^*$ .

Por conseguinte,  $u = x+yi \in \mathbb{Z}[i]^* \Leftrightarrow x^2+y^2 = 1 \Leftrightarrow \begin{cases} x=\pm 1 \\ y=0 \end{cases}$  ou  $\begin{cases} x=0 \\ y=\pm 1 \end{cases} \Leftrightarrow u = \pm 1$  ou  $u = \pm i$ .

Assim:  $\mathbb{Z}[i]^* = \{-1, 1, -i, i\}$ .

**Afirmção:** Seja  $\pi \in \mathbb{Z}[i]$ . Então:  $N(\pi)$  primo de  $\mathbb{Z} \Rightarrow \pi$  primo de  $\mathbb{Z}[i]$ .

*Demonstração:* Como  $\mathbb{Z}[i]$  é um DIP, se  $\pi$  não for primo, então é redutível e portanto  $\pi = ab$ , para alguns  $a, b \in \mathbb{Z}[i] - (\mathbb{Z}[i]^* \cup \{0\})$ . Mas então:  $N(\pi) = N(a)N(b)$  e, pelo que acima se viu,  $N(a) > 1$  e  $N(b) > 1$ , o que mostra que  $N(\pi)$  é um número composto.

Finalmente, observe-se que todo o primo  $\pi$  de  $\mathbb{Z}[i]$  divide algum primo de  $\mathbb{Z}$ , pois  $\pi$  divide  $N(\pi)$  (*porquê?*), que é um inteiro e portanto um produto de primos de  $\mathbb{Z}$ ; como  $\pi$  é primo (em  $\mathbb{Z}[i]$ ), divide algum dos primos deste produto. Assim, para determinar os primos de  $\mathbb{Z}[i]$  basta factorizar, em  $\mathbb{Z}[i]$ , os primos de  $\mathbb{Z}$ . O esquema seguinte mostra os primos (não-associados) de  $\mathbb{Z}[i]$  que provêm da factorização dos primeiros 8 primos positivos de  $\mathbb{Z}$ .

$1+i$	$3$	$2+i$	$2-i$	$7$	$11$	$3+2i$	$3-2i$	$4+i$	$4-i$	$19$	$\dots$
↑	↑	↘	↗	↑	↑	↘	↗	↘	↗	↑	$\dots$
2	3		5	7	11		13		17	19	$\dots$

*Observação/Exercício:* Seja  $p \in \mathbb{N}$  um primo em  $\mathbb{Z}$ . É agora fácil ver que  $p$  é primo em  $\mathbb{Z}[i]$  se e só se  $p$  não é soma de dois quadrados. Se  $p = a^2 + b^2$ , então  $a + bi$  e  $a - bi$  são dois primos não-associados quando  $p \neq 2$ .

# Capítulo 3

## Polinómios Irredutíveis

### 3.1 $\mathbb{Q}[x]$ e $\mathbb{Z}[x]$

Factorizar polinómios é um pouco mais complicado do que factorizar números inteiros, não sendo sequer óbvio como proceder de um modo minimamente eficiente. Não descreveremos aqui nenhum algoritmo de factorização de polinómios<sup>1</sup>, limitando-nos a apresentar alguns critérios de irredutibilidade, em especial para polinómios com coeficientes racionais e inteiros.

Vamos começar por ver que a factorização de polinómios em  $\mathbb{Q}[x]$  pode ser reduzida à factorização em  $\mathbb{Z}[x]$ . Para tal começamos por introduzir o seguinte conceito:

**Definição 3.1.1** *Um polinómio de coeficientes inteiros diz-se **primitivo** se o máximo divisor comum dos seus coeficientes for 1*

*Exemplos:*

1.  $9x^5 + 6x^2 - 10$  é primitivo.
2.  $14x^7 - 21x^3 + 35$  não é primitivo.
3.  $18x^4 - 12x + 6$  não é primitivo.

*Observação:* Se um polinómio de  $\mathbb{Z}[x]$  não for primitivo, então existe um primo  $p$  que divide todos os seus coeficientes (*porquê?*). É claro que um polinómio não-constante que não seja primitivo é redutível em  $\mathbb{Z}[x]$  (*porquê?*).

**Proposição 3.1.2 (“Lema de Gauss”)** *O produto de dois polinómios primitivos é ainda um polinómio primitivo.*

---

<sup>1</sup>Ver: K. Geddes, S. Czapor, G. Labahn, *Algorithms for Computer Algebra*, Kluwer, 1992; H. Cohen *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.

*Demonstração:* Sejam  $f(x) = \sum_{i \geq 0} a_i x^i$  e  $g(x) = \sum_{i \geq 0} b_i x^i$  dois polinômios primitivos e seja  $p$  um primo. Como  $f(x)$  e  $g(x)$  são primitivos, ambos têm coeficientes que não são divisíveis por  $p$ . Sejam  $a_r$  e  $b_s$  os primeiros coeficientes de  $f$  e  $g$ , respectivamente, que não são divisíveis por  $p$ . Como

$$c_{r+s} = (a_0 b_{r+s} + a_1 b_{r+s-1} + \dots + a_{r-1} b_{s+1}) + a_r b_s + (a_{r+1} b_{s-1} + \dots + a_{r+s-1} b_1 + a_{r+s} b_0);$$

$p \mid a_i$  para todo  $i = 0, 1, \dots, r-1$  e  $p \mid b_j$  para todo  $j = 0, 1, \dots, s-1$ , conclui-se que  $p \nmid c_{r+s}$ .

Assim, para todo o primo  $p$ , existe um coeficiente de  $f(x)g(x)$  que não é divisível por  $p$ . Isto prova o que se queria.

**Lema 3.1.3** *Todo o polinômio não-nulo  $f(x) \in \mathbb{Q}[x]$  tem uma única decomposição da forma  $f(x) = c(f)f^*(x)$  com  $c(f) \in \mathbb{Q}^+$  e  $f^*(x) \in \mathbb{Z}[x]$  primitivo.*

*Demonstração:* Seja  $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \frac{a_2}{b_2}x^2 + \dots + \frac{a_n}{b_n}x^n$ , com  $a_i, b_i \in \mathbb{Z}$  ( $\forall i = 0, 1, \dots, n$ ). Tem-se:  $f(x) = \frac{1}{b_0 b_1 \dots b_n} g(x)$ , com  $g(x) \in \mathbb{Z}[x]$  (*porquê?*). Fazendo  $d := \pm$  m.d.c. dos coeficientes de  $g(x)$ , onde o sinal é escolhido de modo a que  $\frac{d}{b_0 b_1 \dots b_n}$  seja positivo, resulta que  $f(x) = \frac{d}{b_0 b_1 \dots b_n} (\frac{1}{d} g(x))$  é uma decomposição com a forma requerida, uma vez que  $\frac{1}{d} g(x)$  é um polinômio primitivo (*porquê?*).

Para provar a unicidade, sejam  $a, b \in \mathbb{Q}^+$  e  $g(x), h(x) \in \mathbb{Z}[x]$  primitivos tais que  $f(x) = ag(x)$  e  $f(x) = bh(x)$ . Resulta daqui que  $g(x) = \frac{b}{a}h(x)$ . Escrevendo  $\frac{b}{a} = \frac{u}{v}$ , com  $u, v \in \mathbb{Z}$ ,  $(u, v) = 1$ , tem-se que  $vg(x) = uh(x)$ . Mas como  $v$  é o m.d.c. dos coeficientes de  $vg(x)$  (*porquê?*) e  $u$  é o m.d.c. dos coeficientes de  $uh(x)$ , conclui-se que  $u = v$  e, por conseguinte, também  $g(x) = h(x)$ .

**Definição 3.1.4** *Ao número racional positivo  $c(f)$ , cuja existência e unicidade acaba de ser provada, chama-se o **conteúdo** de  $f$ .*

*Observação:* O polinômio  $f^*$ , cuja existência e unicidade é provada no lema anterior, é o único polinômio primitivo que é associado a  $f$ .

*Exemplo:*  $f(x) = \frac{9}{2}x^3 + \frac{15}{4}x + 21 = \frac{3}{4}(6x^3 + 5x + 28)$  e  $m.d.c.(6, 5, 28) = 1 \xrightarrow{\text{(porquê?)}}$   
 $c(f) = \frac{3}{4}$ ,  $f^*(x) = 6x^3 + 5x + 28$ .

**Lema 3.1.5** *Dados  $f, g \in \mathbb{Q}[x]$ ,  $c(f \cdot g) = c(f)c(g)$  e  $(f \cdot g)^* = f^* \cdot g^*$ .*

*Demonstração:*  $f(x)g(x) = c(f)f^*c(g)g^* = c(f)c(g)f^*g^*$ . Como  $c(f)c(g)$  é um número racional positivo e, pelo lema de Gauss,  $f^*g^*$  é primitivo, o que queremos provar resulta imediatamente da unicidade descrita no lema anterior.

*Observação/Exercício:*  $f \in \mathbb{Z}[x] \Rightarrow c(f) \in \mathbb{Z}$ .

**Teorema 3.1.6** *Se  $f \in \mathbb{Z}[x]$  for um polinómio não-constante e irredutível em  $\mathbb{Z}[x]$ , então também o é em  $\mathbb{Q}[x]$ .*

*Demonstração:* Suponhamos que  $f$  era redutível em  $\mathbb{Q}[x]$ . Existiriam então dois polinómios  $g, h \in \mathbb{Q}[x] - \mathbb{Q}[x]^*$  tais que  $f = gh$ . Ter-se-ia  $f = c(g)c(h)g^*h^*$ . Pelo lema e observação anteriores,  $c(g)c(h) = c(f) \in \mathbb{Z}$ . Mas então  $f = (c(g)c(h)g^*) \cdot h^*$  seria uma factorização em  $\mathbb{Z}[x]$  em que os factores são polinómios não-constantes (*porquê?*), mostrando assim que  $f$  não seria irredutível em  $\mathbb{Z}[x]$ .

**Teorema 3.1.7**  *$\mathbb{Z}[x]$  é um DFU. Os irredutíveis de  $\mathbb{Z}[x]$  são: os polinómios constantes iguais a primos de  $\mathbb{Z}$  e os polinómios primitivos que são irredutíveis em  $\mathbb{Q}[x]$ .*

*Demonstração:* Cada classe de primos associados de  $\mathbb{Q}[x]$  contém um e um só polinómio primitivo de coeficientes inteiros cujo coeficiente guia é positivo (*porquê?*). Portanto, o conjunto  $\mathcal{P}$  dos polinómios irredutíveis primitivos de coeficiente guia positivo satisfaz as condições do teorema da existência e unicidade da decomposição em primos em DIPs, concluindo-se assim que cada polinómio  $f(x) \in \mathbb{Z}[x] (\subseteq \mathbb{Q}[x] \dots)$  tem uma única factorização da forma:

$$f(x) = c \prod p(x)^{e_p}, \quad \text{com } c \in \mathbb{Q}^*, e_p \in \mathbb{N}_0, \text{ quase todos nulos.}$$

$p(x)$  primitivo com  
coeficiente guia positivo  
e irredutível em  $\mathbb{Q}[x]$

As afirmações feitas são agora fáceis de provar e são deixadas como exercício.

*Observações:*

1. Pelo resultado descrito no exemplo 2, p. 19, temos que  $\mathbb{Z}[x]$  é um exemplo de um DFU que não é um DIP.
2. Os resultados anteriores podem ser adaptados para provar que se  $A$  for um DFU, então  $A[x]$  também o é. Em particular, se  $K$  é um corpo, então  $K[x_1, x_2, \dots, x_n]$  ( $n \in \mathbb{N}$ ) é um DFU,  $\forall n \in \mathbb{N}$  (note que  $K[x_1, \dots, x_n] \simeq K[x_1, \dots, x_{n-1}][x_n] \dots$ ).

É muitas vezes possível obter informação sobre a decomposição em irredutíveis de um polinómio de coeficientes inteiros “reduzindo-o” módulo um primo  $p$ , ou seja considerando o polinómio de  $\mathbb{Z}_p[x]$  que dele se obtém substituindo os seus coeficientes pelas respectivas classes módulo  $p$ , e estudando a decomposição deste. Para tal, é fundamental o facto de a seguinte aplicação ser um homomorfismo (de anéis):

$$\begin{aligned} [\cdot]_p : \quad \mathbb{Z}[x] &\longrightarrow \mathbb{Z}_p[x] \\ \sum_{i \geq 0} a_i x^i &\longmapsto \sum_{i \geq 0} [a_i]_p x^i \end{aligned}$$

(prove que é de facto um homomorfismo).

Para começar tem-se:

**Proposição 3.1.8** *Seja  $f \in \mathbb{Z}[x]$  um polinómio primitivo e  $p$  um número primo. Se  $[f]_p$  for irredutível em  $\mathbb{Z}_p[x]$  e  $\text{gr}([f]_p) = \text{gr}(f)$ , então  $f$  é irredutível em  $\mathbb{Z}[x]$  (e portanto em  $\mathbb{Q}[x]$ , se  $f$  não for constante).*

*Observação:*  $\text{gr}([f]_p) = \text{gr}(f) \Leftrightarrow p \nmid$  coeficiente guia de  $f$ .

*Demonstração:* Suponhamos que  $f = gh$ , com  $g, h \in \mathbb{Z}[x]$ . Então  $[f]_p = [g]_p[h]_p$  e portanto, por hipótese,  $[g]_p \in \mathbb{Z}_p[x]^* = \mathbb{Z}_p^*$  ou  $[h]_p \in \mathbb{Z}_p^*$ , ou seja  $\text{gr}([g]_p) = 0$  ou  $\text{gr}([h]_p) = 0$ .

Por outro lado, como  $\text{gr}(g) + \text{gr}(h) = \text{gr}(f) = \text{gr}([f]_p) = \text{gr}([g]_p) + \text{gr}([h]_p)$  e como  $\text{gr}([\alpha]_p) \leq \text{gr}(\alpha)$ ,  $\forall \alpha \in \mathbb{Z}[x]$ , conclui-se que  $\text{gr}(g) = 0$  ou  $\text{gr}(h) = 0$ . Mas como  $f$  é primitivo, resulta finalmente que  $g = \pm 1$  ou  $h = \pm 1$ , o que prova o que se queria.

Este resultado levanta o problema de determinar se um dado polinómio de  $\mathbb{Z}_p[x]$ , onde  $p$  é um primo, é ou não irredutível. Limitar-nos-emos a indicar um método sistemático, embora computacionalmente muito ineficiente, de listar os irredutíveis (= primos) de  $\mathbb{Z}_p[x]$ . Tal método é uma variante daquilo que é conhecido pelo nome de *crivo de Eratóstenes* (Eratóstenes (c. 284–c. 192 A.C.), mais um dos matemáticos do Museu de Alexandria (ver Introdução ...)), que consiste em escrever os inteiros de 2 a  $n$  ( $n \in \mathbb{N}$ ) e, pondo  $p_1 = 2$ , fazer o seguinte:

- (0)  $q := 2$ ;  $k := 1$ ;
- (1) riscar todos os múltiplos de  $q$  distintos do próprio;
- (2) fazer  $k := k + 1$  e  $p_k :=$  primeiro número não riscado após  $q$ ;
- (3)  $q := p_k$ ;
- (4) ir para (1), enquanto  $k \leq n$ .

Os números  $p_1, p_2, p_3, \dots$  que se obtêm deste modo são todos os números primos de 2 a  $n$  (*porquê?*).

*Exemplo:* ( $n = 27$ )

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27.

Em  $\mathbb{Z}_p[x]$  pode fazer-se algo de análogo, uma vez que os polinómios de um dado grau são em número finito (*porquê?*). Assim, escrevem-se os polinómios de  $\mathbb{Z}_p[x]$  por ordem crescente de grau, com os polinómios de um mesmo grau ordenados de forma arbitrária.

Para uma pessoa não se perder, isto é repetir ou esquecer algum polinómio, é útil usar o seguinte algoritmo: escrevem-se primeiro os elementos de  $\mathbb{Z}_p$  (i.e. 0 e os polinómios de grau 0), e depois de se escreverem todos os polinómios de grau  $n$ , escreve-se o polinómio  $x^{n+1}$  somado a todos os anteriores, pela ordem em que estão, depois faz-se o mesmo para  $2x^{n+1}$ , etc, até  $(p-1)x^{n+1}$ .

Depois, riscam-se sucessivamente os múltiplos dos polinómios que vão “sobrevivendo”, exactamente como no crivo de Eratóstenes. Os múltiplos de um dado

polinómio podem ser calculados multiplicando-o pelos polinómios pela ordem em que estes ficaram escritos (de modo a não esquecer nenhum múltiplo).

*Exemplo:* Os polinómios primos de  $\mathbb{Z}_2[x]$  de grau  $\leq 4$  são:

$0, 1,$

$x, x + 1,$

$x^2, x^2 + 1, x^2 + x, x^2 + x + 1,$

$x^3, x^3 + 1, x^3 + x, x^3 + x + 1, x^3 + x^2, x^3 + x^2 + 1, x^3 + x^2 + x, x^3 + x^2 + x + 1,$

$x^4, x^4 + 1, x^4 + x, x^4 + x + 1, x^4 + x^2, x^4 + x^2 + 1, x^4 + x^2 + x, x^4 + x^2 + x + 1,$

$x^4 + x^3, x^4 + x^3 + 1, x^4 + x^3 + x, x^4 + x^3 + x + 1, x^4 + x^3 + x^2,$

$x^4 + x^3 + x^2 + 1, x^4 + x^3 + x^2 + x, x^4 + x^3 + x^2 + x + 1.$

*Exercício:* Porque é que este processo dá todos os primos de grau  $\leq 4$ , como se afirmou?

*Exemplo:* Usando o facto de  $x^4 + x + 1$  ser irredutível em  $\mathbb{Z}_2[x]$  e a proposição anterior, conclui-se que *todos* os polinómios da forma  $x^4 + 2ax^3 + 2bx^2 + (2c + 1)x + (2d + 1)$  são irredutíveis em  $\mathbb{Z}[x]$  e em  $\mathbb{Q}[x]$ , quaisquer que sejam  $a, b, c, d \in \mathbb{Z}$  (!!)

A redução módulo um primo pode ainda ajudar a descrever a factorização de um polinómio de  $\mathbb{Z}[x]$ , mesmo quando esse polinómio é redutível módulo esse primo. Um exemplo é dado pelo seguinte resultado:

**Proposição 3.1.9 (critério de Eisenstein (1823–52))**

Seja  $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{Z}[x]$  tal que existe um primo  $p$  que satisfaz:  $p|a_i \forall i \in \{0, 1, \dots, n-1\}$ ,  $p \nmid a_n$  e  $p^2 \nmid a_0$ . Então  $f$  é irredutível em  $\mathbb{Q}[x]$  (Se  $f$  for primitivo, então é também irredutível em  $\mathbb{Z}[x]$ ).

*Demonstração:* Tem-se que  $[f]_p = [a_n]_p x^n$  e  $[a_n]_p \neq 0$ . Se  $f$  fosse redutível em  $\mathbb{Q}[x]$ , existiriam polinómios não-constantess  $g, h \in \mathbb{Z}[x]$  tais que  $f = gh$  (pela prova do teorema 3.1.6). Escrevendo  $g = b_0 + b_1x + \dots + b_r x^r$  e  $h = c_0 + c_1x + \dots + c_s x^s$ , com  $b_i, c_j \in \mathbb{Z}$ , ter-se-ia:  $r, s \in \mathbb{N}, r + s = n$ . De  $[g]_p \cdot [h]_p = [f]_p = [a_n]_p x^n$ , do facto de  $x$  ser um primo de  $\mathbb{Z}_p[x]$  e de este anel ser um DFU, resultaria que  $[g]_p = ux^i$ ,  $[h]_p = vx^j$ , para alguns  $u, v \in \mathbb{Z}_p^*$ ;  $0 \leq i \leq r, 0 \leq j \leq s$  com  $i + j = n$ . Como  $r + s = n$ , teria de se ter  $i = r, j = s$  (e portanto  $u = [b_r]_p, v = [c_s]_p$ ). Mas então, em particular  $p|b_0$  e  $p|c_0$  (porquê?), donde se concluiria que  $p^2|a_0 = b_0c_0$ , contradizendo as hipótese feitas. Esta contradição mostra o que se queria.

*Exemplo:* O polinómio  $x^{11} + 3x^5 - 6x^3 + 27x^2 - 9x + 12$  é irredutível em  $\mathbb{Q}[x]$  e em  $\mathbb{Z}[x]$ .

Dois consequências importantes deste resultado são:

**Corolário 3.1.10** *Seja  $p$  um primo. O polinómio  $\Phi_p(x) := 1 + x + x^2 + \dots + x^{p-1}$  (= “ $\frac{x^p-1}{x-1}$ ”), a que se chama o  **$p$ -ésimo polinómio ciclotómico** (as suas raízes são as raízes primitivas  $p$ -ésimas da unidade, que dividem o círculo unitário em  $p$  partes iguais e “ciclotómico”= “que divide o círculo”), é irredutível em  $\mathbb{Q}[x]$  (e em  $\mathbb{Z}[x]$ ).*

*Demonstração:* Faça-se  $f(x) := \Phi_p(x+1)$ . Como  $(x-1)\Phi(x) = x^p - 1$ , tem-se que (porquê?)  $xf(x) = (x+1)^p - 1 = \sum_{i=1}^p \binom{p}{i} x^i$  e portanto (porquê?)  $f(x) = \sum_{i=1}^p \binom{p}{i} x^{i-1} = x^{p-1} + px^{p-2} + \binom{p}{2} x^{p-3} + \dots + \binom{p}{p-2} x + p$ . Mas  $p \mid \binom{p}{i} = \frac{p!}{(p-i)!i!} \forall i = 1, 2, \dots, p-1$  e  $p^2 \nmid \binom{p}{1}$ , e portanto podemos aplicar o critério de Eisenstein para concluir que  $f(x)$  é irredutível. Não é difícil concluir que então  $\Phi_p(x)$  é também irredutível (*exercício!*).

**Corolário 3.1.11** *Se  $a \neq \pm 1$  é um inteiro “livre de quadrados” (i.e. não é divisível por nenhum quadrado  $\neq 1$ ), então  $x^n - a$  é irredutível em  $\mathbb{Q}[x]$  e em  $\mathbb{Z}[x]$ , para todo o  $n \in \mathbb{N}$ . Em particular, conclui-se que  $\mathbb{Q}[x]$  tem uma infinidade de primos e que tem polinómios irredutíveis de todos os graus.*

*Demonstração:* Como  $a \notin \mathbb{Z}^*$ , existe algum primo  $p$  tal que  $p \mid a$ . Como  $a$  é livre de quadrados,  $p^2 \nmid a$  e portanto pode-se aplicar o critério de Eisenstein para concluir o que é afirmado.

## 3.2 $\mathbb{R}[x]$ e $\mathbb{C}[x]$

Contrariamente ao que acontece em  $\mathbb{Q}[x]$  e em  $\mathbb{Z}[x]$ , onde há polinómios irredutíveis de grau arbitrário, em  $\mathbb{C}[x]$  não há polinómios irredutíveis de grau superior a 1, e em  $\mathbb{R}[x]$  não há irredutíveis de grau maior que 2. Isto é consequência do seguinte resultado, conhecido pelo nome um tanto ou quanto exagerado de **Teorema Fundamental da Álgebra**.

**Teorema 3.2.1 (d’Alembert, Euler, de Foncenex, Lagrange, Gauss)**  
*Todo o polinómio não-constante de  $\mathbb{C}[x]$  tem (pelo menos) uma raiz (em  $\mathbb{C}$ ).*

**NOTA:** Uma forma embrionária deste resultado aparece num texto de 1629 de Albert Girard (1592–1632), sem qualquer justificação. O facto de G. W. Leibniz (1646–1716), em 1702, dar o exemplo (relacionado com o problema de integrar funções racionais...):

$$\begin{aligned} x^4 + a^4 &= (x^2 + a^2\sqrt{-1})(x^2 - a^2\sqrt{-1}) \\ &= \left(x + a\sqrt{-\sqrt{-1}}\right) \left(x - a\sqrt{-\sqrt{-1}}\right) \left(x + a\sqrt{\sqrt{-1}}\right) \left(x - a\sqrt{\sqrt{-1}}\right), \end{aligned}$$

afirmando que quando se multiplica quaisquer dois destes quatro factores não se obtém nenhum polinómio quadrático com coeficientes reais (*exercício*: porque é que isto é falso?), mostra que o resultado ainda estava longe de ser completamente intuído no início do século XVIII.

1746: primeira (ideia para uma) prova, usando técnicas analíticas, publicada por Jean le Rond d’Alembert (1771–83);

1749: esboço de uma prova mais algébrica por L. Euler (1707–83);

1777: simplificações da “prova” de Euler sugeridas por D. F. Foncenex (1734–99);

1772: J. L. Lagrange “completa” prova de Euler – de Foncenex, assumindo por seu lado, implicitamente, algumas propriedades dos números complexos;

1799: K. F. Gauss (1777–1855) fornece prova quase completa na sua dissertação de doutoramento, usando as ideias de d’Alembert;

1815: Gauss publica uma prova rigorosa e completa, usando e completando as ideias de Euler, de Foncenex e Lagrange.

*Observação*: A investigação inicial que levou à descoberta do resultado em discussão foi motivada pelo problema de integrar funções racionais (i.e. quocientes de funções polinomiais), tendo-se começado a suspeitar que todo o polinómio com coeficientes reais se podia sempre escrever como produto de polinómios de grau 1 e 2.

*Demonstração do Teorema Fundamental da Álgebra*: A prova que aqui apresentamos resulta de duas propriedades das funções polinomiais de  $\mathbb{C}$  em  $\mathbb{C}$ :

**Lema 3.2.2** *Seja  $f(x) \in \mathbb{C}[x]$  não-constante e  $\alpha \in \mathbb{C}$  tal que  $f(\alpha) \neq 0$ . Então  $\exists z \in \mathbb{C} : |f(z)| < |f(\alpha)|$ .*

*Demonstração*: Fazendo  $g(x) := \frac{1}{f(\alpha)}f(x + \alpha)$ , obtemos um polinómio  $g \in \mathbb{C}[x]$  tal que  $g(0) = 1$  e basta provar que  $\exists z \in \mathbb{C} : |g(z)| < 1$  (*porquê?*).

Escreva-se  $g(x) = 1 + ax^k + x^{k+1}h(x)$ , com  $k \in \mathbb{N}$ ,  $a \in \mathbb{C}^*$  o primeiro coeficiente não-nulo de  $g$  após o termo constante, que existe por  $f$  ser não-constante, e  $h \in \mathbb{C}[x]$ .

Seja  $\gamma$  uma raiz  $k$ -ésima de  $-a^{-1}$ , i.e.  $\gamma^k = -a^{-1}$  (relembre que todo o número complexo tem raízes de índice arbitrário: se  $-a^{-1} = r(\cos \theta + i \sin \theta)$ , com  $r \in \mathbb{R}^+$ ,  $\theta \in [0, 2\pi[$ , podemos tomar  $\gamma = \sqrt[k]{r}(\cos(\frac{\theta}{k}) + i \sin(\frac{\theta}{k}))$ , por exemplo<sup>2</sup>). Tem-se:  $g(\gamma x) = 1 - x^k + x^{k+1}\tilde{h}(x)$ , sendo  $\tilde{h}(x) = \gamma^{k+1}h(\gamma x) \in \mathbb{C}[x]$ . Para  $x \in \mathbb{R}^+$ , com  $0 < x < 1$ , obtém-se:  $|g(\gamma x)| \leq |1 - x^k| + |x|^{k+1}|\tilde{h}(x)| = 1 - x^k + x^{k+1}|\tilde{h}(x)| = 1 - x^k(1 - x|\tilde{h}(x)|)$ .

<sup>2</sup>Note que se usou também aqui o facto de que todo o número real tem uma raiz  $k$ -ésima. Por trás deste facto está o teorema dos valores intermédios...

Uma vez que a aplicação  $[0, 1] \rightarrow \mathbb{R}$   
 $x \mapsto \left| \tilde{h}(x) \right|$  é contínua (exercício!), conclui-

se que  $\left| \tilde{h}(x) \right|$  é limitada para  $x \in ]0, 1[$ . Mas então  $1 - x \left| \tilde{h}(x) \right|$  é positivo para  $x$  suficientemente pequeno (*porquê?*). Resulta de tudo isto que  $|g(\gamma x)| \leq 1$  para  $x$  pequeno, o que termina a prova.

Seja agora  $m := \inf\{|f(z)| : z \in \mathbb{C}\}$ .

A prova do teorema Fundamental da Álgebra fica concluída se mostrarmos que  $m$  é “atingido”, ou seja, que existe um número  $\alpha \in \mathbb{C}$  tal que  $f(\alpha) = m$ , pois resulta imediatamente do lema anterior que então  $m = 0$  e por conseguinte  $\alpha$  é uma raiz de  $f$ .

**Lema 3.2.3**  $\exists \alpha \in \mathbb{C} : |f(\alpha)| = m$ .

*Demonstração:* Seja  $f(x) = a_0 + a_1x + \dots + a_nx^n$  com  $a_0, a_1, \dots, a_n \in \mathbb{C}$  e  $a_n \neq 0$ . Como

$$\begin{aligned} |f(z)| &= |z|^n \cdot \left| \frac{a_0}{z^n} + \frac{a_1}{z^{n-1}} + \dots + \frac{a_{n-1}}{z} + a_n \right| \\ &\geq |z|^n \cdot \left| |a_n| - \left| \frac{a_0}{z^n} + \frac{a_1}{z^{n-1}} + \dots + \frac{a_{n-1}}{z} \right| \right| \end{aligned}$$

e  $\left| \frac{a_0}{z^n} + \frac{a_1}{z^{n-1}} + \dots + \frac{a_{n-1}}{z} \right| \leq \frac{|a_0|}{|z|^n} + \frac{|a_1|}{|z|^{n-1}} + \dots + \frac{|a_{n-1}|}{|z|} \rightarrow 0$  quando  $|z| \rightarrow +\infty$ , resulta que  $|f(z)| \rightarrow +\infty$  quando  $|z| \rightarrow +\infty$ .

Em particular,  $\exists r \in \mathbb{R}^+$  tal que  $|z| > r \Rightarrow |f(z)| > m + 1$  (por exemplo), e portanto  $m = \inf\{|f(z)| : |z| \leq r\}$ . O lema resulta agora do facto de uma função contínua (neste caso a função dada por  $z \mapsto |f(z)|$ ) definida num compacto ( $\{z \in \mathbb{C} : |z| \leq r\}$ ) ter um mínimo. Como foi observado antes do seu enunciado, isto conclui também a prova do Teorema Fundamental da Álgebra.

**Corolário 3.2.4** Em  $\mathbb{C}[x]$  os polinómios irredutíveis são exactamente os polinómios de grau 1.

*Demonstração:* É claro que os polinómios de grau 1 são irredutíveis. Reciprocamente, se  $f(x) \in \mathbb{C}[x]$  é um polinómio irredutível, seja  $\alpha \in \mathbb{C}$  uma sua raiz, cuja existência é assegurada pelo teorema anterior. Então  $x - \alpha | f(x)$ . O quociente tem de ser uma unidade, o que mostra que  $\text{gr}(f) = 1$ .

**Corolário 3.2.5** Em  $\mathbb{R}[x]$  os polinómios irredutíveis são exactamente os polinómios de grau 1 e os polinómios do 2º grau,  $ax^2 + bx + c$  ( $a, b, c \in \mathbb{R}; a \neq 0$ ), tais que  $b^2 - 4ac < 0$ .

*Demonstração:* É claro que os polinómios mencionados são irredutíveis (*porquê?*). Reciprocamente, seja  $f \in \mathbb{R}[x]$  um polinómio irredutível e seja  $\alpha \in \mathbb{C}$  uma

sua raiz. Se  $\alpha$  for real, então um raciocínio inteiramente análogo ao da prova anterior mostra que  $\text{gr}(f) = 1$ .

Suponhamos agora que  $\alpha \notin \mathbb{R}$ . Como a conjugação é um automorfismo de  $\mathbb{C}$ , resulta que também  $\bar{\alpha}$  é uma raiz de  $f$ . Mas  $x - \alpha$  e  $x - \bar{\alpha}$  são primos não-associados (*porquê?*), e portanto  $(x - \alpha)(x - \bar{\alpha}) \mid f(x)$  (em  $\mathbb{C}[x]$ ). Agora, o polinómio  $(x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} = x^2 - \Re(\alpha)x + |\alpha|^2$  (onde  $\Re(z)$  designa a parte real de  $z$ ) tem coeficientes reais. Usando os factos de em domínios de integridade os quocientes serem únicos e, novamente, a conjugação ser um homomorfismo, resulta que  $(x - \alpha)(x - \bar{\alpha}) \mid f(x)$  em  $\mathbb{R}[x]$ . Mas então, por  $f(x)$  ser irredutível, o quociente tem de ser uma unidade e portanto  $\text{gr}(f) = 2$ . Se  $f(x) = ax^2 + bx + c$ , então  $b = 2a\Re(\alpha)$  e  $c = a|\alpha|^2$ . Resulta que  $b^2 - 4ac = a^2(\alpha + \bar{\alpha})^2 - 4a^2\alpha\bar{\alpha} = a^2(\alpha - \bar{\alpha})^2 = a^2(2\Im(\alpha)i)^2 = -4a^2\Im(\alpha)^2 < 0$  (onde  $\Im(z)$  designa a parte imaginária de  $z$ ).

# Capítulo 4

## Teoria de Corpos

### 4.1 Corpos de fracções

Dado um domínio de integridade  $A$ , há um processo natural de com ele construir um corpo que o contém (mais exactamente, contém uma sua cópia isomorfa), inspirado na relação entre  $\mathbb{Z}$  e  $\mathbb{Q}$ , e que passamos a descrever.

No conjunto  $A \times (A - \{0\})$  introduz-se a relação dada por:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc,$$

que é fácil ver ser uma relação de equivalência (*exercício!*). Designemos o conjunto das respectivas classes de equivalência por  $\mathcal{Q}_A$ .

*Notação:*  $\frac{a}{b} := [(a, b)]_{\sim}$ , a classe de equivalência de  $(a, b) \in A \times (A - \{0\})$ .

Em seguida, definem-se as operações:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd} \text{ e } \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd} \quad \left(\frac{a}{b}, \frac{c}{d} \in \mathcal{Q}_A\right).$$

*Exercício:* Verifique que estas operações estão bem-definidas, ou seja, que não dependem das escolhas dos representantes das respectivas classes de equivalência.

É fácil mostrar (*faça-o!*) que  $\mathcal{Q}_A$  munido destas operações é um corpo, a que se chama **o corpo das fracções de  $A$**  e que  $\{\frac{a}{1} : a \in A\}$  é um subanel de  $\mathcal{Q}_A$  que é isomorfo a  $A$ .

*Exemplos:*

1. É claro que  $\mathbb{Q}$  é o (isomorfo ao...) corpo das fracções de  $\mathbb{Z}$ .
2. O corpo das fracções do anel  $K[x]$ , onde  $K$  é um corpo, é usualmente designado por  $K(x)$  e os seus elementos dizem-se as **fracções racionais sobre  $K$** .

*Observação/Exercício:* É agora fácil ver que os domínios de integridade são exactamente os subanáis de corpos.

## 4.2 Extensões de corpos

Um método muito importante de “fabricar” corpos é dado pelo seguinte resultado:

**Proposição 4.2.1** *Se  $K$  é um corpo e  $p(x) \in K[x]$  é um polinómio irredutível, então  $E = K[x]/\langle p(x) \rangle$  é um corpo contendo (uma cópia isomorfa a)  $K$ . O polinómio  $p(x)$  pode então ser visto como um elemento de  $E[x]$  e, como tal, tem uma raiz em  $E$ .*

*Demonstração:* Por comodidade de escrita, escrevemos  $[a(x)]$  para designar o elemento  $a(x) + \langle p(x) \rangle$  de  $E$  ( $a(x) \in K[x]$ ). Para provar que  $E$  é um corpo, temos apenas de mostrar que todo o elemento não-nulo de  $E$  tem inverso. Seja pois  $[a(x)] \in E - \{0\}$ , o que significa que  $p(x) \nmid a(x)$ . Mas então  $\langle a(x), p(x) \rangle = \langle 1 \rangle$  (porquê?), e portanto  $1 = a(x)b(x) + p(x)c(x)$ , para alguns  $b(x), c(x) \in K[x]$ . Em particular, tem-se que  $[a(x)] \cdot [b(x)] = [1]$ , o que mostra o que queríamos.

É fácil ver que  $\{[\lambda] : \lambda \in K\}$  é um subcorpo de  $E$  isomorfo a  $K$ . Finalmente, sendo  $p(x) = a_0 + a_1x + \dots + a_nx^n$ , tem-se:  $p([x]) = [a_0] + [a_1][x] + \dots + [a_n][x^n] = [p(x)] = 0$ . Ou seja,  $[x]$  é uma raiz de  $p(x)$  em  $E$ !

*Observação:*

1. Repare que a construção de  $E$  a partir de  $K$ , e a prova de que é um corpo, é inteiramente análoga à construção de  $\mathbb{Z}_p$  a partir de  $\mathbb{Z}$ , para  $p$  primo, e a prova de que  $\mathbb{Z}_p$  é um corpo.
2. Podemos (e em geral fazê-lo-emos) pensar em  $E$  como os restos dos elementos de  $K[x]$  módulo  $p(x)$ , operando-os como em  $K[x]$  só que o resultado é substituído pelo correspondente resto módulo  $p(x)$  (tal como fazemos em  $\mathbb{Z}_p$ ).

*Exemplos:*

1.  $\mathbb{R}[x]/\langle x^2 + 1 \rangle = \{[a + bx] : a, b \in \mathbb{R}\}$  (onde  $[a + bx] := (a + bx) + \langle x^2 + 1 \rangle$ ), pois qualquer polinómio de  $\mathbb{R}[x]$ , quando dividido por  $x^2 + 1$ , tem como resto um polinómio de grau não superior a 1. Como  $[a + bx] = [c + dx] \Leftrightarrow [(a - c) + (b - d)x] = 0 \Leftrightarrow x^2 + 1 \mid (a - c) + (b - d)x \Leftrightarrow a = c$  e  $b = d$ , os polinómios  $a + bx$  ( $a, b \in \mathbb{R}$ ) representam todas as classes de  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ , sem repetições. Por outro lado:

$$\begin{aligned} [a + bx] + [c + dx] &= [(a + c) + (b + d)x]; \\ [a + bx] \cdot [c + dx] &= [ac + (ad + bc)x + bdx^2] = [(ac - bd) + (ad + bc)x], \end{aligned}$$

pois  $[x]^2 = -1$ . Vê-se assim que a estrutura de corpo de  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$  é completamente determinada (para além dos axiomas) pela relação  $[x]^2 = -1$ , sendo agora muito fácil concluir que  $\mathbb{R}[x]/\langle x^2 + 1 \rangle \simeq \mathbb{C}$  (!)

2.  $\mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$  é um corpo (verifique que  $x^2 + 1$  é irredutível em  $\mathbb{Z}_3[x]$ ) com 9 elementos, que podem ser escritos na forma  $a + bi$ , designando  $x + \langle x^2 + 1 \rangle$  por  $i$  e onde  $a, b \in \mathbb{Z}_3$ . Os elementos deste corpo operam-se formalmente como os números complexos, com a única diferença de que as partes “reais” e “imaginárias” são elementos de  $\mathbb{Z}_3$ .

*Exemplo:*  $(2 + i)(1 + 2i) = 2 + i + 4i + 2i^2 = 2 + 5i - 2 = 2i = -i$ .

3.  $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$  é um corpo ( $x^2 + x + 1$  é irredutível em  $\mathbb{Z}_2[x]$ , como foi visto no exemplo da página 32) com 4 elementos: pondo  $\omega = x + \langle x^2 + x + 1 \rangle$ , os seus elementos podem ser escritos, de um só modo, na forma  $a + b\omega$ , com  $a, b \in \mathbb{Z}_2$ . A sua estrutura de corpo é inteiramente determinada (para além dos axiomas) pela relação:  $\omega^2 = -1 - \omega$ .

*Exemplo:*  $(1 + \omega)^2 = 1 + 2\omega + \omega^2 = 1 + 0 - 1 - \omega = -\omega = \omega$ .

*Observação:* Este é um exemplo de um corpo distinto de  $\mathbb{Z}_2$  e no qual  $1 + 1 = 0$ .

4. Usando uma vez mais o exemplo da página 32, neste caso a irredutibilidade de  $x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$ , tem-se que o anel  $\mathbb{Z}_2[x]/\langle x^4 + x^3 + 1 \rangle$  é um corpo. Pondo  $\theta = x + \langle x^4 + x^3 + 1 \rangle$ , os seus elementos podem ser escritos, de um só modo, na forma  $a + b\theta + c\theta^2 + d\theta^3$ , com  $a, b, c, d \in \mathbb{Z}_2$  (*porquê?*). Vê-se assim tratar-se de um corpo com 16 elementos (*porquê?*). A sua estrutura é inteiramente determinada (para além dos axiomas) pela relação:  $\theta^4 = -1 - \theta^3 = 1 + \theta^3$ .

*Exemplos:*

$$(1 + \theta)(1 + \theta^3) = 1 + \theta + \theta^3 + \theta^4 = \theta;$$

*Cálculo de  $(1 + \theta^2)^{-1}$ :* designando-o por  $a + b\theta + c\theta^2 + d\theta^3$ , tem-se  $1 = (a + b\theta + c\theta^2 + d\theta^3)(1 + \theta^2) = a + b\theta + (a + c)\theta^2 + (b + d)\theta^3 + c\theta^4 + d\theta^5 = a + b\theta + (a + c)\theta^2 + (b + d)\theta^3 + c(-1 - \theta^3) + d(1 - \theta + \theta^3) = (a - c + d) + (b - d)\theta + (a + c)\theta^2 + (b - c)\theta^3$ , donde resulta (pela unicidade da representação na forma  $a + b\theta + c\theta^2 + d\theta^3$ ):

$$\begin{cases} a - c + d = 1 \\ b - d = 0 \\ a + c = 0 \\ b - c = 0 \end{cases}, \text{ que rapidamente se resolve (repare-se que se sabe } a \text{ priori que}$$

este sistema é determinado, pois todo o elemento não-nulo tem um e um só inverso), obtendo-se  $a = b = c = d = 1$ , ou seja,  $(1 + \theta^2)^{-1} = 1 + \theta + \theta^2 + \theta^3$ .

5. Depois de perceber os exemplos anteriores, é agora imediato que se tem  $\mathbb{Q}[x]/\langle x^2 - 2 \rangle = \{[a + bx] : a, b \in \mathbb{Q}\}$  (onde  $[a + bx] := (a + bx) + \langle x^2 - 2 \rangle$ ), sendo a estrutura deste corpo determinada pela relação  $[x]^2 = 2$ . É então claro que  $\mathbb{Q}[x]/\langle x^2 - 2 \rangle \simeq \mathbb{Q}(\sqrt{2})$ .

**Definição 4.2.2** Um corpo  $E$  diz-se uma **extensão** de um corpo  $K$  se  $K$  é subcorpo de  $E$ .

*Notação:*  $E/K :=$  “ $E$  é uma extensão de  $K$ ”.

*Observação:* Esta terminologia pode parecer inteiramente supérflua, e de um ponto de vista estritamente lógico é-o de facto. No entanto revela a diferença de ênfase entre a Teoria de Grupos e a Teoria de Corpos. Na primeira está-se normalmente interessado em determinar as “sub-estruturas” de um grupo, enquanto na segunda predomina o estudo das “sobre-estruturas” de um corpo, em geral corpos que se obtêm daquele por “adjunção” de elementos adicionais.

**Definição 4.2.3** *Diz-se que um polinómio  $f \in K[x]$ ,  $K$  um corpo, se **cinde** sobre uma extensão  $E$  de  $K$  se  $f$  se decompuser como um produto<sup>1</sup> de factores lineares, i.e. de grau 1, em  $E[x]$ .*

*Exemplos:*

1. Todo o polinómio de  $\mathbb{Q}[x]$  se cinde sobre  $\mathbb{C}$ , pelo Teorema Fundamental da Álgebra.
2. O polinómio  $x^2 - 2 \in \mathbb{Q}[x]$  cinde-se sobre  $\mathbb{Q}(\sqrt{2})$ .
3. O polinómio  $x^3 - 2 \in \mathbb{Q}[x]$  não se cinde sobre  $\mathbb{Q}(\sqrt[3]{2})$  (porquê?).

**Teorema 4.2.4 (Kronecker (1736–1813))** *Seja  $K$  um corpo. Para todo o  $f \in K[x]$ , existe uma extensão  $E$  de  $K$  tal que  $f$  se cinde sobre  $E$ .*

*Demonstração:* (Indução sobre o grau de  $f$ )

Se  $\text{gr}(f) = 1$ ,  $f$  já é linear e basta tomar  $E = K$ .

Se  $\text{gr}(f) > 1$ , seja  $p$  um dos factores irreduzíveis de  $f$ . Pela proposição anterior, existe uma extensão  $E$  na qual  $p$  tem uma raiz. Designando tal raiz por  $\alpha$ , tem-se que  $f = (x - \alpha)g$  para algum  $g \in E[x]$ . Como  $\text{gr}(g) = \text{gr}(f) - 1$ , existe, por hipótese de indução, uma extensão  $L$  sobre a qual  $g$  se cinde. Mas é imediato que então também  $f$  se cinde sobre  $L$ .

*Observação muito importante:*

Uma extensão  $E$  de um corpo  $K$  é, em particular, um espaço vectorial sobre  $K$ , se considerarmos  $E$  munido da sua estrutura aditiva de grupo abeliano juntamente com a operação  $K \times E \rightarrow E$  induzida pela multiplicação de  $E$ . É muito fácil verificar que os axiomas de espaço vectorial são de facto satisfeitos (*exercício!*).

---

<sup>1</sup>Como é hábito em Matemática, inclui-se implicitamente nesta definição o caso “extremo”, nomeadamente, o caso de o produto ter um só factor. Mais ainda, convencionamos aqui que um polinómio constante está já cindido. Porquê? Simplesmente para não se andar sempre a escrever “ $f$  não-constante”, e porque tal convenção em nada afecta a teoria que descreveremos.

**Definição 4.2.5** Chama-se **grau da extensão**  $E/K$  à dimensão de  $E$  como espaço vectorial sobre  $K$ , número que é habitualmente denotado por  $[E : K]$ . Diz-se que  $E/K$  é uma **extensão finita** ou **infinita** consoante  $[E : K]$  for finito ou infinito.

*Exemplos:*

1.  $\mathbb{C}/\mathbb{R}$  é uma extensão de grau 2:  $\{1, i\}$  é uma base de  $\mathbb{C}$  sobre  $\mathbb{R}$ .
2.  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$  tem grau 2:  $\{1, \sqrt{2}\}$  é uma base desta extensão.
3.  $\mathbb{R}/\mathbb{Q}$  é uma extensão infinita (*exercício*).

**Definição 4.2.6** O **corpo primo** de um corpo  $K$  é a intersecção de todos os subcorpos de  $K$ , ou seja, é o menor (para a inclusão)<sup>2</sup> subcorpo de  $K$ .

**Proposição 4.2.7** O corpo primo de um qualquer corpo  $K$  é isomorfo ou a  $\mathbb{Q}$  ou a um  $\mathbb{Z}_p$  para algum primo  $p \in \mathbb{N}$ .

*Demonstração:* Seja  $\chi : \mathbb{Z} \rightarrow K$  definida por:

$$\chi(n) := \begin{cases} \underbrace{1 + 1 + \cdots + 1}_{n \text{ vezes}} & , \text{ se } n \in \mathbb{N}; \\ 0 & , \text{ se } n = 0; \\ \underbrace{(-1) + (-1) + \cdots + (-1)}_{-n \text{ vezes}} & , \text{ se } n \in \mathbb{Z} - \mathbb{N}_0, \end{cases}$$

cuja imagem está contida no corpo primo de  $K$  (*porquê?*). É fácil ver (*exercício!*) que  $\chi$  é um homomorfismo (de anéis). Seja  $I = \text{Ker } \chi$ , um ideal de  $\mathbb{Z}$ . Como  $\mathbb{Z}$  é um DIP,  $I = n\mathbb{Z}$  para algum  $n \in \mathbb{N}_0$ . Pelo teorema do homomorfismo, resulta que  $\text{Im } \chi$  é um subanel de  $K$  isomorfo a  $\mathbb{Z}/n\mathbb{Z}$ . Como subanéis de corpos são domínios de integridade, conclui-se que  $n = 0$  ou  $n = p$ , para algum primo  $p$ .

Se  $n = 0$ , isto significa que  $\chi$  é injectiva e portanto  $K$  contém, dentro do seu corpo primo, um subanel isomorfo a  $\mathbb{Z}$ . Como  $K$  contém os inversos dos elementos não-nulos desse subanel, é agora fácil concluir o seu corpo primo é isomorfo a  $\mathbb{Q}$ .

Se  $n = p$ ,  $p$  primo, então  $\text{Im } \chi \simeq \mathbb{Z}_p$  é o corpo primo de  $K$ .

**Definição 4.2.8** Diz-se que um corpo tem **característica 0** se o seu corpo primo for isomorfo a  $\mathbb{Q}$  ( $\Leftrightarrow \underbrace{1 + 1 + \cdots + 1}_{n \text{ vezes}} \neq 0, \forall n \in \mathbb{N}$ , como se viu); diz-se que tem **característica  $p$**  se o seu corpo primo for isomorfo a  $\mathbb{Z}_p$  (sendo  $p$  o menor

<sup>2</sup> Esta definição só faz sentido por a intersecção de uma qualquer família de subcorpos ser ainda um subcorpo. (*Prove isto!*)

inteiro positivo  $n$  tal que  $\underbrace{1+1+\dots+1}_{n \text{ vezes}} = 0$  (porquê?), ou seja  $p$  é a ordem de 1 no grupo aditivo do corpo).

*Exemplos:*

1.  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(x), \mathbb{R}(x), \mathbb{C}(x)$  são corpos de característica 0.
2.  $\mathbb{Z}_2[x]/\langle x^4 + x^3 + 1 \rangle$  (ver exemplo 4, p. 39) tem característica 2.
3.  $\mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$  (ver exemplo 2, p. 39) é um corpo de característica 3.

Agora, se  $K$  é um **corpo finito**, então tem necessariamente característica  $\neq 0$  e portanto  $K$  pode ser visto como uma extensão de  $\mathbb{Z}_p$  para algum primo  $p$ . Como  $K$  é finito,  $K$  é uma extensão finita de  $\mathbb{Z}_p$ . Pondo  $n = [K : \mathbb{Z}_p]$ , tem-se, por resultados de Álgebra Linear, que  $K$  é isomorfo, como espaço vectorial sobre  $\mathbb{Z}_p$ , a  $\mathbb{Z}_p^n$ . Mas então  $\#K = p^n$ . Este simples argumento mostra um facto surpreendente:

**Proposição 4.2.9** *Se  $m \in \mathbb{N}$  não for uma potência de um primo, então não existe nenhum corpo com  $m$  elementos.*

*Exemplo:* Não existe nenhum corpo com 100 elementos!

Reciprocamente tem-se:

**Teorema 4.2.10 (E. Galois, 1830)** *Para todo o primo  $p$  e para todo o  $n \in \mathbb{N}$  existe um corpo com  $p^n$  elementos.*

*Demonstração:* Seja  $p$  um número primo e  $n \in \mathbb{N}$ . Começemos por observar que se existir um corpo com  $p^n$  elementos, então  $K^*$  será um grupo abeliano de ordem  $p^n - 1$ ; pelo teorema de Lagrange visto em Álgebra I,  $a^{p^n - 1} = 1, \forall a \in K^*$ . Resulta assim que todo o elemento de  $K$  seria raiz do polinómio  $x^{p^n} - x$ . Estas considerações sugerem o caminho a seguir para construir um corpo com  $p^n$  elementos.

Considere-se então o polinómio  $x^{p^n} - x \in \mathbb{Z}_p[x]$  e seja  $E$  uma extensão de  $\mathbb{Z}_p$  na qual ele se cinde. Faça-se  $F = \{\alpha \in E : \alpha^{p^n} = \alpha\}$ , i.e.  $F$  é o conjunto das raízes de  $x^{p^n} - x$  em  $E$ . A prova fica completa mostrando que  $\#F = p^n$  e que  $F$  é um subcorpo de  $E$ . Para tal é útil introduzir algumas noções, importantes neste e noutros contextos:

**Definição 4.2.11** *Seja  $K$  um corpo,  $f \in K[x]$  e  $\alpha \in K$  uma raiz de  $f$ . O número  $n = \text{ord}_{(x-\alpha)}(f) \geq 1$  (ver 2.5.25, p. 24) diz-se a **multiplicidade** da raiz  $\alpha$  de  $f$ . Uma raiz cuja multiplicidade é 1 diz-se **simples**; uma raiz diz-se **múltipla** se  $n \geq 2$ .*

*Observação:* Uma raiz  $\alpha$  de  $f$  é múltipla se e só se  $(x - \alpha)^2 | f$ .

**Definição 4.2.12** Dado  $f = \sum_{i \geq 0} a_i x^i \in K[x]$ ,  $K$  corpo, chama-se **derivada formal** de  $f$  ao polinómio  $f' := \sum_{i \geq 1} i a_i x^{i-1}$ .

**Lema 4.2.13** Tem-se:

(a)  $f' = 0 \Leftrightarrow f \in K[x]^* \cup \{0\}$ , quando  $K$  tem característica 0.

(b)  $(f + g)' = f' + g'$ ;  $(\lambda f)' = \lambda f'$ ,  $\forall \lambda \in K; f, g \in K[x]$ .

(c)  $(f \cdot g)' = f' \cdot g + f \cdot g'$ ,  $\forall f, g \in K[x]$ .

*Demonstração:* As afirmações (a) e (b) são deixadas como exercício.

*Prova de (c):* Sejam  $f = \sum_{i \geq 0} a_i x^i$  e  $g = \sum_{j \geq 0} b_j x^j$  ( $a_i, b_j \in K$ ). Então:

$$\begin{aligned} f' \cdot g + f \cdot g' &\stackrel{\text{(porquê?)}}{=} \\ &= \left( \sum_{i \geq 0} (i+1) a_{i+1} x^i \right) \left( \sum_{j \geq 0} b_j x^j \right) + \left( \sum_{i \geq 0} a_i x^i \right) \left( \sum_{j \geq 0} (j+1) b_{j+1} x^j \right) = \\ &\stackrel{\text{(porquê?)}}{=} \sum_{k \geq 0} \left( \sum_{i=0}^k (i+1) a_{i+1} b_{k-i} + \sum_{i=0}^k a_i (k-i+1) b_{k-i+1} \right) x^k = \\ &= \sum_{k \geq 0} \left( \sum_{i=1}^{k+1} i a_i b_{k-i} + \sum_{i=0}^k (k-i+1) a_i b_{k-i+1} \right) x^k = \\ &\stackrel{\text{(porquê?)}}{=} \sum_{k \geq 0} (k+1) \left( \sum_{i=0}^{k+1} a_i b_{k+1-i} \right) x^k = \\ &= (f \cdot g)'. \end{aligned}$$

*Exemplo:* Em corpos de característica não-nula não é verdade que os únicos polinómios de derivada nula sejam os constantes. Por exemplo, o polinómio  $x^p + 1 \in \mathbb{Z}_p[x]$  tem derivada nula.

**Lema 4.2.14** Seja  $f \in K[x]$ ,  $K$  corpo.  $f$  tem raízes múltiplas nalguma extensão de  $K$  se e só se  $\langle f, f' \rangle \neq \langle 1 \rangle$  (em  $K[x]$ ).

*Demonstração:* Se  $\langle f, f' \rangle \neq \langle 1 \rangle$ , então existe  $h \in K[x]$  irredutível tal que  $h|f$  e  $h|f'$ . Seja  $E/K$  tal que  $h$  tem uma raiz em  $E$  e seja  $\alpha$  uma tal raiz. Então, em  $E[x]$ ,  $x - \alpha | f(x)$  e  $x - \alpha | f'(x)$ . Sendo  $g \in E[x]$  tal que  $f(x) = (x - \alpha)g(x)$ , resulta que  $f'(x) = g(x) + (x - \alpha)g'(x)$  e portanto  $x - \alpha | g(x)$ . Conclui-se assim que  $(x - \alpha)^2 | f(x)$ , o que mostra que  $\alpha$  é uma raiz múltipla de  $f$  na extensão  $E$  de  $K$ .

Reciprocamente, se  $\alpha$  é uma raiz múltipla de  $f(x)$  numa extensão  $E$  de  $K$ , então  $f(x) = (x - \alpha)^2 g(x)$  para algum  $g \in E[x]$ . Derivando, obtém-se

$f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2g'(x)$ , o que implica  $x - \alpha \mid f'(x)$  (em  $E[x]$ ). Mas então  $\langle f, f' \rangle_{E[x]} \neq \langle 1 \rangle$ , o que implica  $1 \notin \langle f, f' \rangle_{E[x]}$  e por conseguinte  $1 \notin \langle f, f' \rangle_{K[x]}$ .

*Podemos agora acabar a prova do Teorema de Galois acima enunciado:*

Pondo  $f(x) = x^{p^n} - x$ , tem-se que  $f'(x) = p^n x^{p^n-1} - 1 = -1$  (porquê?) e portanto  $\langle f, f' \rangle = \langle 1 \rangle$ , o que mostra que  $f$  não tem raízes múltiplas em  $E$  (reler o parágrafo antes da definição de raiz múltipla). Donde resulta que  $\#F = p^n$ . Vejamos finalmente que  $F$  é um corpo. Claro que  $F \neq \emptyset$ , pois  $0, 1 \in F$ . Agora, se  $a, b \in F$ , então:

- (i)  $(a - b)^p = a^p - b^p$ , pois  $E$  tem característica  $p$  e portanto  $\binom{p}{i} = 0$ , para todo o  $i \in \{1, \dots, p-1\}$  e  $(-b)^p = -b^p$  tanto no caso em que  $p$  é ímpar, como no caso  $p = 2$ . Por indução  $(a - b)^{p^n} = a^{p^n} - b^{p^n}$ , o que mostra que  $a - b \in F$ ;
- (ii) se  $b \neq 0$ ,  $(ab^{-1})^{p^n} = a^{p^n}(b^{p^n})^{-1} = ab^{-1}$ , mostra que  $ab^{-1} \in F$ .

Fica assim provada a existência de um corpo com  $p^n$  elementos.

Repare-se como o facto de uma extensão ter de um modo natural uma estrutura de espaço vectorial permite obter informações e resultados não triviais (como a não existência de corpos finitos com um certo número de elementos). Regressando à construção de um corpo a partir de um polinómio irreduzível, fazemos agora a seguinte:

*Observação:* Se  $K$  é um corpo e  $p(x) \in K[x]$  um polinómio irreduzível, então a extensão  $E = K[x]/\langle p(x) \rangle$  é finita. O seu grau, i.e. a dimensão de  $E$  como espaço vectorial sobre  $K$ , é igual ao grau de  $p(x)$ , uma vez que os elementos  $1, [x], [x]^2, \dots, [x]^{\text{gr}(p)-1}$  constituem uma base de  $E/K$ . É por haver esta relação entre a dimensão e o grau do polinómio, que se chama *grau* àquela.

Revedo a prova do teorema de Kronecker (4.2.4, p. 40) vê-se que se tem a seguinte versão mais precisa:

**Teorema 4.2.15 (Kronecker, versão mais precisa)** *Dado um corpo  $K$  e  $f \in K[x]$ , existe uma extensão finita  $E/K$  tal que  $f$  se cinde sobre  $E$ .*

*Demonstração:* Este resultado decorre da prova do teorema de Kronecker, da observação anterior e do seguinte resultado, importante para outros fins:

**Proposição 4.2.16 (multiplicatividade dos graus)** *Se  $K \subseteq E \subseteq L$  são corpos tais que  $L/E$  e  $E/K$  são ambas finitas, então  $L/K$  é finita e  $[L : K] = [L : E] \cdot [E : K]$ .*

*Demonstração:* Seja  $\{\alpha_1, \dots, \alpha_m\}$  uma base de  $L/E$  e seja  $\{\beta_1, \dots, \beta_n\}$  uma base de  $E/K$ . Vejamos que  $\{\alpha_i\beta_j : 1 \leq i \leq m, 1 \leq j \leq n\}$  é uma base de  $L/K$ , o que mostra o que se quer:

Que geram:

Dado  $\gamma \in L$ , resulta do facto de os  $\alpha_s$  gerarem  $L/E$  que existem  $\lambda_1, \dots, \lambda_m \in E$  tais que  $\gamma = \sum_{i=1}^m \lambda_i \alpha_i$ . Agora, por os  $\beta_s$  gerarem  $E/K$ , existem, para cada  $i \in \{1, \dots, m\}$ ,  $\mu_{i1}, \dots, \mu_{in} \in K$  tais que  $\lambda_i = \sum_{j=1}^n \mu_{ij} \beta_j$ . Resulta assim que

$$\gamma = \sum_{i=1}^m \sum_{j=1}^n \mu_{ij} \alpha_i \beta_j.$$

Que são linearmente independentes:

Sejam  $\lambda_{ij} \in K$  tais que  $\sum_{i=1}^m \sum_{j=1}^n \lambda_{ij} \alpha_i \beta_j = 0$ . Mas então, de  $\sum_{i=1}^m \left( \sum_{j=1}^n \lambda_{ij} \beta_j \right) \alpha_i = 0$  e da independência linear dos  $\alpha_s$  sobre  $E$  vem que, para todo  $i \in \{1, \dots, m\}$ ,  $\sum_{j=1}^n \lambda_{ij} \beta_j = 0$ . Resulta agora de independência linear dos  $\beta_s$  sobre  $K$  que  $\lambda_{ij} = 0, \forall i, j$ .

**Definição 4.2.17** *Seja  $E/K$  uma extensão de corpos e sejam  $\alpha_1, \dots, \alpha_n \in E$ . Denota-se por  $K(\alpha_1, \dots, \alpha_n)$  o menor (para a inclusão)<sup>3</sup> subcorpo de  $E$  que contém  $K$  e  $\alpha_1, \dots, \alpha_n$ . Diz-se que  $K(\alpha_1, \dots, \alpha_n)$  é o corpo obtido pela **ad-junção** de  $\alpha_1, \dots, \alpha_n$  a  $K$ . Uma extensão  $E/K$  diz-se uma **extensão simples** se  $E = K(\alpha)$  para algum  $\alpha \in E$ .*

*Observação:*  $K[\alpha_1, \dots, \alpha_n]$  designa o menor subanel de  $E$  que contém  $K$  e  $\alpha_1, \dots, \alpha_n$ .

**Proposição 4.2.18** *Seja  $E/K$  uma extensão e  $\alpha \in E$ . Tem-se que  $K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x] \text{ e } g(\alpha) \neq 0 \right\}$ .*

*Demonstração:* É claro que se  $F$  é um subcorpo de  $E$  tal que  $K \subset F$  e  $\alpha \in F$ , então  $\frac{f(\alpha)}{g(\alpha)} \in F$  ( $\forall f, g \in K[x]$  e  $g(\alpha) \neq 0$ ). Por outro lado, é fácil verificar que  $\left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x] \text{ e } g(\alpha) \neq 0 \right\}$  é um subcorpo que contém  $\alpha$  e  $K$ .

*Exercício:* Seja  $E/K$  uma extensão e  $\alpha_1, \dots, \alpha_n \in E$ . Mostre que se tem  $K(\alpha_1, \dots, \alpha_n) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} : f, g \in K[x_1, \dots, x_n] \text{ e } g(\alpha_1, \dots, \alpha_n) \neq 0 \right\}$ .

**Definição 4.2.19** *Seja  $E/K$  uma extensão. Diz-se que um elemento  $\alpha \in E$  é **algébrico sobre  $K$**  se  $\alpha$  for raiz de algum polinómio não-nulo de  $K[x]$ ; caso contrário, diz-se que  $\alpha$  é **transcendente sobre  $K$** . Diz-se que a **extensão  $E/K$  é algébrica** se todos os elementos de  $E$  forem algébricos sobre  $K$ ; caso contrário diz-se que a **extensão é transcendente**.*

<sup>3</sup>Ver a nota de rodapé da página 41.

*Observação:* Quando se diz que um número complexo é algébrico ou transcendente, está-se implicitamente a referir à extensão  $\mathbb{C}/\mathbb{Q}$ .

*Exemplos:*

1.  $\sqrt[3]{2}$  é algébrico: é raiz de  $x^3 - 2 \in \mathbb{Q}[x]$ .
2.  $e$  e  $\pi$  são transcendentos sobre  $\mathbb{Q}$ .  
(As respectivas provas são longas e difíceis, embora um aluno do 2<sup>o</sup> ano as possa seguir<sup>4</sup>. A prova da transcendência de  $\pi$  é um marco histórico, pois estabeleceu a impossibilidade da quadratura do círculo.)
3.  $\pi i$  é algébrico sobre  $\mathbb{R}$  (*porquê?*).
4. Seja  $K$  um corpo e considere-se a extensão  $K(x)/K$ . O polinómio  $x$  de  $K(x)$  é transcendente sobre  $K$  (*porquê?*).

**Proposição 4.2.20**  $E/K$  finita  $\Rightarrow E/K$  algébrica.

*Demonstração:* Seja  $\alpha \in E$ . Como  $E/K$  tem dimensão finita,  $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$  é linearmente dependente sobre  $K$  para  $n$  suficientemente grande (basta tomar  $n = [E : K]$  (*porquê?*)). Mas isto significa que existem  $c_0, c_1, \dots, c_n \in K$  tais que  $c_0 \cdot 1 + c_1 \alpha + \dots + c_n \alpha^n = 0$ , o que mostra que  $\alpha$  é raiz de  $c_0 + c_1 x + \dots + c_n x^n \in K[x]$ .

Dada uma extensão  $E/K$  e um número  $\alpha \in E$  algébrico sobre  $K$ , seja  $I_\alpha := \{f \in K[x] : f(\alpha) = 0\}$ . Como  $I_\alpha$  é o núcleo do homomorfismo (de anéis)  $K[x] \rightarrow E$  dado por  $f \mapsto f(\alpha)$ , resulta que  $I_\alpha$  é um ideal de  $K[x]$ . Mas como  $K[x]$  é um DIP, tem-se que  $I_\alpha = \langle p_\alpha(x) \rangle$  para algum polinómio  $p_\alpha(x)$ , que podemos escolher de modo a ser mónico (*porquê?*). É claro que  $p_\alpha(x) \in K[x] - (K[x]^* \cup \{0\})$ .

**Afirmação:**  $p_\alpha(x)$  é irredutível.

*Razão:* Se não o fosse, ter-se-ia  $p_\alpha(x) = p_1(x)p_2(x)$  para alguns  $p_1, p_2 \in K[x]$ , não-constantas. Mas então  $0 = p_\alpha(\alpha) = p_1(\alpha)p_2(\alpha) \Rightarrow p_1(\alpha) = 0$  ou  $p_2(\alpha) = 0 \Rightarrow p_1 \in I_\alpha$  ou  $p_2 \in I_\alpha \xrightarrow{\text{(porquê?)}} p_\alpha | p_1$  ou  $p_\alpha | p_2 \xrightarrow{\text{(porquê?)}} p_1$  constante ou  $p_2$  constante, o que fornece a desejada contradição.

*Alternativamente, podemos ver que  $p_\alpha$  é primo:*  $p_\alpha | fg \xrightarrow{\text{(porquê?)}} f(\alpha)g(\alpha) = 0 \Rightarrow \Rightarrow f \in I_\alpha$  ou  $g \in I_\alpha \Rightarrow p_\alpha | f$  ou  $p_\alpha | g$ .

**Definição 4.2.21** Dada uma extensão  $E/K$  e  $\alpha \in E$  algébrico sobre  $K$ , o polinómio mónico de menor grau que tem  $\alpha$  como raiz diz-se **o polinómio irredutível de  $\alpha$  sobre  $K$** , ou **o polinómio mínimo de  $\alpha$  sobre  $K$** , e será aqui denotado por  $\text{Irr}(\alpha, K)$ .

<sup>4</sup>Ver, por exemplo: M. Spivak, *Calculus*, Benjamin 19??, Cap. 20; e P. Morandi, *Field and Galois Theory*, Springer 1996, Cap. III, §14.

*Observação:* Pelo que se viu,  $\langle \text{Irr}(\alpha, K) \rangle = \{f \in K[x] : f(\alpha) = 0\}$ .

*Exemplos:*

1.  $\text{Irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$ , uma vez que este polinómio é mónico, irreductível e tem  $\sqrt{2}$  como raiz.
2.  $\text{Irr}(\sqrt{2}, \mathbb{Q}(\sqrt{2})) = x - \sqrt{2}$ .
3.  $\text{Irr}(i, \mathbb{Q}) = \text{Irr}(i, \mathbb{R}) = x^2 + 1$ .
4.  $\text{Irr}(\sqrt{3} - \sqrt{2}, \mathbb{Q}) = x^4 - 10x^2 + 1$  (*Exercício!*).

Considere-se novamente o homomorfismo  $\varphi_\alpha : K[x] \rightarrow E$ . Como  $f \mapsto f(\alpha)$  acima se viu,  $\text{Ker } \varphi_\alpha = \langle \text{Irr}(\alpha, K) \rangle$ . Por outro lado, é claro que  $\text{Im } \varphi_\alpha = K[\alpha]$ . Pelo teorema do homomorfismo resulta que:

$$K[x]/\langle \text{Irr}(\alpha, K) \rangle \simeq K[\alpha].$$

Mas da própria construção resulta que esta aplicação não só é um isomorfismo de anéis como, por  $\varphi_\alpha(\lambda) = \lambda, \forall \lambda \in K$ , é também um isomorfismo de espaços vectoriais sobre  $K$  (*porquê?*). Conclui-se disto o seguinte:

**Proposição 4.2.22** *Seja  $E/K$  uma extensão de corpos e  $\alpha \in E$  algébrico sobre  $K$ . Então  $K[\alpha] = K(\alpha)$ ,  $K(\alpha) \simeq K[x]/\langle \text{Irr}(\alpha, K) \rangle$  e  $[K(\alpha) : K] = \text{gr}(\text{Irr}(\alpha, K))$ , sendo  $\{1, \alpha, \alpha^2, \dots, \alpha^{\text{gr}(\text{Irr}(\alpha, K)) - 1}\}$  uma base de  $K(\alpha)/K$ .*

*Demonstração:* Tudo resulta do que atrás foi visto e dito, e nada melhor do que tentar perceber os detalhes por si próprio (*e é muito importante que o faça!*).

*Exemplos:*

1.  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ , pois  $x^3 - 2$  é o polinómio irreductível de  $\sqrt[3]{2}$  (é irreductível pelo critério de Eisenstein...) e  $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$  é uma base de  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ .
2.  $[\mathbb{Q}(\sqrt{3} - \sqrt{2}) : \mathbb{Q}] = 4$ , por um dos exemplos dados imediatamente após a definição de  $\text{Irr}(\alpha, K)$ .

Vejamos agora que o conjunto dos números algébricos é fechado para somas e produtos, mais exactamente que os algébricos de uma qualquer extensão formam um corpo. Antes disso, é útil destacar a seguinte caracterização dos números algébricos, practicamente já provada.

**Lema 4.2.23** *Seja  $E/K$  uma extensão arbitrária. Um elemento  $\alpha \in E$  é algébrico sobre  $K$  se e só se  $\alpha$  pertence a um subcorpo  $F$  de  $E$  tal que  $F/K$  é finita.*

*Demonstração:* ( $\Rightarrow$ ) Pela proposição anterior,  $K(\alpha)/K$  é finita.

( $\Leftarrow$ ) Se  $\alpha \in F$ , onde  $K \subseteq F \subseteq E$  e  $F/K$  é finita, então  $F/K$  é algébrica. Em particular,  $\alpha$  é algébrico sobre  $K$ .

Estamos agora prontos para o seguinte:

**Teorema 4.2.24** *Seja  $E/K$  um extensão arbitrária de corpos. O conjunto  $\{\alpha \in E : \alpha \text{ é algébrico sobre } K\}$  é um subcorpo de  $E$ .*

*Demonstração:* Sejam  $\alpha, \beta$  números algébricos de  $E/K$ . Então  $K(\alpha)/K$  e  $K(\beta)/K$  são finitas. Considere-se o subcorpo  $K(\alpha, \beta)$  de  $E$ . É útil resumir as relações entre estes vários subcorpos de  $E$  no seguinte diagrama, onde uma linha ligando dois corpos significa que o que está em cima contém o que se encontra debaixo:

$$\begin{array}{ccc} & & E \\ & & \downarrow \\ & & K(\alpha, \beta) \\ & \swarrow & \searrow \\ K(\alpha) & & K(\beta) \\ & \swarrow & \searrow \\ & & K \end{array}$$

Agora, como  $\text{Irr}(\alpha, K(\beta)) \mid \text{Irr}(\alpha, K)$  (*porquê?*), então  $[K(\alpha, \beta) : K(\beta)] \leq [K(\alpha) : K]$  (*porquê?*) e portanto  $K(\alpha, \beta)/K$  é finita. Assim, como  $\alpha + \beta, \alpha \cdot \beta^{-1}$  (se  $\beta \neq 0$ )  $\in K(\alpha, \beta)$ , resulta do lema anterior que estes elementos são algébricos. Isto completa a prova de que o conjunto dos números algébricos de  $E/K$  é um subcorpo de  $E$ .

*Observações:*

1. Resulta em particular que o conjunto dos números algébricos (de  $\mathbb{C}/\mathbb{Q}$ ) é um corpo, assim como o conjunto dos números algébricos reais (i.e. os de  $\mathbb{R}/\mathbb{Q}$ ).
2. Resulta do lema e teorema anteriores que *todos os números construídos partindo de um número finito de números racionais, e usando  $+$ ,  $-$ ,  $\times$ ,  $\div$  e  $\sqrt[n]{\phantom{x}}$ , são algébricos.*

*Exemplo:* O número  $\frac{\sqrt[7]{\sqrt{3}-\frac{1}{\sqrt{2}}}-\sqrt[5]{\sqrt[9]{7}+\sqrt[7]{5}}}{\sqrt[3]{1+\sqrt[6]{1+\frac{3}{\sqrt{2}}}}+\sqrt[7]{\sqrt{3}+\sqrt[4]{\sqrt{7}+\sqrt[5]{11}}}}$  é algébrico!!

Uma das descobertas por detrás da prova da não existência de fórmulas resolventes para equações (polinomiais) de grau  $\geq 5$  é a de que há polinómios (por exemplo,  $x^5 - 6x + 3$ ) que têm raízes que não são da forma mencionada na observação (2).

*Exemplo:* O número  $\gamma = \frac{\sqrt[3]{1+\sqrt{2}+\frac{\sqrt{2}}{3}}}{\sqrt[5]{2}+\sqrt[3]{7}}$  é algébrico e  $\text{gr}(\text{Irr}(\gamma, \mathbb{Q})) \leq 90$ .

*Razão:* Tem-se a seguinte “torre” de extensões simples:

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{1 + \sqrt{2}}, \sqrt[5]{2}, \sqrt[3]{7})$$

$$\left| \leq 3 \text{ (porquê?)} \right.$$

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{1 + \sqrt{2}}, \sqrt[5]{2})$$

$$\left| \leq 5 \text{ (porquê?)} \right.$$

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{1 + \sqrt{2}})$$

$$\left| \leq 3 \text{ (porquê?)} \right.$$

$$\mathbb{Q}(\sqrt{2})$$

$$\left| = 2 \text{ (porquê?)} \right.$$

$$\mathbb{Q}$$

É agora claro que  $\gamma \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{1 + \sqrt{2}}, \sqrt[5]{2}, \sqrt[3]{7})$  e que, pela multiplicatividade dos graus (4.2.16, p. 44), este corpo tem dimensão, sobre  $\mathbb{Q}$ , menor ou igual que  $2 \cdot 3^2 \cdot 5 = 90$ .

**Definição 4.2.25** *Chama-se corpo de cisão (ou corpo de decomposição ou corpo das raízes) de  $f \in K[x]$  ( $K$  corpo) a uma extensão  $E$  de  $K$  na qual  $f$  se cinde e tal que  $f$  não se cinde em nenhum subcorpo próprio (i.e.  $\neq E$ ) de  $E$ .*

**Proposição 4.2.26** *Todo o polinómio de  $K[x]$  tem um corpo de cisão, qualquer que seja o corpo  $K$ .*

*Demonstração:* Seja  $f \in K[x]$ . Pelo teorema de Kronecker (4.2.4, p. 40), existe uma extensão  $E/K$  na qual  $f$  se cinde. Sejam  $\alpha_1, \alpha_2, \dots, \alpha_n$  as raízes de  $f$  em  $E$ .  $K(\alpha_1, \alpha_2, \dots, \alpha_n)$  é então um corpo de cisão de  $f$  (porquê?).

Vamos agora ver que há só um corpo de cisão de um dado polinómio, a menos de isomorfismo. Para tal começamos com:

**Lema 4.2.27** *Seja  $\sigma : K \rightarrow K'$  um isomorfismo de corpos e  $\sigma^* : K[x] \rightarrow K'[x]$  o correspondente isomorfismo dos anéis de polinómios dado por  $\sigma^*(\sum_{i \geq 0} a_i x^i) = \sum_{i \geq 0} \sigma(a_i) x^i$  (ver exemplo 3, p. 14). Seja  $p \in K[x]$  um polinómio irredutível e*

$p^* = \sigma^*(p) \in K'[x]$ , que é também irredutível (porquê?). Se  $\alpha$  e  $\alpha'$  são raízes de  $p(x)$  e  $p^*(x)$ , respectivamente, em extensões  $E$  e  $E'$  de  $K$ , então existe um único isomorfismo  $\tilde{\sigma} : K(\alpha) \rightarrow K(\alpha')$  que estende  $\sigma$ , i.e.  $\tilde{\sigma}(\lambda) = \sigma(\lambda)$ ,  $\forall \lambda \in K$ .

*Observação:* É muitas vezes conveniente resumir a informação contida na conclusão deste resultado no seguinte diagrama:

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\tilde{\sigma}} & K(\alpha') \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sigma} & K' \end{array}$$

onde as aplicações verticais são inclusões e a aplicação a tracejado é aquela cuja existência se quer provar. Um tal **diagrama** diz-se **comutativo** se as compostas  $\xrightarrow{\tilde{\sigma}} \uparrow$  e  $\uparrow \xrightarrow{\sigma}$  coincidirem, o que neste caso é precisamente equivalente a  $\tilde{\sigma}(\lambda) = \sigma(\lambda)$ ,  $\forall \lambda \in K$  !

*Prova do lema:* É fácil ver que  $\sigma^*(\langle p(x) \rangle) = \langle p^*(x) \rangle$ . Isto significa que o núcleo do homomorfismo  $K[x] \rightarrow K'[x]/\langle p^*(x) \rangle$ , que é sobrejec-

$$f \mapsto [\sigma^*(f)]$$

tivo (porquê?), é  $\langle p(x) \rangle$ . Resulta então do teorema do homomorfismo e da proposição 4.2.22, p. 47 que:

$$K(\alpha) \simeq K[x]/\langle p(x) \rangle \simeq K'[x]/\langle p^*(x) \rangle \simeq K(\alpha').$$

Analizando as aplicações envolvidas, conclui-se que este isomorfismo é dado por  $\sum_{i \geq 0} \lambda_i \alpha^i \mapsto \sum_{i \geq 0} \sigma(\lambda_i) (\alpha')^i$  (alternativamente poder-se-ia ter mostrado directamente que esta aplicação está bem-definida e é um isomorfismo: faça-o como exercício!).

A unicidade resulta facilmente do facto de  $K(\alpha)$  ser gerado, sobre  $K$ , pelas potências de  $\alpha$ .

**Teorema 4.2.28** *Sejam:*  $\sigma : K \rightarrow K'$  um isomorfismo de corpos;  $f \in K[x]$ ;  $f^* = \sigma^*(f) \in K'[x]$  (sendo  $\sigma^*$  como no enunciado do lema anterior);  $E$  um corpo de cisão de  $f$  e  $E'$  um corpo de cisão de  $f^*$ .

Então existe um isomorfismo  $\hat{\sigma} : E \rightarrow E'$  tal que  $\hat{\sigma}|_K = \sigma$ . Esquemáticamente:

$$\begin{array}{ccc} E & \xrightarrow{\hat{\sigma}} & E' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sigma} & K' \end{array}$$

*Demonstração:* (Indução sobre  $[E : K]$ )

Se  $[E : K] = 1$ , então  $E = K$  (porquê?) o que significa que  $f$  se cinde em  $K[x]$  e portanto, como  $\sigma^*$  é um isomorfismo,  $f^*$  também se cinde em  $K'[x]$ . Assim,  $E' = K'$  e basta (de facto, tem-se de) tomar  $\hat{\sigma} = \sigma$ .

Suponhamos agora que  $[E : K] > 1$ . Seja  $p(x)$  um factor irreduzível de  $f(x)$  (em  $K[x]$ ) com grau  $\geq 2$  (porque é que existe?) e seja  $\alpha \in E$  uma das raízes de  $p(x)$  (porque é que  $p(x)$  tem raízes em  $E$ ?). Seja  $p^* = \sigma^*(p) \in K'[x]$ . Então  $p^* | f^*$  (porquê?). Seja  $\alpha' \in E'$  uma raiz de  $p^*(x)$  (porque é que existe?). Pelo lema anterior existe um isomorfismo  $\tilde{\sigma} : K(\alpha) \rightarrow K'(\alpha')$  estendendo  $\sigma$ .

$$\begin{array}{ccc} E & \xrightarrow{\tilde{\sigma}} & E' \\ \uparrow & & \uparrow \\ K(\alpha) & \xrightarrow{\tilde{\sigma}} & K'(\alpha') \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sigma} & K' \end{array}$$

Como  $[E : K] = [E : K(\alpha)] \cdot [K(\alpha) : K]$  e  $[K(\alpha) : K] \geq 2$ , tem-se  $[E : K(\alpha)] < [E : K]$ . Por hipótese de indução (explicita-a!), existe  $\hat{\sigma} : E \rightarrow E'$  estendendo  $\tilde{\sigma}$ , o que mostra o que se queria (porquê?).

**Corolário 4.2.29** *Dois quaisquer corpos de cisão de um polinómio  $f \in K[x]$ , onde  $K$  é um corpo, são isomorfos (por um isomorfismo que deixa fixos os elementos de  $K$ ).*

*Demonstração:* Basta aplicar o teorema anterior com  $K' = K$  e  $\sigma = \text{id}_K$ .

**Corolário 4.2.30 (E. H. Moore (1862–1932), 1893)** *Dois corpos finitos com o mesmo número de elementos são isomorfos.*

*Demonstração:* Viu-se na prova do teorema de Galois sobre a existência de corpos finitos (4.2.10, p. 42) que um corpo com  $p^n$  elementos (onde  $p$  é um número primo e  $n \in \mathbb{N}$ ) é um corpo de cisão do polinómio  $x^{p^n} - x \in \mathbb{Z}_p[x]$ .

*Notação:* Denota-se por  $\mathbb{F}_q$  ou por **GF**( $q$ ) (de **G**alois **F**ield) “o” corpo finito com  $q$  elementos, a que por vezes se chama **o corpo de Galois com  $q$  elementos** (que, como se viu, só existe se  $q = p^n$  para alguns  $p$  primo,  $n \in \mathbb{N}$ ).

### 4.3 Uma aplicação dos corpos finitos.

A título de exemplo do que se pode fazer com os resultados que vimos atrás, descrevemos nesta secção uma prova extremamente elegante de um resultado de Fermat que descreve os primos que são diagonais de triângulos rectângulos de lados inteiros (ver p. 6). Para tal começamos por resolver o seguinte problema:

**Questão:** Para que primos  $p$  é que  $-1$  é um quadrado módulo  $p$ ? Equivalentemente, quando é que  $\mathbb{F}_p (= \mathbb{Z}_p)$  tem uma raiz quadrada de  $-1$ ?

*Resposta:* Quando  $p = 2$  a resposta é óbvia. Suponhamos pois  $p \neq 2$ . Seja  $E$  uma extensão de  $\mathbb{F}_p$  na qual  $x^2 + 1 \in \mathbb{F}_p[x]$  se cinde, e seja  $i$  uma das raízes deste polinómio

em  $E$ . Observe que, para  $a \in E$ , se tem:  $a \in \mathbb{F}_p$  se e só se  $a^p = a$  (*porquê?*). Assim, em particular,  $i \in \mathbb{F}_p \Leftrightarrow i^p = i$ . Mas,  $i^p = (i^2)^{\frac{p-1}{2}} i = (-1)^{\frac{p-1}{2}} i$ , e isto é igual a  $i$  quando e só quando  $(-1)^{\frac{p-1}{2}} = 1$  (em  $\mathbb{F}_p$ ) (*porquê?*), o que acontece se e só se  $p \equiv 1 \pmod{4}$ .

**Conclusão:**  $x^2 \equiv -1 \pmod{p}$  ( $p$  primo) tem solução quando e só quando  $p = 2$  ou  $p \equiv 1 \pmod{4}$ .

Seja agora  $p$  um primo congruente com 1 módulo 4. Pelo que se viu,  $p|m^2 + 1$  para algum  $m \in \mathbb{Z}$ . Isto implica que, em  $\mathbb{Z}[i]$ ,  $p|(m+i)(m-i)$ . Como claramente (*porquê?*)  $p \nmid m+i$  e  $p \nmid m-i$ , resulta que  $p$  não é primo em  $\mathbb{Z}[i]$ . Mas então, como  $\mathbb{Z}[i]$  é um DIP,  $p$  é redutível, e portanto  $\exists a, b \in \mathbb{Z}$  tais que  $a + bi | p$ . É agora fácil ver (*faça-o como exercício*) que  $p = a^2 + b^2$ .

*Exercício:*

- Seja  $p$  um primo ímpar e  $E$  uma extensão de  $\mathbb{F}_p$  na qual  $x^2 + 1$  se cinde. Designando por  $i$  uma das raízes de  $x^2 + 1$  em  $E$ , use a relação  $(1+i)^2 = 2i$  para determinar quais os primos  $p$  tais que 2 é um quadrado módulo  $p$ .
- Use (a) para provar o seguinte resultado de L. Euler: se  $p$  é um primo tal que  $p \equiv 3 \pmod{4}$  e  $2p + 1$  é primo, então  $2p + 1 | 2^p - 1$  (em particular, este número, dito de Mersenne, não é primo para  $p > 3$  nas condições descritas; exemplos:  $23 | 2^{11} - 1, 47 | 2^{23} - 1$ ).

*Observação:* Pode agora perceber-se a utilidade da introdução do conceito de polinómio, como “expressão abstracta” ou como aplicações definidas em  $\mathbb{N}_0$  e de suporte finito (ver 1.2), distinguindo-os assim das respectivas funções polinomiais. De facto, usando o “pequeno” teorema de Fermat, vê-se que, para  $p$  primo, há apenas um número finito de funções polinomiais de  $\mathbb{Z}_p$  em  $\mathbb{Z}_p$  (por exemplo:  $x \mapsto x^p$  é igual a  $x \mapsto x$ ). Ora, como se viu, os polinómios permitem construir uma infinidade de extensões de  $\mathbb{Z}_p$ , para cada primo  $p$ , e tais extensões permitem obter resultados não triviais sobre, por exemplo, como acaba de ser ilustrado, os números inteiros!

## 4.4 Brevíssima introdução à teoria de Galois

**A fórmula resolvente do 3º grau** (Scipione del Ferro–Tartaglia–Cardano, [1500–45]): Pretende-se determinar as raízes de  $x^3 + ax^2 + bx + c = 0$  ( $a, b, c \in \mathbb{C} \dots$ ). Fazendo a mudança de variável  $y = x + \frac{a}{3}$  elimina-se o termo em  $x^2$ , reduzindo o problema a encontrar as raízes de  $y^3 + py + q = 0$  (em que  $p, q \in \mathbb{C}$  são funções polinomiais de  $a, b, c$ : explicita essa correspondência). Pondo  $y = u+v$ , obtém-se  $u^3 + v^3 + (3uv+p)(u+v) + q = 0$ . Agora,  $u$  e  $v$  podem ser determinados de modo a se ter  $3uv + p = 0$ , pois o sistema 
$$\begin{cases} u + v = y \\ uv = -\frac{p}{3} \end{cases}$$
 é equivalente a uma equação do 2º grau e estas têm sempre

soluções em  $\mathbb{C}$ .<sup>5</sup> Mas então  $u^3 + v^3 + q = 0$ . Substituindo  $v$  por  $-\frac{p}{3u}$  (isto se  $u \neq 0$ ; deixa-se ao cuidado do leitor perceber o que se passa no caso de se ter  $u = 0$ ), obtém-se  $u^6 + qu^3 - (\frac{p}{3})^3 = 0$ , que é uma equação do 2º grau em  $u^3$ ! Esta equação permite encontrar  $u$ ; depois é só fazer  $v = -\frac{p}{3u}$ ,  $y = u + v$  e finalmente  $x = y - \frac{a}{3}$ .

**A fórmula resolvente do 4º grau** (Lodovico Ferrari, algures no período [1539–1545]): Pretende-se determinar as raízes de  $x^4 + ax^3 + bx^2 + cx + d = 0$  ( $a, b, c, d \in \mathbb{C} \dots$ ). Fazendo  $y = x + \frac{a}{4}$ , elimina-se o termo em  $x^3$ , reduzindo o problema a encontrar as raízes de  $y^4 + ry^2 + sy + t = 0$  (\*) (em que  $r, s, t \in \mathbb{C}$  são funções polinomiais de  $a, b, c, d$ : explicita essa correspondência).

*Método de Descartes, 1637:*

Procurem-se  $u, v, w$  tais que:  $y^4 + ry^2 + sy + t = (y^2 + uy + v)(y^2 - uy + w)$  (\*\*), o que reduz o problema à resolução de duas equações do 2º grau. Igualando os coeficientes respectivos, obtém-se o sistema:

$$\begin{cases} v + w - u^2 = r \\ uw - uv = s \\ vw = t \end{cases}$$

que é equivalente a (multiplique a 1ª equação por  $u$  e adicione o resultado à 2ª; tem-se assim  $w$  em função de  $u$  e depois, substituindo na 1ª, vem  $v$  em função de  $u$ ; finalmente substitua-se  $w$  e  $v$  na 3ª equação pelas respectivas expressões em  $u$  (isto se  $u \neq 0$ ; deixa-se novamente ao cuidado do leitor analisar o caso  $u = 0$ ):

$$\begin{cases} w = \frac{1}{2}(u^2 + r + \frac{s}{u}) \\ v = \frac{1}{2}(u^2 + r - \frac{s}{u}) \\ u^6 + 2ru^4 + (r^2 - 4t)u^2 - s^2 = 0, \end{cases}$$

sendo esta última equação uma cúbica em  $u^2$ !! Usando a fórmula resolvente do 3º grau encontram-se os valores de  $u$ , obtendo-se os de  $v$  e  $w$  das duas primeiras equações do sistema anterior. Depois resolvem-se as correspondentes equações do 2º grau em (\*\*), obtendo-se os valores de  $y$  que são solução de (\*) e, finalmente, é só usar  $x = y - \frac{a}{4}$  para obter as soluções da equação inicial.

Do trabalho de Vandermonde (1735–96), Lagrange (1736–1813), Gauss (1777–1855), Ruffini (1765–1822), Niels Henrik Abel (1802–29) e, fundamentalmente, de Évariste Galois (1811–32), sobre a existência de “fórmulas resolventes” de grau  $\geq 5$ , resultaram muitas das noções que temos vindo a estudar. Vamos agora fazer uma descrição um tanto ou quanto concisa do

<sup>5</sup>É por esta razão que  $\mathbb{C}$  é o sítio “certo” para resolver equações do 3º grau, pelo menos usando o método indicado. Prova-se que, de facto, uma “fórmula resolvente” para equações do 3º grau com coeficientes reais não pode deixar de passar por  $\mathbb{C}$  (ver I. M. Isaacs, *Solution of polynomials by real radicals*, Amer. Math. Monthly **92** (1985) 571–575). Observe-se que os números complexos foram introduzidos por matemáticos do século XVI precisamente para “explicar” certos problemas com a fórmula resolvente de del Ferro–Tartaglia–Cardano.

principal resultado de Galois, num rearranjo feito por E. Artin nos anos 30, que descreve uma condição necessária e suficiente para um polinómio ter como raízes números que são combinações finitas de elementos do corpo dos seus coeficientes, usando as operações de corpo e raízes de índice arbitrário. Para precisar o que se quer dizer com isto, introduz-se os seguintes conceitos:

**Definição 4.4.1** *Uma extensão  $E/K$  diz-se **pura** se  $E = K(\alpha)$ , onde  $\alpha \in E$  é tal que  $\alpha^m \in K$  para algum  $m \in \mathbb{N}$  (i.e.  $\alpha$  é um “radical” de  $K$ ).*

**Definição 4.4.2** *Uma extensão  $E/K$  diz-se uma **radical** se existir uma “torre” de corpos:*

$$K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_t = E$$

*tal que cada  $E_{i+1}/E_i$  é uma extensão pura, para  $i = 0, 1, \dots, t-1$ .*

*Um polinómio  $f \in K[x]$  ( $K$  um corpo), diz-se **resolúvel por radicais** (sobre  $K$ ) se existir uma extensão radical  $E/K$  tal que  $f$  se cinde em  $E$ .*

Repare-se que numa extensão radical  $E/K$ , os elementos de  $E$  são “combinações polinomiais” (que, neste caso, coincidem com as fracções racionais (porquê?)) de radicais de radicais de ... etc (em número finito) ... de elementos de  $K$ , com coeficientes em  $K$ . Ou seja, os elementos de  $E$  são da forma descrita na observação 2, p. 48, com  $\mathbb{Q}$  substituído por  $K$ . A definição acabada de dar de polinómio resolúvel por radicais é pois equivalente a dizer que as suas raízes, num corpo de cisão, são “combinações” de radicais de radicais de ... etc (em número finito) ... de elementos do seu corpo dos coeficientes.

*Observação:* Não é difícil, usando as “fórmulas resolventes”, provar que todos os polinómios de graus 2, 3 e 4, com coeficientes em corpos de característica  $\neq 2, 3$ , são resolúveis por radicais.

**Definição 4.4.3** *Seja  $E/K$  uma extensão de corpos.*

*O grupo de Galois de  $E/K$ , que será denotado por  $\text{Gal}(E/K)$ , é o conjunto dos automorfismos de  $E$  que deixam fixos os elementos de  $K$ , e que se dizem os **automorfismos de Galois de  $E/K$** , munido da operação usual de composição de funções.*

*Se  $f \in K[x]$ , chama-se grupo de Galois de  $f$  sobre  $K$  ao grupo  $\text{Gal}(E/K)$ , onde  $E$  é um qualquer corpo de cisão de  $f$  sobre  $K$ , que denotaremos por  $\text{Gal}(f/K)$  (porque é que está bem-definido?).*

Vejamos que os automorfismos de Galois de uma extensão permutam as raízes, nessa extensão, dos polinómios com coeficientes no corpo de base.

**Lema 4.4.4** *Se  $f \in K[x]$  tem uma raiz  $\alpha$  numa extensão  $E/K$ , então, para cada  $\sigma \in \text{Gal}(E/K)$ ,  $\sigma(\alpha)$  é também uma raiz de  $f$ .*

*Demonstração:* Se  $f = \sum_{i=0}^n c_i x^i$ , então  $0 = \sigma(0) = \sigma(f(\alpha)) = \sigma(\sum_{i=0}^n c_i \alpha^i) = \sum_{i=0}^n \sigma(c_i \alpha^i) = \sum_{i=0}^n \sigma(c_i) \sigma(\alpha^i) = \sum_{i=0}^n c_i \sigma(\alpha)^i = f(\sigma(\alpha))$ .

**Proposição 4.4.5** *Seja  $K$  um corpo,  $f \in K[x]$ . Se  $f$  tem  $n$  raízes distintas num seu corpo de cisão, então  $\text{Gal}(f/K)$  é isomorfo a um subgrupo de  $\mathcal{S}_n$ .*

*Demonstração:* Sejam  $\alpha_1, \alpha_2, \dots, \alpha_n$  as raízes de  $f$  num seu corpo de cisão. Para cada  $\sigma \in \text{Gal}(f/K)$  resulta do lema anterior que  $\sigma(\alpha_i) = \alpha_{\tilde{\sigma}(i)}$  para algum  $\tilde{\sigma}(i) \in \{1, 2, \dots, n\}$ . Como  $\sigma$  é injectiva, é fácil concluir que a função  $\tilde{\sigma} : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  que se assim se obtém também é injectiva, e portanto bijectiva (*porquê?*). Deixa-se como exercício verificar que a aplicação  $\text{Gal}(E/K) \rightarrow \mathcal{S}_n$  é um homomorfismo (de grupos) injectivo.  
 $\sigma \mapsto \tilde{\sigma}$

*Exemplos:*

1. Como  $\mathbb{C} = \mathbb{R}(i)$ , resulta que  $\sigma \in \text{Gal}(\mathbb{C}/\mathbb{R})$  é completamente determinado por  $\sigma(i)$ . Mas, como  $i$  é raiz de  $x^2 + 1$ , tem-se pelo lema anterior que  $\sigma(i) = \pm i$ . Conclui-se assim que  $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{z \mapsto z, z \mapsto \bar{z}\}$ .
2. Vejamos que  $\text{Gal}(x^3 - 2/\mathbb{Q}) \simeq \mathcal{S}_3$ .

Como sabemos, pelo último resultado, que  $\text{Gal}(x^3 - 2/\mathbb{Q})$  é isomorfo a um subgrupo de  $\mathcal{S}_3$ , basta mostrar que  $\#\text{Gal}(x^3 - 2/\mathbb{Q}) = 6$ .

Em primeiro lugar, como (em  $\mathbb{C}$ )

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2) \quad (\text{porquê?}),$$

onde  $\omega$  é um raiz cúbica primitiva da unidade, resulta que o corpo de cisão de  $x^3 - 2$ , em  $\mathbb{C}$ , é  $\mathbb{Q}(\sqrt[3]{2}, \omega)$  (*porquê?*).

Tem-se (*porquê?*):

$$\begin{aligned} \text{Irr}(\sqrt[3]{2}\omega^i, \mathbb{Q}) &= x^3 - 2 \text{ para } i = 0, 1, 2; \\ \text{Irr}(\omega, \mathbb{Q}) &= x^2 + x + 1; \\ \text{Irr}(\omega, \mathbb{Q}(\sqrt[3]{2}\omega^i)) &| \text{Irr}(\omega, \mathbb{Q}) \text{ para } i = 0, 1, 2; \\ \text{Irr}(\sqrt[3]{2}\omega^i, \mathbb{Q}(\omega)) &| \text{Irr}(\sqrt[3]{2}\omega^i, \mathbb{Q}) \text{ para } i = 0, 1, 2, \end{aligned}$$

e portanto (*porquê?*), para  $i = 0, 1, 2$ :

$$\begin{array}{ccc} & \leq_2 & \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}\omega^i, \omega) \\ & & \leq_3 \\ \mathbb{Q}(\sqrt[3]{2}\omega^i) & & \mathbb{Q}(\omega) \\ & \text{3} & \\ & & \text{2} \\ & & \mathbb{Q} \end{array}$$

Resulta, pela multiplicatividade dos graus (proposição 4.2.16, p. 44), que  $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] \leq 6$  e divisível por 2 e 3. Conclui-se assim que  $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$  (sendo  $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \omega, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega\}$  uma base da extensão em consideração (ver a prova de 4.2.16)). Mais ainda, fica assim provado que  $x^2 - 3$  é irredutível em  $\mathbb{Q}(\omega)[x]$  (porquê?) e que também  $x^2 + x + 1$  é irredutível em  $\mathbb{Q}(\sqrt[3]{2}\omega^i)[x]$  para  $i = 0, 1, 2$ .

Usando duas vezes o lema sobre a extensão de isomorfismos (4.2.27 (p. 49)), primeiro para  $x^3 - 2$  e depois para  $x^2 + x + 1$ , e fazendo-o para cada par de raízes destes, o que pode ser esquematizado do seguinte modo:

$$\begin{array}{ccccc}
 \mathbb{Q}(\sqrt[3]{2}, \omega) & \dashrightarrow & & \mathbb{Q}(\sqrt[3]{2}, \omega) & \\
 \uparrow & & \nearrow & \uparrow & \nwarrow \\
 \mathbb{Q}(\sqrt[3]{2}) & \equiv & \mathbb{Q}(\sqrt[3]{2}) & \mathbb{Q}(\sqrt[3]{2}\omega) & \mathbb{Q}(\sqrt[3]{2}\omega^2) \\
 \uparrow & \xrightarrow{\text{id}} & \nwarrow & \uparrow & \nearrow \\
 \mathbb{Q} & & & \mathbb{Q} & 
 \end{array}$$

(onde as setas a tracejado no topo representam as duas possíveis extensões de *cada uma* das três no meio), mostra-se finalmente a existência de seis automorfismos de  $\mathbb{Q}(\sqrt[3]{2}, \omega)$ .

*Exercício:* Descreva esses seis automorfismos explicitamente.

Mais geralmente, para polinómios do tipo  $x^m - a$  tem-se:

**Proposição 4.4.6** *Seja  $K$  um subcorpo de  $\mathbb{C}$  e  $x^m - a \in K[x]$  ( $m \in \mathbb{N}$ ). Tem-se que  $\text{Gal}(x^m - a/K)$  é isomorfo a um subgrupo do grupo  $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$ , que consiste no conjunto  $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$  munido da operação dada por  $(a, b) \cdot (c, d) = (a + bc, bd)$  ( $a, c \in \mathbb{Z}_m$ ;  $b, d \in \mathbb{Z}_m^*$ ).*

*Exercício:* Verifique que  $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$  é de facto um grupo.

*Demonstração:* Se  $\alpha \in \mathbb{C}$  é uma raiz  $m$ -ésima de  $a$  e  $\zeta$  é uma raiz primitiva  $m$ -ésima da unidade (i.e.  $\zeta^m = 1$  e  $\zeta^t \neq 1, \forall 0 < t < m$ ; por exemplo:  $\zeta = \cos \frac{2\pi}{m} + i \sin \frac{2\pi}{m}$ ), então:

$$x^m - a = \prod_{i=0}^{m-1} (x - \alpha\zeta^i) \quad (\text{porquê?}).$$

Resulta disto que o corpo de cisão, em  $\mathbb{C}$ , de  $x^m - a$  é  $K(\alpha, \zeta)$  (porquê?). Assim um elemento  $\sigma \in \text{Gal}(x^m - a/K)$  é completamente determinado por  $\sigma(\alpha)$  e  $\sigma(\zeta)$ . Como os automorfismos de Galois permutam as raízes de polinómios com coeficientes no corpo de base, tem-se:  $\sigma(\alpha) = \alpha\zeta^{i_\sigma}$  e  $\sigma(\zeta) = \zeta^{j_\sigma}$  (porquê?), para alguns  $i_\sigma, j_\sigma \in \{0, 1, \dots, m-1\}$ .

Vejamus que  $j_\sigma$  é primo com  $m$ , para todo o  $\sigma \in \text{Gal}(x^m - a/K)$ . De facto, fazendo  $d = (j_\sigma, m)$ , tem-se:  $\sigma(\zeta^{\frac{m}{d}}) = \sigma(\zeta)^{\frac{m}{d}} = \zeta^{j_\sigma \cdot \frac{m}{d}} = \zeta^{m \cdot \frac{j_\sigma}{d}} = 1$ . Como  $\sigma$  é

injectiva, resulta que  $\zeta^{\frac{m}{d}} = 1$  e portanto, como  $\zeta$  é uma raiz primitiva  $m$ -ésima da unidade, vem que  $d = 1$ . Assim a aplicação:

$$\begin{aligned} \text{Gal}(x^m - a/K) &\rightarrow \mathbb{Z}_m \rtimes \mathbb{Z}_m^* \\ \sigma &\mapsto ([i_\sigma]_m, [j_\sigma]_m) \end{aligned}$$

está bem-definida e deixa-se como exercício a verificação que é um homomorfismo (de grupos) injectivo.

*Exercício:*

- (a) Verifique que  $\mathbb{Z}_3 \rtimes \mathbb{Z}_3^* \simeq \mathcal{S}_3$ .
- (b) Mostre que se  $a \in \mathbb{Z} - \{\pm 1\}$  é livre de quadrados e  $p \in \mathbb{N}$  é um número primo, então  $\text{Gal}(x^p - a/\mathbb{Q}) \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p^*$ .

*Observação:* O grupo  $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$  é um exemplo daquilo a que se chama um “produto semi-directo” (de  $\mathbb{Z}_m$  e  $\mathbb{Z}_m^*$ , neste caso). É um exercício simples verificar que  $\mathbb{Z}_m$  pode ser visto como um subgrupo de  $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$  através de “injecção” natural:

$$\begin{aligned} \mathbb{Z}_m &\rightarrow \mathbb{Z}_m \rtimes \mathbb{Z}_m^* , \\ x &\mapsto (x, 1) \end{aligned}$$

e que como tal é um subgrupo normal, tendo-se ainda que  $\mathbb{Z}_m \rtimes \mathbb{Z}_m^* / \mathbb{Z}_m \simeq \mathbb{Z}_m^*$ .

**Definição 4.4.7** Um grupo  $G$  diz-se **resolúvel** se existir uma cadeia de subgrupos:

$$\{1\} = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_{n-1} \subset G_n = G \quad (n \in \mathbb{N})$$

tal que, para cada  $i \in \{1, \dots, n\}$ ,  $G_{i-1} \triangleleft G_i$  e  $G_i/G_{i-1}$  é abeliano.

*Exemplos:*

1.  $\mathbb{Z}_m \rtimes \mathbb{Z}_m^*$  é resolúvel. Resulta da observação anterior que a cadeia

$$\{1\} \triangleleft \mathbb{Z}_m \triangleleft \mathbb{Z}_m \rtimes \mathbb{Z}_m^*$$

satisfaz as condições requeridas.

2.  $\mathcal{S}_4$  é resolúvel (Clark, p. 63).
3.  $\mathcal{S}_5$  **não** é resolúvel (Clark, p. 63).

**Proposição 4.4.8** *Tem-se que:*

1. Subgrupos de grupos resolúveis são resolúveis.
2. Quocientes de grupos resolúveis são resolúveis.
3. Dado um grupo  $G$  e  $H \triangleleft G$ , tem-se:  $G$  é resolúvel  $\Leftrightarrow H$  e  $G/H$  são resolúveis.

4. Um grupo  $G$  é resolúvel sse existir uma cadeia  $\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$  tal que  $G_i/G_{i-1}$  é resolúvel ( $\forall i = 1, 2, \dots, n$ ).

*Demonstração:* Ver Clark, pp. 53–57.

**Corolário 4.4.9**  $\text{Gal}(x^m - a/K)$  é um grupo resolúvel, para todo o subcorpo  $K$  de  $\mathbb{C}$ ,  $a \in K$  e  $m \in \mathbb{N}$ .

*Demonstração:* Resulta imediatamente de (1) da última proposição e da penúltima.

**Proposição 4.4.10 (Galois)** *Seja  $K \subseteq F \subseteq E$  uma torre de corpos, onde  $E$  é um corpo de cisão de algum polinómio de  $K[x]$ . Então:  $\text{Gal}(E/F)$  é um subgrupo normal de  $\text{Gal}(E/K)$  quando e só quando  $F$  é também um corpo de cisão de um polinómio de  $K[x]$  e, neste caso,*

$$\text{Gal}(F/K) \simeq \text{Gal}(E/K)/\text{Gal}(E/F).$$

*Esquemáticamente:*

$$G \left\{ \begin{array}{l} H \left\{ \begin{array}{l} E \\ | \\ F \end{array} \right\} \\ | \\ K \end{array} \right\} G/H$$

*Demonstração:* Limitamo-nos a esboçar a prova do “quando”.

Seja então  $F = K(\alpha_1, \alpha_2, \dots, \alpha_n)$ , onde  $\alpha_1, \alpha_2, \dots, \alpha_n$  são as raízes de um polinómio  $f \in K[x]$ . Como  $\sigma \in \text{Gal}(E/K)$  permuta as raízes de  $f$ , conclui-se que  $\sigma(F) \subseteq F$ . Portanto, a aplicação:

$$\begin{aligned} \psi : \text{Gal}(E/K) &\rightarrow \text{Gal}(F/K) \\ \sigma &\mapsto \sigma|_F \end{aligned}$$

está bem definida.

É fácil ver que  $\psi$  é um homomorfismo (de grupos) e que  $\text{Ker } \psi = \text{Gal}(E/F)$ , o que mostra que este é um subgrupo normal de  $\text{Gal}(E/K)$ . A sobrejectividade de  $\psi$  decorre imediatamente do resultado sobre a existência de extensões de isomorfismos a corpos de cisão (teorema 4.2.28, p. 50):

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E \\ \uparrow & & \uparrow \\ F & \xrightarrow{\tau} & F \\ & \swarrow \quad \searrow & \\ & K & \end{array} \Rightarrow \psi(\sigma) = \tau.$$



com, para  $i = 1, \dots, s$ :

$$G_i/G_{i-1} \simeq \text{Gal}(\hat{E}_i/\hat{E}_{i-1}),$$

que é um grupo resolúvel pelo corolário 4.4.9, p. 58. Pela proposição anterior e o facto de quocientes de grupos resolúveis serem resolúveis, resulta que  $\text{Gal}(f/K)$  é resolúvel. Fica assim esboçada uma prova de uma das metades de:

**Teorema 4.4.13 (Galois, 1829)** *Seja  $K$  um subcorpo de  $\mathbb{C}$  e  $f \in K[x]$ . Então  $f$  é resolúvel por radicais sse  $\text{Gal}(f/K)$  for um grupo resolúvel.*

*Demonstração:* Ver Clark, p. 135, ou Rotman, p. 55.

**Corolário 4.4.14 (Teorema de Abel–Ruffini)** *Existem polinómios do 5º grau que não são resolúveis por radicais.*

*Esboço de prova:* Seja  $f(x) = x^5 - 4x + 2$  e seja  $G$  o seu grupo de Galois que, pela proposição 4.4.5 (p. 55), podemos considerar como sendo um subgrupo de  $\mathcal{S}_5$ . Seja  $E$  o corpo de cisão de  $f(x)$  em  $\mathbb{C}$ . Pelo teorema 4.4.12 tem-se que  $\#G = [E : \mathbb{Q}]$ . Agora, se  $\alpha \in E$  é uma raiz de  $f$ , então como  $f$  é irreduzível em  $\mathbb{Q}[x]$  (*porquê?*) tem-se que  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$  (*porquê?*), e portanto  $5 | \#G$  (*porquê?*). Pelo teorema de Cauchy provado em Álgebra I, resulta que  $G$  contém um 5–ciclo. Por outro lado, o estudo do gráfico de  $f$  revela que  $f(x)$  tem exactamente 3 raízes reais, e portanto 2 não–reais, necessariamente conjugadas (*porquê?*). Mas então a aplicação  $z \mapsto \bar{z}$  de  $\mathbb{C}$  induz um automorfismo de  $E$  (*porquê?*) que, como elemento de  $G$ , é uma transposição (= 2–ciclo) (*porquê?*). Mas prova-se (ver Clark, §86, p. 64) que um qualquer 5–ciclo e uma transposição geram  $\mathcal{S}_5$ . Conclui-se assim que  $G = \mathcal{S}_5$ , ou seja  $\text{Gal}(f/\mathbb{Q}) \simeq \mathcal{S}_5$ , que não é resolúvel. Pelo teorema de Galois acabado de mencionar, resulta que o polinómio  $x^5 - 4x + 2$ , ou um outro qualquer polinómio do 5º grau com coeficientes em  $\mathbb{Q}$  que seja irreduzível e tenha exactamente 3 raízes reais em  $\mathbb{C}$ , não é resolúvel por radicais.

*Observação:* Para ver a teoria de Galois na sua forma original, consultar: [4], o apêndice 4 de [3] e [5]. A prova de N. H. Abel da inexistência de uma “fórmula resolvente” do 5º grau encontra-se no seu artigo *Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré*, J. reine angew. Math. **1** (1826) 65–84.

# Bibliografia

“... Mas todas estas surpreendentes invenções, de que altura não serão dominadas pelo espírito Daquele que imaginou o meio de comunicar os seus mais secretos pensamentos a qualquer outra pessoa, esteja ela separada dele por uma muito longa distância ou por um muito grande intervalo de tempo, de falar aos que estão nas Índias, aos que ainda não nasceram e não nascerão antes de mil, ou dez mil anos? E com que facilidade! Pela combinação de vinte caracteres sobre uma folha! Que a invenção do alfabeto seja portanto o selo de todas as belas descobertas humanas...”

Galileu Galilei, *Diálogo dos Grandes Sistemas*, Gradiva 1979

## [Básicos]

- [1] A. Clark, *Elements of Abstract Algebra*, Dover, 1984.
- [2] M. Artin, *Algebra*, Prentice–Hall, 1991.
- [3] J. Rotman, *Galois Theory*, Springer–Verlag, 1990.

## [Perspectiva histórica]

- [4] H. M. Edwards, *Galois Theory*, Springer–Verlag, 1984.
- [5] J.-P. Tignol, *Galois’ Theory of Algebraic Equations*, Longman, 1988.

## [Outros]

- [6] C. R. Hadlock, *Field Theory and Its Classical Problems*, Math. Assoc. Amer., 1978.
- [7] T. W. Hungerford, *A Counterexample in Galois Theory*, Amer. Math. Monthly (Jan 1990) 54–57.
- [8] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer–Verlag, 2<sup>a</sup> edição, 1990.
- [9] J. Stillwell, *Galois Theory for Beginners*, Amer. Math. Monthly (Jan 1994) 22–27.

## [Sobre Galois]

- [10] R. Bourgne, J.-P. Azra, *Évariste Galois: écrits et mémoires mathématiques*, Gauthier–Villards, 1962.
- [11] T. Rotman, *Genius and Biographers: the fictionalization of Évariste Galois*, Amer. Math. Monthly **89** (1982) 84–106.

[12] (vários autores), *Présence d'Évariste Galois*, Publication de l'A.P.M.E.P., n<sup>o</sup> 48, 1982.

[Sobre **Emmy Noether**]

[13] J. W. Brewer, M. K. Smith, *Emmy Noether: a tribute to her life and work*, Marcel Dekker, 1981.

[14] A. Dick, *Emmy Noether 1882–1935*, Birkhäuser, 1970.