TEXTOS DE MATEMÁTICA

ANÉIS E CORPOS
— uma introdução —

Gracinda M. S. Gomes

A quadratura do círculo é possível?

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DE LISBOA

Departamento de Matemática

ANÉIS E CORPOS

– uma introdução –

Gracinda M. S. Gomes

Departamento de Matemática

Faculdade de Ciências da Universidade de Lisboa

2ª Edição

2021

Classificação AMS (2020): 97H40; 12-01

ISBN (2ª Edição): 978-972-8394-31-8

Editor: Universidade de Lisboa. Faculdade de Ciências. Departamento de Matemática

Suporte: Electrónico

Formato: PDF

Aos meus pais e ao meu marido

Prefácio

Nesta nova versão do livro, clarificamos aspectos do texto inicial, em particular, revemos algumas demonstrações e reordenamos certos conceitos, resultados e exercícios, com o objectivo de facilitar a compreensão da matéria apresentada.

Agradecemos aos muitos alunos da disciplina Álgebra II, do 2º ano da Licenciatura em Matemática da Faculdade de Ciências da Universidade de Lisboa, os comentários interessados e as palavras de apreço que nos fizeram chegar ao longo dos anos. Um obrigado, em particular, ao Bernardo H. Fernandes e ao Rui Martins.

A preparação deste texto contou com o apoio do Centro de Matemática Computacional e Estotástica, CEMAT, no âmbito das suas actividades de divulgação da Álgebra, área de investigação do Centro, através dos Projectos UID/MULTI/04621/2019, UIDB/04621/2020 e UIDP/04621/2020 da Fundação para a Ciência e Tecnologia, FCT.

Gracinda M.S. Gomes
Lisboa, Julho de 2020

Prefácio da 1ª edição

O estudo que aqui efectuamos é dedicado aos conceitos e resultados que constituem as bases da Teoria dos Anéis, em particular da dos Anéis de Polinómios numa indeterminada, e da Teoria dos Corpos. Como apêndice, incluímos uma breve análise de algumas noções e de resultados da Teoria dos Conjuntos.

Pressupomos que o leitor está familiarizado com aspectos elementares das Teorias dos Espaços Vectoriais e dos Grupos.

As matérias que versamos são fundamentais para a compreensão de outras, tais como as Teorias de Galois, dos Módulos, dos Anéis de Polinómios em mais do que uma indeterminada ou Geometria Algébrica. Na Teoria dos Anéis, os casos comutativo e não comutativo possuem propriedades diferentes e, portanto, têm aplicações distintas. Por exemplo, os anéis não comutativos surgem, em particular, na Física Quântica e os corpos, que se situam no âmbito comutativo, nas Teorias dos Números e dos Códigos, onde os corpos finitos assumem papel relevante, bem como na Ciência da Computação, em que os corpos de característica dois são uma ferramenta importante.

Poderá ler-se sobre a História da Álgebra, por exemplo, em http://www-history.mcs.st-and.ac.uk/.

A versão inicial, pública, deste texto data de 2000, quando pela primeira vez foi facultado aos alunos de Álgebra II da FCUL. Apesar de existirem muitos livros que abordam estes temas (apresento uma selecção na bibiografia), atendendo aos comentários que fui recebendo ao longo dos anos, decidi dar-lhe agora uma forma mais definitiva. O texto é dirigido aos alunos de Álgebra de uma Licenciatura em Matemática. Está escrito de uma maneira simples e com demonstrações detalhadas, incluindo exemplos e exercícios, na expectativa de que sirva para colmatar a ideia, muitas vezes expressa, de que esta matéria é demasiado abstracta e nem sempre fácil de apreender.

Agradeço aos muitos alunos que me fizeram chegar as suas perguntas interessadas e comentários diversos, os quais contribuíram para melhorar o texto. Obrigada também aos colegas Purificação Coelho, Vítor Hugo Fernandes, Fernando Ferreira, Isabel Ferreirim, Amélia Fonseca, Robert Gray, Elisa Simões e, em particular, Mário Branco,

que leram versões preliminares – a sua contribuição foi inestimável. Ao Prof. Eduardo Ducla Soares, estou grata pelas enriquecedoras discussões sobre as ligações entre a Álgebra e a Física. À Patrícia Paraíba obrigada pelo cuidado com que foi alterando as diversas versões deste texto. Ao leitor, agradeço desde já todas as observações que desejar fazer chegar-me.

Gracinda M.S. Gomes
Lisboa, Dezembro de 2011

"... In the realm of algebra, in which the most gifted mathematicians have been busy for centuries, she (Emmy Nöether) discovered methods which have proved of enormous importance in the development of the present-day younger generation of mathematicians. Pure mathematics is, in its way, the poetry of logical ideas. One seeks the most general ideas of operation which will bring together in simple, logical and unified form the largest possible circle of formal relationships. In this effort toward logical beauty spiritual formulas are discovered necessary for the deeper penetration into the laws of nature ..."

Albert Einstein, numa carta ao Editor do New York Times em 5 de Maio de 1935, aquando da morte de Emmy Nöether, a qual se destacou pelo seu trabalho sobre Álgebra, em particular sobre Teoria dos Anéis.
http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Noether_Emmy.html

Índice

Capítulo 1

Anéis

Este capítulo é dedicado ao estudo dos anéis. Um anel é uma estrutura algébrica com duas operações, uma de adição e outra de multiplicação, que satisfazem certas condições. O conjunto dos números inteiros $\mathbb{Z}$ com as operações usuais de adição e multiplicação constitui o nosso protótipo de anel comutativo com identidade.

Começaremos com uma análise de vários conceitos e resultados básicos, muitos dos quais generalizam outros já estudados na Teoria dos Grupos. A bem conhecida construção do corpo dos racionais $\mathbb{Q}$ a partir do domínio de integridade dos inteiros $\mathbb{Z}$ será generalizada à construção do corpo de fracções de um domínio de integridade arbitrário. Trataremos ainda os conceitos de divisibilidade e de factorização em anéis comutativos com identidade, considerando as classes especiais dos domínios de integridade, euclidianos, de ideais principais e de factorização única.

1.1 Conceitos e resultados gerais

Recordemos alguns conceitos.

Dado um conjunto A, uma aplicação θ de $A\times A$ em A diz-se uma *operação binária* em A; neste caso, dado $(a,b)\in A\times A$, representamos $\theta(a,b)$ por $a\,\theta\,b$. Um tal par (A,θ), com $A\neq\emptyset$, diz-se um *grupóide*. A operação θ diz-se *associativa* se, para quaisquer $a,b,c\in A$,

$$(a\,\theta\,b)\,\theta\,c = a\,\theta\,(b\,\theta\,c)$$

e diz-se *comutativa* se

$$a\,\theta\,b = b\,\theta\,a$$

para quaisquer $a, b \in A$. O grupóide (A, θ) diz-se um *semigrupo* se θ é associativa e diz-se *comutativo* ou *abeliano* se θ é comutativa. (Esta última designação está associada ao nome do matemático Abel.)

Um elemento $u \in A$ diz-se *identidade* de um grupóide (A, θ) se

$$a\,\theta\,u = u\,\theta\,a = a$$

para qualquer $a \in A$. Observemos que se um grupóide (A, θ) tem identidade, ela é única.

Num grupóide (A, θ) com identidade u, um elemento $b \in A$ diz-se *inverso* de $a \in A$ se

$$a\,\theta\,b = b\,\theta\,a = u$$

Notemos que num semigrupo com identidade, se um elemento tiver inverso, esse inverso é único.

Um semigrupo com identidade diz-se um *monóide*. Um monóide em que todos os elementos têm inverso designa-se por *grupo*.

Notação. Frequentemente usamos notação multiplicativa ou aditiva para representar uma operação binária. Se a notação é multiplicativa escrevemos $(A, \cdot)$ e $a\,b$ em vez de (A, θ) e $a\,\theta\,b$, respectivamente. Neste caso, a identidade pode designar-se por *um*, 1, e o inverso de um elemento a por a^{-1}. Se a notação é aditiva escrevemos $(A, +)$ e $a + b$, designamos a identidade por *zero*, 0, e ao inverso de a chamamos *simétrico* de a e representamo-lo por $-a$. Não havendo perigo de confusão escrevemos apenas A em vez de (A, θ).

Num semigrupo (A, θ), dados $a_1, a_2, a_3 \in A$, como a operação θ é associativa temos $a_1\,\theta\,(a_2\,\theta\,a_3) = (a_1\,\theta\,a_2)\,\theta\,a_3$, pelo que este elemento se pode representar, sem ambiguidade, por $a_1\,\theta\,a_2\,\theta\,a_3$. De um modo geral, dados $a_1, \ldots, a_n \in A$, em que $n \in \mathbb{N}$ e $n \geq 3$, representamos

o elemento $((((a_1\,\theta\,a_2)\,\theta\,a_3)\,\theta\,a_4)\cdots)\,\theta\,a_n$ por $a_1\,\theta\,a_2\,\theta\cdots\theta\,a_n$. Podemos provar, por indução sobre n, que o cálculo de $a_1\,\theta\,a_2\,\theta\cdots\theta\,a_n$ é independente de onde se colocam os parêntesis. Em notação multiplicativa, este elemento denota-se por $a_1\,a_2\cdots a_n$ ou por $\prod_{i=1}^{n} a_i$ e, em notação aditiva, por $a_1 + a_2 + \cdots + a_n$ ou por $\sum_{i=1}^{n} a_i$. Quando $a_1 = a_2 = \cdots = a_n$, escrevemos a_1^n e $n\,a_1$, respectivamente. Se A é um monóide, com notação multiplicativa ou aditiva, e $n = 0$ definimos a^n e na como sendo 1 e 0, respectivamente. Se A é um grupo, dados $a \in A$, $n \in \mathbb{Z}$ e $n < 0$, também definimos a^n e na como sendo $(a^{-n})^{-1}$ e $-(-n)a$, respectivamente.

Definição. Um anel é um terno $(A, +, \cdot)$ em que $(A, +)$ é um grupo comutativo, $(A, \cdot)$ é um semigrupo e em que a multiplicação é *distributiva* em relação à adição, isto é, para quaisquer $a, b, c \in A$,

$$(a + b)\,c = a\,c + b\,c$$
$$c\,(a + b) = c\,a + c\,b$$

Um anel $(A, +, \cdot)$ em que $(A, \cdot)$ tem identidade diferente do zero de $(A, +)$, diz-se *anel com identidade*; se o semigrupo $(A, \cdot)$ é comutativo o *anel* $(A, +, \cdot)$ diz-se *comutativo*.

Num anel A, dados $a, b \in A$ designamos o elemento $a + (-b)$ por $a - b$.

Propriedades de um anel. *Seja $(A, +, \cdot)$ um anel. Dados $a, b, c \in A$, temos*

I) $a + c = b + c \;\Rightarrow\; a = b$;
$-(-a) = a$;
$-(a + b) = -a - b$;
$(-n)\,a = -(n\,a), \quad com \;\; n \in \mathbb{Z}$;
$(m + n)\,a = m\,a + n\,a, \quad com \;\; m, n \in \mathbb{Z}$;

II) $0\,a = a\,0 = 0$;
$a\,(-b) = (-a)\,b = -(a\,b)$;
$(-a)\,(-b) = a\,b$;
$a^{m+n} = a^m\,a^n, \quad com \;\; m, n \in \mathbb{N}$;
$(a^m)^n = a^{mn}, \quad com \;\; m, n \in \mathbb{N}$.

Demonstração: Começemos por notar que as propriedades I) são consequência do facto de $(A, +)$ ser um grupo comutativo.

Para provarmos que $0\,a = 0$, basta observar que

$$0 + 0\,a = 0\,a = (0 + 0)\,a = 0\,a + 0\,a$$

e aplicar a primeira propriedade de I). Mostra-se, analogamente, que $a\,0 = 0$.

Uma vez que

$$a\,(-b) + a\,b = a\,(-b + b) = a\,0 = 0$$

temos que $a\,(-b)$ é o simétrico de $a\,b$. Analogamente, obtemos $-(ab) = (-a)b$. Assim,

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$$

As duas últimas propriedades de II) são consequência do facto de $(A, \cdot)$ ser um semigrupo. ∎

Observemos que se $(A, +, \cdot)$ é um anel em que o zero de $(A, +)$ é identidade de $(A, \cdot)$, então $A = \{0\}$. De facto, dado $a \in A$, por um lado temos $0 = a\,0$ e, por outro, $a = a\,0$. Portanto $A = \{0\}$.

Exemplos.

1) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ são anéis comutativos com identidade, que usualmente designamos apenas por $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, respectivamente.

2) $(\mathbb{N}, +, \cdot)$ não é anel.

3) $(3\,\mathbb{Z}, +, \cdot)$ é anel comutativo sem identidade ($3\mathbb{Z}$ designa o conjunto dos inteiros que são múltiplos de 3).

4) O conjunto das matrizes quadradas de ordem $n > 1$ de entradas em $\mathbb{R}$ com as operações usuais de adição e multiplicação, $(M_n(\mathbb{R}), +, \cdot)$, é anel com identidade não comutativo.

5) Seja $\mathcal{P}(X)$ o conjunto das partes de um conjunto X. Definimos uma operação de adição em $\mathcal{P}(X)$ por

$$A + B = (A \cup B) \setminus (A \cap B)$$

para quaisquer $A, B \subseteq X$. Então $(\mathcal{P}(X), +, \cap)$ é anel comutativo com identidade, que satisfaz a propriedade $A^2 = A$, neste caso $A \cap A = A$, para qualquer $A \in \mathcal{P}(X)$, pelo que se diz um *anel de Boole*. Esta operação de adição chama-se *diferença simétrica*.

Desde que não haja perigo de confusão, escreveremos apenas A em vez de $(A, +, \cdot)$.

Definição. Dados um anel A e elementos $a, b \in A\backslash\{0\}$ tais que $a\,b = 0$ dizemos que a e b são *divisores de zero*.

Definição. Um anel comutativo com identidade e sem divisores de zero diz-se um *domínio de integridade*.

Um anel comutativo com identidade em que todo o elemento não nulo tem inverso diz-se um *corpo*.

É claro que todo o *corpo* A é um domínio de integridade. De facto, se $a, b \in A$ são tais que $ab = 0$, então $a = 0$ ou $b = 0$, pois se $a \neq 0$ existe a^{-1} e obtemos $0 = a^{-1}(ab) = (a^{-1}a)b = b$, e, analogamente $b \neq 0$ implica $a = 0$. Logo não há divisores de zero em A.

Nota. Chamamos a atenção do leitor para o facto de alguns livros apresentarem a definição de domínio de integridade para anéis não necessariamente comutativos. Também se designa por *anel de divisão* "um corpo não necessariamente comutativo", isto é, um anel com identidade em que todo todo o elemento não nulo tem inverso.

Exemplos.

1) Os anéis $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.

2) O anel $\mathbb{Z}$ é domínio de integridade, mas não é corpo pois, por exemplo, 2 não tem inverso.

3) O anel $(\mathbb{Z}_4, +, \cdot)$ em que $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ e as operações são

dadas pelas seguintes tabelas de Cayley:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

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

é anel comutativo com identidade mas não é domínio de integridade pois, por exemplo, 2 é divisor de zero.

4) O anel $(\mathbb{Z}_5, +, \cdot)$ com as operações dadas por:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

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

é corpo.

5) O anel $(\mathcal{T}(\mathbb{R}), +, \cdot)$, em que $\mathcal{T}(\mathbb{R})$ é o conjunto das aplicações (transformações) de $\mathbb{R}$ em $\mathbb{R}$ com as operações definidas por: dados $f, g \in \mathcal{T}(\mathbb{R})$ e $x \in \mathbb{R}$

$$(f+g)(x) = f(x) + g(x) \quad \text{e} \quad (f\,g)(x) = f(x)\,g(x)$$

é comutativo com identidade mas não é domínio de integridade.

6) Seja Q o conjunto das matrizes de tipo 2×2 sobre $\mathbb{C}$ da forma

$$\begin{pmatrix} s+it & u+iv \\ -u+iv & s-it \end{pmatrix}$$

em que $s, t, u, v \in \mathbb{R}$, com as operações usuais de multiplicação e adição. A estrutura $(Q, +, \cdot)$ constitui um anel de divisão que não é corpo. Aos elementos de Q chamamos *quaterniões*.

Definição. Sejam A um anel e $B \subseteq A$. Diz-se que B é *subanel* de $(A, +, \cdot)$ se $x + y, x\,y \in B$, para quaisquer $x, y \in B$, e com estas operações B é também um anel.

Observamos que muitos autores exigem que um subanel B de um anel A com identidade 1 contenha 1. Não é esta a definição que aqui adoptamos e sempre que quisermos exigir a presença de 1 em B diremos *subanel com identidade*.

Exemplos.

1) $\mathbb{Z}$ é subanel de $\mathbb{Q}$.

2) Se A é anel, $\{0\}$ e A são subanéis de A.

3) $\mathbb{N}$ não é subanel de $\mathbb{Z}$.

4) Seja $R = \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$. É fácil verificar que R é um subanel com identidade de $(\mathbb{C}, +, \cdot)$.

5) Seja $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, o anel com identidade 1, com as operações de adição e multiplicação módulo-6, definido à semelhança dos exemplos $\mathbb{Z}_4$ e $\mathbb{Z}_5$ já apresentados. Este anel admite $B = \{0, 3\}$ como subanel mas não como subanel com identidade visto que 3 é identidade de B e $3 \neq 1$.

Observação. Normalmente designamos R por $\mathbb{Z}[\sqrt{-5}]$. De modo análogo, definimos os subanéis $\mathbb{Z}[\sqrt{-n}]$ e $\mathbb{Q}[\sqrt{-n}]$ de $\mathbb{C}$, para qualquer $n \in \mathbb{N}$. O anel $\mathbb{Z}[\sqrt{-1}]$ é usualmente denotado por $\mathbb{Z}[i]$ e chama-se *anel dos inteiros de Gauss*. Definimos o anel $\mathbb{Z}[\sqrt{5}]$ como sendo $\{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$ e também, analogamente, os subanéis $\mathbb{Z}[\sqrt{n}]$ e $\mathbb{Q}[\sqrt{n}]$ de $\mathbb{R}$, com $n \in \mathbb{N}$.

Em seguida, apresentamos dois critérios para verificar que uma parte de um anel é um seu subanel. As demonstrações ficam ao cuidado do leitor.

Critério de subanel 1. *Sejam A um anel e $B \subseteq A$. Então B é subanel de A se e só se, para quaisquer $x, y \in B$,*

$$\begin{gathered} 0 \in B \\ x + y,\ x\,y \in B \\ -\,x \in B\,. \end{gathered}$$

Critério de subanel 2. *Sejam A um anel e $B \subseteq A$. Então B é subanel de A se e só se, para quaisquer $x, y \in B$,*

$$\begin{gathered} 0 \in B \\ x - y,\ x\,y \in B\,. \end{gathered}$$

O resultado seguinte demonstra-se facilmente usando um destes critérios.

Proposição 1. *Sejam A um anel e $\mathcal{F} = \{A_i\}_{i\in I} \neq \emptyset$ uma família de subanéis de A. Então $\bigcap_{i\in I} A_i$ é subanel de A.*

O conceito de ideal, que passamos a apresentar, desempenha na Teoria dos Anéis um papel semelhante ao desempenhado pelo conceito de subgrupo normal na Teoria dos Grupos.

Definição. Sejam A um anel e I um subanel de A. Diz-se que I é *ideal* de A se $ac, ca \in I$, para quaisquer $a \in I$ e $c \in A$. Escrevemos $I \trianglelefteq A$.

É fácil verificar que

1) **Critério de ideal.** Um subconjunto I de um anel A é ideal de A se e só se, para quaisquer $a, b \in I$ e $c \in A$,

$$\begin{gathered} 0 \in I \\ a - b,\ ac,\ ca\ \in I\,. \end{gathered}$$

2) Se A é um anel com identidade 1 e I é um ideal de A, então $1 \in I$ se e só se $I = A$. De facto, se $1 \in I$ então $a = a\,1 \in I$, para qualquer $a \in A$. Um *ideal* $I \neq A$ diz-se *próprio*.

3) A intersecção de uma família não vazia de ideais de um anel A é ideal de A.

Como consequência da última observação podemos garantir que, dado um subconjunto X de um anel A, existe sempre o menor ideal de A que contém X, o qual é a intersecção de todos os ideais que contêm X. (Note-se que, em particular, A é ideal de A e contém X.) Este ideal diz-se o *ideal gerado* por X e denota-se por $\langle X \rangle$. Se $X = \{a_1, \ldots, a_n\}$ escrevemos apenas $\langle a_1, \ldots, a_n \rangle$.

Definição. Um *ideal* I de um anel A diz-se *principal* se existir um elemento $a \in I$ que o gere.

Exemplos.

1) Dados um anel A e $a \in A$, se A é comutativo, então $aA = \{a\,x \colon x \in A\}$ é ideal de A. Além disso, se A tem identidade, então aA é o ideal de A gerado por a.

2) O subanel $2\,\mathbb{Z}$ é ideal de $\mathbb{Z}$.

3) Dados um anel arbitrário A e $a \in A$, temos

$$\langle a \rangle = \Big\{ n\,a + b\,a + a\,c + \sum_{i=1}^{r} b_i\,a\,c_i \colon \\ r \in \mathbb{N};\ n \in \mathbb{Z};\ b, c, b_i, c_i \in A,\ i = 1, \ldots, r \Big\}$$

4) Todo o ideal de $\mathbb{Z}$ é principal e, portanto, é da forma $\langle m \rangle$, para algum $m \in \mathbb{Z}$, sendo $\langle m \rangle = m\mathbb{Z}$ por $\mathbb{Z}$ ser comutativo e ter identidade.

5) Veremos, à frente, que no anel $\mathbb{Z}[x]$, dos polinómios na indeterminada x com coeficientes em $\mathbb{Z}$, nem todo o ideal é principal.

Podemos definir apenas ideal esquerdo [direito] mas no nosso contexto só nos interessa tomar ideais bilaterais. Apresentamos agora a soma e o produto de ideais.

Definição. Seja A um anel. Dados I e J subanéis de A, definimos a sua *soma*

$$I + J = \Big\{ x + y \colon\ x \in I,\ y \in J \Big\}$$

Se I, J são ideais de A, também definimos o seu *produto*

$$IJ = \Big\{ x_1\, y_1 + \cdots + x_n\, y_n \colon\ n \in \mathbb{N};\ x_i \in I,\ y_i \in J,\ i = 1, \ldots, n \Big\}$$

A soma $I + J$ de subanéis I e J de um anel A pode não ser um subanel de A. Por exemplo, $\mathbb{Z}[i] = \{a + b\, i \,:\, a, b \in \mathbb{Z}\}$ e $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ são subanéis de $(\mathbb{C}, +, \cdot)$ mas $\mathbb{Z}[i] + \mathbb{Z}[\sqrt{2}]$ não é subanel de $\mathbb{C}$ pois $i\sqrt{2} \notin \mathbb{Z}[i] + \mathbb{Z}[\sqrt{2}]$.

No entanto, se I ou J for ideal de A, a soma $I + J$ é subanel de A. Suponhamos que I é um ideal de A e J é um subanel de A. Temos $0 = 0 + 0 \in I + J$ e, dados $i, j \in I,\ s_1, s_2 \in J$,

$$(i + s_1) - (j + s_2) = (i - j) + (s_1 - s_2) \ \in\ I + J$$

e

$$(i + s_1)\,(j + s_2) = (i\, j + i\, s_2 + s_1\, j) + s_1\, s_2 \ \in\ I + J$$

pelo que $I + J$ é um subanel de A que claramente contém I. Mais ainda,

Proposição 2. *Sejam A um anel e I, J ideais de A. Então $I + J$ e IJ são ideais de A tais que*

$$I, J \subseteq I + J \quad \text{e} \quad IJ \subseteq I \cap J.$$

Recordemos que, se G e H são semigrupos, uma aplicação f de G em H diz-se um *morfismo* se

$$f(a\, b) = f(a)\, f(b)$$

para quaisquer $a, b \in G$. Se G e H são grupos com identidades 1_G e 1_H respectivamente, temos obrigatoriamente $f(1_G) = 1_H$, $f(a^{-1}) = f(a)^{-1}$ e $f(a\, b^{-1}) = f(a)\, f(b)^{-1}$, para quaisquer $a, b \in G$.

Definição. Sejam $(A, +, \cdot)$ e $(B, \circledast, \odot)$ anéis. Dizemos que uma aplicação f de A em B é um *morfismo de anéis* se, para quaisquer $a, b \in A$,

$$f(a+b) = f(a) \circledast f(b)$$

e

$$f(a \cdot b) = f(a) \odot f(b)$$

Se A e B são anéis com identidade, um morfismo f de A em B diz-se um *morfismo de anéis com identidade* se $f(1_A) = 1_B$, sendo 1_A a identidade de A e 1_B a identidade de B.

Não havendo perigo de confusão, denotamos as identidades 1_A e 1_B por 1 e as correspondentes operações nos anéis A e B pelos mesmos símbolos $+$ e $\cdot$, escrevendo apenas $f(a+b) = f(a) + f(b)$, $f(a\,b) = f(a)\,f(b)$ e $f(1) = 1$.

Exemplos.

1) A aplicação $f\colon \mathbb{Z} \to \mathbb{Z}_2$ definida por

$$f(x) = \begin{cases} 0 & \text{se } x \text{ é par,} \\ 1 & \text{se } x \text{ é ímpar} \end{cases}$$

é um morfismo de anéis com identidade.

2) Seja $g\colon \mathbb{Z} \to \mathbb{Z}$ definida por $g(n) = 2\,n$, para qualquer $n \in \mathbb{Z}$. A aplicação g não é um morfismo, pois não respeita a operação de multiplicação embora respeite a adição.

Definição. Dado um morfismo f de A em B, chamamos *núcleo* ou *kernel* do morfismo f ao conjunto $\{a \in A\colon f(a) = 0\}$, que designamos por $\operatorname{Ker} f$ (kernel significa núcleo em Inglês). Designamos a sua *imagem* por $f(A)$.

A seguinte proposição dá-nos a conhecer algumas propriedades básicas dos morfismos entre anéis.

Proposição 3. *Sejam A e B anéis e $f\colon A \to B$ um morfismo. Então*

a) $f(0) = 0$;

b) *Se A' é subanel de A, então $f(A')$ é subanel de B;*
Se B' é subanel de B, então $f^{-1}(B')$ é subanel de A;

c) $\operatorname{Ker} f$ *é ideal de A;*

d) f *é injectiva se e só se* $\operatorname{Ker} f = \{0\}$.

Demonstração: Seja $f\colon A \to B$ um morfismo de anéis. Então f é um morfismo entre os grupos $(A, +)$ e $(B, +)$ pelo que temos, $f(0) = 0$ e, para quaisquer $a, b \in A$, e também $f(a-b) = f(a) - f(b)$. Em particular, fica, assim, demonstrada a alínea **a**).

b) Seja A' um subanel de A. Como $0 \in A'$, obtemos $0 = f(0) \in f(A')$. Tomemos $x, y \in f(A')$. Então existem $a, b \in A'$ tais que $x = f(a)$ e $y = f(b)$. Logo, $x\,y = f(a)\,f(b) = f(a\,b) \in f(A')$ e $x - y = f(a) - f(b) = f(a - b) \in f(A')$, pois f é morfismo e $a\,b, a - b \in A'$. Portanto, $f(A')$ é subanel de B.

Seja B' um subanel de B. Como $f(0) = 0$ e $0 \in B'$, temos $0 \in f^{-1}(B')$. Tomemos $a, b \in f^{-1}(B')$ então $f(a), f(b) \in B'$, donde $f(a) - f(b)$, $f(a)\,f(b) \in B'$. Sendo f morfismo, obtemos $f(a - b)$, $f(ab) \in B'$ pelo que $a - b$, $ab \in f^{-1}(B')$. Logo $f^{-1}(B')$ é subanel de A.

c) Pela alínea a), já sabemos que $0 \in \operatorname{Ker} f$. Sejam $a, b \in \operatorname{Ker} f$. Então

$$f(a - b) = f(a) - f(b) = 0 - 0 = 0$$

pelo que $a - b \in \operatorname{Ker} f$; se $c \in A$ temos também

$$f(a\,c) = f(a)\,f(c) = 0\,f(c) = 0$$

e, analogamente, $f(c\,a) = 0$, donde $a\,c, c\,a \in \operatorname{Ker} f$. Portanto, $\operatorname{Ker} f$ é ideal de A.

d) Suponhamos que f é injectiva. Já sabemos que $0 \in \operatorname{Ker} f$. Seja $a \in \operatorname{Ker} f$. Então $f(a) = 0 = f(0)$, donde $a = 0$. Portanto,

$\operatorname{Ker} f = \{0\}$. Reciprocamente, admitamos que $\operatorname{Ker} f = \{0\}$. Sejam $a, b \in A$ tais que $f(a) = f(b)$. Então $f(a) - f(b) = 0$, donde $f(a-b) = 0$. Assim, $a - b \in \operatorname{Ker} f$. Logo $a - b = 0$ e concluímos que $a = b$. Portanto, f é injectiva. ∎

Como habitualmente, um morfismo injectivo [sobrejectivo, bijectivo] diz-se um *monomorfismo* ou *mergulho* [*epimorfismo*, *isomorfismo*]. Se existe um isomorfismo entre os anéis A e B dizemos que os anéis são *isomorfos* e escrevemos $A \simeq B$. Se $A = B$, um isomorfismo diz-se um *automorfismo*.

Se $f\colon A \to B$ é uma aplicação sobrejectiva [injectiva], escrevemos frequentemente $f\colon A \twoheadrightarrow B$ $[f\colon A \hookrightarrow B]$.

Facilmente se demonstra o seguinte

Proposição 4. *Sejam A, B e C anéis, $f\colon A \to B$ e $g\colon B \to C$ morfismos. Então*

a) *A composição $g \circ f$ é morfismo de A em C;*

b) *Se f é isomorfismo então f^{-1} é isomorfismo de B para A.*

Apresentamos agora a noção de relação de congruência num anel, começando por recordar que uma equivalência num conjunto A é uma relação binária em A que é reflexiva, simétrica e transitiva.

Definição. Uma relação de equivalência ρ num anel A diz-se uma *congruência* em A se respeita as operações de adição e multiplicação, isto é, dados $a, b, c \in A$,

$$(a,b) \in \rho \implies (a+c, b+c),\ (a\,c, b\,c),\ (c\,a, c\,b) \in \rho$$

Observemos que uma equivalência ρ é uma congruência num anel $(A, +, \cdot)$ se e só se é congruência nos semigrupos $(A, +)$ e $(A, \cdot)$.

Notação. Dado $a \in A$, denotamos a ρ-classe de a por $[a]_\rho$ ou apenas por $[a]$ se não houver perigo de confusão. Designamos

o conjunto de todas as ρ-classes por *conjunto quociente de A por ρ*, e representamo-lo por A/ρ. Escrevemos também $a\,\rho\,b$ em vez de $(a,b)\in\rho$. Denotamos por $\mathrm{Cong}(A)$ o conjunto de todas as congruências em A.

O seguinte resultado é consequência imediata do estudo das congruências em semigrupos.

Critério de congruência. *Sejam A um anel e ρ uma relação de equivalência em A. A relação ρ é uma congruência em A se e só se, para quaisquer $a,b,c,d\in A$,*

$$(a,b),\,(c,d)\in\rho \implies (a+c,b+d),\,(a\,c,b\,d)\in\rho$$

Exemplo.

Dados $p,q\in\mathbb{Z}$ dizemos que p *divide* q se existe $s\in\mathbb{Z}$ tal que $q=ps$. Dizemos também que o *resto da divisão* de q por p é r se $0\leq r<|p|$ e existe $t\in\mathbb{Z}$ tal que $q=p\,t+r$. É bem sabido que nesta divisão t e r são únicos.

A relação $\sim_m$, com $m\in\mathbb{Z}$, definida em $(\mathbb{Z},+,\cdot)$ por: dados $a,b\in\mathbb{Z}$,

$$a\sim_m b \quad \text{ se e só se } \quad m \text{ divide } a-b$$

é uma relação de congruência em $(\mathbb{Z},+,\cdot)$. Dois elementos $\sim_m$-congruentes dizem-se *congruentes módulo-m* e o conjunto quociente $\mathbb{Z}/\sim_m$ designa-se por $\mathbb{Z}_m$. Frequentemente designamos uma classe $[a]_{\sim_m}$ simplesmente por $[a]_m$.

Convém observar que dois inteiros a e b são *congruentes módulo-m* se e só se divididos por m dão o mesmo resto.

Atendendo ao critério anterior, dados um anel A e uma congruência ρ em A, no conjunto quociente A/ρ podemos definir operações de adição e multiplicação do seguinte modo: dados $a,b\in A$,

$$[a]+[b]=[a+b]$$

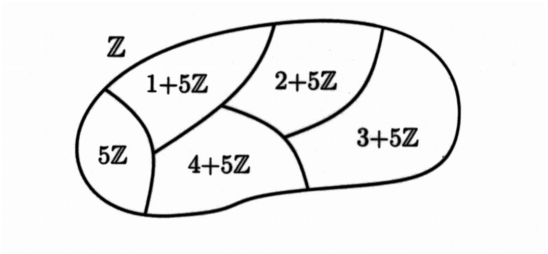
$$[a]\,[b] = [a\,b]$$

e facilmente se mostra que se obtém um anel, que se designa por *anel quociente* de A *por* ρ.

Proposição 5. *Sejam A um anel e ρ uma congruência em A. Então $(A/\rho, +, \cdot)$ é anel.*

Exemplos.

1) A partição de $\mathbb{Z}$ em $\sim_5$-classes é a seguinte



obtemos $\mathbb{Z}/\sim_5 = \Big\{[0],[1],[2],[3],[4]\Big\}$, com $[j] = j + 5\,\mathbb{Z}$ $(= \{j + 5m : m \in \mathbb{Z}\})$ e $0 \leq j \leq 4$, que a menos de isomorfismo não é mais do que o anel $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ apresentado atrás.

2) A seguinte correspondência é um epimorfismo

$$\begin{aligned} f\colon\ \mathbb{Z}_{18} &\to \mathbb{Z}_3 \\ [m]_{18} &\mapsto [m]_3 \end{aligned}$$

Mostremos agora como se relacionam os conceitos de ideal, morfismo e congruência.

Definição. Sejam A um anel e I um ideal de A. Definimos em A uma relação binária $\sim_I$ do seguinte modo: dados $a, b \in A$,

$$a \sim_I b \quad \text{ se e só se } \quad a - b \in I$$

Escreveremos apenas $\sim$ se não houver perigo de confusão.

Proposição 6. *Sejam A um anel e I um ideal de A. Então $\sim_I$ é uma congruência em A.*

Demonstração: Seja $a \in A$. Como $a - a = 0 \in I$, temos $a \sim a$. Logo $\sim$ é reflexiva. Sejam $a, b \in A$ tais que $a \sim b$. Então $a - b \in I$ e, portanto, $-(a - b) \in I$, isto é $b - a \in I$. Logo $b \sim a$. Concluímos que $\sim$ é simétrica. Tomemos $a, b, c \in A$ tais que $a \sim b$ e $b \sim c$. Então $a-b$, $b-c \in I$, logo $a-c = a-b+b-c \in I$, donde $a \sim c$. Portanto, $\sim$ é transitiva.

Sejam $a, b, c \in A$ tais que $a \sim b$. Então $a - b \in I$. Assim, $(a - b)\, c$, $c\,(a - b)$, $a + c - c - b \in I$, isto é, $a\, c - b\, c$, $c\, a - c\, b$, $a + c - (b + c) \in I$. Portanto, $a\, c \sim b\, c$, $c\, a \sim c\, b$ e $a+c \sim b+c$. Logo $\sim$ é uma congruência em A. ∎

A relação $\sim_I$ diz-se a *congruência definida em A pelo ideal I*.

Descrição do anel A/I. Observemos que, dados um anel A, um ideal I de A e $a \in A$, a $\sim_I$-classe de a é o subconjunto $a + I = \{a + x\colon\ x \in I\}$ de A. De facto, se $b \in [a]_{\sim_I}$, então $b - a \in I$, donde

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

Reciprocamente, se $x \in I$, temos $(a + x) - a = x \in I$, pelo que $a + x \sim_I a$. Logo $a + x \in [a]_{\sim_I}$.

Em particular, a classe do elemento zero é $0 + I$, ou seja, I.

Representemos o anel quociente $A/{\sim_I}$ por A/I. Acabámos de mostrar que $A/I = \{a + I\colon\ a \in A\}$, com as operações definidas por

$$\begin{aligned}(a + I) + (b + I) &= (a + b) + I\\ (a + I)\,(b + I) &= a\, b + I\end{aligned}$$

para quaisquer $a, b \in A$, sendo I o zero de A/I.

Exemplo.

Consideremos o anel $\mathbb{Z}$ e o ideal $\langle m\rangle$, com $m \in \mathbb{Z}$. Então, como já observámos, $\langle m\rangle = m\,\mathbb{Z}$ e temos

$$\mathbb{Z}/\langle m\rangle = \Big\{a + m\,\mathbb{Z}\colon\ a \in \mathbb{Z}\Big\}.$$

Além disso, dados $a, b \in \mathbb{Z}$,

$$\begin{aligned} a \sim_{\langle m \rangle} b &\iff a - b \in \langle m \rangle \\ &\iff a - b \in m\,\mathbb{Z} \\ &\iff \exists\, p \in \mathbb{Z},\quad a - b = m\,p \\ &\iff a \sim_m b \end{aligned}$$

Logo $\sim_{\langle m \rangle}$ coincide com $\sim_m$.

Vamos agora mostrar que todo o ideal está associado a uma congruência e, reciprocamente, toda a congruência está associada a um ideal.

Teorema 7. *Seja A um anel. Se I é ideal de A, então $\sim_I$ é uma congruência em A tal que $[0]_{\sim_I} = I$.*

Reciprocamente, se ρ é uma congruência em A, então $[0]_\rho$ é um ideal de A e $\rho = \sim_{[0]_\rho}$.

Demonstração: A primeira parte deste teorema resulta da Proposição 6 e da descrição de A/I que se lhe segue. Provemos então a segunda parte.

Suponhamos que ρ é uma congruência em A. Sejam $a \in [0]_\rho$ e $b \in A$. Então $a\ \rho\ 0$ pelo que $a\,b\ \rho\ 0\,b$ e $b\,a\ \rho\ b\,0$, donde $a\,b, b\,a \in [0]_\rho$. Tomemos $a, b \in [0]_\rho$. Temos $a\ \rho\ 0$ e $0\ \rho\ b$, donde $a\ \rho\ b$. Logo $a–b\ \rho\ b–b$ e, portanto, $a-b \in [0]_\rho$. É claro que $0 \in [0]_\rho$. Concluímos assim que $[0]_\rho$ é ideal de A.

Sejam $a, b \in A$ tais que $a\ \rho\ b$. Então $a-b\ \rho\ b-b$, donde $a-b \in [0]_\rho$ e, portanto, $a \sim_{[0]_\rho} b$. Reciprocamente, se $a \sim_{[0]_\rho} b$, então $a-b \in [0]_\rho$, logo $a-b\ \rho\ 0$, donde $a-b+b\ \rho\ 0+b$, isto é, $a\ \rho\ b$. Assim, temos $\rho = \sim_{[0]_\rho}$. ∎

O teorema anterior diz-nos que num anel A uma congruência fica perfeitamente determinada pela classe do zero. Deste teorema, conclui-se também que a correspondência $\rho \mapsto [0]_\rho$ é uma bijecção entre o conjunto das congruências em A e o conjunto dos ideais de A. Além disso, é claro que esta bijecção respeita a relação de inclu-

são, isto é, $\rho \subseteq \theta$ se e só se $[0]_\rho \subseteq [0]_\theta$. Devemos pois ter presente a seguinte bijecção

$$\begin{array}{rcl} \text{Ideais}(A) & \longleftrightarrow & \text{Cong}(A) \\ I & \longmapsto & \sim_I \\ [0]_\rho & \longleftarrow\!\shortmid & \rho \end{array}$$

Em seguida, vamos ver que a um morfismo está também associada uma congruência.

Definição. Dado um morfismo $f : A \to B$ entre anéis A e B, definimos em A uma relação binária $\equiv_f$, *relação igualdade de imagem*, do seguinte modo: dados $a, b \in A$,

$$a \equiv_f b \quad \text{ se e só se } \quad f(a) = f(b)$$

Teorema 8. *Sejam A e B anéis. Se $f\colon A \to B$ é um morfismo, então a relação igualdade de imagem $\equiv_f$ é uma congruência em A tal que $f(A) \simeq A/\equiv_f$. Além disso, esta congruência $\equiv_f$ coincide com a congruência $\sim_{\operatorname{Ker} f}$ definida pelo ideal $\operatorname{Ker} f$.*

Se ρ é uma congruência em A, então a aplicação canónica

$$\begin{array}{rl} \rho^\natural\colon & A \twoheadrightarrow A/\rho \\ & a \mapsto [a]_\rho \end{array}$$

é um epimorfismo e ρ coincide com $\equiv_{\rho^\natural}$, relação igualdade de imagem por $\rho^\natural$.

Demonstração: Seja $f\colon A \to B$ um morfismo. Para simplificar a escrita denotemos $\equiv_f$ por $\equiv$.

É fácil provar que $\equiv$ é uma congruência em A. Dado $a \in A$ denotemos a sua $\equiv$-classe por $[a]$. Pela Proposição 3 b), temos que $f(A)$ é um anel.

Seja

$$\begin{array}{rl} \theta\colon & A/\equiv \to f(A) \\ & [a] \mapsto f(a) \end{array}$$

Em primeiro lugar, observemos que esta correspondência é uma aplicação pois, para quaisquer $[a], [b] \in A/\equiv$, se $[a] = [b]$ então $a \equiv b$ e, portanto, $f(a) = f(b)$.

Dado $x \in f(A)$, existe $a \in A$ tal que $x = f(a)$, donde $x = \theta([a])$. Logo θ é sobrejectiva. Mostremos que θ é morfismo. Sejam $a, b \in A$. Então

$$\theta([a]\,[b]) = \theta([a\,b]) = f(a\,b) = f(a)\,f(b) = \theta([a])\,\theta([b])$$

pois f é morfismo. Analogamente, provamos que

$$\theta([a]+[b]) = \theta([a]) + \theta([b])$$

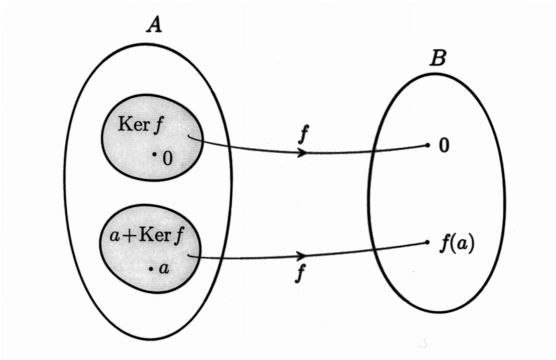
Suponhamos agora que $\theta([a]) = \theta([b])$. Então $f(a) = f(b)$, donde $a \equiv b$ e, portanto, $[a] = [b]$. Assim, θ é injectiva. Concluímos que θ é isomorfismo.

Tomemos $a, b \in A$. Então

$$\begin{aligned} a \equiv b &\iff f(a) = f(b) \iff f(a) - f(b) = 0 \\ &\iff f(a-b) = 0 \iff a-b \in \operatorname{Ker} f \\ &\iff a \sim_{\operatorname{Ker} f} b \end{aligned}$$

logo as congruências $\equiv$ e $\sim_{\operatorname{Ker} f}$ coincidem.

A seguinte representação gráfica é sugestiva do comportamento do morfismo $f\colon A \to B$:



Consideremos agora uma congruência ρ em A. É fácil provar que a sobrejecção canónica

$$\begin{aligned} \rho^\natural\colon\ & A \to A/\rho \\ & a \mapsto [a]_\rho \end{aligned}$$

é um morfismo, atendendo à definição do anel A/ρ.

Finalmente, provemos que ρ e $\equiv_{\rho^\natural}$ são iguais. Tomemos $a, b \in A$, então

$$\begin{aligned} a\ \rho\ b &\iff [a]_\rho = [b]_\rho \iff \rho^\natural(a) = \rho^\natural(b) \\ &\iff a \equiv_{\rho^\natural} b \end{aligned}$$

Logo as congruências ρ e $\equiv_{\rho^\natural}$ coincidem. ∎

O epimorfismo $\rho^\natural$ designa-se por *epimorfismo canónico* associado a ρ.

Exemplo.

Sejam A_1 e A_2 anéis. No *produto cartesiano* $A_1 \times A_2$ definimos operações de adição e multiplicação por: dados (a_1, a_2), $(b_1, b_2) \in A_1 \times A_2$,

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

e

$$(a_1, a_2)\,(b_1, b_2) = (a_1\, b_1,\ a_2\, b_2).$$

Com estas operações, $A_1 \times A_2$ é anel. Seja $I = A_1 \times \{0\}$. Então $I \trianglelefteq A_1 \times A_2$ e a projecção $p_2 : A_1 \times A_2 \to A_2$, definida por $(a_1, a_2) \mapsto a_2$, é um epimorfismo com kernel I, donde

$$A_2 = p_2\,(A_1 \times A_2) \simeq (A_1 \times A_2)/I$$

já que $\equiv_{p_2} = \sim_{\operatorname{Ker} p_2}$ e $\operatorname{Ker} p_2 = I$.

Os dois últimos teoremas mostram-nos que os conceitos de morfismo, congruência e ideal estão intrinsecamente relacionados. Notemos, no entanto, que podemos ter morfismos distintos $f : A \to B$ e $g : A \to C$ com $\operatorname{Ker} f = \operatorname{Ker} g$ e, portanto, definindo a mesma congruência em A. Porém, tem-se necessariamente $f(A) \simeq g(A)$. Basta tomar, por exemplo, $f : \mathbb{Z} \times \mathbb{Q} \to \mathbb{Q}$, $(a, b) \mapsto b$, e $g : \mathbb{Z} \times \mathbb{Q} \to \mathbb{Q} \times \mathbb{R}$, $(a, b) \mapsto (b, 0)$.

O teorema seguinte relaciona os subanéis de um anel A, que contêm um ideal I, com os subanéis do anel quociente A/I.

Teorema 9. *Sejam A um anel e I um seu ideal. Existe uma correspondência bijectiva entre o conjunto dos subanéis de A que contêm I e o conjunto dos subanéis de A/I. Mais ainda, segundo esta correspondência, os ideais de A que contêm I correspondem aos ideais de A/I.*

Demonstração: Sejam $\mathrm{Sub}_I(A)$ o conjunto dos subanéis de A que contêm I e $\mathrm{Sub}(A/I)$ o conjunto dos subanéis de A/I. Consideremos as correspondências

$$\begin{aligned} \theta_1 \colon \ \mathrm{Sub}_I(A) &\longrightarrow \mathrm{Sub}(A/I) \\ R &\longmapsto \{a+I \colon a \in R\} \end{aligned}$$

e

$$\begin{aligned} \theta_2 \colon \ \mathrm{Sub}(A/I) &\longrightarrow \mathrm{Sub}_I(A) \\ S &\longmapsto \{a \in A \colon a+I \in S\} \end{aligned}$$

Tendo em conta o epimorfismo canónico de A em A/I do Teorema 8, bem como a Proposição 3, concluimos que a correspondência θ_1 é uma aplicação.

Por outro lado, dados $S \in \mathrm{Sub}(A/I)$ e $i \in I$, temos $i+I = I \in S$, donde $i \in \theta_2(S)$. Assim, $I \subseteq \theta_2(S)$. Provemos em seguida que $\theta_2(S)$ é um subanel de A, concluindo então que θ_2 também é uma aplicação. Como $0+I = I \in S$, obtemos $0 \in \theta_2(S)$. Dados $a, b \in \theta_2(S)$, temos $a+I$, $b+I \in S$, donde $(a+I)-(b+I)$, $(a+I)\,(b+I) \in S$. Portanto, $(a-b)+I$, $ab+I \in S$ e obtemos $a-b$, $ab \in \theta_2(S)$. Logo $\theta_2(S)$ é um subanel de A que contém I.

Vejamos agora que θ_1 e θ_2 são aplicações inversas uma da outra.

Dado $R \in \mathrm{Sub}_I(A)$, temos

$$\theta_2(\theta_1(R)) = \theta_2(\{a+I \colon a \in R\})$$

É claro que $R \subseteq \theta_2(\theta_1(R))$ por definição de θ_2. Tomemos $b \in \theta_2\theta_1(R))$. Temos $b+I \in \theta_1(R)$, isto é, $b+I = a+I$, com $a \in R$. Então $b-a \in I$. Logo $b-a = i$, para certo $i \in I$ e, portanto,

$$b = a+i \ \in \ R+I \subseteq R$$

já que $I \subseteq R$. Assim, $R = \theta_2(\theta_1(R))$.

Reciprocamente, tomemos agora $S \in \mathrm{Sub}(A/I)$. Então

$$\theta_2(S) \;=\; \{a \in A\colon\; a + I \in S\}$$

pelo que

$$\theta_1(\theta_2(S)) \;=\; \{a + I\colon\; a \in \theta_2(S)\} \subseteq S$$

Por outro lado, dado $s \in S$, temos $s = a + I$, para certo $a \in A$, donde $a \in \theta_2(S)$ e $s \in \theta_1(\theta_2(S))$. Logo $\theta_1(\theta_2(S)) = S$. Portanto, θ_1 e θ_2 são bijecções inversas uma da outra.

Seja J um ideal de A tal que $I \subseteq J$. Provemos que $\theta_1(J)$ é ideal de A/I. Como J é subanel de A, então $\theta_1(J)$ é subanel de A/I. Por outro lado, se $a + I \in \theta_1(J)$ com $a \in J$, dado $c + I$ com $c \in A$, temos

$$(a + I)\,(c + I) = ac + I \;\in\; \theta_1(J)$$

e

$$(c + I)\,(a + I) = ca + I \;\in\; \theta_1(J)$$

pois $ac, ca \in J$. Logo $\theta_1(J)$ é ideal de A/I.

Reciprocamente, seja M um ideal de A/I. Então M é subanel de A/I e, pelo provado atrás, $\theta_2(M)$ está em $\mathrm{Sub}_I(A)$. Além disso, dados $a \in \theta_2(M)$ e $c \in A$, temos $a + I \in M$, donde $(c + I)(a + I)$, $(a + I)(c + I) \in M$ por M ser ideal de A/I. Logo, $ca+I$, $ac+I \in M$, donde ca, $ac \in \theta_2(M)$. Concluímos pois que $\theta_2(M)$ é um ideal de A que contém I. ∎

Observação. Notemos que dado R subanel [ideal] arbitrário de A então $M(R) = \{a + I : a \in R\}$ é subanel [ideal] de A/I, mas tal não contradiz o resultado pois $M(R) = M(R + I)$ sendo $R + I$ um subanel [ideal] de A que contém I.

Teorema 10. *Sejam A e B anéis e $f\colon A \to B$ um morfismo. Seja J ideal de B. Então $f^{-1}(J)$ é ideal de A. Além disso, a correspondência*

$$A/f^{-1}(J) \to B/J$$
$$a + f^{-1}(J) \mapsto f(a) + J$$

é um mergulho.

Demonstração: Como $0 \in J$ e $f(0) = 0$, temos $0 \in f^{-1}(J)$. Sejam $a, b \in f^{-1}(J)$ e $c \in A$. Então $f(a), f(b) \in J$, donde

$$\begin{aligned} f(a-b) = f(a) - f(b) &\in J \\ f(a\,c) = f(a)\,f(c) &\in J \\ f(c\,a) = f(c)\,f(a) &\in J \end{aligned}$$

Logo $a - b$, $a\,c$, $ca \in f^{-1}(J)$. Portanto, $f^{-1}(J)$ é ideal de A e podemos considerar o quociente $A/f^{-1}(J)$.

Consideremos a correspondência

$$\begin{aligned} \theta\colon\ A/f^{-1}(J) &\to B/J \\ a + f^{-1}(J) &\mapsto f(a) + J \end{aligned}$$

Sejam $a, b \in A$ tais que $a + f^{-1}(J) = b + f^{-1}(J)$. Então $a - b \in f^{-1}(J)$, donde $f(a-b) \in J$. Logo $f(a) - f(b) \in J$ e, portanto, $f(a) + J = f(b) + J$. Assim, θ é aplicação. Por outro lado, para quaisquer $a, b \in A$,

$$\begin{aligned} \theta\Big(\Big(a + f^{-1}(J)\Big)\,\Big(b + f^{-1}(J)\Big)\Big) &= \theta\Big(a\,b + f^{-1}(J)\Big) = f(a\,b) + J \\ &= \Big(f(a)\,f(b)\Big) + J \\ &= \Big(f(a) + J\Big)\,\Big(f(b) + J\Big) \\ &= \theta\Big(a + f^{-1}(J)\Big)\,\theta\Big(b + f^{-1}(J)\Big) \end{aligned}$$

Analogamente, provamos que θ respeita a operação de adição. Logo θ é um morfismo.

Dados $a, b \in A$, suponhamos que $\theta(a + f^{-1}(J)) = \theta(b + f^{-1}(J))$. Então $f(a) + J = f(b) + J$, donde $f(a) - f(b) \in J$, pelo que $f(a-b) \in J$. Portanto, $a - b \in f^{-1}(J)$ e temos $a + f^{-1}(J) = b + f^{-1}(J)$. Logo θ é injectiva. Provámos pois que θ é um mergulho. ∎

Nota. Suponhamos que A e B são anéis com identidade e $f\colon A \to B$ é um morfismo entre anéis com identidade. Se J é ideal de B, então já vimos que B/J e $A/f^{-1}(J)$ são anéis. Além disso, se $J \neq B$ e $f^{-1}(J) \neq A$ então são anéis com identidade $1_B + J$ e

$1_A + f^{-1}(J)$, respectivamente, e o mergulho θ da última demonstração também é morfismo de anéis com identidade, pois

$$\theta\Big(1_A + f^{-1}(J)\Big) = f(1_A) + J = 1_B + J.$$

1.2 Teoremas do Isomorfismo

Vamos agora estudar mais alguns resultados que tratam de morfismos, ideais e anéis quocientes.

1º Teorema do Isomorfismo. *Sejam A e B anéis e $\theta\colon A \to B$ um morfismo. Então $\theta(A)$ é subanel de B, $\operatorname{Ker}\theta$ é ideal de A e tem-se $\theta(A) \simeq A/\operatorname{Ker}\theta$.*

Demonstração. As duas primeiras afirmações resultam da Proposição 3. A terceira é consequência do Teorema 8. ∎

Alguns autores também chamam a este resultado teorema de homomorfismo. Vejamos agora o que nos diz o chamado 2º Teorema do Isomorfismo.

2º Teorema do Isomorfismo. *Sejam A um anel, I um ideal de A e S um subanel de A. Então*

a) *$I + S = \{i + s\colon i \in I,\ s \in S\}$ é subanel de A e contém I;*

b) *$I \cap S$ é ideal de S;*

c) *$S/(I \cap S) \simeq (I + S)/I$.*

Demonstração:

a) Este facto já foi mencionado atrás.

b) Sendo I e S subanéis de A, temos que $I \cap S$ é subanel de A e, estando contido em S, é subanel de S. Por outro lado, dados $i \in I \cap S$ e $s \in S$, temos $is, si \in I$ por I ser ideal de A, e $is, si \in S$ por S ser subanel, logo $is, si \in I \cap S$. Portanto $I \cap S$ é ideal de S.

c) Poderíamos provar directamente que $S/(I \cap S) \simeq (I+S)/I$, isto é, apresentando um isomorfismo concreto entre estes anéis; no entanto, vamos fazer a demonstração usando o epimorfismo canónico $\theta\colon\ A \twoheadrightarrow A/I$, $a \mapsto a+I$.

Comecemos por observar que, atendendo à alínea a), podemos falar no quociente $(I+S)/I$.

Consideremos agora a restrição de θ a S,

$$\phi\colon\ S \to A/I\,, \qquad s \mapsto s+I$$

É claro que, sendo θ um morfismo, ϕ também o é e temos $\phi(S) \simeq S/\operatorname{Ker}\phi$, pelo 1º Teorema do Isomorfismo. Ora, por um lado, $\operatorname{Ker}\phi = \{s \in S\colon\ s+I = I\} = \{s \in S\colon\ s \in I\} = I \cap S$ e, por outro, $\phi(S) = \theta(S)$. Mas $\theta(S) = \{s+I\colon\ s \in S\} = (I+S)/I$. De facto, como $S \subseteq I+S$ obtemos $\theta(S) \subseteq (I+S)/I$ e, dados $i \in I$, $s \in S$, tem-se $(i+s)+I = (i+I)+(s+I) = I+(s+I) = s+I \in \theta(S)$. Assim, $S/(I \cap S) \simeq (I+S)/I$, como pretendíamos. ∎

Vejamos um exemplo de aplicação do teorema anterior.

Exemplo.

Sejam $A = \mathbb{Z}$ e $I = 4\,\mathbb{Z}$. Então $I \trianglelefteq A$. Seja $S = 6\,\mathbb{Z}$, subanel de $\mathbb{Z}$. Temos

$$\begin{aligned} I+S &= \left\{4x+6y\colon\ x,y \in \mathbb{Z}\right\} \\ I \cap S &= 12\,\mathbb{Z} \end{aligned}$$

Observemos que $I+S = 2\,\mathbb{Z}$. De facto, $I+S \subseteq 2\,\mathbb{Z}$ e dado $2u$, com $u \in \mathbb{Z}$, temos $2 = 6-4$, donde

$$2u \;=\; (-4+6)\,u \;=\; -4u+6u \;\in\; I+S$$

Pelo 2º Teorema do Isomorfismo, obtemos

$$S/(I \cap S) \simeq (I+S)/I, \qquad \text{isto é,} \qquad 6\,\mathbb{Z}/12\,\mathbb{Z} \simeq 2\,\mathbb{Z}/4\,\mathbb{Z}$$

Vejamos quais são os elementos de $6\,\mathbb{Z}/12\,\mathbb{Z}$ e as tabelas de Cayley que definem as operações neste anel. Temos

$$6\,\mathbb{Z} = \Big\{\ldots, -12, -6, 0, 6, 12, 18, 24, 30, \ldots\Big\}$$
$$12\,\mathbb{Z} = \Big\{\ldots, -12, 0, 12, 24, \ldots\Big\}$$

Os elementos de $6\,\mathbb{Z}$ são da forma $6(2k)$ ou $6(2k+1)$, com $k \in \mathbb{Z}$. Temos

$$6(2k) + 12\,\mathbb{Z} = 12\,\mathbb{Z} = [0]$$
$$6(2k+1) + 12\,\mathbb{Z} = 6 + 12\,\mathbb{Z} = [6]$$

Assim, $6\,\mathbb{Z}/12\,\mathbb{Z}$ tem apenas dois elementos, nomeadamente [0] e [6], e as respectivas tabelas de Cayley são as seguintes:

$+$	[0]	[6]
[0]	[0]	[6]
[6]	[6]	[0]

$\cdot$	[0]	[6]
[0]	[0]	[0]
[6]	[0]	[0]

O terceiro teorema do isomorfismo, cuja demonstração deixamos ao cuidado do leitor (ver Allenby, por exemplo), diz-nos o seguinte:

3º Teorema do Isomorfismo. *Sejam A um anel e I e K ideais de A tais que $I \subseteq K$. Então*

a) *I é ideal de K e o anel $K/I = \{k + I\colon\ k \in K\}$ é ideal de A/I;*

b) *$(A/I)/(K/I) \simeq A/K$.*

1.3 Característica de um anel com identidade

Dado um anel com identidade, pode acontecer que exista $m \in \mathbb{N}$ tal que $m\,1 = 0$. Por exemplo, em $(\mathbb{Z}_n, +, \cdot)$ temos $n\,1 = 0$, mas para $(\mathbb{Z}, +, \cdot)$ não existe um m nestas condições.

Definição. Seja A um anel com identidade. Se existe $m \in \mathbb{N}$ tal que $m\,1 = 0$, dizemos que A tem *característica* n, sendo $n = \min\{m \in \mathbb{N}\colon m\,1 = 0\}$. Se não existe $m \in \mathbb{N}$ nestas condições, dizemos que A tem *característica* 0.

Denotamos a característica de A por $c(A)$.

Observemos que a condição $m\,1 = 0$ é equivalente à condição $m\,a = 0$, para qualquer $a \in A$.

Exemplo.

Temos $c(\mathbb{Z}_n) = n$, com $n \geqslant 2$, e $c(\mathbb{Z}) = 0$.

É fácil provar que, dado um anel A com identidade 1_A, se B é um subanel com identidade 1_B igual a 1_A, então $c(B) = c(A)$.

Teorema 11. *Seja A um anel com identidade. Seja $\varphi\colon \mathbb{Z} \to A$ a aplicação definida por $\varphi(x) = x\,1$, para qualquer $x \in \mathbb{Z}$. Então*

a) *φ é morfismo de anéis com identidade;*

b) *São equivalentes as condições seguintes: dado $n \in \mathbb{N}$ e $n \geqslant 2$,*

1) *$c(A) = n$;*

2) *n é gerador do ideal* $\operatorname{Ker}\varphi$*;*

3) *$\varphi(\mathbb{Z})$ é subanel com identidade de A isomorfo a $\mathbb{Z}_n$.*

Demonstração: **a**) Dados $m, u \in \mathbb{Z}$, é claro que $\varphi(m+u) = \varphi(m)+\varphi(u)$, $\varphi(m\,u) = \varphi(m)\,\varphi(u)$ e $\varphi(1) = 1$. Portanto, φ é morfismo de anéis com identidade.

b) Provemos que 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 1).

1) $\Rightarrow$ 2) Temos $\operatorname{Ker}\varphi = \{m \in \mathbb{Z} : m1 = 0\}$. Como φ é morfismo então $\operatorname{Ker}\varphi$ é um ideal de $\mathbb{Z}$ e é gerado pelo menor $m \in \mathbb{N}_0$ em $\operatorname{Ker}\varphi$ (ver Exercício 13), isto é pela característica de A.

2) $\Rightarrow$ 3) Pelo 1º Teorema do Isomorfismo, temos $\mathbb{Z}/\operatorname{Ker}\varphi \simeq \varphi(\mathbb{Z})$.

Como $\operatorname{Ker}\varphi = \langle n \rangle$ por hipótese, concluímos que $\mathbb{Z}_n \simeq \varphi(\mathbb{Z})$.

3) $\Rightarrow$ 1) Comecemos por observar que se dois anéis com identidade são isomorfos (como anéis com identidade), então têm a mesma característica. Suponhamos que $\mathbb{Z}_n \simeq \varphi(\mathbb{Z})$. Como $c(\mathbb{Z}_n) = n$, então $c(\varphi(\mathbb{Z})) = n$. Por outro lado, sendo $\varphi(\mathbb{Z})$ um subanel de A tal que $1 \in \varphi(\mathbb{Z})$, temos $c(\varphi(\mathbb{Z})) = c(A)$. Portanto, $c(A) = n$. ∎

Nota. Sendo $\varphi\colon \mathbb{Z} \to A$ o morfismo de anéis com identidade do teorema anterior, é claro que $c(A) = 0$ se e só se $\operatorname{Ker}\varphi = \{0\}$. Logo, se $c(A) = 0$, então φ é um mergulho e $\mathbb{Z} \simeq \varphi(\mathbb{Z})$.

1.4 Extensões de anéis

Dado um anel A, pretendemos saber se é possível mergulhá-lo noutro anel B com uma estrutura mais rica, por exemplo, num corpo.

Definição. Sejam A e B anéis. Dizemos que B é *extensão* de um anel A se existe um mergulho de A em B, o que é equivalente a dizer que A é isomorfo a um subanel de B.

Quando A e B têm identidade, os mergulhos considerados serão de anel com identidade, a não ser que se diga algo em contrário.

Comecemos por mostrar que todo o anel sem identidade se mergulha num anel com identidade.

Teorema 12. *Todo o anel sem identidade A admite uma extensão que é anel com identidade.*

Demonstração: Seja $B = A \times \mathbb{Z}$. Em B definimos operações de adição e de multiplicação do seguinte modo: dados $a_1, a_2 \in A$, $m_1, m_2 \in \mathbb{Z}$,

$$(a_1, m_1) + (a_2, m_2) = (a_1 + a_2, m_1 + m_2)$$
$$(a_1, m_1)\,(a_2, m_2) = (a_1\,a_2 + m_2\,a_1 + m_1\,a_2,\ m_1\,m_2)$$

Obtemos um anel com zero $(0,0)$ e identidade $(0,1)$. Seja

$$\begin{aligned} f\colon\ & A \to B \\ & a \mapsto (a,0) \end{aligned}$$

é fácil provar que f é morfismo injectivo, pelo que B é extensão de A. ∎

Já provámos que todo o anel se mergulha num anel com identidade. Queremos agora saber quando é que um anel B com identidade se mergulha num corpo. Se B é mergulhável num corpo K, então é isomorfo a um subanel de K, logo tem de ser comutativo e não pode ter divisores de zero. Portanto, B tem de ser um domínio de integridade.

Vamos agora mostrar que, de facto, todo o domínio de integridade admite uma extensão que é corpo.

Teorema 13. *Seja D um domínio de integridade. Então existe um corpo K que é extensão de D.*

Demonstração: No conjunto $D \times (D\backslash\{0\})$ definamos uma relação binária $\sim$ do seguinte modo: dados $(a,b),(c,d) \in D\times(D\backslash\{0\})$,

$$(a,b) \sim (c,d) \quad \text{se e só se} \quad ad = bc$$

Como D é comutativo, a relação $\sim$ é reflexiva e simétrica. Sejam $(a,b),(c,d),(e,f) \in D\times(D\backslash\{0\})$ tais que $(a,b)\sim(c,d)$ e $(c,d)\sim(e,f)$. Então, $ad = bc$ e $cf = de$, donde

$$adf = bcf = bde$$

Logo $adf - bde = 0$, pelo que $d(af - be) = 0$. Como D não tem divisores de zero e $d \neq 0$, então $af - be = 0$. Logo $af = be$ e, portanto, $(a,b) \sim (e,f)$. Assim, $\sim$ é transitiva. Concluímos que $\sim$ é uma equivalência em $D\times(D\backslash\{0\})$.

Dado um elemento $(a,b) \in D \times (D\backslash\{0\})$, representemos a sua $\sim$-classe pela fracção $\frac{a}{b}$ e denotemos por K o conjunto quociente $(D \times (D\backslash\{0\}))/\sim$. Em K definimos operações de adição e de multiplicação do seguinte modo: dados $\frac{a}{b}, \frac{c}{d} \in K$,

$$\frac{a}{b} + \frac{c}{d} = \frac{a\,d + b\,c}{b\,d} \quad \text{e} \quad \frac{a}{b}\,\frac{c}{d} = \frac{a\,c}{b\,d}$$

Vejamos que estas operações estão bem definidas. Comecemos por observar que dados $\frac{a}{b}, \frac{c}{d} \in K$, temos $b\,d \neq 0$, pois $b, d \in D\backslash\{0\}$ e D é domínio de integridade. Assim, $\frac{a\,d+b\,c}{b\,d}, \frac{a\,c}{b\,d} \in K$. Consideremos $\frac{a}{b} = \frac{a'}{b'}$ e $\frac{c}{d} = \frac{c'}{d'}$. Então $a\,b' = b\,a'$ e $c\,d' = d\,c'$. Vejamos que $\frac{a\,c}{b\,d} = \frac{a'c'}{b'd'}$. De facto, temos $a'c'b\,d = b\,a'd\,c' = a\,b'c\,d' = b'd'a\,c$. Quanto à demonstração da igualdade $\frac{a\,d+b\,c}{b\,d} = \frac{a'd'+b'c'}{b'd'}$, observemos que

$$a\,b' - b\,a' = 0 = d\,c' - c\,d'$$

pelo que

$$(a\,b' - b\,a')\,d\,d' = (d\,c' - c\,d')\,b\,b'$$

Como D é comutativo, obtemos

$$a\,d\,b'd' - b\,d\,a'd' = b\,d\,b'c' - b\,c\,b'd'$$

donde

$$a\,d\,b'd' + b\,c\,b'd' = b\,d\,a'd' + b\,d\,b'c'$$

e, portanto,

$$\frac{a\,d+b\,c}{b\,d} = \frac{a'd'+b'c'}{b'd'}\ .$$

O leitor está agora em condições de poder provar que $(K, +, \cdot)$ é corpo com zero $\frac{0}{1}$ e identidade $\frac{1}{1}$. Notemos que se $a \in D\backslash\{0\}$, então $\frac{a}{a} = \frac{1}{1}$ e $\frac{0}{a} = \frac{0}{1}$. Observemos também que o inverso de $\frac{a}{b} \neq \frac{0}{1}$ é $\frac{b}{a}$.

Encontrado o corpo $(K, +, \cdot)$, consideremos a aplicação

$$\begin{aligned} \theta\colon\ D &\to K \\ a &\mapsto \frac{a}{1} \end{aligned}$$

e mostremos que θ é um mergulho. Suponhamos que $a, b \in D$ são tais que $\frac{a}{1} = \frac{b}{1}$. Então $a\,1 = b\,1$ e, portanto, $a = b$. Logo θ é injectiva. Temos também

$$\theta(a\,b) = \frac{a\,b}{1} = \frac{a}{1}\,\frac{b}{1} = \theta(a)\,\theta(b)$$

$$\theta(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \theta(a) + \theta(b)$$

Finalmente, $\theta(1) = \frac{1}{1}$. Assim, θ é um mergulho de anéis com identidade. ∎

Definição. Dado um domínio de integridade D, ao corpo K construído no teorema anterior damos o nome de *corpo das fracções* de D.

Em geral, um elemento a do domínio de integridade D identifica-se com o elemento $\frac{a}{1}$ do seu corpo das fracções K.

Vamos agora mostrar que, em certo sentido, K é o "menor" corpo que é extensão de D.

Teorema 14. *Sejam D um domínio de integridade e C um corpo que é extensão de D. Então C é extensão do corpo K das fracções de D.*

Demonstração: Seja $g\colon D \hookrightarrow C$ um mergulho. Definamos

$$\begin{aligned} \overline{g}\colon\ & K \to C \\ & \frac{a}{b} \mapsto g(a)\, g(b)^{-1} \end{aligned}$$

Vejamos que $\overline{g}$ está bem definida. Como g é injectivo, temos $g(b) = 0$ se e só se $b = 0$, pelo que dado $\frac{a}{b} \in K$ existe $g(b)^{-1}$. Suponhamos $\frac{a}{b} = \frac{c}{d} \in K$. Então $a\,d = b\,c$, donde $g(a\,d) = g(b\,c)$. Logo $g(a)\, g(d) = g(b)\, g(c)$, em que $g(d), g(b) \neq 0$. Portanto, $g(a)\, g(b)^{-1} = g(c)\, g(d)^{-1}$. Concluímos que $\overline{g}$ está bem definida.

Sejam $\frac{a}{b}, \frac{c}{d} \in K$. Então

$$\begin{aligned} \overline{g}\left(\frac{a}{b}\,\frac{c}{d}\right) = \overline{g}\left(\frac{a\,c}{b\,d}\right) &= g(a\,c)\, g(b\,d)^{-1} \\ &= g(a)\, g(c)\, \Big(g(b)\, g(d)\Big)^{-1} \\ &= g(a)\, g(c)\, g(d)^{-1}\, g(b)^{-1} \\ &= g(a)\, g(b)^{-1}\, g(c)\, g(d)^{-1} = \overline{g}\left(\frac{a}{b}\right) \overline{g}\left(\frac{c}{d}\right) \end{aligned}$$

e

$$\begin{aligned}\overline{g}\Big(\frac{a}{b}+\frac{c}{d}\Big) &= \overline{g}\Big(\frac{a\,d+b\,c}{b\,d}\Big) = g(a\,d+b\,c)\,g(b\,d)^{-1}\\ &= \Big(g(a)\,g(d)+g(b)\,g(c)\Big)\,g(d)^{-1}\,g(b)^{-1}\\ &= g(a)\,g(b)^{-1}+g(c)\,g(d)^{-1}\\ &= \overline{g}\Big(\frac{a}{b}\Big)+\overline{g}\Big(\frac{c}{d}\Big)\end{aligned}$$

Além disso, $\overline{g}(\frac{1}{1}) = g(1)\,g(1)^{-1} = 1$. Portanto, $\overline{g}$ é um morfismo de anéis com identidade. Finalmente, provemos que $\overline{g}$ é injectiva. Se $\overline{g}(\frac{a}{b}) = \overline{g}(\frac{c}{d})$, então $g(a)\,g(b)^{-1} = g(c)\,g(d)^{-1}$, donde $g(a)\,g(d) = g(c)\,g(b)$. Logo, $g(a\,d) = g(c\,b)$ e, portanto, $a\,d = c\,b$, pois g é injectiva. Assim, $\frac{a}{b} = \frac{c}{d}$. Fica assim provado que $\overline{g}$ é um mergulho de K em C. Note que ao calcularmos o inverso $g(bd)^{-1}$ usámos $(g(b)\,g(d))^{-1} = g(d)^{-1}\,g(b)^{-1}$, como é usual num grupo, porém num corpo C tal é igual a $g(b)^{-1}\,g(d)^{-1}$, por $(C\backslash\{0\},\cdot)$ ser um grupo comutativo. Fizemo-lo propositadamente para recordar ao leitor o que se passa num grupo arbitrário.∎

Observemos ainda que a aplicação $\overline{g}$, definida na demonstração anterior, é o único mergulho de K em C que estende g. Vejamos que $\overline{g}$ estende g. De facto, para qualquer $a \in D$, temos

$$\overline{g}(a) = g(a)$$

identificando a com $\frac{a}{1}$, pois $\overline{g}(\frac{a}{1}) = g(a)\,g(1)^{-1} = g(a)$. Por outro lado, se houvesse outro mergulho θ de K em C que estendesse g, isto é, tal que, para qualquer $a \in D$, se tivesse $\theta(a) = g(a)$, então, dados $a, b \in D$ tais que $b \neq 0$, teríamos

$$\begin{aligned}\theta\Big(\frac{a}{b}\Big) &= \theta\Big(\frac{a}{1}\,\frac{1}{b}\Big) = \theta\Big(\frac{a}{1}\Big)\,\theta\Big(\frac{1}{b}\Big)\\ &= \theta\Big(\frac{a}{1}\Big)\,\theta\Big(\Big(\frac{b}{1}\Big)^{-1}\Big) = \theta\Big(\frac{a}{1}\Big)\,\Big(\theta\Big(\frac{b}{1}\Big)\Big)^{-1}\\ &= g(a)\,g(b)^{-1} = \overline{g}\Big(\frac{a}{b}\Big)\end{aligned}$$

Portanto, $\theta = \overline{g}$.

Exemplo.

Como bem se conhece, $\mathbb{Q}$ é o corpo das fracções de $\mathbb{Z}$.

1.5 Ideais primos e maximais de anéis comutativos com identidade

Já vimos que a partir de um anel A e de um ideal I de A podemos construir um novo anel: o anel quociente A/I. Partindo, agora, de um anel comutativo com identidade, vamos considerar certos ideais especiais os quais determinam quocientes que ou são domínios de integridade ou são corpos.

Definição. Seja A um anel comutativo. Um ideal I de A diz-se *primo* se $I \neq A$ e

$$\forall\, x, y \in A,\ x\,y \in I \Longrightarrow x \in I \text{ ou } y \in I$$

Exemplos.

Consideremos o anel $(\mathbb{Z}, +, \cdot)$ e os ideais $\langle 5\rangle$ e $\langle 6\rangle$. Temos $\langle 5\rangle = 5\,\mathbb{Z} \neq \mathbb{Z}$ e $\langle 6\rangle = 6\,\mathbb{Z} \neq \mathbb{Z}$. O ideal $\langle 5\rangle$ é primo pois, dados $x, y \in \mathbb{Z}$,

$$\begin{aligned} x\,y \in 5\,\mathbb{Z} &\Longrightarrow 5 \text{ divide } x\,y \\ &\Longrightarrow 5 \text{ divide } x \ \text{ ou } \ 5 \text{ divide } y \\ &\Longrightarrow x \in 5\,\mathbb{Z} \ \text{ ou } \ y \in 5\,\mathbb{Z} \end{aligned}$$

Já o ideal $\langle 6\rangle$ não é primo, visto que $2 \cdot 3 \in \langle 6\rangle$ e $2, 3 \notin \langle 6\rangle$.

Teorema 15. *Sejam A um anel comutativo com identidade e I um ideal de A. Então I é primo se e só se A/I é domínio de integridade.*

Demonstração: Suponhamos que I é primo. Então $I \neq A$, pelo que $1 \notin I$. Logo, $1 + I \neq I$. Portanto, A/I é um anel com identidade

$1 + I$. Como A é comutativo, A/I também o é. Provemos que A/I não tem divisores de zero. Sejam $x, y \in A$ tais que $(x+I)\,(y+I) = I$. Então $x\,y + I = I$, donde $x\,y \in I$. Como I é primo, temos $x \in I$ ou $y \in I$, logo $x + I = I$ ou $y + I = I$. Portanto, A/I é domínio de integridade.

Reciprocamente, suponhamos que A/I é domínio de integridade. Sejam $x, y \in A$ tais que $x\,y \in I$. Então $I = x\,y + I = (x + I)\,(y + I)$ e, como A/I não tem divisores de zero, temos $I = x + I$ ou $I = y + I$. Logo $x \in I$ ou $y \in I$. Por outro lado, sendo A/I domínio de integridade, temos $1 + I \neq I$, donde $1 \notin I$ e, portanto, $I \neq A$. Concluímos assim que I é um ideal primo. ∎

Vamos agora caracterizar os ideais que determinam quocientes que são corpos.

Definição. Seja A um anel comutativo. Um ideal I de A diz-se *maximal* se $I \neq A$ e

$$\forall\, J \trianglelefteq A,\ I \subseteq J \subsetneqq A \Longrightarrow I = J$$

isto é, o ideal I é elemento maximal do conjunto dos ideais próprios de A para a relação de inclusão. Tenha presente que a segunda condição é equivalente a

$$\forall\, J \trianglelefteq A,\ I \subsetneqq J \Longrightarrow J = A$$

Exemplos. Consideremos o anel $(\mathbb{Z}, +, \cdot)$. O ideal $\{0\}$ é primo, mas não é maximal. O ideal $\langle 5\rangle$ é primo e maximal. O ideal $\langle 10\rangle$ não é maximal, pois $\langle 10\rangle \subsetneqq \langle 5\rangle \subsetneqq \mathbb{Z}$, e não é primo, pois $2 \cdot 5 \in \langle 10\rangle$ mas $2, 5 \notin \langle 10\rangle$. Também podemos ter ideais maximais não primos? Vamos ver que não.

Teorema 16. *Sejam A um anel comutativo com identidade e I um ideal de A. Então, I é maximal se e só se A/I é corpo.*

Demonstração: Suponhamos que I é maximal. Então $I \neq A$ e, portanto, $1 + I \neq I$. Seja $x \in A$ tal que $x + I \neq I$. Então $x \notin I$.

Provemos que $x + I$ tem inverso em A/I. Consideremos os ideais $\langle x \rangle$ e $I + \langle x \rangle$. Como $I \subsetneq I + \langle x \rangle$ e I é maximal, temos $I + \langle x \rangle = A$. Logo, $1 \in I + \langle x \rangle$. Uma vez que A é comutativo com identidade, $\langle x \rangle = xA$ e, portanto, existem $i \in I$ e $t \in A$ tais que $1 = i + x\,t$, donde

$$1 + I = (i + I) + (x + I)\,(t + I) = (x + I)\,(t + I)$$

pelo que o elemento não nulo $x + I$ de A/I tem inverso $t + I$. Como A/I é comutativo com identidade, concluímos que A/I é corpo.

Reciprocamente, suponhamos que A/I é corpo. Então $I \neq 1 + I$, donde $1 \notin I$ e, portanto, $I \neq A$. Tomemos um ideal J de A tal que $I \subsetneq J$. Seja $x \in J \backslash I$. Então $x + I \neq I$ pelo que existe inverso de $x + I$, digamos $y + I$. Assim

$$1 + I = (x + I)\,(y + I) = x\,y + I$$

donde $1 = x\,y + z$, para certo $z \in I$. Como $I \subseteq J$, temos $z \in J$ e, como $x \in J$, concluímos que $1 \in J$. Logo $J = A$. Portanto, I é maximal. ∎

Proposição 17. *Seja A um anel comutativo com identidade. Se um ideal I de A é maximal, então é primo.*

Demonstração: Suponhamos I maximal. Então, pelo Teorema 16, o anel A/I é corpo. Logo A/I é domínio de integridade e, portanto, pelo Teorema 15, o ideal I é primo. ∎

1.6 Elementos primos e elementos irredutíveis num anel comutativo com identidade

Recordemos que no nosso protótipo, $\mathbb{Z}$, existem elementos com comportamento muito especial: os números primos. É bem sabido, por exemplo, que todo o inteiro maior do que 1 se pode factorizar em primos, de modo único a menos da ordem dos factores (Teorema Fundamental da Aritmética).

Num anel A arbitrário também podem existir elementos especiais, que designamos por elementos irredutíveis e, sob certas condições, pode ser possível, como veremos à frente, factorizar certos elementos em irredutíveis.

Definição. Seja A um anel com identidade 1. Um elemento $a \in A$ diz-se *unidade* de A se existe $b \in A$ tal que $a\,b = b\,a = 1$.

Representamos por $\mathcal{U}(A)$ o conjunto das unidades de A. É claro que $(\mathcal{U}(A), \cdot)$ constitui um grupo.

Exemplos.

Temos $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$, $\mathcal{U}(\mathbb{Q}) = \mathbb{Q}\backslash\{0\}$ e $\mathcal{U}(\mathbb{Z}_4) = \{1, 3\}$.

Definição. Seja A um anel comutativo com identidade. Dados $a, b \in A$, dizemos que a é *associado* de b se existe $u \in \mathcal{U}(A)$ tal que $a = b\,u$.

Observemos que se $u \in \mathcal{U}(A)$ e $a = b\,u$, então $b = a\,u^{-1}$. Logo, b é associado de a. Dizemos, por isso, que a e b são *elementos associados*.

Notemos também que a é associado de 1 se e só se $a \in \mathcal{U}(A)$.

Definição. Seja A um anel comutativo com identidade. Um elemento $a \in A$ não nulo que não seja unidade de A diz-se *irredutível* se, para quaisquer $x, y \in A$,

$$a = x\,y \implies x \in \mathcal{U}(A) \text{ ou } y \in \mathcal{U}(A)$$

Convém ter presente que se $a \in A$ é irredutível e $u \in \mathcal{U}(A)$, então ua é irredutível.

Definição. Um domínio de integridade em que todo o ideal é principal diz-se um *domínio de ideais principais* (DIP).

Exemplo.

O anel $\mathbb{Z}$ é um domínio de ideais principais.

Num domínio de ideais principais, os elementos irredutíveis estão intrinsecamente relacionados com os ideais maximais.

Teorema 18. *Sejam D um domínio de integridade e $a \in D\backslash\{0\}$. Então*

a) *se $\langle a\rangle$ é ideal maximal de D, então a é irredutível;*

b) *se D é domínio de ideais principais, $\langle a\rangle$ é ideal maximal se e só se a é irredutível.*

Antes de passarmos a demonstrar este teorema, provemos alguns resultados que convém ter presente.

Lema 19. *Seja A um anel comutativo com identidade. Dados $a, b \in A$, temos*

$$\langle a\rangle \subseteq \langle b\rangle \quad \text{se e só se } \exists\, x \in A,\ \ a = b\,x\ .$$

Demonstração: Recordemos que dado $a \in A$, temos $\langle a\rangle = a\,A$. É claro que se $a = b\,x$, então $\langle a\rangle \subseteq \langle b\rangle$. Reciprocamente, se $\langle a\rangle \subseteq \langle b\rangle$, então $a \in \langle b\rangle = b\,A$, donde $a = b\,x$, para algum $x \in A$. ∎

Lema 20. *Seja D um domínio de integridade. Dados $a, b \in D$, temos:*

a) *$\langle a\rangle = \langle b\rangle$ se e só se a e b são associados;*

b) *$\langle a\rangle = D$ se e só se $a \in \mathcal{U}(D)$.*

Demonstração: **a**) Se a e b são associados, então existe $u \in \mathcal{U}(D)$ tal que $a = b\,u$ e $b = a\,u^{-1}$, donde, pelo Lema 19, temos $\langle a\rangle \subseteq \langle b\rangle$ e $\langle b\rangle \subseteq \langle a\rangle$. Logo $\langle a\rangle = \langle b\rangle$.

Reciprocamente, se $\langle a\rangle = \langle b\rangle$, então existem $x, y \in D$ tais que $a = b\,x$ e $b = a\,y$. Logo $a = a\,y\,x$ donde $a(1 - y\,x) = 0$. Se $a \neq 0$, como D é domínio de integridade, obtemos $1 - y\,x = 0$, pelo que $1 = y\,x$; logo $x \in \mathcal{U}(D)$ e, assim, a e b são associados. Se $a = 0$ temos

$b = 0$ e, portanto, são associados.

b) Tendo em conta que $D = \langle 1 \rangle$ e que a é associado de 1 se e só se $a \in \mathcal{U}(D)$, o resultado sai de a). ∎

Demonstração do Teorema 18: **a**) Suponhamos que $\langle a \rangle$ é maximal. Então $\langle a \rangle \neq D$, pelo que $a \notin \mathcal{U}(D)$. Se $a = x\,y$ para certos $x, y \in D$, então

$$\langle a \rangle \subseteq \langle x \rangle$$

Como $\langle a \rangle$ é maximal, temos $\langle x \rangle = D$ ou $\langle x \rangle = \langle a \rangle$. Se $\langle x \rangle = D$, pela alínea b) do lema anterior, $x \in \mathcal{U}(D)$. Se $\langle a \rangle = \langle x \rangle$, pela alínea a) do mesmo lema, $a = x\,u$ para certo $u \in \mathcal{U}(D)$. Então $x\,y = x\,u$ donde $x(y - u) = 0$, pelo que $y - u = 0$ (visto que $x \neq 0$, pois $a = x\,y \neq 0$). Portanto, $y = u \in \mathcal{U}(D)$. Logo a é irredutível.

b) Reciprocamente, suponhamos que D é domínio de ideais principais e que a é irredutível. Então $a \notin \mathcal{U}(D)$, donde $\langle a \rangle \neq D$. Seja I um ideal de D tal que $\langle a \rangle \subseteq I$. Como D é domínio de ideais principais, existe $x \in D$ tal que $I = \langle x \rangle$. Então $a = x\,y$, para certo $y \in D$. Sendo a irredutível, temos $x \in \mathcal{U}(D)$ ou $y \in \mathcal{U}(D)$. Se $x \in \mathcal{U}(D)$, então $\langle x \rangle = D$, pelo Lema 20.b). Se $y \in \mathcal{U}(D)$, então $\langle a \rangle = \langle x \rangle$, pelo Lema 20.a). Logo $\langle a \rangle$ é maximal. ∎

Corolário 18.1. *Sejam D um domínio de ideais principais e $a \in D \backslash \{0\}$. Então $D/\langle a \rangle$ é corpo se e só se a é irredutível.*

Demonstração: Já provámos que $D/\langle a \rangle$ é corpo se e só se $\langle a \rangle$ é maximal. O resultado sai então do teorema anterior. ∎

Seja A um anel comutativo. Dados $p, x \in A$, dizemos que p *divide* x se $x = p\,y$, para algum $y \in A$. Não havendo perigo de confusão, escrevemos p/x.

Em $\mathbb{Z}$, um elemento p diz-se *primo* se $p \notin \{-1, 1, 0\}$ e

$$p/a\,b \implies p/a \text{ ou } p/b$$

Por outro lado, já definimos um elemento *irredutível* $p \in \mathbb{Z}$ como

sendo $p \notin \{-1, 1, 0\}$ tal que

$$p = x\,y \implies x \in \{-1, 1\} \text{ ou } y \in \{-1, 1\}$$

Como é bem conhecido, em $\mathbb{Z}$ estas definições são equivalentes.

Vamos, agora, definir elemento primo num anel comutativo com identidade arbitrário, observando desde já que há anéis em que os conceitos de elemento primo e de elemento irredutível não coincidem.

No que se segue, convém ter presente que se x é um elemento irredutível de um anel A comutativo com identidade e $p \in A$ é tal que p/x e $p \notin \mathcal{U}(A)$, então p e x são associados.

Definição. Seja A um anel comutativo com identidade. Um elemento $p \in A$ não nulo e que não seja unidade diz-se *primo* se, dados $a, b \in A$,

$$p/a\,b \implies p/a \text{ ou } p/b$$

Proposição 21. *Seja D um domínio de integridade. Se $p \in D$ é primo, então p é irredutível.*

Demonstração: Se p é primo, então $p \in D\backslash\Big(\{0\} \cup \mathcal{U}(D)\Big)$. Suponhamos que $p = xy$. Então p/xy, pelo que p/x ou p/y. Se p/x, temos $x = pa$, para algum $a \in D$. Então $p = pay$, pelo que $p(1 - ay) = 0$ donde, como $p \neq 0$, temos $1 - ay = 0$. Logo, $1 = ay$ e, assim, $y \in \mathcal{U}(D)$. Analogamente, se p/y, então $x \in \mathcal{U}(D)$. Portanto, p é irredutível. ∎

Proposição 22. *Seja D um domínio de ideais principais. Um elemento $p \in D$ é primo se e só se é irredutível.*

Demonstração: Seja $p \notin \{0\} \cup \mathcal{U}(D)$. Atendendo à proposição anterior, resta provar que se p é irredutível, então p é primo. Suponhamos que p é irredutível e que p/ab com $a, b \in D$. Se $ab = 0$, é claro que, em D, temos $a = 0$ ou $b = 0$, logo p/a ou p/b. Se $ab \neq 0$, então $a, b \neq 0$. Tomemos $I = \langle p, b\rangle$. Sendo D um domínio de ideais

principais, existe $d \in D$ tal que $I = \langle d \rangle = d\,D$. Seja $x \in D$ tal que $p = dx$. Como p é irredutível, $x \in \mathcal{U}(D)$ ou $d \in \mathcal{U}(D)$, não podendo ser ambos unidades pois o produto de unidades é unidade e $p \notin \mathcal{U}(D)$. Suponhamos que $x \in \mathcal{U}(D)$. Então, pelo Lema 20.a), $\langle d \rangle = \langle p \rangle$ e, portanto, $b \in \langle p \rangle$. Logo p/b. Se $d \in \mathcal{U}(D)$, ficamos com $\langle d \rangle = D$ e obtemos $D = \langle p, b \rangle = \langle p \rangle + \langle b \rangle = p\,D + b\,D$. Assim, existem $u, v \in D$ tais que $1 = pu + bv$, donde $a = apu + abv$. Como p/ab, temos que p/a. Concluímos pois que p é primo. ∎

Exemplos.

1) Como $\mathbb{Z}$ é domínio de ideais principais, os conceitos de primo e irredutível são equivalentes em $\mathbb{Z}$, como já observámos.

2) Seja $R = \mathbb{Z}[\sqrt{-5}]$. Como já observámos, R é um subanel com identidade de $(\mathbb{C}, +, \cdot)$, pelo que R é domínio de integridade. Temos $\mathcal{U}(R) = \{-1, 1\}$. Consideremos o elemento 2. Podemos provar que, em R, o elemento 2 é irredutível. Mas 2 não é primo pois, por exemplo, 2 divide $(1 + \sqrt{5}\,i)\,(1 - \sqrt{5}\,i) = 6$, mas 2 não divide $1 + \sqrt{5}\,i$, nem $1 - \sqrt{5}\,i$. Logo, pela proposição anterior, concluímos que R não é domínio de ideais principais.

1.7 Domínios euclidianos

A classe dos domínios de ideais principais contém uma classe especial, a dos domínios euclidianos.

Definição. Um *domínio euclidiano* é um domínio de integridade D munido de uma aplicação δ de $D\backslash\{0\}$ em $\mathbb{N}_0$ tal que, para quaisquer $a, b \in D\backslash\{0\}$,

i) $\delta(a) \leq \delta(a\,b)$;

ii) existem $m, r \in D$ tais que $a = m\,b + r$, com $r = 0$ ou $r \neq 0$ e, neste caso, $\delta(r) < \delta(b)$.

A aplicação δ diz-se uma *norma* em D.

Exemplos.

1) Os seguintes domínios de integridade são euclidianos:

a) $\mathbb{Z}$ com $\delta(a) = |a|$, para qualquer $a \in \mathbb{Z}\backslash\{0\}$;

b) Qualquer corpo K com $\delta(a) = 1$, para qualquer $a \in K\backslash\{0\}$;

c) $\mathbb{Z}[i]$ com $\delta(a + b\,i) = a^2 + b^2$, para qualquer elemento $a + b\,i$ não nulo de $\mathbb{Z}[i]$ (ver Allenby);

d) $\mathbb{Z}[\sqrt{-2}]$ com $\delta(a+b\sqrt{-2}) = a^2+2\,b^2$, para qualquer elemento $a + b\sqrt{-2}$ de $\mathbb{Z}[\sqrt{-2}]$ não nulo.

Nota. Observe que $\mathbb{C} = \mathbb{R}[i]$ com δ definido por $\delta(a+bi) = a^2+b^2$ não forma um domínio euclidiano.

2) O domínio de integridade $\mathbb{Z}[\sqrt{-6}]$ não é euclidiano (ver Exercício 35-b).

Teorema 23. *Todo o domínio euclidiano é domínio de ideais principais.*

Demonstração: Sejam D um domínio euclidiano e I um ideal de D. Se $I = \{0\}$, então $I = \langle 0\rangle$ e, portanto, I é principal. Suponhamos que $I \neq \{0\}$. Tomemos

$$\Big\{\delta(x)\colon\, x \in I\backslash\{0\}\Big\}$$

Tratando-se de um subconjunto não vazio de $\mathbb{N}_0$, tem elemento mínimo, digamos $\delta(b)$, com $b \in I\backslash\{0\}$. Vamos provar que $I = \langle b\rangle$.

É claro que $0 \in \langle b\rangle$. Seja $a \in I \setminus \{0\}$. Então existem $m, r \in D$ tais que $a = m\,b + r$, com $r = 0$ ou $r \neq 0$ e, neste caso, $\delta(r) < \delta(b)$. Se $r = 0$, temos $a = m\,b \in \langle b\rangle$. Se tivéssemos $r \neq 0$, obtínhamos $r = a - m\,b \in I\backslash\{0\}$ com $\delta(r) < \delta(b)$, o que é absurdo pela definição de b. Portanto, $I \subseteq \langle b\rangle$ e, como $b \in I$, temos $I = \langle b\rangle$. ∎

Exemplos.

1) Os domínios de integridade $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{-2}]$ e todo o

corpo K são domínios de ideais principais, visto serem euclidianos. A demonstração anterior dá-nos um método para achar um gerador de um ideal arbitrário destes anéis.

2) O domínio de integridade $\mathbb{Q}[\sqrt{-19}]$ é de ideais principais mas não é euclidiano (ver Allenby).

1.8 Domínios de factorização única

Estudaremos agora domínios de integridade onde todo o elemento não nulo que não seja unidade se pode escrever como produto de elementos irredutíveis.

Definição. Um domínio de integridade D diz-se um *domínio de factorização única* (DFU) se:

a) todo o elemento $a \in D\backslash\Big(\{0\} \cup \mathcal{U}(D)\Big)$ pode ser escrito como produto de elementos irredutíveis;

b) se $p_1 \cdots p_m = q_1 \cdots q_n$, com p_i, q_j irredutíveis, $i = 1, \ldots, m$ e $j = 1, \ldots, n$, então $m = n$ e, para uma permutação σ de $\{1, \ldots, n\}$, p_i é associado de $q_{\sigma(i)}$, com $i = 1, \ldots, n$.

Exemplos.

1) O anel $\mathbb{Z}$ é um DFU. Por exemplo, $30 = 2 \cdot 3 \cdot 5 = (-5)(-2)\,3$ sendo a permutação σ associada definida por $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$ correspondendo à troca da posição dos irredutíveis, neste caso, a menos do sinal.

2) Um K corpo é trivialmente DFU, pois $K\backslash\Big(\{0\} \cup \mathcal{U}(K)\Big) = \emptyset$.

3) O anel $\mathbb{Z}[\sqrt{-5}]$ não é domínio de factorização única pois temos

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})\,(1 - \sqrt{-5})$$

em que 2, 3, $1+\sqrt{-5}$ e $1-\sqrt{-5}$ são elementos irredutíveis não associados.

Dos exemplos **2)** e **3)** concluímos que um subanel de um domínio de factorização única pode não ser de factorização única. Tomemos como exemplo o subanel $\mathbb{Z}[\sqrt{-5}]$ do corpo $\mathbb{C}$.

Definição. Seja A um anel comutativo. Dados $a, b \in A$, um elemento $d \in A$ diz-se um *máximo divisor comum (mdc)* de a e b se d/a e d/b e, para qualquer $c \in A$,

$$c/a \text{ e } c/b \implies c/d$$

Exemplos.

1) Em $\mathbb{Z}$, tomemos $x = 36$ e $y = -56$. Temos $x = 2^2 \cdot 3^2$ e $y = -2^3 \cdot 7$. Então $d_1 = 2^2$ e $d_2 = -2^2$ são mdc de x e y.

2) Em $\mathbb{Z}[\sqrt{-5}]$ os elementos $6\ (= (1 + \sqrt{-5})(1 - \sqrt{-5}))$ e $2(1 + \sqrt{-5})$ têm divisores comuns mas não têm mdc (ver Sobral).

3) O domínio de integridade $\mathbb{Z}[\sqrt{-6}]$ não é de factorização única (ver Exercício 35).

Nota. Num anel comutativo A, podemos, naturalmente, definir *máximo divisor comum* de n elementos $a_1, \ldots, a_n$.

Exemplo.

Em $\mathbb{Z}$, os elementos 2 e -2 são mdc de 4, -6 e 10.

No que se segue convém ter presente as seguintes observações:

1) Se A é um anel comutativo com identidade e $a \in A$, então a é mdc de 0 e a.

2) Num anel comutativo com identidade A, se existe um mdc d de $a, b \in A$, então dado $u \in \mathcal{U}(A)$ o elemento ud é também mdc de a e b.

3) Num domínio de integridade D, dados $a, b \in D$, tem-se que

a/b e b/a se e só se a e b são associados, o que é consequência imediata dos Lemas 19 e 20.a).

4) Se D é domínio de integridade e d_1, d_2 são mdc de $a, b \in D$, então d_1 e d_2 são associados, pois dividem-se mutuamente.

Lema 24. *Sejam D um domínio de factorização única e $a, c \in D \backslash \Big(\{0\} \cup \mathcal{U}(D) \Big)$. Se c/a, então c é produto de associados de factores irredutíveis de a.*

Demonstração: Se c/a, então existe $x \in D$ tal que $a = c\,x$. Consideremos a factorização em irredutíveis $a = p_1 \cdots p_m$.

Se $x \in \mathcal{U}(D)$, então $c = a\,x^{-1} = p_1 \cdots p_{m-1}(p_m\,x^{-1})$ e obtemos o resultado.

Se $x \notin \mathcal{U}(D)$, consideremos as factorizações em irredutíveis de c e de x:

$$c = r_1 \cdots r_t\,, \qquad x = s_1 \cdots s_k$$

Então

$$p_1 \cdots p_m = a = r_1 \cdots r_t\, s_1 \cdots s_k$$

Como a decomposição em irredutíveis é única, a menos da ordem e do produto por unidades, cada r_i, com $i = 1, \ldots, t$, é associado de algum p_j, com $j = 1, \ldots, m$, como pretendíamos. ∎

Teorema 25. *Num domínio de factorização única, quaisquer dois elementos têm máximo divisor comum.*

Demonstração: Seja D um DFU. Sejam $x, y \in D$. Se $x = 0$, então y é máximo divisor comum de x e y. Se $x \in \mathcal{U}(D)$, então $y = y\,x^{-1}\,x$, logo x/y pelo que x é mdc de x e y.

Suponhamos, então, que $x, y \notin \mathcal{U}(D) \cup \{0\}$. Consideremos as factorizações em irredutíveis de x e de y:

$$x = p_1 \cdots p_m$$

$$y = q_1 \cdots q_n$$

Sem perda de generalidade, admitamos que $p_1, \ldots, p_k$ são todos os factores irredutíveis comuns a x e a y, a menos do produto por unidades. Tomemos $d = p_1 \cdots p_k$. Então d/x e d/y. Pelo lema anterior, se existe $c \in D \setminus \mathcal{U}(D)$ tal que c/x e c/y, então c é produto de associados de factores irredutíveis comuns a x e a y, logo c/d. Portanto, d é mdc de x e y.

Se não existem factores irredutíveis comuns, então não existe um tal elemento c, pelo que 1 é mdc de x e y. ∎

Num anel comutativo A, podemos também definir *menor* (ou *mínimo*) *múltiplo comum* (mmc) de n elementos $a_1, \ldots, a_n \in A$: dizemos que $m \in A$ é mmc de $a_1, \ldots, a_n$ se

$$\forall\, i = 1, \ldots, n,\ a_i/m$$

$$\forall\, p \in A,\ \ (\forall\, i = 1, \ldots, n,\ a_i/p) \implies m/p$$

Notemos que dado $a \in A$ se tem que 0 é mmc de a e 0.

A demonstração da afirmação seguinte fica ao cuidado do leitor.

Teorema 26. *Num domínio de factorização única, existe mmc de quaisquer n elementos $a_1, \ldots, a_n$.*

Observemos ainda que num domínio de integridade D, dados $a, b \in D$, se m_1 é mmc de a e b e m_2 é associado de m_1, então m_2 é mmc de a e b e se m_1 e m_2 são mmc de a e b, então m_1 e m_2 são associados.

Exemplo.

Em $\mathbb{Z}$, tomemos $a = 5^2 \cdot 3^3 \cdot 7$ e $b = -5 \cdot 2^2 \cdot 11$. Então $m = 5^2 \cdot 3^3 \cdot 7 \cdot 2^2 \cdot 11$ e $-m$ são mmc de a e b.

Nota. Num domínio de integridade D, dados $a, b \in D$, um mdc d de a, b denota-se por $\mathrm{mdc}(a, b)$, tendo o cuidado de não esquecer que d é mdc de a, b se e só se, para qualquer $u \in \mathcal{U}(D)$, ud é mdc de

a e b. Em geral, há mais do que um mdc! Analogamente, escrevemos $\text{mmc}(a, b)$.

No caso particular de $\mathbb{Z}$, dados $a, b \in \mathbb{Z}$ normalmente, ao escrevermos $\text{mdc}(a, b)$ estamos a pensar no mdc positivo. Analogamente, mmc (a, b) denota, em geral, o menor múltiplo comum positivo de a e b.

Teorema 27. *Todo o domínio de ideais principais é domínio de factorização única.*

Demonstração: Seja D um domínio de ideais principais. Comecemos por provar que toda a cadeia de ideais de D estritamente ascendente

$$I_1 \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_n \subsetneqq \cdots$$

é finita. Tomemos $I = \bigcup I_n$. É fácil verificar que I é ideal de D. Logo, como D é domínio de ideais principais, existe $d \in D$ tal que $I = \langle d \rangle$. Então existe $k \in \mathbb{N}$ tal que $d \in I_k$, pelo que $\langle d \rangle \subseteq I_k$. Assim, $I = I_k$ e, como a cadeia é estritamente ascendente, temos k finito e

$$I_1 \subsetneqq I_2 \subsetneqq \cdots \subsetneqq I_k = I$$

Suponhamos que existe $x \in D \setminus \Big(\{0\} \cup \mathcal{U}(D)\Big)$ tal que x não é factorizável em irredutíveis. Seja S o conjunto destes elementos não factorizáveis. Temos $S \neq \emptyset$, por hipótese.

Consideremos $\mathcal{J} = \{\langle x \rangle : x \in S\}$. Uma vez que D não possui cadeias de ideais estritamente ascendentes infinitas, o conjunto parcialmente ordenado $(\mathcal{J}, \subseteq)$ possui elementos maximais.

Seja $a \in S$ tal que $\langle a \rangle$ é maximal entre os elementos de $\mathcal{J}$. Por definição de S, $a \neq 0$ e a não é irredutível, donde existem $b, c \in D \setminus \mathcal{U}(D)$ tais que $a = bc$. Sendo $a \neq 0$ e a não factorizável em irredutíveis, temos $b, c \neq 0$ com b ou c não factorizável em irredutíveis. Logo $b \in S$ ou $c \in S$.

Se $b \in S$, como $\langle a \rangle \subseteq \langle b \rangle$ e $\langle a \rangle$ é maximal em $\mathcal{J}$, obtemos $\langle a \rangle = \langle b \rangle$. Logo a e b são associados. Seja $u \in \mathcal{U}(D)$ tal que $a = bu$. Então $bc = bu$ e, como $b \neq 0$, concluímos que $c = u \in \mathcal{U}(D)$, o que é

absurdo. Analogamente, chegamos a um absurdo se admitirmos que $c \in S$. Logo $S = \emptyset$, ou seja, em D todo o elemento não nulo que não seja unidade decompõe-se em factores irredutíveis.

Para concluirmos a demonstração provemos, por indução, que uma tal factorização é única a menos da ordem dos factores e do produto por unidades.

Suponhamos $a = p_1\, p_2 \cdots p_m = q_1\, q_2 \cdots q_n$, em que $a \notin \{0\} \cup \mathcal{U}(D)$ e $p_1, \ldots, p_m, q_1, \ldots, q_n$ são irredutíveis.

Admitamos $m = 1$. Se $n > 1$, temos $p_1 = q_1\, q_2 \cdots q_n$. Como p_1 é irredutível então $q_1 \in \mathcal{U}(D)$ ou $(q_2 \cdots q_n) \in \mathcal{U}(D)$. Uma vez que $q_1 \notin \mathcal{U}(D)$, concluímos que $q_2 \cdots q_n \in \mathcal{U}(D)$, o que é absurdo pois se existe $x \in D$ tal que $1 = x\, q_2 \cdots q_n$, então $q_j \in \mathcal{U}(D)$ para $j = 2, \ldots, n$. Portanto, $n = 1$.

Admitamos agora que o resultado é válido para $m \geq 1$. Se $p_1 \cdots p_{m+1} = q_1 \cdots q_n$, atendendo ao caso anterior temos $n > 1$ e, além disso, $p_{m+1} / q_1 \cdots q_n$. Como p_{m+1} é irredutível, então p_{m+1} é primo, pois D é domínio de ideais principais. Logo, existe $j \in \{1, \ldots, n\}$ tal que p_{m+1} / q_j. Sem perda de generalidade, vamos admitir que $j = n$. Sendo q_n irredutível e $p_{m+1} \notin \mathcal{U}(D)$, temos q_n associado de p_{m+1}. Seja $u \in \mathcal{U}(D)$ tal que $q_n = p_{m+1}\, u$. Obtemos

$$p_1 \cdots p_m\, p_{m+1} = q_1\, q_2 \cdots q_{n-1}\, p_{m+1}\, u$$

donde, no domínio de integridade D, temos

$$p_1 \cdots p_m = q_1\, q_2 \cdots (q_{n-1}\, u)$$

Aplicando a hipótese de indução, ficamos com $m = n - 1$ e cada p_i $(i = 1, \ldots, m)$ é associado de algum q_j $(j = 1, \ldots, n-2)$ ou de $q_{n-1}u$. Assim, $m + 1 = n$ e cada p_i $(i = 1, \ldots, m+1)$ é associado de algum q_j $(j = 1, \ldots, n)$. Portanto, o resultado é válido para qualquer natural m, pelo princípio de indução.

Concluímos pois que D é um DFU. ∎

Exemplo.

O anel $\mathbb{Z}$ é de facto um domínio de factorização única, pois é domínio de ideais principais, o que prova o Teorema Fundamental da Aritmética: todos os números inteiros positivos maiores

do que 1 podem ser decompostos num produto de números primos, sendo esta decomposição única a menos de permutação de factores.

Acabámos de provar que todo o domínio de ideais principais é domínio de factorização única, porém a condição recíproca não é verdadeira. O anel $\mathbb{Z}[x]$ dos polinómios com coeficientes em $\mathbb{Z}$ é DFU mas não é DIP, por exemplo, o ideal $\langle 2, x\rangle$ não é principal (ver Allenby).

Corolário 27.1. *Se D é um domínio de ideais principais e $a, b \in D$, então existe* $\mathrm{mdc}(a, b)$ *e* $\mathrm{mmc}(a, b)$.

Demonstração: Pelo Teorema 27, o domínio D é DFU, pelo que este resultado é consequência dos Teoremas 25 e 26. ∎

A demonstração dos últimos resultados que aqui apresentamos fica ao cuidado do leitor.

Teorema 28. *Sejam D um domínio de ideais principais e $a, b, d, m \in D$. Tem-se*

a) $\langle a\rangle + \langle b\rangle = \langle d\rangle$ *se e só se* $d =$ *mdc* (a, b);

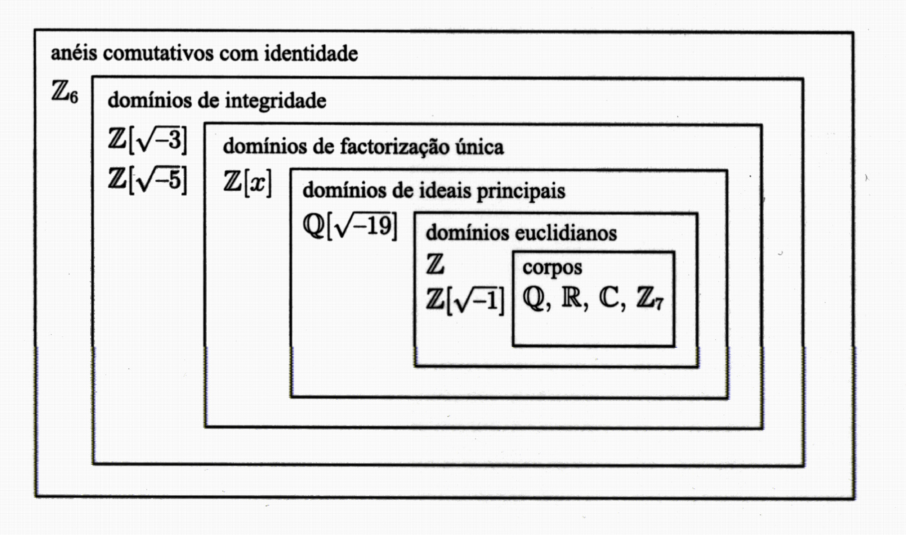
b) $\langle a\rangle \cap \langle b\rangle = \langle m\rangle$ *se e só se* $m =$ *mmc* (a, b).

Assim, podemos afirmar o seguinte.

Corolário 28.1. (Bézout) *Sejam D um domínio de ideais principais e $a, b, d \in D$. Se d é mdc de a e b, então existem $x, y \in D$ tais que $d = a\,x + b\,y$.*

Recordemos que em $\mathbb{Z}$, dois elementos a e b dizem-se *primos entre si* se $\mathrm{mdc}\ (a, b) = 1$. Por este último corolário, $a, b \in \mathbb{Z}$ são primos entre si se e só se existem $x, y \in \mathbb{Z}$ tais que $1 = a\,x + b\,y$.

Em face do estudo que acabámos de fazer, podemos apresentar o seguinte esquema que resume a relação entre os anéis considerados.



1.9 Um teorema de Fermat

Terminamos este capítulo com a apresentação de um teorema de Fermat sobre decomposição de números primos, cuja demonstração podemos obter fazendo uso do anel dos inteiros de Gauss $\mathbb{Z}[i]$.

Começamos por observar que no anel de Gauss $\mathbb{Z}[i]$, temos $\mathcal{U}(\mathbb{Z}[i]) = \{-1, 1, -i, i\}$ e a norma δ, definida por $\delta(a + bi) = a^2 + b^2$ para $a, b \in \mathbb{Z}$, é tal que $\delta(uv) = \delta(u)\delta(v)$, para quaisquer $u, v \in \mathbb{Z}[i]\backslash\{0\}$.

Tenhamos também presente os seguintes resultados.

Lema 29. *Dado $p \in \mathbb{N}\backslash\{2\}$ primo, se $a \in \mathbb{Z}_p\backslash\{0\}$ tem ordem multiplicativa 2, então $a = -1$.*

Demonstração: Se $a^2 = 1$ em $\mathbb{Z}_p$, então $a^2 - 1 = 0$, pelo que $(a - 1)(a + 1) = 0$ no corpo $\mathbb{Z}_p$. Assim $a - 1 = 0$ ou $a + 1 = 0$, isto é

$a = 1$ ou $a = -1$. Como $o(a) = 2$ temos $a \neq 1$. Portanto, $a = -1$. ∎

Lema 30. *O grupo multiplicativo* $(\mathbb{Z}_p\backslash\{0\}, \cdot)$ *é cíclico, de ordem* $p - 1$.

Demonstração: Provar que o grupo multiplicativo $(\mathbb{Z}_p\backslash\{0\}, \cdot)$ é cíclico corresponde a provar a existência de um seu elemento com ordem $p - 1$, uma vez que tem $p - 1$ elementos.

Tomemos $m = \text{mmc}\ (o(1), o(2), \ldots, o(p-1))$, onde $o(i)$ denota a ordem multiplicativa do elemento i. É claro que

$$\forall k \in \mathbb{Z}_p\backslash\{0\}, \quad k^m = 1$$

pois $o(k)/m$. Portanto, $x^m - 1$ é um polinómio de grau m que no corpo $\mathbb{Z}_p$ tem pelo menos $p - 1$ raízes, donde $m \geq p - 1$. Por outro lado, pelo Exercício 31, no grupo multiplicativo $\mathbb{Z}_p\backslash\{0\}$ existe um elemento c de ordem m, logo $m \leq p - 1$. Logo, $m = p - 1$ e concluímos que $(\mathbb{Z}_p\backslash\{0\}, \cdot)$ é cíclico. ∎

Teorema 31. (Fermat) *Seja* $p \in \mathbb{N}\backslash\{2\}$ *primo. Então* $p = a^2 + b^2$, *para certos* $a, b \in \mathbb{Z}$ *se e só se* $p \equiv 1 \pmod 4$.

Demonstração: Suponhamos que $p = a^2 + b^2$, com $a, b \in \mathbb{Z}$. Se a e b forem pares, então $2/p$, donde p não é primo pois $p \neq 2$. Se a e b forem ímpares, então $a = 2k + 1$ e $b = 2m + 1$, com $k, m \in \mathbb{Z}$. Neste caso, $p = (2k+1)^2 + (2m+1)^2 = 4k^2 + 4k + 1 + 4m^2 + 4m + 1$, pelo que mais uma vez $2/p$. Assim, sem perda de generalidade, podemos supor que a é par e b é ímpar. Suponhamos $a = 2k$ e $b = 2m + 1$, com $k, m \in \mathbb{Z}$. Temos $p = 4k^2 + 4m^2 + 4m + 1$ e, portanto, $p \equiv 1 \pmod 4$.

Reciprocamente, admitamos que $p \equiv 1(\mod 4)$. Então 4 divide $p - 1$. Consideremos agora o grupo $(\mathbb{Z}_p\backslash\{0\}, \cdot)$ de ordem $p - 1$. Pelo lema anterior, $(\mathbb{Z}_p\backslash\{0\}, \cdot)$ é cíclico e, como 4 divide $p - 1$, existe $n \in \mathbb{Z}_p\backslash\{0\}$ tal que n tem ordem multiplicativa 4. Logo, n^2 tem ordem multiplicativa 2. Pelo Lema 29, temos $n^2 = -1$ em $\mathbb{Z}_p$, pelo que p divide $n^2 + 1$ em $\mathbb{Z}$.

Tomemos agora o anel de Gauss $\mathbb{Z}[i]$. Então p divide $(n - i)(n + i)$ no anel $\mathbb{Z}[i]$.

Se p fosse irredutível em $\mathbb{Z}[i]$, teríamos que $p/n-i$ ou $p/n+i$. Se $p/n+i$, então $n+i=p(a+bi)$, para algum $a+bi \in \mathbb{Z}[i]$. Logo $1=pb$, o que é impossivel. Analogamente, se $p/n-i$, então $-1=pb$ o que também é falso.

Concluímos pois que p não é irredutível em $\mathbb{Z}[i]$. Assim, existem $a+bi, c+di \in \mathbb{Z}[i]\backslash\mathcal{U}(\mathbb{Z}[i])$ tais que $p=(a+bi)(c+di)$. Logo $\delta(p)=p^2$ e $\delta(p) = (a^2+b^2)(c^2+d^2)$, com $a^2+b^2, c^2+d^2 \neq 1$. Como p é primo, p divide a^2+b^2 ou p divide c^2+d^2. Admitamos, por exemplo, que p divide a^2+b^2, então $a^2+b^2 = pm$, com $m \in \mathbb{N}$, e portanto $p=m(c^2+d^2)$. Logo, como $c^2+d^2 \neq 1$ e p é primo, obtemos $m=1$. Assim, $p=c^2+d^2$, como se pretendia. ∎

Exercícios

1. a) Seja (A, θ) um grupóide. Mostre que A admite, no máximo, um elemento identidade.
   b) Mostre que num monóide cada elemento tem, no máximo, um inverso.

2. Prove que num grupo comutativo $(A, +)$ se tem

$$a + c = b + c \;\Rightarrow\; a = b \;;$$
$$-(-a) = a \;;$$
$$-(a + b) = -a - b \;;$$
$$(-n)\, a = -(n\, a), \quad \text{com} \;\; n \in \mathbb{Z} \;;$$
$$(m + n)\, a = m\, a + n\, a, \quad \text{com} \;\; m, n \in \mathbb{Z}.$$

3. Considere no conjunto $\mathcal{F}(\mathbb{R})$ das funções de $\mathbb{R}$ em $\mathbb{R}$ as operações binárias $+$ e $\cdot$ definidas, respectivamente, por

$$\forall\, f, g \in \mathcal{F}(\mathbb{R}), \;\; \forall\, x \in \mathbb{R}, \quad (f + g)(x) = f(x) + g(x)$$
$$\forall\, f, g \in \mathcal{F}(\mathbb{R}), \;\; \forall\, x \in \mathbb{R}, \quad (f \cdot g)(x) = f(x)\, g(x)$$

   a) Mostre que $(\mathcal{F}(\mathbb{R}), +, \cdot)$ é um anel comutativo com identidade.
   b) $(\mathcal{F}(\mathbb{R}), +, \cdot)$ é domínio de integridade?
   c) Diga, justificando, se $(\mathcal{F}(\mathbb{R}), +, \cdot)$ é corpo.
   d) Prove que $(\mathcal{F}(\mathbb{R}), +, \circ)$ não é anel, onde $\circ$ é a operação composição de funções.

4. a) Seja X um conjunto. Considere o semigrupo $(\mathcal{P}(X), +)$ em que a operação binária $+$ está definida por

$$\forall\, A, B \in \mathcal{P}(X), \quad A + B = (A \cup B) \setminus (A \cap B) \; [= A \setminus B \cup B \setminus A]$$

   Mostre que $(\mathcal{P}(X), +, \cap)$ é um anel comutativo com identidade.

b) Prove que num anel de Boole $(A, +, \cdot)$, isto é, num anel comutativo com identidade em que todo o elemento a é tal que $a^2 = a$ (dizemos que a é *idempotente*), tem-se $a + a = 0$, para $a \in A$.

5. Sejam A um anel e B um subconjunto de A. Mostre que B é subanel de A se e só se satisfaz as seguintes condições:

   (i) $0 \in B$;

   (ii) $\forall\, x, y \in B,\ \ x + y \in B$;

   (iii) $\forall\, x, y \in B,\ \ x\, y \in B$;

   (iv) $\forall\, x \in B,\ \ -x \in B$.

6. Sejam A um anel e B um subconjunto de A. Mostre que B é subanel de A se e só se satisfaz as seguintes condições:

   (i) $0 \in B$;

   (ii) $\forall\, x, y \in B,\ \ x - y \in B$;

   (iii) $\forall\, x, y \in B,\ \ x\, y \in B$.

7. Sejam A um anel e I um subconjunto de A. Mostre que I é ideal de A se e só se satisfaz as seguintes condições:

   (i) $0 \in I$;

   (ii) $\forall\, x, y \in I,\ \ x - y \in I$;

   (iii) $\forall\, x \in I,\ \ \forall\, a \in A,\ \ x\, a, a\, x \in I$.

8. Considere o anel $\mathcal{M}_2(\mathbb{R})$ das matrizes quadradas de ordem 2 sobre o corpo $\mathbb{R}$. Dê exemplo de um subanel de $\mathcal{M}_2(\mathbb{R})$ que não seja seu ideal.

9. Sejam A um anel, I um conjunto não vazio e $\{A_i\}_{i \in I}$ uma família de subanéis de A. Mostre que $\bigcap_{i \in I} A_i$ é subanel de A.

10. Sejam A um anel e I, J ideais de A. Mostre que

    a) (i) $I + J$ é ideal de A;
    (ii) IJ é ideal de A;

    b) (i) $I \cup J \subseteq I + J$ e $I + J$ é o menor ideal de A que contém $I \cup J$;
    (ii) $IJ \subseteq I \cap J$.

11. Sejam A um anel comutativo com identidade e $a_1, \ldots, a_n \in A$. Mostre que

    a) o ideal de A gerado por $\{a_1, \ldots, a_n\}$ é o conjunto

    $$\Big\{x_1\, a_1 + \cdots + x_n\, a_n : \quad x_1, \ldots, x_n \in A\Big\}$$

    b) $\langle a_1, \ldots, a_n\rangle = \langle a_1\rangle + \cdots + \langle a_n\rangle$.

12. Sejam A um anel e ρ uma relação de equivalência em A. Mostre que ρ é relação de congruência se e só se

    $$\forall\, a, b, c, d \in A, \quad (a, b), (c, d) \in \rho \;\Rightarrow\; (a + c,\, b + d), (a\, c,\, b\, d) \in \rho$$

13. Mostre que todo o ideal I do anel $\mathbb{Z}$ é principal, tendo como gerador 0 se $I = \{0\}$ ou o menor $m \in \mathbb{N}$ nele contido, bem como o seu simétrico, se $I \neq \{0\}$.

14. Sejam A um anel com identidade, B um anel e $f\colon A \to B$ um morfismo de anéis. Mostre que

    a) Se A é comutativo, então $f(A)$ é comutativo;

    b) Se f é não nulo (isto é, para algum $x \in A$, $f(x) \neq 0$), então $f(1) \neq 0$ e $f(1)$ é a identidade de $f(A)$;

    c) Se f é não nulo e A é corpo, então $f(A)$ também é corpo.

15. Sejam A, B anéis e $\varphi : A \to B$ um isomorfismo de anéis. Mostre que φ^{-1} é também um isomorfismo de anéis.

16. Sejam A e B anéis isomorfos. Mostre que

    a) Se A é comutativo, então B é comutativo;

    b) Se A é um anel com identidade, então B é um anel com identidade;

    c) Se A é domínio de integridade, então B é domínio de integridade;

    d) Se A é corpo, então B é corpo.

17. Considere o anel $\mathbb{Z}$ e os seus ideais $I = 15\mathbb{Z}$ e $S = 20\mathbb{Z}$. Mostre que

    a) $I \cap S = 60\mathbb{Z} = \langle \text{mmc}(15, 20) \rangle$;

    b) $I + S = 5\mathbb{Z} = \langle \text{mdc}(15, 20) \rangle$;

    c) $5\mathbb{Z}/15\mathbb{Z} \simeq 20\mathbb{Z}/60\mathbb{Z}$;

    d) $\#(5\mathbb{Z}/15\mathbb{Z}) = 3$.

    e) Determine as tabelas de Cayley das operações do anel $5\mathbb{Z}/15\mathbb{Z}$.

18. Demonstre o 3º Teorema do Isomorfismo.

19. Sejam A um anel comutativo com identidade e $I \neq A$ um ideal de A. Mostre que I é ideal maximal de A se e só se para qualquer $a \in A$ tal que $a \notin I$, se tem $\langle a \rangle + I = A$.

20. Sejam A, B anéis comutativos com identidade, $f : A \twoheadrightarrow B$ um epimorfismo de anéis com identidade e I um ideal de B. Mostre que

    a) Os anéis $A/f^{-1}(I)$ e B/I são isomorfos;

    b) Se I é primo, então $f^{-1}(I)$ é primo;

    c) Se I é maximal, então $f^{-1}(I)$ é maximal.

21. Sejam A um anel comutativo com identidade e J um ideal próprio de A. Prove que existe um ideal maximal de A que contém J.

22. Seja A um anel com identidade e seja n a característica de A. Mostre que

    a) Para todo o $a \in A$, $na = 0$;

    b) Se m é um número natural tal que $m1 = 0$, então n é divisor de m;

    c) Se B é subanel com identidade de A, então $c(B) = n$;

    d) Se B é um anel com identidade isomorfo a A, então $c(A) = c(B)$.

23. Mostre que $(\mathbb{Z}_3, +, \cdot)$ é isomorfo a um subanel A de $(\mathbb{Z}_6, +, \cdot)$. Compare as características de A e $\mathbb{Z}_6$ e analise-as face ao exercício anterior.

24. Seja A um anel comutativo com identidade. Para cada $a \in A$, considere a aplicação

$$\begin{array}{rccc} \varphi_a\colon & A & \to & A \\ & x & \to & a\,x \end{array}$$

    Mostre que A é domínio de integridade se e só se, para qualquer $a \in A\backslash\{0\}$, a aplicação φ_a é injectiva.

25. a) Sejam A um anel comutativo com identidade e $p \in A\backslash\{0\}$. Mostre que p é elemento primo de A se e só se o ideal de A gerado por p é ideal primo de A.

    b) Seja $n \in \mathbb{Z}\backslash\{0\}$. Considere o ideal $\langle n\rangle$ de $\mathbb{Z}$. Mostre que $\langle n\rangle$ é ideal primo de $\mathbb{Z}$ se e só se n é um número inteiro primo.

26. Mostre que num domínio de ideais principais todo o ideal primo não nulo é maximal.

27. a) Sejam A um anel comutativo com identidade e $a, b, d \in A$. Mostre que se $\langle a, b\rangle = \langle d\rangle$, então d é um m.d.c. de a e b.

    b) Sejam A um domínio de ideais principais e $a, b \in A$. Prove que

    (i) Existe um m.d.c. de a e b;

    (ii) Se $d \in A$ é um m.d.c. de a e b, então $\langle a, b\rangle = \langle d\rangle$.

28. (Identidade de Bézout) Sejam $a, b \in \mathbb{Z}$ primos entre si. Mostre que existem $x, y \in \mathbb{Z}$ tais que $1 = a\,x + b\,y$.

29. a) Sejam A um anel comutativo com identidade e $a, b, m \in A$. Mostre que se $\langle a\rangle \cap \langle b\rangle = \langle m\rangle$, então m é um m.m.c. de a e b.

    b) Sejam A um domínio de ideais principais e $a, b \in A$. Prove que

    (i) Existe um m.m.c. de a e b;

    (ii) Se $m \in A$ é um m.m.c. de a e b, então $\langle a\rangle \cap \langle b\rangle = \langle m\rangle$.

30. a) Sejam $a_1, \ldots, a_n \in \mathbb{Z}$ não todos nulos e $d = \text{mdc}(a_1, \ldots, a_n)$. Mostre que
$$\text{mdc}\Big(\frac{a_1}{d}, \ldots, \frac{a_n}{d}\Big) = 1$$

    b) Sejam $a, b \in \mathbb{Z}$ e $x \in \mathbb{N}$. Prove que
$$\text{mdc}(xa,\, xb) \;=\; x\ \text{mdc}(a, b)$$

    c) Sejam $a, r, s \in \mathbb{Z}$, com r, s primos entre si. Mostre que se r divide as, então r divide a.

31. Seja K um corpo.

    a) Sejam $a, b \in K$ com ordens multiplicativas m, n, respectivamente. Considere $r = mdc(m, n)$ e n' tal que $n = rn'$. Tem-se $mn' = mmc(m, n)$. Mostre

    i) $b' := b^r$ tem ordem multiplicativa n';

ii) ab' tem ordem multiplicativa $mmc(m, n)$.

b) Sejam $a_1, \ldots, a_n \in K$ com ordens multiplicativas m_i, para $i \in \{1, \ldots, n\}$. Mostre que existe $c \in K$ com ordem multiplicativa $mmc(m_1, \ldots m_n)$.

32. Considere o anel $(\mathbb{Z}, +, \cdot)$.

a) Sejam $a \in \mathbb{Z}$ e $b \in \mathbb{N}$.

(i) Considere o conjunto $S = \{a - bx \mid x \in \mathbb{Z},\ a - bx \geq 0\}$. Prove que S tem elemento mínimo r e que $r < b$.

(ii) Mostre que existem $q \in \mathbb{Z}$ e $r \in \mathbb{N}_0$ tais que $a = bq + r$ e $0 \leq r < b$.

b) Sejam $a \in \mathbb{Z}$ e $b \in \mathbb{Z} \setminus \{0\}$. Demonstre que existem inteiros únicos q e r tais que $a = bq + r$ e $0 \leq r < |b|$.

c) Conclua que $(\mathbb{Z}, +, \cdot)$ é um domínio euclidiano, definindo uma norma δ por $\delta(a) = |a|$, para qualquer $a \in \mathbb{Z} \setminus \{0\}$.

33. Seja R um domínio euclidiano com norma δ. Mostre que

a) Para qualquer $a \in R$, $a \neq 0$, se tem $\delta(1) \leq \delta(a)$ em $\mathbb{N}_0$;

b) $\delta(a) = \delta(1)$ se e só se a é uma unidade de R;

c) Se $a, b \in R \setminus \{0\}$ são associados, então $\delta(a) = \delta(b)$.

34. Considere o conjunto dos inteiros de Gauss $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ e a aplicação $\delta : \mathbb{Z}[i] \setminus \{0\} \longrightarrow \mathbb{N}$, definida por $\delta(a + bi) = a^2 + b^2$.
Mostre que

a) Para quaisquer $x, y \in \mathbb{Z}[i] \setminus \{0\}$, $\delta(xy) = \delta(x)\delta(y)$;

b) $\mathcal{U}(\mathbb{Z}[i]) = \{-1, 1, -i, i\}$;

c) Se $a \in \mathbb{Z}$ e $x \in \mathbb{N}$, então existem $u, u_1 \in \mathbb{Z}$ tais que $a = ux + u_1$, com $|u_1| \leq \frac{x}{2}$;

d) Se $y \in \mathbb{Z}[i]$ e $x \in \mathbb{N}$, então existem $t, r \in \mathbb{Z}[i]$ tais que $y = tx + r$, onde $r = 0$ ou, se $r \neq 0$, $\delta(r) < \delta(x)$;

e) Se $y \in \mathbb{Z}[i]$ e $x \in \mathbb{Z}[i] \setminus \{0\}$, então $x\overline{x} \in \mathbb{N}$ e existem $t, r \in \mathbb{Z}[i]$ tais que $y\overline{x} = tx\overline{x} + r$, onde $r = 0$ ou, se $r \neq 0$, $\delta(r) < \delta(x\overline{x})$;

f) $\mathbb{Z}[i]$ é domínio euclidiano, com norma δ.

35. Considere o subconjunto de $\mathbb{C}$

$$\mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} : \ a, b \in \mathbb{Z}\right\}$$

Mostre que, com as operações de adição e multiplicação usuais em $\mathbb{C}$,

a) $\mathbb{Z}[\sqrt{-5}]$ é domínio de integridade;

b) $\mathcal{U}(\mathbb{Z}[\sqrt{-5}]) = \{1, -1\}$;
(Pode demonstrar directamente ou pode começar por observar que se $u \in \mathbb{Z}[\sqrt{-5}]$, então $\overline{u} \in \mathbb{Z}[\sqrt{-5}]$, $|u|^2 \in \mathbb{N}_0$ e que $u \in \mathcal{U}(\mathbb{Z}[\sqrt{-5}])$ se e só se $|u|^2 = 1$.)

c) (i) 2 divide $(1 + \sqrt{-5})(1 - \sqrt{-5})$;
(ii) Para todo o $u \in \mathbb{Z}[\sqrt{-5}]$, $|u|^2 \neq 2$;
(iii) 2 é um elemento irredutível, mas não primo em $\mathbb{Z}[\sqrt{-5}]$.

d) $\mathbb{Z}[\sqrt{-5}]$ não é domínio de ideais principais.

e) $\mathbb{Z}[\sqrt{-5}]$ não é domínio euclidiano e então $|\cdot|$ não é uma norma.

36. a) Seja $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : \ a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ e considere a aplicação $\delta : \mathbb{Z}[\sqrt{-2}] \setminus \{0\} \longrightarrow \mathbb{N}$ definida por $\delta(a + b\sqrt{-2}) = a^2 + 2b^2$.
Mostre que

(i) Para quaisquer $x, y \in \mathbb{Z}[\sqrt{-2}] \setminus \{0\}$, $\delta(xy) = \delta(x)\delta(y)$;
(ii) Se $y \in \mathbb{Z}[\sqrt{-2}]$ e $x \in \mathbb{N}$, então existem $t, r \in \mathbb{Z}[\sqrt{-2}]$ tais que $y = tx + r$, onde $r = 0$ ou, se $r \neq 0$, tem-se $\delta(r) < \delta(x)$;
(iii) Se $y \in \mathbb{Z}[\sqrt{-2}]$ e $x \in \mathbb{Z}[\sqrt{-2}] \setminus \{0\}$, então $x\overline{x} \in \mathbb{N}$ e existem $t, r \in \mathbb{Z}[\sqrt{-2}]$ tais que $y\overline{x} = tx\overline{x} + r$, onde $r = 0$ ou, se $r \neq 0$, $\delta(r) < \delta(x\overline{x})$;

(iv) $\mathbb{Z}[\sqrt{-2}]$ é domínio euclidiano, com norma δ.

b) Considere o domínio de integridade $\mathbb{Z}[\sqrt{-6}] = \{a+b\sqrt{-6} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ e a aplicação $\theta : \mathbb{Z}[\sqrt{-6}]\backslash\{0\} \to \mathbb{N}$, definida por $\theta(a + b\sqrt{-6}) = a^2 + 6\,b^2$.
Mostre que

(i) Para quaisquer $x, y \in \mathbb{Z}[\sqrt{-6}]\backslash\{0\}$, $\theta(xy) = \theta(x)\,\theta(y)$;

(ii) $\mathcal{U}(\mathbb{Z}[\sqrt{-6}]) = \{-1, 1\}$;

(iii) $10 = 2.5 = (2 + \sqrt{-6})(2 - \sqrt{-6})$ são decomposições de 10 em elementos irredutíveis de $\mathbb{Z}[\sqrt{-6}]$ não associados;

(iv) $\mathbb{Z}[\sqrt{-6}]$ não é um domínio de factorização única;

(v) $\mathbb{Z}[\sqrt{-6}]$ não é um domínio euclidiano;

(vi) θ não define uma norma em $\mathbb{Z}[\sqrt{-6}]$, tão pouco se pode definir uma norma em $\mathbb{Z}[\sqrt{-6}]$.

c) Mostre que o domínio de integridade $\mathbb{Z}[\sqrt{-19}]$ não é de factorização única.

d) Mostre que o domínio de integridade $\mathbb{Q}[\sqrt{-19}]$ é de ideais principais e, portanto, é de factorização única.

37. Pesquise na literatura outros exemplos de

a) Elementos $d \in \mathbb{Z}$ tais que $\mathbb{Z}[\sqrt{d}]$ não seja domínio de factorização única;

b) Domínios de integridade da forma $\mathbb{Q}[\sqrt{d}]$ que sejam euclidianos e exemplos que não o sejam.

38. Diga, justificando, se são verdadeiras ou falsas as seguintes afirmações:

a) Todo o par de elementos de um anel comutativo e com identidade, tem *mdc*;

b) Todo o corpo é domínio de integridade;

c) Todo o domínio de integridade é um corpo;

d) Se $n > 1$, o anel $\mathbb{Z}_n$ é um domínio de integridade se só se é um corpo.

39. Mostre que em $\mathbb{Z}[i]$ se tem

    a) 2 é produto de uma unidade pelo quadrado de um elemento irredutível em $\mathbb{Z}[i]$;

    b) um elemento $p \in \mathbb{Z}\backslash\{2\}$ primo é irredutível em $\mathbb{Z}[i]$ se e só se $p \equiv 3 \pmod 4$ (use o teorema de Fermat).

40. Sejam D um corpo, $a, b \in D$ e $m, n \in \mathbb{N}$ números primos entre si. Mostre que

    a) Existem $s, t \in \mathbb{Z}$ tais que $a = a^{ms}a^{nt}$;

    b) Se $a^m = b^m$ e $a^n = b^n$, então $a = b$;

    c) A alínea anterior também é verdadeira quando D é apenas um domínio de integridade.

41. Considere a aplicação $\phi : \mathbb{Z}_{10} \mapsto \mathbb{Z}_5$ definida por $\phi([n]_{10}) = [n]_5$, para $n \in \mathbb{Z}$.

    a) Mostre que ϕ está bem definida e que é um morfismo sobrejectivo de anéis com identidade.

    b) Calcule explicitamente $\mathrm{Ker}(\phi)$.

    c) Prove que $\mathrm{Ker}(\phi)$ é um ideal maximal de $\mathbb{Z}_{10}$.

42. a) No anel das matrizes $M_2(\mathbb{R})$, mostre que $A = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$ *é divisor de zero à esquerda* e à *direita*, ou seja existem $B, C \in M_2(\mathbb{R})$ tais que $AB = 0$ e $CA = 0$, respectivamente.

    b) Seja $S = \mathbb{Z}^{\mathbb{N}}$ o conjunto das sucessões em $\mathbb{Z}$. Em S, definimos uma operação de adição + componente a componente, isto é, dados $(a_i)_{i\in\mathbb{N}}$, $(b_i)_{i\in\mathbb{N}} \in S$,

    $$(a_i)_{i\in\mathbb{N}} + (b_i)_{i\in\mathbb{N}} = (a_i + b_i)_{i\in\mathbb{N}}$$

    (i) Mostre que $(S, +)$ é um grupo comutativo.

(ii) Seja $A = \mathrm{End}(S,+)$ o conjunto dos morfismos de $(S,+)$. Um elemento típico de A tem a forma $\alpha : S \to S$, $(a_i)_{i\in\mathbb{N}} \mapsto (\alpha(a_i))_{i\in\mathbb{N}}$, e pode ser representado por $\alpha = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots \\ \alpha(a_1) & \alpha(a_2) & \alpha(a_3) & \cdots \end{pmatrix}$. Entre os elementos de A podemos definir operações de adição $+$ (componente a componente) e de composição $\circ$.

Prove que $(A,+,\circ)$ é um anel com zero e identidade $\bar{0} = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots \\ 0 & 0 & 0 & \cdots \end{pmatrix}$ e $\bar{1} = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots \\ a_1 & a_2 & a_3 & \cdots \end{pmatrix}$ respectivamente.

Considere os seguintes elementos de A

$$R = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots \\ 0 & a_1 & a_2 & \cdots \end{pmatrix},\ L = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots \\ a_2 & a_3 & a_4 & \cdots \end{pmatrix}$$

$$T = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots \\ a_1 & 0 & 0 & \cdots \end{pmatrix}$$

Mostre que $L \circ T = T \circ R = \bar{0}$ e $L \circ R = \bar{1}$.

Conclua que $L\,[R]$ é divisor de zero à direita [esquerda].

Prove que $L\,[R]$ não é divisor de zero à esquerda [direita].

Capítulo 2

Anéis de polinómios sobre anéis comutativos com identidade

Neste capítulo faremos um estudo de anéis de polinómios numa indeterminada, analisando e aplicando, neste caso particular, diversos conceitos e resultados já estudados no capítulo anterior, tais como divisibilidade e factorização.

Descreveremos o corpo $\frac{K[x]}{\langle f(x)\rangle}$ construído a partir de um corpo K e de um polinómio $f(x)$ irredutível no anel de polinómios $K[x]$.

Por fim, efectuaremos um estudo de polinómios com coeficientes em $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

2.1 Conceitos e resultados gerais

Começamos por apresentar uma definição formal de polinómio numa indeterminada.

Definição. Seja A um anel. Uma sucessão $p = (a_i)_{i\in\mathbb{N}_0}$ de elementos de A tal que $a_i = 0$ a partir de certa ordem $m \in \mathbb{N}_0$, diz-se um *polinómio*.

Seja A um anel com identidade. Se $p = (a_i)_{i\in\mathbb{N}_0}$ e $a_i = 0$, para todo o $i \in \mathbb{N}_0$, escrevemos $p = 0$.

Podemos escrever $(a_0, a_1, a_2, \dots)$ em vez de $(a_i)_{i\in\mathbb{N}_0}$.

Um polinómio $(a, 0, 0, \dots, 0, \dots)$ diz-se uma *constante* e é representado apenas por a.

Dois *polinómios* $(a_i)_{i\in\mathbb{N}_0}$ e $(b_i)_{i\in\mathbb{N}_0}$ dizem-se *iguais* se e só se, para qualquer $i \in \mathbb{N}_0$, $a_i = b_i$.

Dado um polinómio $p \neq 0$, chamamos *grau* de p ao maior $m \in \mathbb{N}_0$ tal que $a_m \neq 0$. Se $p = 0$, definimos grau de p como sendo $-\infty$.

No conjunto $S(A)$ de todos os polinómios em A, definimos operações de adição e de multiplicação do seguinte modo: dados $p = (a_i)_{i\in\mathbb{N}_0}$ e $q = (b_i)_{i\in\mathbb{N}_0}$,

$$p + q = (a_i + b_i)_{i\in\mathbb{N}_0}$$
$$p\,q = (c_i)_{i\in\mathbb{N}_0} \quad \text{em que} \quad c_i = \sum_{j+k=i} a_j\, b_k$$

Proposição 1. *Seja A um anel* [*comutativo / com identidade*]. *Então $S(A)$ é um anel* [*comutativo / com identidade*]. *Além disso, $\varphi\colon A \to S(A)$ definido por $\varphi(a) = (a, 0, 0, 0, \dots)$, para cada $a \in A$, é um mergulho de anéis* [*com identidade*].

Demonstração: Notemos apenas que $p = 0$ é o zero de $S(A)$ e $(a_0, a_1, a_2, \dots)$ tem como simétrico $(-a_0, -a_1, -a_2, \dots)$. O resto da demonstração fica ao cuidado do leitor. ∎

Consideremos $x = (0, 1, 0, \dots, 0, \dots)$. Podemos provar facilmente que, para qualquer $n \in \mathbb{N}$,

$$x^n = (\underbrace{0, 0, \dots, 0}_{n \text{ vezes}}, 1, 0, \dots)$$

Definindo $x^0 = (1, 0, 0, \dots)$, a identidade de $S(A)$, podemos então verificar que dado $p = (a_0, a_1, \dots, a_n, 0, 0, \dots)$,

$$p = a_0 + a_1\, x + a_2\, x^2 + \cdots + a_n\, x^n = a_n\, x^n + \cdots + a_1\, x + a_0 = \sum_{i=0}^{n} a_i x^i$$

O polinómio x (de grau 1) chama-se *indeterminada* sobre A.

Com esta notação, o polinómio p poderá denotar-se por $p(x)$. Usaremos as duas notações consoante for mais conveniente na escrita.

Um elemento $p(x) = a_0 + a_1\,x + a_2\,x^2 + \cdots + a_n\,x^n$ de $S(A)$ diz-se um *polinómio na indeterminada x com coeficientes em A*. Se $p(x)$ tem grau $n \geq 0$, ao coeficiente a_n chamamos *coeficiente director* de $p(x)$.

Um polinómio diz-se *mónico* se o seu coeficiente director é 1.

Usualmente, sendo A um anel comutativo com identidade, o anel $S(A)$ representa-se por $A[x]$.

Exemplos.

1) Seja $A = \mathbb{Z}$. Tomemos $p = (2, -3, 0, 5, 0, 0, \dots)$. Então

$$\begin{aligned} p &= (2,0,0,\dots) + (0,-3,0,0,\dots) + (0,0,0,5,0,\dots) \\ &= 2 - 3\,x + 5\,x^3 \end{aligned}$$

2) Sejam $p(x) = 2 - 3x + 5x^3$ e $q(x) = 3 + x + x^2$ elementos de $\mathbb{Z}[x]$. Temos

$$\begin{aligned} p(x) + q(x) &= 5 - 2x + x^2 + 5x^3 \\ p(x)q(x) &= 6 - 7x - x^2 + 12x^3 + 5x^4 + 5x^5 \end{aligned}$$

No que se segue, A será sempre um anel comutativo com identidade.

Definição. Sejam A um anel e $p(x) = a_0 + a_1\,x + \cdots + a_n\,x^n$ um polinómio com coeficientes em A. Definimos

$$\begin{aligned} f_p\colon\ & A \to A \\ & a \mapsto a_0 + a_1\,a + \cdots + a_n\,a^n \end{aligned}$$

Trata-se de uma aplicação de A em A, usualmente denominada por *função polinomial definida por p*. Para $a \in A$, escreveremos $p(a)$ em vez de $f_p(a)$.

Observemos que se $p(x) = c$ é constante, então a função polinomial

$$\begin{aligned} f_p\colon\ & A \to A \\ & a \mapsto p(a) = c \end{aligned}$$

é constante. Em particular, se $p(x) = 1$, então $p(a) = 1$, para qualquer $a \in A$.

Notemos ainda que dados um anel A e polinómios $p(x), q(x) \in A[x]$, podemos ter $p(x) \neq q(x)$ e $f_p = f_q$, como mostra o exemplo seguinte.

Exemplo.

Sejam $A = \mathbb{Z}_2$, $p(x) = 1 + x$ e $q(x) = 1 + x^3$. Logo $p \neq q$, mas

$$\begin{aligned} f_p\colon\ & \mathbb{Z}_2 \to \mathbb{Z}_2 \\ & 0 \mapsto 1 \\ & 1 \mapsto 0 \end{aligned} \qquad \text{e} \qquad \begin{aligned} f_q\colon\ & \mathbb{Z}_2 \to \mathbb{Z}_2 \\ & 0 \mapsto 1 \\ & 1 \mapsto 0 \end{aligned}$$

donde $f_p = f_q$.

Não se confunda o conjunto $A[x]$ de todos os polinómios com coeficientes num anel A com o conjunto $\mathcal{F}_p(A)$ das funções polinomiais em A. Não só a natureza dos seus objectos é diferente, como também, frequentemente, os seus cardinais o são. Por exemplo, $\#\mathbb{Z}_n[x] = \aleph_0$ e $\#\mathcal{F}_p(\mathbb{Z}_n) \leq \#\mathbb{Z}_n^{\mathbb{Z}_n} = n^n$, assim $\mathbb{Z}_n[x]$ é infinito e $\mathcal{F}_p(\mathbb{Z}_n)$ é finito.

Definição. Sejam A um anel e $p(x) \in A[x]$. Um elemento $\alpha \in A$ diz-se *raiz do polinómio* $p(x)$ se $p(\alpha) = 0$, isto é, α é um zero da função polinomial $f_p\colon A \to A$.

O resultado seguinte é fácil de provar.

Teorema 2. *Seja A um anel comutativo com identidade. Se $a \in A$, a aplicação de substituição*

$$\begin{aligned} \xi_a\colon\ & A[x] \to A \\ & p(x) \mapsto p(a) \end{aligned}$$

é um morfismo de anéis com identidade. Além disso, $\operatorname{Ker}\xi_a$ *é o ideal de* $A[x]$ *constituído por todos os polinómios de coeficientes em* A *que admitem* a *como raiz.*

Teorema 3. *Se* A *é domínio de integridade, então* $A[x]$ *também é domínio de integridade.*

Demonstração: Pela Proposição 1, o anel $A[x]$ é comutativo com identidade. Suponhamos que A é domínio de integridade. Sejam $p(x) = a_0 + a_1\,x + \cdots + a_n\,x^n \neq 0$ e $q(x) = b_0 + b_1\,x + \cdots + b_m\,x^m \neq 0$, com $\operatorname{grau} p(x) = n$ e $\operatorname{grau} q(x) = m$. Então $a_n, b_m \neq 0$ e

$$p(x)\,q(x) = a_0\,b_0 + (a_0\,b_1 + a_1\,b_0)\,x + \cdots + a_n\,b_m\,x^{n+m}$$

Como A não tem divisores de zero e $a_n\,b_m \neq 0$, obtemos $p(x)\,q(x) \neq 0$. Logo, $A[x]$ também não tem divisores de zero, e concluímos que $A[x]$ é domínio de integridade.

Nota. Observemos que se A é domínio de integridade, então $\mathcal{U}(A[x]) = \mathcal{U}(A)$. Daqui resulta que, mesmo que A seja um corpo, o anel $A[x]$ nunca é corpo, por exemplo x não é unidade.

Da demonstração do último teorema, concluímos que

Corolário 3.1. *Se* A *é um domínio de integridade e* $p(x), q(x) \in A[x]\backslash\{0\}$ *têm grau* n *e* m*, respectivamente, então* $p(x)\,q(x)$ *tem grau* $n + m$*.* ∎

De um modo geral, se A é um anel comutativo com identidade arbitrário, dados $p(x), q(x) \in A[x]$, temos

$$\begin{aligned}\operatorname{grau}\big(p(x) + q(x)\big) &\leq \max\big\{\operatorname{grau} p(x), \operatorname{grau} q(x)\big\}\\ \operatorname{grau}\big(p(x)\,q(x)\big) &\leq \operatorname{grau} p(x) + \operatorname{grau} q(x)\end{aligned}$$

Se $q(x)$ ou $p(x)$ é mónico, então

$$\operatorname{grau}\big(p(x)\,q(x)\big) = \operatorname{grau}\,p(x) + \operatorname{grau}\,q(x).$$

Recordemos que o grau do polinómio nulo foi definido como sendo $-\infty$. Assim, o Corolário 3.1 e estas últimas observações fazem sentido mesmo quando $p(x)$ ou $q(x)$ é 0, usando a convenção usual $n+(-\infty) = -\infty + n = -\infty$, para qualquer $n \in \mathbb{N}_0$.

Em seguida, vamos mostrar que todo o morfismo de um anel A num anel B pode estender-se a um morfismo entre os anéis $A[x]$ e $B[x]$.

Teorema 4. *Sejam A e B anéis comutativos com identidade e $f\colon A \to B$ um morfismo de anéis com identidade. Então existe um único morfismo de anéis com identidade $\overline{f}\colon A[x] \to B[x]$ que estende f e respeita a indeterminada, isto é $\overline{f}(a) = f(a)$, para qualquer $a \in A$, e $\overline{f}(x) = x$. Mais ainda, se f é mergulho [isomorfismo], então $\overline{f}$ também o é.*

Demonstração: Dado $f\colon A \to B$, definimos $\overline{f}\colon A[x] \to B[x]$ por, para qualquer $p(x) = a_0 + a_1\, x + \cdots + a_n\, x^n \in A[x]$,

$$\overline{f}(p(x)) = f(a_0) + f(a_1)\, x + \cdots + f(a_n)\, x^n$$

Esta aplicação satisfaz as condições do teorema. ∎

2.2 Anéis de polinómios em mais de uma indeterminada

Algumas breves palavras sobre polinómios em mais do que uma indeterminada.

Dado um anel A comutativo com identidade, já sabemos que podemos considerar o anel comutativo com identidade $B = A[x]$. Em seguida, podemos formar o anel de polinómios com coeficientes em B. Neste caso, designamos a nova indeterminada por uma letra necessariamente diferente de x, por exemplo y. De facto, no novo anel $B[y]$, o elemento x, que pertence a B, designa a constante $(x, \overline{0}, \overline{0}, \dots)$ e não a indeterminada $y = (\overline{0}, \overline{1}, \overline{0}, \overline{0}, \dots)$, em que $\overline{0}$ é o zero de B e $\overline{1}$ é o um de B. Este novo anel representa-se por $A[x][y]$. Os elementos $\sum_{j=0}^{m}(\sum_{i=0}^{n_j} a_{ij}x^i)\, y^j$ de $A[x][y]$ podem ser reescritos na forma $\sum a_{ij}\, x^i\, y^j$, em que $a_{ij} \in A$, $i, j \in \mathbb{N}_0$, com apenas um número finito de coeficientes a_{ij} não nulos.

Exemplo.

Consideremos o anel $\mathbb{Z}$, temos $x+1$, $x^2+2\,x+3$, $x^3+1 \in \mathbb{Z}[x]$, donde

$$(x+1)+(x^2+2\,x+3)\,y+(x^3+1)\,y^2 \ \in \ \mathbb{Z}[x][y]$$

Podemos reescrever este polinómio na indeterminada y, como sendo

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

ou ainda encará-lo como um polinómio na indeterminada x com coeficiente em $\mathbb{Z}[y]$, nomeadamente

$$(1+3y+y^2)+(1+2y)x+yx^2+y^2x^3$$

Denotamos o anel $A[x][y]$ por $A[x,y]$. De modo análogo, podemos definir um novo anel comutativo com identidade $A[x,y,z]$ na indeterminada z com coeficientes em $A[x,y]$. Mais geralmente, dado um anel comutativo com identidade A é possível definir o anel de polinómios $A[x_1,\ldots,x_n]$, em n indeterminadas $x_1,\ldots,x_n$ com coeficientes em A.

Dado um anel comutativo com identidade A, consideremos o conjunto Pol_n das funções $f : \mathbb{N}^n \to A$ tais que $f(u) \neq 0$ para apenas um número finito de elementos $u \in \mathbb{N}^n$, com as operações de adição e multiplicação definidas por, dados $f, g \in \mathrm{Pol}_n$ e $u \in \mathbb{N}^n$,

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

Este conjunto Pol_n é anel comutativo com identidade. Em particular, Pol_1 é o anel $A[x]$ definido atrás e Pol_2 é isomorfo ao anel $A[x_1,x_2]$.

Notemos que $A[x_1][x_2] \simeq \mathrm{Pol}_2 \simeq A[x_2][x_1]$ e que, mais geralmente,

$$A[x_1,\ldots,x_k][x_{k+1},\ldots,x_n] \simeq \mathrm{Pol}_n \simeq A[x_{k+1},\ldots,x_n][x_1,\ldots,x_k]$$

(ver Hungerford).

Quanto ao grau de um polinómio em mais do que uma indeterminada, temos o conceito de grau total e o de grau relativo a uma indeterminada.

Exemplos.

1) O polinómio do exemplo anterior, tem grau 2 em relação à indeterminada y, 3 em relação à indeterminada x e o grau total é o máximo dos graus dos monómios que é 5 (sendo o grau de um monómio igual à soma dos graus das indeterminadas que nele surgem), relativo ao grau de x^3y^2.

2) Consideremos o polinómio

$$q(x) = 3x^2y^2z^2 + 3xz^4 - 6y^3z \in \mathbb{Z}[x]$$

este polinómio tem grau 2 em relação a x, 3 em relação a y, 4 em relação a z e grau total 6 relativo a $3x^2y^2z^2$.

2.3 Divisão de polinómios

Passamos, agora, ao estudo de algumas propriedades de um anel de polinómios $A[x]$, idênticas a propriedades bem conhecidas em $\mathbb{Z}$, nomeadamente: divisão de Euclides, determinação do máximo divisor comum e factorização única.

Seja A um anel comutativo com identidade. Recordemos que dados $f(x), g(x) \in A[x]$, dizemos que $f(x)$ *divide* $g(x)$ se existe $h(x) \in A[x]$ tal que $g(x) = f(x)\,h(x)$ e que, neste caso, escrevemos $f(x)/g(x)$.

Teorema 5. (Algoritmo da divisão de Euclides) *Seja A um anel comutativo com identidade. Sejam $f(x), g(x) \in A[x]$ em que $g(x)$ é mónico. Então existem $q(x), r(x) \in A[x]$ únicos tais que $f(x) = g(x)\,q(x) + r(x)$ e $\operatorname{grau} r(x) < \operatorname{grau} g(x)$.*

Demonstração: Em primeiro lugar, observemos que se $\operatorname{grau} f(x) < \operatorname{grau} g(x)$, temos $f(x) = g(x)\,0 + f(x)$.

Admitamos então que grau $f(x) \geq$ grau $g(x)$. Vamos provar o resultado por indução sobre grau $f(x) -$ grau $g(x)$.

Seja $f(x) = a_m\, x^m + \cdots + a_1\, x + a_0$, com grau $f(x) = m$, e $g(x) = x^n + b_{n-1}\, x^{n-1} + \cdots + b_1\, x + b_0$, em que grau $g(x) = n$.

Se $m - n = 0$, isto é, $m = n$, então

$$f(x) = g(x)\, a_n + \Big((a_{n-1} - b_{n-1}\, a_n)\, x^{n-1} + \cdots + (a_0 - b_0\, a_n)\Big)$$

pelo que podemos tomar

$$q(x) = a_n \quad \text{e} \quad r(x) = (a_{n-1} - b_{n-1}\, a_n)\, x^{n-1} + \cdots + (a_0 - b_0\, a_n)$$

onde grau $r(x) \leq n - 1$.

Suponhamos agora que o resultado é verdadeiro para quaisquer polinómios $f^*(x), g^*(x) \in A[x]$ tais que grau $f^*(x) -$ grau $g^*(x) < k$, com $k \geq 1$. Sejam $f(x)$ e $g(x)$, como atrás, tais que $m - n = k$. Neste caso, temos

$$f(x) = g(x)\, a_m\, x^k + h(x)$$

em que

$$\begin{aligned} h(x) = (a_{m-1} - b_{n-1}\, a_m)\, x^{m-1} + \cdots + (a_{m-n} - b_0\, a_m)\, x^{m-n} \\ + \; a_{m-n-1}\, x^{m-n-1} + \cdots + a_0 \end{aligned}$$

com grau $h(x) \leq m - 1 < m =$ grau $f(x)$.

Se grau $h(x) <$ grau $g(x)$, obtemos o resultado pretendido.

Se grau $h(x) \geq$ grau $g(x)$, como

$$\text{grau}\, h(x) - \text{grau}\, g(x) < m - \text{grau}\, g(x) = k$$

por hipótese de indução, existem $l(x)$ e $r(x)$ tais que

$$h(x) = g(x)\, l(x) + r(x)$$

com grau $r(x) <$ grau $g(x)$. Logo

$$\begin{aligned} f(x) &= g(x)\, a_m\, x^k + g(x)\, l(x) + r(x) \\ &= g(x)\, \Big(a_m\, x^k + l(x)\Big) + r(x) \end{aligned}$$

com $\operatorname{grau} r(x) < \operatorname{grau} g(x)$.

O resultado fica demonstrado atendendo ao princípio de indução.

Resta provar a unicidade de $q(x)$ e $r(x)$.

Sejam $q^*(x)$, $r^*(x)$ tais que $\operatorname{grau} r^*(x) < \operatorname{grau} g(x)$ e $f(x) = g(x)\,q^*(x) + r^*(x)$. Então $g(x)(q(x) - q^*(x)) = r^*(x) - r(x)$. Se $q(x) \neq q^*(x)$, então $q(x) - q^*(x) \neq 0$, pelo que tem grau maior ou igual a 0. Como $g(x)$ é mónico, temos

$$\begin{aligned}\operatorname{grau}\Big(g(x)\,(q(x) - q^*(x))\Big) &= \operatorname{grau} g(x) + \operatorname{grau}\big(q(x) - q^*(x)\big) \qquad (*)\\ &\geq \operatorname{grau} g(x) > \max\big\{\operatorname{grau} r(x), \operatorname{grau} r^*(x)\big\}\\ &\geq \operatorname{grau}\big(r^*(x) - r(x)\big)\end{aligned}$$

o que é absurdo. Logo $q(x) = q^*(x)$ e, portanto, obtemos também $r^*(x) = r(x)$. ∎

Corolário 5.1. *Seja A um domínio de integridade. Dados $f(x)$ e $g(x) \in A[x]$, se existem $q(x), r(x) \in A[x]$ tais que $f(x) = g(x)\,q(x) + r(x)$, com $\operatorname{grau} r(x) < \operatorname{grau} g(x)$, então $q(x)$ e $r(x)$ são únicos nestas condições.*

Demonstração: É análoga à segunda parte da prova do teorema anterior, atendendo a que, neste caso, A é domínio de integridade e portanto a igualdade acima $(*)$ é válida atendendo ao Corolário 3.1. ∎

O próximo resultado mostra que se partirmos de um corpo, podemos estender o Teorema 5 substituindo a condição "$g(x)$ é mónico" por "$g(x) \neq 0$".

Corolário 5.2. *Seja K um corpo. Dados $f(x), g(x) \in K[x]$ tais que $g(x) \neq 0$, existem $q(x)$ e $r(x)$ únicos tais que*

$$f(x) = g(x)\,q(x) + r(x) \quad \text{e} \quad \operatorname{grau} r(x) < \operatorname{grau} g(x)$$

Demonstração: Suponhamos que

$$g(x) = b_0 + b_1\,x + \cdots + b_n\,x^n, \quad \text{com} \;\; b_n \neq 0$$

Como K é corpo, existe $b_n^{-1} \in K$ e

$$f(x) = g(x)\,q(x) + r(x) \iff b_n^{-1}\,f(x) = \left(b_n^{-1}\,g(x)\right)q(x) + b_n^{-1}\,r(x)$$

Notemos que $\operatorname{grau} b_n^{-1} g(x) = n$ e $b_n^{-1}\,g(x)$ é mónico. Então, pelo Teorema 5, existem $q_1(x)$ e $r_1(x)$ únicos tais que $\operatorname{grau} r_1(x) < n$ e

$$b_n^{-1}\,f(x) = \left(b_n^{-1}\,g(x)\right)q_1(x) + r_1(x)$$

Portanto, existem $q(x)(= q_1(x))$ e $r(x)\,(= b_n\,r_1(x))$ únicos tais que $f(x) = g(x)\,q(x) + r(x)$, com $\operatorname{grau} r(x) < n$. ∎

A $q(x)$ chamamos o *quociente* da divisão de $f(x)$ por $g(x)$ e a $r(x)$ o *resto* dessa divisão.

Exemplo.

Sejam $f(x) = x^4 - 3\,x^3 + 2\,x^2 + 4\,x - 1$ e $g(x) = x^2 - 2\,x + 3$ polinómios em $\mathbb{Z}$. Temos $g(x)$ mónico e $\operatorname{grau} g(x) < \operatorname{grau} f(x)$. Pretendemos dividir $f(x)$ por $g(x)$:

$$\begin{array}{rl|l}
x^4 - 3\,x^3 + 2\,x^2 + 4\,x - 1 & & x^2 - 2\,x + 3 \\
\cline{3-3}
-x^4 + 2\,x^3 - 3\,x^2 & & x^2 - x - 3 \\
\cline{1-1}
\quad - x^3 - x^2 + 4\,x - 1 & & \\
\quad\;\; x^3 - 2\,x^2 + 3\,x & & \\
\cline{1-1}
\quad\quad - 3\,x^2 + 7\,x - 1 & & \\
\quad\quad + 3\,x^2 - 6\,x + 9 & & \\
\cline{1-1}
\quad\quad\quad x + 8 & &
\end{array}$$

Em $\mathbb{Z}[x]$, temos

$$f(x) = g(x)(x^2 - x - 3) + (x + 8)$$

Nota. Sejam D um domínio de integridade e K um corpo que é extensão de D. Se $f(x), g(x) \in D[x]$ e $g(x)$ é mónico, então, pelo Corolário 5.2, a divisão de $f(x)$ por $g(x)$ em $D[x]$ é possível e coincide com a divisão de $f(x)$ por $g(x)$ em $K[x]$.

Exemplo.

Se tomarmos os polinómios do exemplo anterior como polinómios em $\mathbb{Q}$, em $\mathbb{Q}[x]$ temos pois

$$f(x) = g(x)\,(x^2 - x - 3) + (x + 8)$$

Os próximos exemplos mostram que o Corolário 5.2 pode não ser verdadeiro se K não é corpo.

Exemplos.

1) Em $\mathbb{Z}[x]$ não é possível dividir $3\,x^2 + 1$ por $2\,x + 1$.

2) Em $\mathbb{Z}_4[x]$ temos

$$3{+}3\,x{+}2\,x^2{+}2\,x^3 = (1{+}x)\,(3{+}2\,x^2) = (1{+}3\,x)\,(3{+}2\,x^2){+}2\,x$$

logo a divisão é possível mas não é única.

Proposição 6. *Se K é um corpo, então $K[x]$ é domínio euclidiano.*

Demonstração: Pelo Teorema 3, o anel $K[x]$ é domínio de integridade. Pelo Corolário 5.2, a aplicação δ de $K[x]\backslash\{0\}$ em $\mathbb{N}_0$ definida por $\delta(p(x)) = \operatorname{grau} p(x)$ (ou por $\delta(p(x)) = 2^{\operatorname{grau} p(x)}$), para qualquer $p(x) \in K[x]\backslash\{0\}$, é uma norma. Logo $K[x]$ é euclidiano. ∎

Pela demonstração anterior, vemos que um domínio de integridade pode ser euclidiano em relação a mais do que uma norma.

Observação. Dados K um corpo, $f(x) \in K[x]$ e $g(x) \in K[x]\backslash\{0\}$, para dividirmos $f(x)$ por $g(x)$ já apresentámos o seguinte método, fornecido pelo Corolário 5.2: sendo b_n o coeficiente director de $g(x)$,

1) dividimos $b_n^{-1}\,f(x)$ por $b_n^{-1}\,g(x)$, usando o algoritmo do Teorema 5, obtendo

$$b_n^{-1}\,f(x) = b_n^{-1}\,g(x)\,q(x) + r(x)$$

2) escrevemos

$$f(x) = g(x)\,q(x) + b_n\,r(x)$$

Porém, como K é corpo existe um algoritmo que permite dividir directamente polinómios arbitrários $f(x)$ por $g(x)$, com $g(x) \neq 0$.

Teorema 7. (Algoritmo da divisão de Euclides) *Sejam K um corpo, $f(x), g(x) \in K[x]$ tais que $g(x) \neq 0$. Então existem polinóminos $q(x), r(x) \in K[x]$ únicos tais que*

$$f(x) = g(x)\, q(x) + r(x), \text{ com } \operatorname{grau} r(x) < \operatorname{grau} g(x) \ .$$

Demonstração: Já sabemos que o resultado é verdadeiro, pelo Corolário 5.2. No entanto, tratando-se de um corpo, podemos apresentar outra demonstração da existência, que nos fornece um algoritmo para determinar $q(x)$ e $r(x)$, o qual generaliza o apresentado no Teorema 5.

Se $\operatorname{grau} f(x) < \operatorname{grau} g(x)$, tomamos $q(x) = 0$ e $r(x) = f(x)$.

Se $\operatorname{grau} f(x) \geq \operatorname{grau} g(x)$, então $f(x) \neq 0$ e sendo

$$\begin{aligned} f(x) &= a_m x^m + \cdots + a_1 x + a_0, \quad \text{com } a_m \neq 0 \\ g(x) &= b_n x^n + \cdots + b_1 x + b_0, \quad \text{com } b_n \neq 0 \end{aligned}$$

vamos demonstrar o resultado por indução em m.

Se $m = 0$, temos $f(x) = a_0$ e, como $n \leq m$ e $g(x) \neq 0$, então $g(x) = b_0 \neq 0$. Neste caso, $a_0 = (a_0\, b_0^{-1})\, b_0 + 0$.

Para simplificar a escrita, usemos a notação p em vez de $p(x)$. Suponhamos $m > 0$ e admitamos que o resultado é válido para polinómios de grau menor do que m. Definindo $q_1 = a_m\, b_n^{-1}\, x^{m-n}$ e $r_1 = f - g q_1 = a_m x^m + \cdots + a_1 x + a_0 - (a_m x^m + \cdots + a_m b_n^{-1} b_0 x^{m-n})$ obtemos

$$f = g\, q_1 + r_1$$

Como $\operatorname{grau} r_1 < m$, existem $\overline{q}$, $\overline{r}$ tais que

$$r_1 = g\, \overline{q} + \overline{r}, \quad \text{com} \quad \operatorname{grau} \overline{r} < \operatorname{grau} g$$

donde

$$f = g\, q_1 + g\, \overline{q} + \overline{r} = g(q_1 + \overline{q}) + \overline{r}$$

como pretendíamos. ∎

Exemplos.

1) Em $\mathbb{Q}[x]$, sejam

$$f(x) = 1 + 2\,x^2 + 2\,x^4 \quad \text{e} \quad g(x) = 1 + 2\,x$$

Temos grau $g(x) <$ grau $f(x)$, com $m = 4$ e $n = 1$. Seja

$$q_1(x) = a_4\, b_1^{-1}\, x^{4-1} = 2.2^{-1}x^{4-1} = x^3$$

Então

$$f(x) = g(x)\, x^3 + r_1(x)$$

onde

$$\begin{aligned} r_1(x) &= f(x) - q_1(x)\, g(x) \\ &= 1 + 2\,x^2 + 2\,x^4 - x^3\,(1 + 2\,x) \\ &= 1 + 2\,x^2 + 2\,x^4 - x^3 - 2\,x^4 = 1 + 2\,x^2 - x^3 \end{aligned}$$

Vamos agora dividir $r_1(x) = 1 + 2\,x^2 - x^3$ por $g(x)$. Sejam

$$q_2(x) = (-1)2^{-1}x^{3-1} = -\frac{1}{2}\,x^2$$

$$r_2(x) = 1 + 2\,x^2 - x^3 - \left(-\frac{1}{2}\,x^2\right)(1 + 2\,x) = 1 + \frac{5}{2}\,x^2$$

Depois dividimos $r_2(x)$ por $g(x)$ e, assim sucessivamente, pelo que chegamos a

$$f(x) = g(x)\left(x^3 - \frac{1}{2}\,x^2 + \frac{5}{4}\,x - \frac{5}{8}\right) + \frac{13}{8}$$

Trata-se do algoritmo bem conhecido:

$$\begin{array}{r|l}
2\,x^4 + 2\,x^2 + 1 & 2\,x + 1 \\
\cancel{-2x^4} - x^3 & \hline
\cancel{\quad} - x^3 + 2\,x^2 + 1 & x^3 - \frac{1}{2}\,x^2 + \frac{5}{4}\,x - \frac{5}{8} \\
\cancel{+x^3} + \frac{1}{2}\,x^2 & \\ \hline
\cancel{\quad} \frac{5}{2}\cancel{x^2} + 1 & \\
\cancel{-\frac{5}{2}}\,x^2 - \frac{5}{4}\,x & \\ \hline
\cancel{\quad} - \cancel{\frac{5}{4}}\,x + 1 & \\
\cancel{+\frac{5}{4}}\,x + \frac{5}{8} & \\ \hline
\frac{13}{8} &
\end{array}$$

2) Em $\mathbb{Z}_3[x]$, sejam $f(x) = 1 + 2\,x^2 + 2\,x^4$ e $g(x) = 1 + 2\,x$. Recordando que em $\mathbb{Z}_3$, se tem $2^{-1} = 2$, $-2 = 1$ e $-1 = 2$, obtemos

$$\begin{array}{rrrr|l} 2\,x^4 & & +\,2\,x^2 & +\,1 & 2\,x+1 \\ -2\,x^4 & -\,x^3 & & & \hline x^3 + x^2 + 2^{-1}\,x + 2^{-1} \\ \hline & 2\,x^3 & +\,2\,x^2 & +\,1 & \\ & -\,2\,x^3 & -\,x^2 & & \\ \hline & & x^2 & +\,1 & \\ & & -\,x^2 - 2^{-1}\,x & & \\ \hline & & & x+1 & \\ & & & -\,x - 2^{-1} & \\ \hline & & & 2 & \end{array}$$

donde

$$f(x) = g(x)\,(x^3 + x^2 + 2\,x + 2) + 2$$

3) Sejam $f(x) = x^4 + 2\,x^3 + 2\,x^2 + 4\,x + 4$ e $g(x) = x^2 + 3\,x + 3$ elementos de $\mathbb{Z}_5[x]$. Vamos dividir $f(x)$ por $g(x)$, aplicando o Teorema 4 com o morfismo $\theta_5\colon \mathbb{Z} \to \mathbb{Z}_5$, $n \mapsto [n]_{\mathrm{mod}\,5}$. Começamos por pensar em $f(x)$ e $g(x)$ como sendo polinómios de $\mathbb{Z}[x]$. Pelo Teorema 5, podemos dividir $f(x)$ por $g(x)$ em $\mathbb{Z}[x]$, pois $g(x)$ é mónico, e obtemos $f(x) = g(x)\,(x^2 - x + 2) + (6\,x - 2)$ em $\mathbb{Z}[x]$. Pelo Teorema 4, temos

$$f(x) = g(x)\,(x^2 + 4\,x + 2) + (x + 3) \quad \text{em} \quad \mathbb{Z}_5[x].$$

4) Sejam $f(x) = 3x^4 + 2x$ e $g(x) = 4x^3 + 1$ elementos de $\mathbb{Z}_5[x]$. Não podemos dividir $f(x)$ por $g(x)$ usando o método do exemplo anterior pois $f(x)$ não se pode dividir por $g(x)$ em $\mathbb{Z}[x]$, visto que 4 não divide 3 em $\mathbb{Z}$. Neste caso, divide-se $f(x)$ por $g(x)$ usando o método do Teorema 7, tal como no exemplo 2.

Teorema 8. (do Resto) *Seja A um anel comutativo com identidade. Se $f(x) \in A[x]$ e $a \in A$, então o resto da divisão de $f(x)$ pelo polinómio $x - a$ é $f(a)$.*

Demonstração: Sendo $x - a$ mónico, pelo Teorema 5, existem $q(x), r(x) \in A[x]$ tais que

$$f(x) = (x - a)\, q(x) + r(x)$$

com $\text{grau}(x - a) > \text{grau}\, r(x)$. Como $\text{grau}(x - a) = 1$, temos $r(x)$ constante. Considerando a aplicação de substituição ξ_a, do Teorema 2, obtemos

$$f(a) = (a - a)\, q(a) + r(a)$$

donde $f(a) = r(a)$. Sendo $r(x)$ um polinómio constante, concluímos que $r(x) = r(a) = f(a)$. ∎

Exemplo.

Dado $f(x) = x^3 + 5\,x - 5 \in \mathbb{R}[x]$, o resto da divisão de $f(x)$ por $x - 2$ é $f(2) = 13$ e o resto da divisão de $f(x)$ por $x + 2$ é $f(-2) = -23$.

Vejamos algumas consequências do Teorema do Resto.

Corolário 8.1. *Se A é um anel comutativo com identidade, $f(x) \in A[x]$ e $a \in A$, então $x - a$ divide $f(x)$ se e só se $f(a) = 0$.*

Demonstração: É consequência imediata do teorema anterior, tendo em conta que $x - a$ divide $f(x)$ se e só se o resto da divisão de $f(x)$ por $x - a$ é 0. ∎

Corolário 8.2. *Seja A um domínio de integridade. Se um polinómio $f(x) \in A[x]\backslash\{0\}$ tem grau n, então $f(x)$ tem no máximo n raízes distintas.*

Demonstração: Provemos o resultado por indução sobre o grau de $f(x)$.

Se $\text{grau}\, f(x) = 0$, então $f(x)$ é constante não nula, pelo que $f(x)$ não tem raízes.

Se $\text{grau}\, f(x) = 1$, suponhamos $f(x) = a_0 + a_1\, x$ com $a_1 \neq 0$. Então, se $\alpha, \beta \in A$ são raízes de $f(x)$, temos $a_0 + a_1\, \alpha = 0 = a_0 + a_1\, \beta$, donde

$a_1\,\alpha = a_1\,\beta$, pelo que $a_1(\alpha - \beta) = 0$ no domínio de integridade A. Logo, $\alpha - \beta = 0$ e, assim, $\alpha = \beta$. Portanto, $f(x)$ tem, no máximo, uma raiz.

Admitamos que o resultado é válido para polinómios com grau $n \geq 0$. Seja $f(x)$ um polinómio de grau $n+1$. Se $f(x)$ não tem raízes, nada há a provar. Se $f(x)$ tem uma raiz α então, pelo Corolário 8.1, o polinómio $x - \alpha$ divide $f(x)$ e, portanto, existe $g(x)$ tal que

$$f(x) = (x - \alpha)\, g(x)$$

Logo, pelo Corolário 3.1, o polinómio $g(x)$ tem grau n. Se $\beta \neq \alpha$ é raiz de $f(x)$, então pelo Teorema 2, temos $0 = f(\beta) = (\beta - \alpha)\, g(\beta)$, donde, $g(\beta) = 0$ no domínio A. Reciprocamente, se γ é raiz de $g(x)$, é claro que é raiz de $f(x)$. Assim, as raízes de $f(x)$ distintas de α são exactamente as raízes de $g(x)$ distintas de α. Ora, por hipótese de indução, $g(x)$ tem no máximo n raízes distintas, logo $f(x)$ tem no máximo $n+1$ raízes distintas. O resultado fica demonstrado pelo princípio de indução. ∎

Observemos que, no corolário anterior, precisamos, de facto, que A seja domínio de integridade. Por exemplo, em $\mathbb{Z}_4[x]$ o polinómio $f(x) = 2\,x$ tem grau 1, mas tem duas raízes em $\mathbb{Z}_4$, nomeadamente 0 e 2.

Definição. Sejam A um anel comutativo com identidade e $f(x) \in A[x]$. Uma raiz $\alpha \in A$ de $f(x)$ diz-se de *multiplicidade* k se $(x - \alpha)^k$ divide $f(x)$ mas $(x - \alpha)^{k+1}$ não divide $f(x)$.

Se $k = 1$ a raiz diz-se *simples* e se $k > 1$ a raiz diz-se *múltipla*.

Exemplos.

1) Seja $f(x) = 1 - 2\,x + x^2 \in \mathbb{Z}[x]$. Então $\alpha = 1$ é raiz de multiplicidade 2 de $f(x)$, pois $f(x) = (x-1)^2$ e $(x-1)^3$ não divide $f(x)$.

2) Seja $g(x) = (x-2)(1 - 2x + x^2) \in \mathbb{Z}[x]$. Então 1 é raiz de multiplicidade 2 de $g(x)$ e 2 é raiz de multiplicidade 1 de $g(x)$.

É claro que se A é um anel comutativo com identidade e $f(x) \in A[x]$ é tal que $\alpha_1, \ldots, \alpha_p \in A$ são as suas raízes distintas que têm multiplicidade $n_1, \ldots, n_p \in \mathbb{N}$, respectivamente, então $n_1 + \cdots + n_p \leq$ grau $f(x)$.

2.4 Máximo divisor comum

Seja A um anel comutativo com identidade. Recordemos que dados $f(x), g(x) \in A[x]$, um polinómio $d(x) \in A[x]$ diz-se um *divisor comum* de $f(x)$ e $g(x)$ se, obviamente, $d(x)$ divide $f(x)$ e divide $g(x)$ e um divisor comum $d(x)$ de $f(x)$ e $g(x)$ diz-se um *máximo divisor comum* se todo o polinómio $q(x) \in A[x]$ divisor comum de $f(x)$ e de $g(x)$ é também divisor de $d(x)$.

Exemplo. Em $\mathbb{Z}[x]$, o polinómio $x + 1$ é máximo divisor comum de $x^2 - 1$ e de $(x + 1)(x + 3)$.

Lembremos também que se K é um corpo então $K[x]$ é domínio de integridade, pelo que dados $f(x), g(x) \in K[x]$, se $d_1(x)$ e $d_2(x)$ são máximos divisores comuns de $f(x)$ e $g(x)$, então $d_1(x)$ e $d_2(x)$ são associados e, além disso, todo o associado de $d_1(x)$ é máximo divisor comum de $f(x)$ e $g(x)$.

Já provámos atrás que se K é um corpo, então $K[x]$ é um domínio euclidiano, deste facto segue-se o seguinte.

Teorema 9. *Seja K um corpo. Então $K[x]$ é domínio de ideais principais.*

Demonstração: É consequência da Proposição 6 e do facto de, pelo Teorema I.23, todo o domínio euclidiano ser domínio de ideais principais. ∎

Nota. Se I é ideal não nulo de $K[x]$, tendo em conta as demonstrações da Proposição 6 e do Teorema I.23, concluímos que $I = \langle d(x) \rangle$, onde $d(x)$ é um polinómio não nulo arbitrário de grau mínimo em I.

Observemos ainda que se a é o coeficiente director de $d(x)$, então $a^{-1}\,d(x)$ é mónico e $I = \langle a^{-1}\,d(x)\rangle$. Por outro lado, se $c(x) \in K[x]$ é gerador de I, então $c(x)$ e $d(x)$ são associados e, portanto, têm o mesmo grau. Estas observações permitem-nos concluir que I tem um único gerador mónico.

Corolário 9.1. *Sejam K um corpo e $f(x), g(x) \in K[x]$. Então existem mdc e mmc de $f(x)$ e $g(x)$.*

Demonstração: O resultado sai do Corolário I.27.1 e do teorema anterior. ∎

Chamamos a atenção para a definição seguinte em $K[x]$.

Definição. Seja K um corpo. Dados $f(x), g(x) \in K[x]\backslash\{0\}$, o máximo divisor comum mónico de $f(x)$ e $g(x)$ designa-se por $\mathrm{mdc}(f(x), g(x))$.

Teorema 10. *Sejam K um corpo e $f(x), g(x) \in K[x]\backslash\{0\}$. O polinómio* $\mathrm{mdc}(f(x), g(x))$ *escreve-se como $a(x)\,f(x) + b(x)\,g(x)$, com $a(x), b(x) \in K[x]$.*

Demonstração: É consequência do Teorema 9 e do Corolário I.28.1. ∎

Dado um corpo K, atendendo à nota anterior e ao Teorema I.28, $\mathrm{mdc}(f(x), g(x))$ é o único polinómio mónico de menor grau que se escreve na forma $a(x)\,f(x)+b(x)\,g(x)$, com $a(x), b(x) \in K[x]$, uma vez que é gerador do ideal $\langle f(x)\rangle + \langle g(x)\rangle$.

Como podemos calcular $\mathrm{mdc}(f(x), g(x))$?

Se $f(x), g(x) \in K[x]\backslash\{0\}$ são tais que $f(x)$ divide $g(x)$, então $\mathrm{mdc}(f(x), g(x)) = a^{-1}f(x)$ em que a é o coeficiente director de $f(x)$.

O próximo algoritmo dá-nos um método para calcular $\mathrm{mdc}(f(x), g(x))$, quando $f(x)$ não divide $g(x)$ nem $g(x)$ divide $f(x)$, e também nos permitir determinar $a(x)$ e $b(x)$ tais que $\mathrm{mdc}(f(x), g(x)) =$

$a(x)f(x) + b(x)g(x)$.

Teorema 11. (Algoritmo do mdc) *Sejam K um corpo e $f(x), g(x)$ em $K[x]\backslash\{0\}$ tais que $g(x)$ não divide $f(x)$. Seja $r_k(x)$ o último resto não nulo que se obtém aplicando sucessivamente o algoritmo da divisão do modo seguinte*

$$\begin{aligned}
&\text{(a)} && f(x) = g(x)\,q(x) + r(x), && \textit{com}\ \ \operatorname{grau} r(x) < \operatorname{grau} g(x)\\
&\text{(b)} && g(x) = r(x)\,q_1(x) + r_1(x), && \textit{com}\ \ \operatorname{grau} r_1(x) < \operatorname{grau} r(x)\\
&\text{(1)} && r(x) = r_1(x)\,q_2(x) + r_2(x), && \textit{com}\ \ \operatorname{grau} r_2(x) < \operatorname{grau} r_1(x)\\
&\qquad \vdots\\
&\text{(k}-1\text{)} && r_{k-2}(x) = r_{k-1}(x)\,q_k(x) + r_k(x), && \textit{com}\ \operatorname{grau} r_k(x) < \operatorname{grau} r_{k-1}(x)\\
&\text{(k)} && r_{k-1}(x) = r_k(x)\,q_{k+1}(x)
\end{aligned}$$

Então $r_k(x)$ é um máximo divisor comum de $f(x)$ e $g(x)$ e, sendo $a \in K$ o coeficiente director de $r_k(x)$,

$$\operatorname{mdc}(f(x), g(x)) = a^{-1}\, r_k(x)$$

Demonstração: Pela igualdade (k), temos que $r_k(x)/r_{k-1}(x)$. Então, pela igualdade $(\mathrm{k}-1)$, concluímos que $r_k(x)/r_{k-2}(x)$. Sucessivamente

$$r_k(x)/r_{k-3}(x)\,, \quad \ldots\,, \quad r_k(x)/r_1(x)$$

Logo $r_k(x)/r(x)$, por (1). Portanto $r_k(x)/g(x)$, por (b), e $r_k(x)/f(x)$, por (a).

Tomemos $h(x) \in K[x]$ tal que $h(x)/f(x)$ e $h(x)/g(x)$. Por (a), temos $r(x) = f(x) - g(x)\,q(x)$, donde $h(x)/r(x)$. De (b), vem $r_1(x) = g(x) - r(x)\,q_1(x)$ pelo que $h(x)/r_1(x)$. Sucessivamente, concluímos que $h(x)/r_{k-2}(x)$ e $h(x)/r_{k-1}(x)$. Então $h(x)/r_k(x)$, pela condição $(\mathrm{k}-1)$. Portanto, $r_k(x)$ é um máximo divisor comum de $f(x)$ e $g(x)$. Logo

$$\operatorname{mdc}(f(x), g(x)) = a^{-1}\, r_k(x)$$

em que $a \in K$ é o coeficiente director de $r_k(x)$. ∎

Observação: A partir da igualdade $(k-1)$ obtemos

$$r_k(x) = r_{k-2}(x) - r_{k-1}(x)q_k(x)$$

aplicando sucessivamente as igualdades $(k-2), \ldots, (1)$ e, finalmente, (b) e (a) obtemos

$$r_k(x) = a_1(x)\, f(x) + a_2(x)\, g(x)$$

para certos $a_1(x)$, $b_1(x) \in K[x]$, donde

$$\mathrm{mdc}(f(x), g(x)) = \left(a^{-1}a_1(x)\right) f(x) + \left(a^{-1}a_2(x)\right) g(x)$$

Vejamos alguns exemplos de aplicação deste algoritmo, que esquematicamente representamos por

$$\begin{array}{rl} f & \big\lfloor\, g \\ r & \quad q \end{array}$$

$$\begin{array}{rl} g & \big\lfloor\, r \\ r_1 & \quad q_1 \end{array}$$

$$\begin{array}{rl} r & \big\lfloor\, r_1 \\ r_2 & \quad q_2 \end{array}$$

$$\vdots$$

$$\begin{array}{rl} r_{k-2} & \big\lfloor\, r_{k-1} \\ r_k & \quad q_k \end{array}$$

$$\begin{array}{rl} r_{k-1} & \big\lfloor\, r_k \\ 0 & \quad q_{k+1} \end{array}$$

Exemplos.

1) Sejam $f(x) = x^4 + 2\,x^2 + x + 1$ e $g(x) = x^2 - 1$ polinómios de $\mathbb{R}[x]$.

Vamos determinar $\mathrm{mdc}(f(x), g(x))$:

$$\begin{array}{rl|l} x^4+2\,x^2+x+1 & & x^2-1 \\ \cline{3-3} -x^4+\ \ x^2 & & x^2+3 \\ \cline{1-1} \quad +3\,x^2+x+1 & & \\ \quad -3\,x^2\quad\ +3 & & \\ \cline{1-1} \qquad\qquad x+4 & & \end{array}$$

$$\begin{array}{rl|l} x^2 & -1 & x+4 \\ \cline{3-3} -x^2-4\,x & & x-4 \\ \cline{1-1} \quad -4\,x\ -1 & & \\ \quad +4\,x+16 & & \\ \cline{1-1} \qquad\quad 15 & & \end{array}$$

Nota: Observemos que ao atingirmos um resto que é uma constante não nula, alcançámos o último resto não nulo. De facto, se obtivermos $r = s\,u + a$ com $a \in K\backslash\{0\}$, então $s = a(a^{-1}s) + 0$ donde a é o último resto não nulo.

$$\begin{array}{rl|l} x+4 & & 15 \\ \cline{3-3} -x & & \frac{1}{15}\,x+\frac{4}{15} \\ \cline{1-1} \quad 0+4 & & \\ \quad -4 & & \\ \cline{1-1} \qquad 0 & & \end{array}$$

Portanto, $r_k(x) = 15$. Logo

$$\mathrm{mdc}(f(x), g(x)) = 15^{-1}\, r_k(x) = 1$$

2) Sejam $f(x) = x^4+2\,x^3+2\,x^2+4\,x+4$, $g(x) = x^2+3\,x+3 \in \mathbb{Z}_5[x]$. Calculemos $\mathrm{mdc}(f(x), g(x))$ em $\mathbb{Z}_5[x]$.

Vamos efectuar as divisões em $\mathbb{Z}_5[x]$:

$$\begin{array}{rl|l} x^4+2x^3+2x^2+4x+4 & & x^2+3x+3 \\ \cline{3-3} -x^4-3x^3-3x^2 & & x^2-x+2 \quad = x^2+4x+2 \\ \cline{1-1} \quad -x^3-x^2+4x+4 & & \\ \quad +x^3+3x^2+3x & & \\ \cline{1-1} \quad +2x^2+7x+4 & & \\ \quad -2x^2-6x-6 & & \\ \cline{1-1} \quad x-2 & = x+3 & \end{array}$$

$$\begin{array}{rl|l} x^2+3x+3 & & x+3 \\ \cline{3-3} -x^2-3x & & x \\ \cline{1-1} \quad 3 & & \end{array}$$

Então $\text{mdc}(f(x), g(x)) = 3^{-1}.3 = 1$

3) Sejam $f(x) = x^4+2x^3+x^2+x+1$ e $g(x) = 2x^3+2x^2+2x+2$ em $\mathbb{Z}_3[x]$. Determinemos $\text{mdc}(f(x), g(x))$.

$$\begin{array}{rl|l} x^4+2x^3+x^2+x+1 & & 2x^3+2x^2+2x+2 \\ \cline{3-3} -x^4-x^3-x^2-x & & 2x+2 \\ \cline{1-1} \quad +x^3+1 & & \\ \quad -x^3-x^2-x-1 & & \\ \cline{1-1} \quad -x^2-x & = 2x^2+2x & (f = g\,q+r) \end{array}$$

$$\begin{array}{rl|l} 2x^3+2x^2+2x+2 & & 2x^2+2x \\ \cline{3-3} -2x^3-2x^2 & & x \\ \cline{1-1} \quad 2x+2 & & (g = r\,q_1+r_1) \end{array}$$

$$\begin{array}{rl|l} 2x^2+2x & & 2x+2 \\ \cline{3-3} -2x^2-2x & & x \\ \cline{1-1} \quad 0 & & (r = r_1\,q_2) \end{array}$$

Portanto, $r_1 = 2\,x + 2$ é mdc de $f(x)$ e $g(x)$, donde

$$\mathrm{mdc}\Big(f(x), g(x)\Big) = 2^{-1}\, r_1 = 2^{-1}\,(2\,x + 2) = 4\,x + 4 = x + 1$$

Procuremos agora a expressão de $\mathrm{mdc}\big(f(x), g(x)\big)$ garantida pelo Teorema 10. Temos

$$\begin{aligned} r_1 &= g - r\,q_1 = g - (f - g\,q)\,q_1 = g - f\,q_1 + g\,q\,q_1 \\ &= (-q_1)\,f + (1 + q\,q_1)\,g \\ &= (2\,x)\,f + (1 + 2\,x + 2\,x^2)\,g \end{aligned}$$

logo

$$\mathrm{mdc}(f, g) = (4\,x)\,f + \big(2 + 4\,x + 4\,x^2\big)\,g = x\,f + \big(2 + x + x^2\big)\,g$$

2.5 Polinómios irredutíveis

Nesta secção, vamos estudar os elementos irredutíveis de $K[x]$, sendo K um corpo. Vimos atrás que se K é um corpo, então $K[x]$ é domínio de ideais principais, com $\mathcal{U}(K[x]) = K\backslash\{0\}$, pelo que podemos garantir o seguinte.

Teorema 12. *Seja K um corpo. Dado $p(x) \in K[x]$, então $p(x)$ é irredutível se e só se $p(x)$ é primo.*

Demonstração: Pela Proposição I.22, visto que $K[x]$ é domínio de ideais principais, pelo Teorema 9. ∎

Vejamos alguns exemplos de polinómios irredutíveis.

Exemplos.

1) O polinómio $x^2 + 2$ é irredutível em $\mathbb{R}[x]$ mas não o é em $\mathbb{C}[x]$.

2) O polinómio $x^3 - x^2 + x - 1$ não é irredutível em $\mathbb{R}[x]$.

3) Observe que o polinómio $3x^2 + 6$ é irredutível em $\mathbb{R}[x]$ mas não o é em $\mathbb{Z}[x]$. Recorde que $\mathcal{U}(Z[x]) = \{-1, 1\}$.

Sendo K um corpo, $K[x]$ é domínio de ideais principais e, portanto, pelo Teorema I.27, é domínio de factorização única. Logo qualquer polinómio não constante de $K[x]$ pode decompor-se num produto de polinómios irredutíveis, que é único a menos da ordem dos factores e do produto por unidades. Podemos, no entanto, dizer um pouco mais.

Teorema 13. (Factorização única) *Seja K um corpo.*

a) *$K[x]$ é um domínio de factorização única.*

b) *Dado $f(x) \in K[x]\backslash K$, existem $p_1(x), \ldots, p_n(x) \in K[x]$ mónicos e irredutíveis e $a \in K\backslash\{0\}$ tais que*

$$f(x) = a\, p_1(x) \cdots p_n(x)$$

Mais ainda, esta factorização é única a menos da ordem dos factores.

Demonstração: Resta demonstrar a alínea b). Sabemos que existem $q_1(x), \ldots, q_n(x)$ polinómios irredutíveis, únicos a menos do produto por unidades, tais que $f(x) = q_1(x) \cdots q_n(x)$. Seja a_i o coeficiente director de $q_i(x)$, com $i = 1, \ldots, n$. Então

$$f(x) = (a_1 \cdots a_n)\,(a_1^{-1}\, q_1(x)) \cdots (a_n^{-1}\, q_n(x))$$

com $a_i^{-1}\, q_i(x)$ mónico irredutível, para $i = 1, \ldots, n$, e $a_1 \cdots a_n \in K\backslash\{0\}$. Então $a_1 \cdots a_n$ é o coeficiente director de $f(x)$. Sejam $b \in K\backslash\{0\}$ e $r_1(x), \ldots, r_m(x) \in K[x]$ mónicos e irredutíveis tais que

$$f(x) = b\, r_1(x) \cdots r_m(x)$$

Então b é o coeficiente director de $f(x)$. Logo $b = a_1 \cdots a_n$ e no domínio de integridade $K[x]$ obtemos

$$(a_1^{-1}\, q_1(x)) \cdots (a_n^{-1}\, q_n(x)) = r_1(x) \cdots r_m(x)$$

Como $K[x]$ é domínio de factorização única , temos $m = n$ e cada $a_i^{-1}\, q_i(x)$ é associado de algum $r_j(x)$, com $j, i = 1, \ldots, n$. Podemos supôr $i = j$. Atendendo a que cada $r_i(x)$ e cada $a_i^{-1}\, q_i(x)$ é mónico, com $i = 1, \ldots, n$, obtemos $r_i(x) = a_i^{-1}\, q_i(x)$. Logo esta factorização é única. ∎

Em seguida, dados um corpo K e um polinómio irredutível $f(x)$ de $K[x]$, vamos construir um novo corpo, nomeadamente o corpo $K[x]/\langle f(x)\rangle$.

Teorema 14. *Sejam K um corpo e $f(x) \in K[x]$ irredutível. Então $K[x]/\langle f(x)\rangle$ é corpo.*

Demonstração: Resulta do Corolário I.18.1, pois $K[x]$ é domínio de ideais principais. ∎

2.6 Descrição do corpo $K[x]/\langle f(x)\rangle$

Dados um corpo K e um polinómio irredutível mónico $f(x) \in K[x]$, vamos descrever o corpo quociente

$$K[x]/\langle f(x)\rangle = \Big\{ g(x) + \langle f(x)\rangle : g(x) \in K[x] \Big\}$$

Seja $g(x) \in K[x]$. Pelo Teorema 7, existem $q(x), r(x)$ únicos tais que

$$g(x) = f(x)\, q(x) + r(x)$$

com $\operatorname{grau} r(x) < \operatorname{grau} f(x)$. Então

$$g(x) + \langle f(x)\rangle = r(x) + \langle f(x)\rangle$$

ou seja, $g(x)$ e $r(x)$ pertencem à mesma $\sim_{\langle f(x)\rangle}$-classe, donde

$$K[x]/\langle f(x)\rangle = \Big\{ r(x) + \langle f(x)\rangle :\ r(x) \in K[x],\ \operatorname{grau} r(x) < \operatorname{grau} f(x) \Big\}.$$

Seja $f(x) = a_0 + a_1\, x + \cdots + a_{n-1}\, x^{n-1} + x^n$. Definimos $X = x + \langle f(x)\rangle$ e, dado $a \in K$, identificamos a com a sua classe $a + \langle f(x)\rangle$.

Note que, no que se segue, de facto não há perigo de ambiguidade pois se $a + \langle f(x)\rangle = b + \langle f(x)\rangle$, com $a, b \in K$, então $a - b \in \langle f(x)\rangle$, donde $f(x)$ divide $a - b \in K$. Como $f(x)$ tem grau maior ou igual a 1, concluímos que $a - b = 0$ e, portanto, $a = b$.

Com esta notação, se $r(x) = b_0 + b_1\, x + \cdots + b_{n-1}\, x^{n-1}$, temos $r(x) + \langle f(x)\rangle = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1}$. Por outro lado, de $x^n = f(x) - a_0 - a_1\, x - \cdots - a_{n-1}\, x^{n-1}$, resulta

$$X^n = -a_0 - a_1 X - \cdots - a_{n-1} X^{n-1}$$

Temos, então,

$$K[x]/\langle f(x)\rangle = \left\{b_0 + b_1X + \cdots + b_{n-1}X^{n-1} \colon b_0, \ldots, b_{n-1} \in K\right\}$$

com $X^n = -a_0 - a_1X - \cdots - a_{n-1}X^{n-1}$.

Além disso, cada elemento de $K[x]/\langle f(x)\rangle$ escreve-se de modo único na forma $b_0 + b_1X + \cdots + b_{n-1}X^{n-1}$, com $b_0, \ldots, b_{n-1} \in K$. De facto, se $b_0 + b_1X + \cdots + b_{n-1}\ X^{n-1} = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$, com $b_0, b_1, \ldots, b_{n-1}, c_0, c_1, \ldots, c_{n-1} \in K$, então $(b_0 - c_0) + (b_1 - c_1)X + \cdots + (b_{n-1} - c_{n-1})X^{n-1} = 0$ em $K[x]/\langle f(x)\rangle$, ou seja, o polinómio $(b_0 - c_0) + (b_1 - c_1)x + \cdots + (b_{n-1} - c_{n-1})x^{n-1}$ pertence ao ideal $\langle f(x)\rangle$. Logo $f(x)$ divide $(b_0 - c_0) + (b_1 - c_1)x + \cdots + (b_{n-1} - c_{n-1})x^{n-1}$ e, como grau $f(x) = n$, este polinómio tem de ser nulo. Obtemos $b_i - c_i = 0$, donde $b_i = c_i$, para $i = 0, \ldots, n-1$.

Exemplos.

1) Tomemos o polinómio $x^2 + 1$ irredutível em $\mathbb{R}[x]$. Então

$$\begin{aligned} \mathbb{R}[x]/\langle x^2+1\rangle &= \{b_0 + b_1X \colon b_0, b_1 \in \mathbb{R}\}, \quad \text{com } X^2 = -1 \\ &\simeq \mathbb{C} \end{aligned}$$

Note-se que X é raiz de $x^2 + 1$ em $\mathbb{R}[x]/\langle x^2 + 1\rangle$.

2) $\mathbb{Q}[x]/\langle x^2 + 1\rangle = \{b_0 + b_1X \colon b_0, b_1 \in \mathbb{Q}\}$, com $X^2 = -1$.

3) Seja $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Temos $X^2 = -1 - X = 1 + X$,

$$\begin{aligned} \mathbb{Z}_2[x]/\langle f(x)\rangle &= \{b_0 + b_1X \colon b_0, b_1 \in \mathbb{Z}_2\} \\ &= \{0,\ 1,\ X,\ 1+X\} \end{aligned}$$

onde as operações estão definidas do seguinte modo

$+$	0	1	X	$1+X$
0	0	1	X	$1+X$
1	1	0	$1+X$	X
X	X	$1+X$	0	1
$1+X$	$1+X$	X	1	0

$\cdot$	0	1	X	$1+X$
0	0	0	0	0
1	0	1	X	$1+X$
X	0	X	$1+X$	1
$1+X$	0	$1+X$	1	X

Temos, por exemplo, $-X = X$ e $X^{-1} = 1 + X$.

Observações.

1) Se tomarmos $f(x) \in K[x]$ irredutível com coeficiente director a não nulo, então sabemos que $a^{-1}f(x)$ é mónico e irredutível e $\langle f(x)\rangle = \langle a^{-1}f(x)\rangle$. Para obtermos a descrição de $K[x]/\langle f(x)\rangle$ podemos usar um método semelhante ao anterior, tendo em conta o coeficiente director de $f(x)$, ou tomar a sua descrição via $a^{-1}f(x)$.

2) Suponhamos que K é corpo e $f(x) \in K[x]$ é mónico e tem grau 1. Então $f(x) = a + x$, para certo $a \in K$. Podemos construir o corpo $K[x]/\langle f(x)\rangle$, obtendo-se

$$K[x]/\langle f(x)\rangle = \Big\{b + \langle f(x)\rangle \colon\ b \in K\Big\}$$

Vemos que o corpo obtido é isomorfo a K.

3) Seja $f(x)$ um polinómio irredutível em $K[x]$. A aplicação $K \hookrightarrow K[x]/\langle f(x)\rangle$, $a \mapsto a + \langle f(x)\rangle$, é um mergulho, pelo que o corpo $K[x]/\langle f(x)\rangle$ é extensão do corpo K.

4) Seja $f(x) = a_0 + a_1\, x + \cdots + a_{n-1}\, x^{n-1} + a_n\, x^n$ um polinómio irredutível em $K[x]$. Se grau $f(x) = n > 1$, então $f(x)$ não tem raízes em K. Consideremos o corpo

$$K[x]/\langle f(x)\rangle = \Big\{b_0+b_1X+\cdots+b_{n-1}X^{n-1} \colon\ b_0, b_1, \ldots, b_{n-1} \in K\Big\}$$
$$\text{com}\quad X^n = -a_0\, a_n^{-1} - a_1\, a_n^{-1}X - \cdots - a_{n-1}\, a_n^{-1}X^{n-1}$$

É claro que X é raiz do polinómio $f(x)$ considerado como polinómio com coeficientes neste novo corpo $K[x]/\langle f(x)\rangle$.

Por exemplo, X é raiz do polinómio x^2+1 no corpo $\mathbb{R}[x]/\langle x^2+1\rangle$, pois X^2+1 é a classe de x^2+1, ou seja, é o ideal $\langle x^2+1\rangle$, que é o zero do corpo quociente $\mathbb{R}[x]/\langle x^2+1\rangle$.

Definição. Sejam K um corpo, $f(x) \in K[x]$ e K^* um corpo que é extensão de K. Dizemos que K^* é *corpo de ruptura* de $f(x)$ se $f(x)$ tem uma raiz em K^*.

Exemplos.

1) Dado $f(x) = x^2+1 \in \mathbb{R}[x]$, o corpo $\mathbb{C}$ é um corpo de ruptura de $f(x)$.

2) Seja $f(x) \in K[x]$ irredutível. Então $K[x]/\langle f(x)\rangle$ é corpo de ruptura de $f(x)$, pois X é raiz de $f(x)$ neste corpo.

Teorema 15. (Kronecker) *Sejam K um corpo e $f(x) \in K[x]\backslash K$. Então existe um corpo de ruptura K^* de $f(x)$.*

Demonstração: Seja $f(x) \in K[x]\backslash K$. Se f tem raízes em K, tomamos $K^* = K$. Suponhamos que $f(x)$ não tem raízes em K. Pelo Teorema 13, podemos considerar $f(x) = a\, f_1(x) \cdots f_p(x)$, onde $f_i(x)$ é irredutível e mónico, com $i = 1, \ldots, p$, e $a \in K\backslash\{0\}$. Observemos que cada $f_i(x)$ não tem raízes em K. Tomemos $K^* = K[x]/\langle f_1(x)\rangle$, o qual é uma extensão de K. Então $X = x + \langle f_1(x)\rangle \in K^*$ é raiz de $f_1(x)$ em K^*, logo é raiz de $f(x)$ em K^*. Portanto K^* é um corpo de ruptura de $f(x)$. ∎

Mais ainda, podemos garantir o seguinte.

Teorema 16. *Sejam K um corpo e $f(x) \in K[x]\backslash K$. Então existe um corpo Ω, que é extensão de K, tal que $f(x)$ se decompõe em factores de grau 1 em $\Omega[x]$.*

Demonstração: Seja K um corpo. Demonstremos o resultado por indução sobre o grau n de um polinómio. Se $n = 1$ e $f(x) \in K[x]$

tem grau 1, tomemos $\Omega = K$. Admitamos que o resultado é válido para $n-1$ e provemo-lo para n.

Se grau $f(x) = n > 1$, então $f(x)$ decompõe-se em $K[x]$ num produto de factores irredutíveis com grau maior ou igual a 1. Sejam $g(x), h(x) \in K[x]$ tais que $f(x) = g(x)h(x)$, com $g(x)$ irredutível em $K[x]$ e grau $g(x) \geqslant 1$. Pelo Teorema 15, existe uma extensão K^* de K onde $g(x)$ tem uma raiz a. Logo $g(x) = (x-a)u(x)$, com $a \in K^*$ e $u(x) \in K^*[x]$. Então $f(x) = (x-a)\,u(x)\,h(x)$ em $K^*[x]$, tendo-se grau $u(x)\,h(x) = n-1$. Por hipótese de indução, existe uma extensão K' de K^*, logo de K, tal que $u(x)\,h(x)$ se decompõe em polinómios de grau 1 em $K'[x]$. Tomemos $\Omega = K'$. O resultado fica demonstrado pelo princípio de indução. ∎

No que se segue, deve ter-se presente que um polinómio de grau n se decompõe em factores de grau 1 em $\Omega[x]$ se e só se tem n raízes (distintas ou não) em Ω.

Observemos ainda que a demonstração do Teorema 16 nos garante a existência de uma extensão Ω de um corpo K onde $f(x) \in K[x]$ se decompõe em factores de grau 1, mas é em conjunto com a demonstração do Teorema 15 que obtemos um método para calcular uma tal extensão. Além disso, Ω não tem de ser único.

Exemplo.

Consideremos $f(x) = (x^2-2)(x^2+1) \in \mathbb{Q}[x]$. Em $\mathbb{C}[x]$, temos $f(x) = (x-\sqrt{2})\,(x+\sqrt{2})\,(x-i)\,(x+i)$ e em $\mathbb{Q}(\sqrt{2})[x]$ obtemos a decomposição $f(x) = (x-\sqrt{2})(x+\sqrt{2})(x^2+1)$. Em $\mathbb{Q}(\sqrt{2},i)[x]$, temos também $f(x) = (x-\sqrt{2})(x+\sqrt{2})(x-i)(x+i)$, sendo $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$ e $\mathbb{Q}(\sqrt{2},i) = \{a_1 + a_2\sqrt{2} + a_3 i + a_4\sqrt{2}i : a_1,a_2,a_3,a_4 \in \mathbb{Q}\}$ subcorpos de $\mathbb{C}$.

2.7 Polinómios de coeficientes em $\mathbb{Z}$ e em $\mathbb{Q}$

Pretendemos agora estudar polinómios irredutíveis de coeficientes em $\mathbb{Z}$ e em $\mathbb{Q}$.

Recordemos que um polinómio de coeficientes em $\mathbb{Q}$ é irredutível em $\mathbb{Q}[x]$ se e só se é primo em $\mathbb{Q}[x]$, uma vez que $\mathbb{Q}[x]$ é domínio de

ideais principais. Veremos que o mesmo se passa em $\mathbb{Z}[x]$, embora $\mathbb{Z}[x]$ não seja domínio de ideais principais.

Definição. Um polinómio $a_0 + a_1\,x + \cdots + a_n\,x^n \in \mathbb{Z}[x]\backslash\mathbb{Z}$ diz-se *primitivo* se $\text{mdc}(a_0, a_1, \ldots, a_n) = 1$ em $\mathbb{Z}$.

Exemplos.

O polinómio $10\,x^2 + 15\,x + 6 \in \mathbb{Z}[x]$ é primitivo, mas o polinómio $8 - 42\,x + 2\,x^2 + 72\,x^3$ não o é. Um polinómio da forma $a f(x)$, com $a \in \mathbb{Z}\backslash\{-1, 1\}$ e $f(x) \in \mathbb{Z}[x]$, nunca é primitivo.

Proposição 17. *Seja $f(x) \in \mathbb{Q}[x]\backslash\mathbb{Q}$. Então existe um polinómio primitivo $F(x) \in \mathbb{Z}[x]$ tal que $f(x) = \alpha\,F(x)$, com $\alpha \in \mathbb{Q}$ e $\alpha > 0$, sendo* $\text{grau}\, f(x) = \text{grau}\, F(x)$.

Demonstração: Seja

$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}\,x + \cdots + \frac{a_n}{b_n}\,x^n$$

com $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, $b_0, b_1, \ldots, b_n \in \mathbb{Z}\backslash\{0\}$, $\text{mdc}(a_i, b_i) = 1$, para $i = 0, \ldots, n$, e grau $f(x) = n \geq 1$. Tomemos $M = \text{mmc}(b_0, b_1, \ldots, b_n)$.

Sejam $t_i \in \mathbb{Z}$, com $i = 0, \ldots, n$, tais que $M = b_i\,t_i$. Então

$$f(x) = \frac{t_0\,a_0}{M} + \frac{t_1\,a_1}{M}\,x + \cdots + \frac{t_n\,a_n}{M}\,x^n$$

Tomemos $D = \text{mdc}(t_0\,a_0, t_1\,a_1, \ldots, t_n\,a_n)$. Então $\frac{D}{M} > 0$ e

$$f(x) = \frac{D}{M}\left(\frac{t_0\,a_0}{D} + \frac{t_1\,a_1}{D}\,x + \cdots + \frac{t_n\,a_n}{D}\,x^n\right)$$

Como $D/t_i\,a_i$ em $\mathbb{Z}$, então $\frac{t_i\,a_i}{D} \in \mathbb{Z}$, para $i = 0, \ldots, n$. Além disso,

$$\text{mdc}\left(\frac{t_0\,a_0}{D},\ \frac{t_1\,a_1}{D},\ \ldots,\ \frac{t_n\,a_n}{D}\right) = 1$$

Logo

$$F(x) = \frac{t_0\,a_0}{D} + \frac{t_1\,a_1}{D}\,x + \cdots + \frac{t_n\,a_n}{D}\,x^n \in \mathbb{Z}[x]$$

é primitivo e é associado de $f(x)$ em $\mathbb{Q}[x]$, tendo-se $f(x) = \frac{D}{M}\, F(x)$, com $\frac{D}{M} > 0$ e grau $F(x) =$ grau $f(x)$. ∎

Vejamos um exemplo.

Exemplo.

Seja $f(x) = \frac{3}{5} - 9\,x + \frac{18}{7}\,x^2 \in \mathbb{Q}[x]$.

Temos $M = \text{mmc}(5, 1, 7) = 35$ e

$$f(x) = \frac{21}{35} - \frac{315}{35}\,x + \frac{90}{35}\,x^2 = \frac{1}{35}\,(21 - 315\,x + 90\,x^2)$$

Ora, $D = \text{mdc}(21, -315, 90) = 3$, donde $f(x) = \frac{3}{35}F(x)$, em que $F(x) = 7 - 105\,x + 30\,x^2$.

Em seguida, vamos ver como se comportam os polinómios primitivos em relação ao produto.

Teorema 18. *Sejam $F(x), G(x) \in \mathbb{Z}[x]$ primitivos. Então $F(x)\,G(x)$ também o é.*

Demonstração: Suponhamos $F(x) = a_0 + a_1\,x + \cdots + a_m\,x^m$ e $G(x) = b_0 + b_1\,x + \cdots + b_n\,x^n$, com $a_m, b_n \neq 0$. Então $m, n \geq 1$, $\text{mdc}(a_0, a_1, \ldots, a_m) = 1$ e $\text{mdc}(b_0, b_1, \ldots, b_n) = 1$. Logo

$$F(x)\,G(x) = c_0 + c_1\,x + \cdots + c_{m+n}\,x^{m+n}$$

com

$$c_i = \sum_{k+\ell=i} a_k\,b_\ell\,, \qquad i = 0, \ldots, m+n$$

Se $F(x)\,G(x)$ não é primitivo, então $\text{mdc}(c_0, c_1, \ldots, c_{m+n}) \neq 1$. Seja $p \in \mathbb{N}$ primo tal que p/c_i, com $i = 0, \ldots, m+n$. Seja $s \in \{0, \ldots, m\}$ o menor índice tal que $p \not| \, a_s$. Note-se que s existe por termos $\text{mdc}\{a_0, \ldots, a_n\} = 1$. Analogamente, tomemos $t \in \{0, \ldots, n\}$ o menor índice tal que $p \not| \, b_t$. Consideremos o coeficiente

$$c_{s+t} \;=\; \sum_{\substack{k+\ell=s+t \\ k<s}} a_k\,b_\ell + a_s\,b_t \;+ \sum_{\substack{k+\ell=s+t \\ \ell<t}} a_k\,b_\ell$$

Como p é primo e não divide a_s nem b_t, então p não divide $a_s\, b_t$. Por outro lado, por definição de s e t, temos que p divide todas as outras parcelas de c_{s+t}. Ora, por hipótese, p divide c_{s+t}, pelo que p divide $a_s b_t$, o que é absurdo. Assim, concluímos que $F(x)G(x)$ é primitivo. ∎

Teorema 19. (Gauss) *Seja $F(x) \in \mathbb{Z}[x]\backslash\mathbb{Z}$ tal que $F(x) = g(x)h(x)$, com $g(x), h(x) \in \mathbb{Q}[x]\backslash\mathbb{Q}$. Então existem $G(x), H(x) \in \mathbb{Z}[x]$ tais que $F(x) = G(x)H(x)$, com* grau $G(x) =$ grau $g(x)$ *e* grau $H(x) =$ grau $h(x)$.

Demonstração: Seja $F(x) = a_0 + a_1x + \ldots + a_nx^n$, em que $a_0, \ldots, a_n \in \mathbb{Z}$, $a_n \neq 0$ e $n > 1$.

i) Admitamos que $F(x)$ é primitivo. Atendendo à Proposição 17, podemos tomar $G(x) = \alpha^{-1}\, g(x)$ e $H(x) = \beta^{-1}\, h(x)$ polinómios primitivos de $\mathbb{Z}[x]$ associados em $\mathbb{Q}[x]$ de $g(x)$ e $h(x)$, respectivamente, com $\alpha^{-1}, \beta^{-1} \in \mathbb{Q}^+$. Suponhamos $\alpha = \frac{a}{b}$ e $\beta = \frac{c}{d}$, com $a, b, c, d \in \mathbb{N}$ e $\text{mdc}(a, b) = \text{mdc}(c, d) = 1$.

Temos $F(x) = \frac{a}{b}\frac{c}{d}G(x)H(x)$, donde $bdF(x) = acG(x)H(x)$. Sejam $b_0, \ldots, b_n$ os coeficientes de $G(x)H(x)$. Obtemos $bda_i = acb_i$, em que $i = 0, \ldots, n$. Então $\text{mdc}(bd\, a_0, \ldots, bd\, a_n) = \text{mdc}(ac\, b_0, \ldots, ac\, b_n)$, donde

$$bd\, \text{mdc}(a_0, \ldots, a_n) = ac\, \text{mdc}(b_0, \ldots, b_n)$$

Como $F(x)$ é primitivo, $\text{mdc}(a_0, \ldots, a_n) = 1$. Por outro lado, pelo Teorema 18, sendo $G(x)$ e $H(x)$ primitivos, $G(x)\, H(x)$ também o é, pelo que $\text{mdc}(b_0, \ldots, b_n) = 1$. Logo $bd = ac$, donde $F(x) = G(x)\, H(x)$, como pretendíamos.

(**ii**) Admitamos agora que $F(x)$ não é primitivo. Neste caso, temos $F(x) = d\, F_1(x)$ em que $d = \text{mdc}(a_0, \ldots, a_n) \neq 1$ e $F_1(x) = \frac{1}{d}\, F(x) \in \mathbb{Z}[x]$ é primitivo, com grau $F(x) =$ grau $F_1(x)$. Então $F_1(x) \in \mathbb{Z}[x]\backslash\mathbb{Z}$ e

$$F_1(x) = \left(\frac{1}{d}\, g(x)\right) h(x)$$

Por (i), sabemos que existem $G_1(x)$ e $H_1(x) \in \mathbb{Z}[x]$ tais que grau $G_1(x) =$ grau$(\frac{1}{d}\, g(x)) =$ grau $g(x)$, grau $H_1(x) =$ grau $h(x)$ e

$$F_1(x) = G_1(x)\, H_1(x)$$

Portanto, $F(x) = (d\,G_1(x))\,H_1(x)$, com $d\,G_1(x) \in \mathbb{Z}[x]$, sendo

$$\text{grau}\, d\,G_1(x) = \text{grau}\, g(x) \qquad \text{e} \qquad \text{grau}\, H_1(x) = \text{grau}\, h(x),$$

como queríamos demonstrar. ∎

Corolário 19.1. *Seja $F(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$. Se $F(x)$ não é irredutível em $\mathbb{Q}[x]$, então $F(x)$ não é irredutível em $\mathbb{Z}[x]$.*

Demonstração: Como $F(x) \in \mathbb{Z}[x]\setminus\mathbb{Z}$, então $F(x) \notin \mathbb{Q}$. Uma vez que $F(x)$ não é irredutível em $\mathbb{Q}[x]$ temos $F(x) = g(x)\,h(x)$, para alguns $g(x), h(x) \in \mathbb{Q}[x]$ com $\text{grau}\, g(x) \geq 1$ e $\text{grau}\, h(x) \geq 1$. Então, pelo teorema anterior, existem $G(x), H(x) \in \mathbb{Z}[x]$ tais que $F(x) = G(x)\,H(x)$, com $\text{grau}\, G(x) = \text{grau}\, g(x)$ e $\text{grau}\, H(x) = \text{grau}\, h(x)$. Logo $F(x)$ não é irredutível em $\mathbb{Z}[x]$. ∎

Observemos que o corolário anterior não é válido para elementos $F(x) \in \mathbb{Z}$. Por exemplo, o elemento 5 é irredutível em $\mathbb{Z}[x]$, mas não o é em $\mathbb{Q}[x]$, pois é unidade de $\mathbb{Q}[x]$. Tenhamos também presente que este corolário equivale a dizer que dado $F(x) \in \mathbb{Z}[x]\setminus\mathbb{Z}$, se $F(x)$ é irredutível em $\mathbb{Z}[x]$, então $F(x)$ é irredutível em $\mathbb{Q}[x]$.

Corolário 19.2. *Seja $F(x) \in \mathbb{Z}[x]$ primitivo. Então $F(x)$ é irredutível em $\mathbb{Q}[x]$ se e só se é irredutível em $\mathbb{Z}[x]$.*

Demonstração: Como $F(x)$ é primitivo, então $F(x) \notin \mathbb{Z}$. Pelo corolário anterior, se $F(x)$ é irredutível em $\mathbb{Z}[x]$, então $F(x)$ é irredutível em $\mathbb{Q}[x]$. Reciprocamente, suponhamos que $F(x)$ é irredutível em $\mathbb{Q}[x]$. Se $F(x) = G(x)\,H(x)$, com $G(x), H(x) \in \mathbb{Z}[x]$, então, como $F(x)$ é irredutível em $\mathbb{Q}[x]$, temos $G(x)$ ou $H(x)$ em $\mathbb{Q}\setminus\{0\}$. Logo $G(x) \in \mathbb{Z}$ ou $H(x) \in \mathbb{Z}$. Se tivéssemos $G(x)$ ou $H(x)$ em $\mathbb{Z}\setminus\{-1,1\}$, então $F(x)$ não seria primitivo. Assim, temos $G(x)$ ou $H(x)$ em $\{-1,1\} = \mathcal{U}(\mathbb{Z}[x])$, donde $F(x)$ é irredutível em $\mathbb{Z}[x]$. ∎

Notemos que este último corolário não é válido para polinómios de $\mathbb{Z}[x]$ não primitivos. Por exemplo, $F(x) = 6 + 6\,x \in \mathbb{Z}[x]$ pode ser escrito como $6(1 + x)$, em que 6, $1+x \notin \mathcal{U}(\mathbb{Z}[x])$, pelo que não é

irredutível em $\mathbb{Z}[x]$, embora o seja em $\mathbb{Q}[x]$.

Vamos agora provar que em $\mathbb{Z}[x]$ os elementos irredutíveis coincidem com os elementos primos, embora $\mathbb{Z}[x]$ não seja domínio de ideais principais.

Teorema 20. *Seja $f(x) \in \mathbb{Z}[x]$. Então $f(x)$ é irredutível em $\mathbb{Z}[x]$ se e só se é primo em $\mathbb{Z}[x]$.*

Antes de demonstrar este teorema, provemos o resultado seguinte.

Lema 21. *Seja $a \in \mathbb{Z}\backslash\{-1, 0, 1\}$. Então*

a) *a é primo em $\mathbb{Z}[x]$ se e só se a é primo em $\mathbb{Z}$;*

b) *a é irredutível em $\mathbb{Z}[x]$ se e só se a é primo em $\mathbb{Z}$;*

c) *a é primo em $\mathbb{Z}[x]$ se e só se a é irredutível em $\mathbb{Z}[x]$.*

Demonstração: **a**) É claro que se a é primo em $\mathbb{Z}[x]$, então a é primo em $\mathbb{Z}$. Reciprocamente, suponhamos que a é primo em $\mathbb{Z}$ e que $a/f(x)\,g(x)$, com $f(x), g(x) \in \mathbb{Z}[x]$. Se $f(x) = 0$ ou $g(x) = 0$, então $a/f(x)$ ou $a/g(x)$ respectivamente. Admitamos então que $f(x) \neq 0$ e $g(x) \neq 0$. Seja $r(x) \in \mathbb{Z}[x]$ tal que $f(x)\,g(x) = a\,r(x)$. Sejam D_f, D_g e D_r os máximos divisores comuns positivos dos coeficientes de $f(x)$, $g(x)$ e $r(x)$, respectivamente. Então

$$D_g\,D_f\Big(\frac{1}{D_f}f(x)\Big)\Big(\frac{1}{D_g}\,g(x)\Big) \;=\; a\,D_r\Big(\frac{1}{D_r}\,r(x)\Big)$$

sendo $\frac{1}{D_f}f(x)$, $\frac{1}{D_g}\,g(x)$, $\frac{1}{D_r}\,r(x) \in \mathbb{Z}[x]$ primitivos ou iguais a 1 ou -1. Assim $D_g\,D_f = |a|\,D_r$. Como a é primo em $\mathbb{Z}$, então a/D_g ou a/D_f. Logo $a/g(x)$ ou $a/f(x)$, pelo que a é primo em $\mathbb{Z}[x]$.

b) Se a é irredutível em $\mathbb{Z}[x]$, então a é irredutível em $\mathbb{Z}$, uma vez que $\mathcal{U}(\mathbb{Z}[x]) = \mathcal{U}(\mathbb{Z})$ e $\mathbb{Z} \subseteq \mathbb{Z}[x]$. Portanto, como $\mathbb{Z}$ é domínio de ideais principais, a é primo em $\mathbb{Z}$. Reciprocamente, se a é primo em $\mathbb{Z}$, então a é irredutível em $\mathbb{Z}$ e facilmente se conclui que é também irredutível em $\mathbb{Z}[x]$.

c) É consequência das alíneas anteriores. ∎

Demonstração do Teorema 20: Se $f(x)$ é constante, então $f(x) \in \mathbb{Z}$ e o resultado é consequência do lema anterior.

Suponhamos que grau $f(x) \geq 1$. Se $f(x)$ é primo, então $f(x)$ é irredutível pois $\mathbb{Z}[x]$ é domínio de integridade, mas a condição recíproca não é imediata, já que $\mathbb{Z}[x]$ não é domínio de ideais principais.

Admitamos que $f(x)$ é irredutível em $\mathbb{Z}[x]$. Sejam $g(x), h(x) \in \mathbb{Z}[x]$ tais que $f(x)$ divide $g(x)\,h(x)$ em $\mathbb{Z}[x]$.

Se $f(x)$ não fosse primitivo, teríamos $f(x) = D(\frac{1}{D}\,f(x))$, em que D é mdc dos seus coeficientes e $D > 1$. Então $D \notin \mathcal{U}(\mathbb{Z}[x])$ e, por outro lado, $f(x) \notin \mathcal{U}(\mathbb{Z}[x])$, donde $f(x)$ não seria irredutível em $\mathbb{Z}[x]$. (Observemos que acabámos de provar que um polinómio $f(x) \in \mathbb{Z}[x]\backslash\mathbb{Z}$ não primitivo é sempre não irredutível em $\mathbb{Z}[x]$.) Portanto, $f(x)$ é primitivo. Logo, pelo Corolário 19.2, o polinómio $f(x)$ também é irredutível em $\mathbb{Q}[x]$, pelo que $f(x)$ é primo em $\mathbb{Q}[x]$, visto que $\mathbb{Q}[x]$ é domínio de ideais principais. Como $f(x)$ divide $g(x)\,h(x)$ em $\mathbb{Z}[x]$, então $f(x)$ divide $g(x)\,h(x)$ em $\mathbb{Q}[x]$, donde $f(x)$ divide $g(x)$ ou $h(x)$ em $\mathbb{Q}[x]$. Suponhamos que $f(x)$ divide $g(x)$ em $\mathbb{Q}[x]$. Seja $r(x) \in \mathbb{Q}[x]$ tal que $g(x) = f(x)\,r(x)$.

Se $r(x) \in \mathbb{Q}$, tomemos $\alpha = |r(x)|$ e $R(x) = \frac{r(x)}{\alpha}$, donde $R(x) \in \{-1, 1\}$; se $r(x) \notin \mathbb{Q}$, tomemos $R(x) \in \mathbb{Z}[x]$ primitivo e $\alpha \in \mathbb{Q}^+$ tal que $r(x) = \alpha\,R(x)$.

Sejam $a, b \in \mathbb{N}$ tais que $\alpha = \frac{a}{b}$ e $\text{mdc}(a, b) = 1$. Logo

$$b\,g(x) = a\,f(x)\,R(x)$$

Seja d o mdc positivo dos coeficientes de $g(x)$. Então $\frac{1}{d}\,g(x) \in \mathbb{Z}[x]$ é primitivo e temos

$$b\,d\left(\frac{1}{d}\,g(x)\right) = a\,f(x)\,R(x)$$

Pelo Teorema 18, o polinómio $f(x)\,R(x)$ também é primitivo e obtemos $b\,d = a$. Logo b/a, pelo que $b = \text{mdc}(a, b)$, donde $b = 1$. Assim, $\alpha = a \in \mathbb{N}$ e $r(x) = a\,R(x) \in \mathbb{Z}[x]$. Portanto, $f(x)$ divide $g(x)$ em $\mathbb{Z}[x]$.

Analogamente se estuda o caso em que $f(x)$ divide $h(x)$. Conclu?mos pois que $f(x)$ é primo em $\mathbb{Z}[x]$. ∎

Apresentaremos agora um teste que nos permite garantir que certos polinómios de coeficientes em $\mathbb{Z}$ são irredutíveis em $\mathbb{Q}[x]$.

Teorema 22. (Teste de Eisenstein) *Seja* $F(x) = a_0 + a_1 x + \cdots + a_n\, x^n \in \mathbb{Z}[x]$, *com* $a_n \neq 0$ *e* $n \geq 2$. *Se existe um primo* $p \in \mathbb{Z}$ *tal que*

a) p/a_0, p/a_1, ..., p/a_{n-1}, $p \not| \, a_n$,

b) $p^2 \not| \, a_0$,

então $F(x)$ *é irredutível em* $\mathbb{Q}[x]$.

Demonstração: Suponhamos que $F(x)$ não é irredutível em $\mathbb{Q}[x]$. Então existem $g(x), h(x) \in \mathbb{Q}[x] \backslash \mathbb{Q}$ tais que $F(x) = g(x)\, h(x)$. Pelo Teorema de Gauss, existem $G(x), H(x) \in \mathbb{Z}[x]$ tais que $F(x) = G(x)\, H(x)$, com grau $G(x) =$ grau $g(x)$ e grau $H(x) =$ grau $h(x)$.

Consideremos $G(x) = b_0 + b_1\, x + \cdots + b_r\, x^r$, com $b_r \neq 0$, e $H(x) = c_0 + c_1\, x + \cdots + c_s\, x^s$, com $c_s \neq 0$. Temos $1 \leq r, s < n$. Então $a_0 = b_0\, c_0$. Como p é primo e p/a_0, então p/b_0 ou p/c_0.

Suponhamos que p/b_0. Então $p \not| \, c_0$, porque $p^2 \not| \, a_0$. Consideremos agora o coeficiente a_1. Temos $a_1 = b_0\, c_1 + b_1\, c_0$ e, como p/a_1, p/b_0, $p \not| \, c_0$ e p é primo, então p/b_1.

Vejamos que se p/b_i, para qualquer $i \leq k$, com $k < r$, então p/b_{k+1}. Como

$$a_{k+1} = \sum_{\substack{j+i=k+1 \\ i \leq k}} c_j\, b_i + c_0\, b_{k+1}$$

e p/a_{k+1}, temos que $p/c_0\, b_{k+1}$. Ora p é primo e $p \not| \, c_0$, logo p/b_{k+1}. Assim, p/b_i para qualquer $i \leq r$ e, em particular, p/b_r. Portanto, p/a_n, pois $a_n = b_r\, c_s$, o que é absurdo.

Se admitirmos que p/c_0 chegamos, de modo análogo, a um absurdo. Logo $F(x)$ é irredutível em $\mathbb{Q}[x]$. ∎

Exemplo.

Provemos que $f(x) = \frac{1}{5} - 3\,x + \frac{6}{5}\,x^2 - x^3 + \frac{4}{5}\,x^4 + \frac{2}{15}\,x^5$ é irredutível em $\mathbb{Q}[x]$. Comecemos por escrever

$$f(x) = \frac{1}{15}\left(3 - 45\,x + 18\,x^2 - 15\,x^3 + 12\,x^4 + 2\,x^5\right)$$

Seja $F(x) = 3 - 45\,x + 18\,x^2 - 15\,x^3 + 12\,x^4 + 2\,x^5 \in \mathbb{Z}[x]$. Temos que

$$3/3, \quad 3/-45, \quad 3/18, \quad 3/-15, \quad 3/12, \quad 3 \not| \, 2, \quad 9 \not| \, 3$$

logo, pelo critério de Eisenstein, $F(x)$ é irredutível em $\mathbb{Q}[x]$. Portanto, $f(x)$ é irredutível em $\mathbb{Q}[x]$, pois é associado de $F(x)$ em $\mathbb{Q}[x]$.

O resultado seguinte dá-nos um método para procurarmos raízes racionais de polinómios de coeficientes inteiros.

Teorema 23. (Teste da raiz racional) *Seja* $F(x) = a_0 + a_1\,x + \cdots + a_n\,x^n \in \mathbb{Z}[x]$, *com* $a_n \neq 0$. *Seja* $\frac{r}{s} \in \mathbb{Q}$, *com* $\mathrm{mdc}(r,s) = 1$, *uma raiz de* $F(x)$. *Então* r/a_0 *e* s/a_n.

Demonstração: Como $\frac{r}{s}$ é raiz de $F(x)$, obtemos

$$0 = a_0 + a_1\,\frac{r}{s} + a_2\,\frac{r^2}{s^2} + \cdots + a_n\,\frac{r^n}{s^n}$$

donde

$$0 = a_0\,s^n + a_1\,r\,s^{n-1} + a_2\,r^2\,s^{n-2} + \cdots + a_{n-1}\,r^{n-1}\,s + a_n\,r^n$$

Então $r/a_0\,s^n$ e $s/a_n\,r^n$. Como $\mathrm{mdc}(r,s) = 1$, temos que r/a_0 e s/a_n. ∎

Exemplo.

Provemos que $F(x) = x^3 + 2\,x^2 + 4\,x + 2$ não tem raízes em $\mathbb{Q}$. Se tivesse uma raiz racional $\frac{r}{s}$, com $\text{mdc}(r,s) = 1$, teríamos que $r/2$ e $s/1$. Logo $r \in \{-2, 2, -1, 1\}$ e $s \in \{-1, 1\}$, donde $\frac{r}{s} \in \{-2, 2, -1, 1\}$. Porém $F(-2), F(2), F(-1), F(1) \neq 0$. Observemos que, neste caso, podemos concluir que $F(x)$ é irredutível em $\mathbb{Q}[x]$, já que tem grau 3 e não tem raízes em $\mathbb{Q}$.

2.8 Polinómios de coeficientes em $\mathbb{R}$ e em $\mathbb{C}$

Começamos por enunciar o Teorema Fundamental da Álgebra demonstrado pela primeira vez por Gauss (nascido em 1777), que apresentou seis demonstrações diferentes deste resultado. A demonstração deste teorema pode ser feita algebricamente ou, mais simplesmente, usando resultados de Análise Complexa (ver Allenby ou Howie (2003), respectivamente).

Teorema Fundamental da Álgebra 24. *Todo o polinómio não constante de coeficientes em $\mathbb{C}$ admite uma raiz em $\mathbb{C}$.*

É claro que é consequência deste resultado o facto seguinte.

Corolário 24.1. *Todo o polinómio não constante de coeficientes em $\mathbb{C}$ decompõe-se em factores de grau 1 de $\mathbb{C}[x]$.*

No que respeita a polinómios de coeficientes reais, pretendemos mostrar que todo o polinómio não constante se decompõe num produto de polinómios de grau 1 ou 2.

Consideremos $f(x) \in \mathbb{R}[x]\backslash\mathbb{R}$. Pelo Teorema 24, o polinómio $f(x)$ admite uma raiz $\beta \in \mathbb{C}$. Sendo $\beta = a + b\,i$, com $a, b \in \mathbb{R}$, podemos ver que

$$0 = \overline{f(a + b\,i)} = f(a - b\,i)$$

donde $\overline{\beta}$, o conjugado de β, também é raiz de $f(x)$. Efectivamente, escrevendo $f(x) = \sum_{j=1}^{n} a_j\,x^j$ com $a_j \in \mathbb{R}$, se $\beta \in \mathbb{C}\backslash\mathbb{R}$ é tal que

$f(\beta) = 0$, então

$$0 = \overline{0} = \overline{f(\beta)} = \overline{\sum_{j=1}^{n} a_j\, \beta^j} = \sum_{j=1}^{n} \overline{a_j\, \beta^j} = \sum_{j=1}^{n} a_j\, \overline{\beta^j} = \sum_{j=1}^{n} a_j \overline{\beta}^j = f(\overline{\beta})$$

Vamos mostrar que β e $\overline{\beta}$ têm a mesma multiplicidade. Temos

$$(x-\beta)\,(x-\overline{\beta}) = x^2 - 2\,a\,x + a^2 + b^2 \;\in\; \mathbb{R}[x]$$

Se $\beta \in \mathbb{C}\backslash\mathbb{R}$, então $\beta \neq \overline{\beta}$ e sabemos que $(x-\beta)\,(x-\overline{\beta})$ divide $f(x)$ em $\mathbb{C}[x]$. Logo existe $h(x) \in \mathbb{C}[x]$ tal que $f(x) = h(x)\,(x-\beta)\,(x-\overline{\beta})$. Além disso, como $(x-\beta)\,(x-\overline{\beta}) \in \mathbb{R}[x]$, pelo Teorema 7, existem $h_1(x), r(x) \in \mathbb{R}[x]$ tais que

$$f(x) = h_1(x)\,(x-\beta)\,(x-\overline{\beta}) + r(x), \qquad \text{com} \quad \operatorname{grau} r(x) < 2$$

Ora $\mathbb{R}[x] \subseteq \mathbb{C}[x]$ e a divisão em $\mathbb{C}[x]$ efectua-se de modo único, donde $h(x) = h_1(x)$ e $r(x) = 0$. Portanto, $h(x) \in \mathbb{R}[x]$. Admitamos que β tem multiplicidade k e $\overline{\beta}$ tem multiplicidade ℓ. Se $k \geq 2$, então β é raiz de $h(x)$. Logo $\overline{\beta}$ também é raiz de $h(x)$, pelo que $\left((x-\beta)(x-\overline{\beta})\right)^2$ divide $f(x)$. Sucessivamente concluímos que $\left((x-\beta)\,(x-\overline{\beta})\right)^k$ divide $f(x)$ em $\mathbb{R}[x]$. Logo $k \leq \ell$. Como $\overline{\overline{\beta}} = \beta$, o mesmo raciocínio aplicado a $\overline{\beta}$ permite-nos concluir que $\ell \leq k$. Portanto $\ell = k$.

Assim, concluímos que num polinómio $f(x) \in \mathbb{R}[x]\backslash\mathbb{R}$ as raízes complexas não reais surgem aos pares.

No que se segue, devemos ter em conta que se K é um corpo, $f(x) \in K[x]$, e $\alpha_1, \ldots, \alpha_r \in K$ são raízes distintas de $f(x)$ com multiplicidade $m_1, \ldots, m_r$ respectivamente, então existe $h(x) \in K[x]$ tal que

$$f(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_r)^{m_r}\, h(x)$$

e $\alpha_1, \ldots, \alpha_r$ não são raízes de $h(x)$.

Teorema 25. *Todo o polinómio de $\mathbb{R}[x]\backslash\mathbb{R}$ é produto de polinómios de grau 1 ou 2.*

Demonstração: Seja $f(x) \in \mathbb{R}[x]\backslash\mathbb{R}$ com $\operatorname{grau} n \geq 1$. Suponhamos que $f(x)$ tem exactamente p raízes reais distintas $\alpha_1, \ldots, \alpha_p$ e $2k$

raízes complexas não reais distintas $\beta_1, \ldots, \beta_k$, $\overline{\beta}_1, \ldots, \overline{\beta}_k$. Sejam r_i a multiplicidade de α_i, com $i = 1, \ldots, p$ e m_j a multiplicidade de β_j, com $j = 1, \ldots, k$. Então

$$f(x) = (x-\alpha_1)^{r_1} \cdots (x-\alpha_p)^{r_p} \left((x-\beta_1)(x-\overline{\beta}_1)\right)^{m_1}$$

$$\cdots\cdots\cdots \left((x-\beta_k)(x-\overline{\beta}_k)\right)^{m_k} h(x)$$

para algum $h(x) \in \mathbb{C}[x]$, em que $h(x)$ não tem raízes em $\mathbb{C}$, pois $f(x)$ não tem outras raízes em $\mathbb{C}$. Pelo Teorema 24, o polinómio $h(x)$ é uma constante de $\mathbb{C}[x]$. Assim, $h(x) \in \mathbb{C}$ e, como $f(x) \in \mathbb{R}[x]$, obtemos $h(x) \in \mathbb{R}$. Portanto $f(x)$ decompõe-se em $\mathbb{R}[x]$ em polinómios de grau 1 ou de grau 2. ∎

Do teorema anterior, resulta imediatamente o seguinte.

Corolário 25.1. *Se $f(x) \in \mathbb{R}[x]$ é irredutível em $\mathbb{R}[x]$, então* grau $f(x)$ *é 1 ou 2.*

Exemplos.

1) O polinómio $f(x) = x^2 - 2$ é irredutível em $\mathbb{Q}[x]$ mas não o é em $\mathbb{R}[x]$.

2) O polinómio $f(x) = x^2 + 2$ é irredutível em $\mathbb{R}[x]$, mas não o é em $\mathbb{C}[x]$.

Para mais resultados sobre polinómios veja-se, por exemplo, Allenby, Brison ou Freitas.

Exercícios

1. Seja A um anel comutativo com identidade. Mostre que o subconjunto de $A[x]$

$$A^0 = \left\{ a_1\, x + \cdots + a_n\, x^n \mid \ n \in \mathbb{N} \text{ e } a_1, \ldots, a_n \in A \right\}$$

é um ideal de $A[x]$.

2. Indique, caso exista, um natural $n > 1$ tal que $x^2 + 3$ divida $x^5 - 3\,x^4 + 3\,x^3 - 9\,x$ em $\mathbb{Z}_n[x]$.

3. Considere em $\mathbb{Z}_3[x]$ os polinómios $f(x) = x^{12} + x^9 + x^4 + x^3$ e $g = x^3 + 1$. Determine os polinómios $q(x), r(x) \in \mathbb{Z}_3[x]$ tais que $f(x) = g(x)q(x) + r(x)$ e $gr(r(x)) < gr(g(x))$.

4. No domínio de integridade $\mathbb{Z}[x]$, considere os ideais $\langle 3 \rangle$ e $\langle 3, x \rangle$. Mostre que

   a) (i) $x \notin \langle 3 \rangle$;
   (ii) $1 \notin \langle 3, x \rangle$;

   b) O ideal $\langle 3, x \rangle$ não é principal. Conclua que $\mathbb{Z}[x]$ não é domínio de ideais principais.

5. Considere em $\mathbb{Q}[x]$ os polinómios

$$f(x) = x^4 + 3\,x^3 - x^2 - 5\,x + 2 \quad \text{e} \quad g(x) = x^3 + 4\,x^2 + 2\,x - 4$$

Determine o mdc de $f(x)$ e $g(x)$ e escreva-o na forma $a(x)f(x) + b(x)\,g(x)$, com $a(x), b(x) \in \mathbb{Q}[x]$.

6. Considere os polinómios de $\mathbb{R}[x]$

$$f(x) = x^4 - x^3 - 2x^2 + 3x - 1 \ \text{ e } \ g(x) = x^3 + x^2 - x - 1$$

a) Determine $\operatorname{mdc}(f(x), g(x))$;

b) Diga, justificando, se o polinómio $x^2 - 1$ pertence ao ideal de $\mathbb{R}[x]$ gerado por $\{f(x), g(x)\}$.

7. Considere o ideal $I = \langle x^3 + x^2, x^6 + 2x^4 + 2x^2 \rangle$ de $\mathbb{R}[x]$.

a) Determine um polinómio $h(x) \in \mathbb{R}[x]$ tal que $I = \langle h(x) \rangle$.

b) Diga, justificando, se I é ideal primo.

8. Seja K um corpo e $f, g \in K[x]$. Mostre que existe $a \in K$ tal que

$$a \operatorname{mdc}(f, g) \operatorname{mmc}(f, g) = fg.$$

9. Em $\mathbb{Z}_5[x]$ considere os polinómios $f(x) = -x^2 + 2x + 3$ e $g(x) = x^3 + x^2 + 2x + 2$.

a) Mostre que $x^2 + x \in \langle f(x), g(x) \rangle$.

b) Diga, justificando, se $\mathbb{Z}_5[x]/\langle f(x), g(x) \rangle$ é um corpo.

10. Considere em $\mathbb{Z}_2[x]$ o polinómio $f(x) = x^3 + x + 1$.

a) Mostre que $\mathbb{Z}_2[x]/\langle f(x) \rangle$ é um corpo.

b) Determine o inverso de $x + \langle f(x) \rangle$.

c) Calcule um polinómio $g(x) \in \mathbb{Z}_2[x]$ com grau 2 e tal que

$$g(x) + \langle f(x) \rangle = x^5 + x^3 + x + \langle f(x) \rangle$$

d) Prove que, para cada polinómio $t(x) \in \mathbb{Z}_2[x]$, existe um e um só polinómio $s(x) \in \mathbb{Z}_2[x]$ com grau menor do que 3 tal que $s(x) + \langle f(x) \rangle = t(x) + \langle f(x) \rangle$.

11. Seja $f(x) = 2x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$.

a) Mostre que $\langle f(x) \rangle$ é um ideal maximal de $\mathbb{Z}_3[x]$.

b) Descreva o corpo $\mathbb{Z}_3[x]/\langle f(x)\rangle$.

c) Determine o inverso de $2x+1+\langle f(x)\rangle$.

d) Verifique que $x+1+\langle f(x)\rangle = 2x^4+x^3+1+\langle f(x)\rangle$.

12. Seja $p(x) = 2x^3 + x + 1 \in \mathbb{Z}_3[x]$.

a) Mostre que $\mathbb{Z}_3[x]/\langle p(x)\rangle$ é um corpo.

b) Designando por X o elemento $x+\langle p(x)\rangle$, calcule (apresentando o resultado na forma simplificada)

(i) $(1+2X^2)+(1+X+X^2)$;

(ii) $(1+2X^2)\cdot(1+X+X^2)$;

(iii) o inverso e o simétrico de X.

c) Calcule o cardinal de $\mathbb{Z}_3[x]/\langle p(x)\rangle$.

13. Considere o polinómio $f(x) = x^3 + 2\,x + 1 \in \mathbb{Z}_3[x]$. Mostre que $f(x)$ é irredutível em $\mathbb{Z}_3[x]$ e determine um corpo de ruptura de $f(x)$.

14. Diga, justificando, se cada uma das afirmações seguintes é verdadeira ou falsa:

a) Se K é um corpo, então $K[x]$ também é corpo.

b) Todo o polinómio com coeficientes num corpo K admite uma raiz em K.

c) Todo o polinómio irredutível em $\mathbb{Q}[x]$ é também irredutível em $\mathbb{R}[x]$.

d) Polinómios primos entre si e com coeficientes num corpo K têm graus diferentes.

15. Considere em $\mathbb{Z}[x]$ o polinómio

$$f(x) = x^5 - 9\,x^4 + 30\,x^3 - 46\,x^2 + 33\,x - 9$$

Determine as raízes racionais de $f(x)$.

16. Diga, justificando, se cada um dos seguintes polinómios é irredutível em $\mathbb{Q}[x]$

    a) $x^3 + 3\,x^2 + 9\,x + 3$;

    b) $x^3 + 3\,x^2 + 3\,x + 9$;

    c) $2\,x^5 - 27\,x^2 + 3$;

    d) $2\,x^2 - 3\,x + 4$;

    e) $x^4 + 3\,x^3 + 6\,x^2 + 6\,x + 2$;

    f) $2\,x^4 + x^3 - 8\,x^2 + x - 10$;

    g) $x^4 + 9$.

17. Definição: Sejam K um corpo e $f(x) \in K[x]$. Chamamos *derivada de* $f(x)$ ao polinómio $f'(x) \in K[x]$ definido do modo seguinte: se $f(x)$ é constante, então $f'(x) = 0$;
    se $f(x) = \sum_{i=0}^{n} a_i\,x^i$ é um polinómio em que $1 \leq \text{grau}\, f(x) = n$, com $n \in \mathbb{N}$, então

$$f'(x) = \sum_{i=1}^{n} i\,a_i\,x^{i-1}$$

    a) Sejam K um corpo e $f(x), g(x) \in K[x]$. Mostre que

        (i) $(f(x) + g(x))' = f'(x) + g'(x)$;

        (ii) $(f(x)\,g(x))' = f'(x)g(x) + f(x)\,g'(x)$;

        (iii) $\forall\ \alpha \in K, \forall\ n \in \mathbb{N},\ \ ((x-\alpha)^n)' = n\,(x-\alpha)^{n-1}$
        (convenção: $(x-\alpha)^0 = 1$).

    b) Seja K um corpo. Mostre que, se $f(x) \in K[x]$ e $\alpha \in K$ é raiz de $f(x)$, então α é raiz múltipla de $f(x)$ se e só se α é raiz de $f'(x)$.

    c) Considere em $\mathbb{Q}[x]$ o polinómio

$$f(x) \;=\; \frac{1}{5}\,x^5 - x^4 + \frac{4}{3}\,x^3 + 17\,x + \frac{293}{15}$$

    Usando a alínea b), mostre que $f(x)$ não admite raízes múltiplas em $\mathbb{Q}$.

18. Considere o polinómio $f(x) = x^4 - 4x^3 + 4x^2 - 4 \in \mathbb{Q}[x]$.

    a) Verifique que $1 + i$ é raiz de $f(x)$.

    b) Diga, justificando, se $f(x)$ é irredutível em $\mathbb{Q}[x]$.

19. Em $\mathbb{Q}[x]$ considere os polinómios $g(x) = x^5 - 2x^4 + 5x^3 - 3x^2 + 6$ e $h(x) = x^3 + 3x + 3$.

    a) Sabendo que $1 - i$ é raiz de $g(x)$, decomponha $g(x)$ em factores irredutíveis de $\mathbb{Q}[x]$.

    b) Descreva os ideais $\langle g(x)\rangle \cap \langle h(x)\rangle$ e $\langle g(x)\rangle + \langle h(x)\rangle$.

20. Seja J o ideal de $\mathbb{Q}[x]$ gerado por $x^4 + 3x^3 + 2x^2 + 8x + 6$.

    a) Mostre que $\mathbb{Q}[x]/J$ não é um corpo.

    b) Dê um exemplo dum divisor de zero de $\mathbb{Q}[x]/J$.

21. Considere o polinómio $f(x) = x^5 - 2x^4 + 5x^3 - 10x^2 + 4x - 8$.

    a) (i) Decomponha $f(x)$ em factores irredutíveis de $\mathbb{Q}[x]$.

    (ii) Decomponha $f(x)$ em factores irredutíveis de $\mathbb{C}[x]$.

    b) (i) Calcule $\text{mdc}(f(x), x^3 - x^2 + 4x - 4)$ em $\mathbb{Q}[x]$.

    (ii) Seja $h(x)$ o máximo divisor comum calculado na alínea anterior e considere o anel $K = \mathbb{Q}[x]/\langle h(x)\rangle$. Mostre que K é um corpo e descreva os seus elementos.

    (iii) Calcule o inverso de $(x - 1) + \langle h(x)\rangle$.

22. a) Tendo em conta que $\mathbb{Z}$ é domínio de factorização única, mostre que $\mathbb{Z}[x]$ também o é (tenha presente o estudo efectuado sobre polinómios de coeficientes em $\mathbb{Z}$ e em $\mathbb{Q}$).

    b) Mostre que, mais geralmente, se D é um domínio de factorização única então $D[x]$ também o é (generalize o caso anterior, considerando o corpo das fracções de D).

Capítulo 3

Corpos

Neste capítulo estudamos vários tipos de extensões de corpos, nomeadamente extensões finitas, algébricas, transcendentes e simples.

O estudo de extensões aparecerá directamente ligado ao estudo de polinómios.

Alguns dos resultados aqui obtidos serão aplicados no capítulo seguinte na resolução de alguns problemas geométricos.

3.1 Conceitos e resultados gerais

Começamos por fazer algumas observações sobre corpos, cujas demonstrações deixamos ao cuidado do leitor.

Seja K um corpo. Um subanel de K que seja corpo diz-se um *subcorpo* de K.

Notemos que, por um lado, $\{0\}$ não é subcorpo de K, pois não contém a identidade 1 e, por outro, se I é ideal de K, então $I = \{0\}$ ou $I = K$. Atendendo a este facto e à Proposição I.3, concluímos que se $\varphi\colon K \to A$ é morfismo de anéis, entre K e um anel A, como $\operatorname{Ker}\varphi$ é ideal de K, então $\operatorname{Ker}\varphi = \{0\}$ ou $\operatorname{Ker}\varphi = K$. Neste último caso, temos $\varphi(x) = 0$ para qualquer $x \in K$, donde φ é o morfismo nulo. No primeiro caso, φ é um mergulho e, portanto, A é uma extensão de

K. Observemos também que se A é um corpo e φ não é o morfismo nulo, então φ é um morfismo entre os grupos $(K,+)$ e $(A,+)$ e entre os grupos $(K\backslash\{0\},\cdot)$ e $(A\backslash\{0\},\cdot)$, pelo que, além de termos $\varphi(0)=0$, também temos $\varphi(1)=1$. Assim, podemos afirmar que todo o morfismo não nulo entre corpos é um mergulho de anéis com identidade.

Enunciamos agora dois critérios de subcorpo, cujas demonstrações ficam como exercício.

Critério de subcorpo 1.

Sejam K um corpo e $A\subseteq K$. Então A é subcorpo de K se e só se

a) $0,1\in A$,

b) $\forall\, x\in A,\ -x\in A$,

c) $\forall\, x,y\in A,\ x+y\in A$,

d) $\forall\, x\in A\backslash\{0\},\ x^{-1}\in A$,

e) $\forall\, x,y\in A,\ x\,y\in A$.

Critério de subcorpo 2.

Sejam K um corpo e $A\subseteq K$. Então A é subcorpo de K se e só se

a) $0,1\in A$,

b) $\forall\, x,y\in A,\ x-y\in A$,

c) $\forall\, x\in A,\ \forall\, y\in A\backslash\{0\},\ x\,y^{-1}\in A$.

De entre os subcorpos de um corpo, o subcorpo primo tem importância especial, como veremos.

Definição. Um corpo K diz-se *primo* se não tem subcorpos próprios.

Exemplos.

Os corpos $\mathbb{Q}$ e $\mathbb{Z}_p$, com p primo, são primos.

Dado um corpo K, é fácil verificar que a intersecção de subcorpos ainda é subcorpo, donde a intersecção de todos os subcorpos de K é um subcorpo, que designamos por P_K. É claro que P_K é um corpo primo. A P_K chamamos o *subcorpo primo de* K.

Podemos, então, afirmar que todo o corpo K contém um único subcorpo primo e, portanto, que todo o corpo é extensão de um corpo primo.

Vejamos como se relaciona a característica de um corpo com o seu subcorpo primo.

Recordemos que um corpo tem característica 0 ou p, sendo p primo.

Teorema 1. *Seja K um corpo. Se $c(K) = 0$, então $P_K \simeq \mathbb{Q}$. Se $c(K) = p$, primo, então $P_K \simeq \mathbb{Z}_p$.*

Demonstração: Seja $\theta : \mathbb{Z} \to P_K$ o morfismo definido por $\theta(m) = m1$, para qualquer $m \in \mathbb{Z}$. Então $\operatorname{Ker}\theta = \langle c(K)\rangle$, pelo Teorema I.11.

Se $c(K) = 0$, obtemos $\operatorname{Ker}\theta = \{0\}$, donde θ é um monomorfismo. Neste caso, temos $\mathbb{Z} \simeq \theta(\mathbb{Z}) \subseteq P_K$, pelo que P_K é extensão do corpo F das fracções de $\theta(\mathbb{Z})$, pelo Teorema I.14. Por P_K ser primo, $P_K = F$. Por outro lado, $F \simeq \mathbb{Q}$, corpo das fracções de $\mathbb{Z}$.

Se $c(K) = p$, obtemos $\mathbb{Z}_p \simeq \theta(\mathbb{Z})$, pelo que $\theta(\mathbb{Z})$ é corpo. Uma vez que $\theta(\mathbb{Z}) \subseteq P_K$, temos $\theta(\mathbb{Z}) = P_K$. Logo $\mathbb{Z}_p \simeq P_K$. ∎

3.2 Extensões algébricas e extensões finitas

Nesta secção, começamos por apresentar os conceitos de elemento algébrico e de polinómio mínimo associado. Estudaremos extensões algébricas e extensões finitas, passando pela demonstração de resultados sobre o grau de uma extensão.

Se K e E são corpos tais que E é extensão de K e $\varphi\colon K \hookrightarrow E$ é um mergulho, então $K \simeq \varphi(K)$, sendo $\varphi(K)$ um subcorpo de E. Assim, com o objectivo de facilitar a escrita, quando dissermos que E é extensão de K admitiremos que K é subcorpo de E.

Definição. Sejam K e E corpos, sendo E extensão de K. Seja α um elemento de E. Diz-se que α é *algébrico sobre* K se existe $f(x) \in K[x]\backslash\{0\}$ tal que $f(\alpha) = 0$, isto é, se α é raiz de um polinómio não nulo de coeficientes em K.

Neste caso, $f(x)$ diz-se um *polinómio anulador de* α sobre K. (Observemos que grau $f(x) \geq 1$, por definição de $f(x)$.) Se α não é algébrico, α diz-se *transcendente* sobre K.

Exemplos.

O elemento $i \in \mathbb{C}$ é algébrico sobre $\mathbb{R}$, pois é raiz de $x^2+1 \in \mathbb{R}[x]$. Prova-se que e e π são transcendentes sobre $\mathbb{Q}$. (Este facto foi provado pela primeira vez por Lindemann em 1882; podemos encontrar demonstrações, por exemplo, em Jacobson, Lang ou Hernstein.)

Teorema 2. *Sejam E e K corpos, sendo E uma extensão de K. Seja $\alpha \in E$ um elemento algébrico sobre K. Dado $f(x) \in K[x]$ um polinómio anulador de α de grau mínimo com coeficiente director a, temos*

a) *Se $g(x) \in K[x]$ é polinómio anulador de α, então $f(x)/g(x)$;*

b) *$\widetilde{f}(x) = a^{-1} f(x)$ é o único polinómio mónico anulador de α de grau mínimo;*

c) *$\widetilde{f}(x)$ é irredutível em $K[x]$.*

Demonstração: **a**) Pelo Teorema II.7, existem $q(x), r(x) \in K[x]$ tais que $g(x) = f(x)\,q(x) + r(x)$ e grau $r(x) <$ grau $f(x)$. Como $f(\alpha) = g(\alpha) = 0$, então $r(\alpha) = 0$. Logo, por definição de $f(x)$, temos $r(x) = 0$, donde $f(x)/g(x)$.

b) Tomemos $\widetilde{f}(x) = a^{-1} f(x)$. É claro que $\widetilde{f}(x)$ é mónico, grau $f(x) =$ grau $\widetilde{f}(x)$ e $\widetilde{f}(\alpha) = 0$. Seja $g(x)$ um polinómio mónico anulador de α de grau mínimo. Por a), sabemos que $\widetilde{f}(x)/g(x)$. Logo $\widetilde{f}(x) = c\,g(x)$, para algum $c \in K\backslash\{0\}$, uma vez que têm o mesmo grau. Como $\widetilde{f}(x)$ e $g(x)$ são mónicos, temos $c = 1$, donde $g(x) = \widetilde{f}(x)$.

c) Suponhamos que $\widetilde{f}(x)$ não é irredutível em $K[x]$. Dado que

$\widetilde{f}(x)$ não é constante, existem $g(x), h(x) \in K[x]$ tais que $\widetilde{f}(x) = g(x)\,h(x)$, com grau $h(x)$, grau $g(x) \geq 1$. Então $0 = \widetilde{f}(\alpha) = g(\alpha)\,h(\alpha)$ no corpo E. Logo $g(\alpha) = 0$ ou $h(\alpha) = 0$. Como $h(x), g(x) \in K[x]$ são não nulos com grau $h(x)$ e grau $g(x)$ menores do que grau $\widetilde{f}(x)$, temos um absurdo. Portanto, $\widetilde{f}(x)$ é irredutível. ∎

Observemos que, do teorema anterior, também podemos concluir que qualquer polinómio de $K[x]$ de grau mínimo anulador de um elemento $\alpha \in E$, não necessariamente mónico, é irredutível em $K[x]$, pois vai ser associado de $\widetilde{f}(x)$.

Definição. Sejam E e K corpos tais que E é extensão de K. Dado $\alpha \in E$ um elemento algébrico sobre K, ao único polinómio de $K[x]$ anulador de α, mónico e de grau mínimo, damos o nome de *polinómio mínimo de α sobre K*.

Exemplo.

Consideremos $\mathbb{Q} \subseteq \mathbb{R}$ e $\sqrt{2} \in \mathbb{R}$. Seja $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Temos $f(\sqrt{2}) = 0$ e, portanto, $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$. O polinómio $f(x)$ é mónico e anulador de $\sqrt{2}$. Além disso, como $\sqrt{2} \notin \mathbb{Q}$ e grau $f(x) = 2$, o polinómio $f(x)$ tem grau mínimo entre os polinómios de $\mathbb{Q}[x]$ que admitem $\sqrt{2}$ como raiz. Logo $f(x)$ é o polinómio mínimo de $\sqrt{2}$.

Corolário 2.1. *Sejam E e K corpos, tais que E é uma extensão de K. Seja $f(x) \in K[x]$ um polinómio irredutível, mónico e anulador de um elemento $\alpha \in E$. Então $f(x)$ é o polinómio mínimo de α sobre K.*

Demonstração: Como $f(x)$ é um polinómio de $K[x]$ anulador de α, então existe $\widetilde{f}(x) \in K[x]$ tal que $\widetilde{f}(x)$ é o polinómio mínimo de α. Pelo Teorema 2, sabemos que $\widetilde{f}(x)$ divide $f(x)$. Como $\widetilde{f}(x)$ não é constante e $f(x)$ é irredutível, sendo ambos mónicos, concluímos que $\widetilde{f}(x) = f(x)$. ∎

Dados K e E corpos tais que E é extensão de K e $\alpha \in E$, pretendemos agora determinar, a menos de isomorfismo, o menor subcorpo

de E que contém $K \cup \{\alpha\}$, o qual designamos por $K(\alpha)$.

É claro que $K(\alpha)$ existe (na "pior" das hipóteses temos $K(\alpha) = E$). Se $\alpha = 0$, temos que $K(\alpha) = K$ obviamente. No que se segue $\alpha \neq 0$. Observemos, desde já, que α é raiz de um polinómio de coeficientes em $K(\alpha)$, nomeadamente do polinómio $x - \alpha \in K(\alpha)[x]$.

Comecemos por considerar o subconjunto de E

$$K[\alpha] = \left\{ a_0 + a_1\,\alpha + \cdots + a_m\,\alpha^m \colon\ m \in \mathbb{N}_0,\ a_0, \ldots, a_m \in K \right\}$$

É fácil verificar que $K[\alpha]$ é um subanel comutativo com identidade de E, que contém $K \cup \{\alpha\}$ e que é domínio de integridade. Além disso, temos $K[\alpha] \subseteq K(\alpha)$. Então $K(\alpha)$ é o corpo das fracções de $K[\alpha]$, pelo Teorema I.14 e pela definição de $K(\alpha)$. Logo

$$K(\alpha) = \left\{ f(\alpha)\, g(\alpha)^{-1} \colon\ f(x), g(x) \in K[x],\ g(\alpha) \neq 0 \right\}$$

Tomemos

$$\begin{array}{rcl} \psi_\alpha \colon K[x] & \to & E \\ f(x) = a_0 + a_1\,x + \cdots + a_m\,x^m & \mapsto & f(\alpha) = a_0 + a_1\alpha + \cdots + a_m\,\alpha^m \end{array}$$

trata-se de um morfismo (é um caso mais geral do que o considerado no Teorema II.2), com $\operatorname{Ker}\psi_\alpha = \{f(x) \in K[x] :\ f(\alpha) = 0\}$ e $\operatorname{Im}\psi_\alpha = K[\alpha]$.

Precisamos analisar separadamente o caso em que α é algébrico e o caso em que α é transcendente.

Suponhamos que α é transcendente sobre K. Então não existe nenhum polinómio $f(x) \in K[x]$ não nulo tal que $f(\alpha) = 0$, ou seja, $\operatorname{Ker}\psi_\alpha = \{0\}$. Neste caso, ψ_α é injectivo e

$$\begin{array}{c} K[x] \to K[\alpha] \\ f(x) = a_0 + a_1\,x + \cdots + a_m\,x^m \ \mapsto\ a_0 + a_1\,\alpha + \cdots + a_m\,\alpha^m = f(\alpha) \end{array}$$

é um isomorfismo, logo o corpo $K(\alpha)$ é isomorfo ao corpo das fracções do domínio de integridade $K[x]$, que designamos por $K(x)$.

Consideremos o caso em que α é algébrico sobre K. Pelo 1º Teorema do Isomorfismo, concluímos que

$$K[\alpha] \simeq K[x]/\operatorname{Ker}\psi_\alpha$$

Seja $\widetilde{f}(x) \in K[x]$ o polinómio mínimo de α sobre K. Então $\widetilde{f}(\alpha) = 0$ e, portanto, $\widetilde{f}(x) \in \operatorname{Ker} \psi_\alpha$. Atendendo ao Teorema 2 e à Nota após o Teorema II.9, podemos garantir que

$$\operatorname{Ker} \psi_\alpha = \langle \widetilde{f}(x) \rangle$$

logo

$$K[\alpha] \simeq K[x]/\langle \widetilde{f}(x) \rangle$$

Como $\widetilde{f}(x)$ é um polinómio irredutível em $K[x]$, pelo Teorema II.14 podemos afirmar que $K[x]/\langle \widetilde{f}(x) \rangle$ é um corpo. Portanto, neste caso, $K[\alpha]$ é corpo, donde $K[\alpha] = K(\alpha)$. Mais ainda, o isomorfismo

$$\theta : K[x]/\langle \widetilde{f}(x) \rangle \to K[\alpha]$$

$$g(x) + \langle \widetilde{f}(x) \rangle \mapsto g(\alpha)$$

é tal que $\theta(x + \langle \widetilde{f}(x) \rangle) = \alpha$ e $\theta(a + \langle \widetilde{f}(x) \rangle) = a$ quando $a \in K$. Tendo em conta a descrição de $K[x]/\langle \widetilde{f}(x) \rangle$ estudada no capítulo anterior, concluímos que

$$K(\alpha) = K[\alpha] = \left\{ a_0 + a_1\,\alpha + \cdots + a_{n-1}\,\alpha^{n-1} \colon\ a_0, a_1, \ldots, a_{n-1} \in K \right\}$$

sendo $n = \operatorname{grau} \widetilde{f}(x)$ e $\widetilde{f}(\alpha) = 0$.

Reciprocamente, admitamos agora que $K[\alpha] \simeq K[x]$. Como $K[x]$ não é corpo, então $K[\alpha]$ também não o é, logo α é transcendente sobre K. Caso contrário, $K[\alpha] = K(\alpha)$ e $K[\alpha]$ seria corpo.

Se tivermos $K[\alpha] = K(\alpha)$, então $\alpha^{-1} \in K[\alpha]$ donde $\alpha^{-1} = a_0 + a_1\alpha + \ldots + a_n\alpha^n$, para alguns $n \in \mathbb{N}$ e $a_0, \ldots, a_n \in K$. Logo $1 = a_0\alpha + a_1\alpha^2 + \ldots + a_n\alpha^{n+1}$ e, portanto, α é raiz do polinómio $f(x) = -1 + a_0x + a_1x^2 + \ldots + a_nx^{n+1} \in K[x]$, pelo que α é algébrico sobre K.

Ficou, pois, demonstrado o seguinte resultado

Teorema 3. *Sejam E e K corpos tais que E é extensão de K. Seja $\alpha \in E$.*

a) *O elemento α é algébrico sobre K se e só se $K(\alpha) = K[\alpha]$ e $K(\alpha)$ é isomorfo ao corpo quociente $K[x]/\langle \widetilde{f}(x) \rangle$, em que $\widetilde{f}(x) \in K[x]$ é o polinómio mínimo de α sobre K.*

b) *O elemento α é transcendente sobre K se e só se $K[\alpha] \simeq K[x]$, tendo-se $K(\alpha)$ isomorfo ao corpo das fracções de $K[x]$.*

Analisemos alguns exemplos.

Exemplos.

1) Consideremos $\mathbb{R} \subseteq \mathbb{C}$ e $i \in \mathbb{C}$. Como i é algébrico sobre $\mathbb{R}$ e o seu polinómio mínimo é $x^2 + 1$, temos

$$\mathbb{R}(i) = \left\{ a_0 + a_1\, i \colon\ a_0, a_1 \in \mathbb{R} \right\} = \mathbb{C}$$

2) O real π é, como já afirmámos, transcendente sobre $\mathbb{Q}$, donde $\mathbb{Q}[\pi] \subsetneqq \mathbb{Q}(\pi)$. Mais ainda, temos $\mathbb{Q} \subsetneqq \mathbb{Q}[\pi] \subsetneqq \mathbb{Q}(\pi) \subsetneqq \mathbb{R}$. Por exemplo, $\frac{1}{\pi} \in \mathbb{Q}(\pi)$ mas $\frac{1}{\pi} \notin \mathbb{Q}[\pi]$. Se $\frac{1}{\pi} \in \mathbb{Q}[\pi]$, então $\frac{1}{\pi} = a_0 + a_1\, \pi + \cdots + a_n\, \pi^n$, para alguns $a_0, a_1, \ldots, a_n \in \mathbb{Q}$, e $n \in \mathbb{N}$, donde

$$0 = -1 + a_0\, \pi + a_1\, \pi^2 + \cdots + a_n\, \pi^{n+1}$$

e, portanto, π seria raiz do polinómio não nulo

$$-1 + a_0\, x + a_1\, x^2 + \cdots + a_n\, x^{n+1} \ \in \ \mathbb{Q}[x]$$

o que é absurdo. Por outro lado, $\mathbb{Q}(\pi)$ é numerável pelo que $\mathbb{Q}(\pi) \neq \mathbb{R}$.

Dados K e E corpos tais que E é extensão de K e $\alpha \in E$, no teorema anterior contruímos a extensão $K(\alpha)$ de K que é subcorpo de E, tendo-se $K \subseteq K(\alpha) \subseteq E$.

Definição. Se E e K são corpos tais que E é extensão de K e $\alpha \in E$, dizemos que $K(\alpha)$ é uma *extensão simples* de K.

Mais geralmente, dados K e E corpos tais que E é extensão de K e $A \subseteq E$, podemos considerar o subcorpo de E gerado por $K \cup A$.

Se $A = \{\alpha_1, \ldots, \alpha_n\}$, denotamos este subcorpo por $K(\alpha_1, \ldots, \alpha_n)$. É fácil ver que, se $n > 1$, temos

$$K(\alpha_1, \ldots, \alpha_n) = \Big(K(\alpha_1, \ldots, \alpha_{n-1})\Big)(\alpha_n)$$

donde

$$K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1)(\alpha_2)\cdots(\alpha_n)$$

Vejamos agora o que se entende por extensão algébrica.

Definição. Dados E e K corpos tais que E é extensão de K, dizemos que E é *extensão algébrica* de K se todos os elementos de E são algébricos sobre K. Caso contrário, dizemos que E é *extensão transcendente* de K.

É claro que todo o corpo é extensão algébrica de si próprio.

Se tomarmos E e K corpos tais que E é extensão de K, podemos encarar E como um espaço vectorial sobre K, sendo o produto por escalares dado pela multiplicação em E. É esta abordagem que nos conduz ao conceito de extensão finita.

Definição. Sejam E e K corpos tais que E é extensão de K. À dimensão de E como espaço vectorial sobre K (finita ou não) damos o nome de *grau da extensão E sobre K*. Dizemos que E é uma *extensão finita* de K se o grau de E sobre K for finito. O grau de E sobre K representa-se por $[E:K]$.

Como se relacionam as extensões algébricas com as finitas?

Teorema 4. *Sejam E e K corpos tais que E é uma extensão de K. Se $\alpha \in E$ é algébrico sobre K, então $K(\alpha)$ é uma extensão finita de K, com grau $[K(\alpha):K]$ igual ao grau do polinómio mínimo de α sobre K.*

Demonstração: Seja $\widetilde{f}(x)$ o polinómio mínimo de α sobre K. Tomemos $\widetilde{f}(x) = b_0 + b_1\, x + \cdots + b_{n-1}\, x^{n-1} + x^n$. Sabemos, pela prova

do Teorema 3, que

$$K(\alpha) = \left\{ a_0 + a_1\,\alpha + \cdots + a_{n-1}\,\alpha^{n-1} \colon\ a_0, a_1, \ldots, a_{n-1} \in K \right\}$$

com $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} + \alpha^n = 0$. Então $\{1, \alpha, \ldots, \alpha^{n-1}\}$ constitui um conjunto de geradores do espaço vectorial $K(\alpha)$ sobre K. Se estes vectores não fossem linearmente independentes, existiria uma sua combinação linear $a_0 + a_1\,\alpha + \cdots + a_{n-1}\,\alpha^{n-1}$ nula, com algum coeficiente $a_i \neq 0$. Então α seria raiz do polinómio $g(x) = a_0 + a_1\,x + \cdots + a_{n-1}\,x^{n-1} \in K[x]\backslash\{0\}$, com grau $g(x) < n = \text{grau}\,\widetilde{f}(x)$, o que é absurdo por definição do polinómio mínimo $\widetilde{f}(x)$. Portanto, $(1, \alpha, \ldots, \alpha^{n-1})$ constitui uma base de $K(\alpha)$ sobre K. Logo $[K(\alpha) : K] = n$ e $K(\alpha)$ é extensão finita de K. ∎

O resultado anterior garantiu-nos que toda a extensão simples $K(\alpha)$ de um corpo K, associada a um elemento algébrico α, é extensão finita. O teorema que se segue permite-nos afirmar que toda a extensão finita é algébrica.

Teorema 5. *Sejam E e K corpos tais que E é extensão finita de K. Então E é extensão algébrica de K.*

Demonstração: Suponhamos que $[E : K] = n$. Seja $\alpha \in E$. Consideremos o sistema de vectores

$$\left(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n\right)$$

do espaço vectorial E. Tratando-se de um sistema com $n+1$ vectores, num espaço vectorial de dimensão n, é necessariamente linearmente dependente sobre K. Logo, existem $a_0, a_1, \ldots, a_{n-1}, a_n$ escalares de K, não todos nulos, tais que

$$a_0\,1 + a_1\,\alpha + \cdots + a_{n-1}\,\alpha^{n-1} + a_n\,\alpha^n = 0$$

Portanto, α é raiz do polinómio

$$f(x) = a_0 + a_1\,x + \cdots + a_{n-1}\,x^{n-1} + a_n\,x^n \ \in\ K[x]\backslash\{0\}$$

pelo que α é algébrico sobre K. ∎

A condição recíproca deste último teorema não é verdadeira. Por exemplo, o corpo $\overline{\mathbb{Q}}$ formado por todos os números complexos que são algébricos sobre $\mathbb{Q}$ é uma extensão algébrica de $\mathbb{Q}$, por definição, mas prova-se que não é uma extensão finita de $\mathbb{Q}$ (ver Exercício 12).

Corolário 5.1. *Sejam E e K corpos tais que E é extensão de K e $\alpha \in E$. Então α é algébrico sobre K se e só se $K(\alpha)$ é extensão algébrica de K.*

Demonstração: A implicação directa é consequência dos Teoremas 4 e 5, quanto à recíproca, é imediata. ∎

Corolário 5.2. *Sejam E e K corpos tais que E é extensão de K. Então $\alpha \in E$ é transcendente sobre K se e só se $K(\alpha)$ não é extensão finita de K.*

Demonstração: É consequência imediata do Teorema 5, pois se α é transcendente sobre K, então $K(\alpha)$ não é extensão algébrica de K logo não é finita.

Se $[K(\alpha) : K]$ não é finito, pelo Teorema 4 temos que α não é algébrico, logo α é transcendente. ∎

Em seguida, vemos como relacionar os graus de sucessivas extensões finitas.

Teorema da Torre 6. *Sejam E, K e F corpos tais que E é extensão de K e K é extensão de F. Então $[E:K]$ e $[K:F]$ são finitos se e só se $[E:F]$ é finito. Neste caso, $[E:F] = [E:K]\,[K:F]$.*

Demonstração: Temos $F \subseteq K \subseteq E$. Suponhamos $[E : K]$ e $[K:F]$ finitos. Sejam $(a_1, \ldots, a_n)$ uma base de E sobre K e $(b_1, \ldots, b_m)$ uma base de K sobre F.

Provemos que $X = (a_i\, b_j : i = 1, \ldots, n;\ j = 1, \ldots, m)$ é uma base de E sobre F. Dado $u \in E$ existem $\alpha_1, \ldots, \alpha_n \in K$ tais que $u = \alpha_1 a_1 + \cdots + \alpha_n a_n$ e existem $\beta_{11}, \ldots, \beta_{1m}, \ldots, \beta_{n1}, \ldots, \beta_{nm} \in F$

tais que $\alpha_i = \beta_{i1} b_1 + \cdots + \beta_{im} b_m$, com $i = 1, \ldots, n$. Logo, em E, temos

$$\begin{aligned} u &= \sum_{i=1}^{n} \alpha_i \, a_i = \sum_{i=1}^{n} \Big(\sum_{j=1}^{m} \beta_{ij} \, b_j \Big) \, a_i \\ &= \sum_{i=1}^{n} \Big(\sum_{j=1}^{m} (\beta_{ij} \, b_j \, a_i) \Big) = \sum_{i=1,\, j=1}^{n,m} \beta_{ij} (a_i \, b_j) \end{aligned}$$

Portanto, X é um conjunto de geradores de E sobre F, donde $[E\!:\!F]$ é finita. Suponhamos agora que temos

$$0 = \sum_{i=1,\, j=1}^{n,m} \beta_{ij} (a_i \, b_j)$$

com $\beta_{ij} \in F$. Podemos escrever

$$0 = \sum_{i=1,\, j=1}^{n,m} \Big((\beta_{ij} \, b_j) \, a_i \Big) = \sum_{i=1}^{n} \Big(\sum_{j=1}^{m} \beta_{ij} \, b_j \Big) \, a_i$$

Como $(a_1, \ldots, a_n)$ é base de E sobre K, obtemos $\sum_{j=1}^{m} \beta_{ij} \, b_j = 0$, para qualquer $i = 1, \ldots, n$. Então $\beta_{ij} = 0$, para qualquer $i = 1, \ldots, n$ e $j = 1, \ldots, m$, pois $(b_1, \ldots, b_m)$ é base de K sobre F. Logo os vectores de X são linearmente independentes. Portanto, X é uma base de E sobre F e temos

$$[E\!:\!F] = [E\!:\!K] \, [K\!:\!F]$$

Suponhamos agora que $[E\!:\!F]$ é finito. Seja $\{b_i : i \in I\}$ um conjunto de elementos de K linearmente independente sobre F. Então $\{b_i : i \in I\}$ é também um conjunto de elementos de E linearmente independentes sobre F. Logo $\#I \leq [E : F]$, pelo que I tem de ser finito e, portanto, $[K\!:\!F]$ é finito.

Seja $(c_1, \ldots, c_p)$ uma base de E sobre F. Dado $u \in E$, existem $\lambda_1, \ldots, \lambda_p \in F \subseteq K$ tais que $u = \lambda_1 \, c_1 + \cdots + \lambda_p \, c_p$, logo $\{c_1, \ldots, c_p\}$ é um conjunto de geradores de E sobre K, donde $[E : K]$ é também finito. ∎

Exemplos.

1) Sejam $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ e $K = \mathbb{Q}(\sqrt{2})$. Temos $\mathbb{Q} \subseteq K \subseteq E$.

O polinómio x^2-2 é o polinómio mínimo de $\sqrt{2}$ sobre $\mathbb{Q}$. Logo $[K:\mathbb{Q}]=2$ e temos $K=\{a+b\sqrt{2}\colon\ a,b\in\mathbb{Q}\}$, com base $(1,\sqrt{2})$ sobre $\mathbb{Q}$.

Tomemos agora $x^2-3\in K[x]$. Este polinómio mónico é anulador de $\sqrt{3}$. Vejamos que x^2-3 é irredutível em $K[x]$. Se não fosse irredutível, teríamos $\sqrt{3}\in K$, donde $\sqrt{3}=a+b\sqrt{2}$, para alguns $a,b\in\mathbb{Q}$. Se $b=0$, obtemos $\sqrt{3}\in\mathbb{Q}$ e se $a=0$, então $3=2b^2$, um absurdo em ambos os casos. Logo $a,b\neq 0$. Por outro lado, temos $3=a^2+2ab\sqrt{2}+2b^2$, isto é, $0=(-3+a^2+2b^2)+2ab\sqrt{2}$. Sendo $(1,\sqrt{2})$ uma base de K sobre $\mathbb{Q}$, concluímos que $ab=0$, o que é novamente absurdo. Então $x^2-3\in K[x]$ é irredutível e vai ser o polinómio mínimo de $\sqrt{3}$ sobre K, donde $[E:K]=[K(\sqrt{3}):K]=2$ e temos $K(\sqrt{3})=\{c+d\sqrt{3}:c,d\in K\}$, com base $(1,\sqrt{3})$ sobre K. Atendendo ao Teorema 6, podemos afirmar que $[E:\mathbb{Q}]=2\times 2=4$ e que $E=\mathbb{Q}(\sqrt{2},\sqrt{3})=\{a_1+a_2\sqrt{2}+a_3\sqrt{3}+a_4\sqrt{6}\colon\ a_1,a_2,a_3,a_4\in\mathbb{Q}\}$, sendo $(1,\sqrt{2},\sqrt{3},\sqrt{6})$ uma base de E sobre $\mathbb{Q}$.

2) Seja $f(x)=x^n-p\in\mathbb{Q}[x]$, com $n\in\mathbb{N}\backslash\{1\}$ e $p\in\mathbb{N}$ primo. Sabemos que $f(x)$ é irredutível em $\mathbb{Q}[x]$, pelo teste de Eisenstein, e que tem $\sqrt[n]{p}\in\mathbb{R}$ como raiz em $\mathbb{R}$. Então $[\mathbb{Q}(\sqrt[n]{p}):\mathbb{Q}]=n$.

Este facto permite-nos concluir que $\mathbb{Q}$ tem extensões finitas de todos os graus.

O próximo resultado generaliza o Teorema 4.

Corolário 6.1. *Sejam E e K corpos tais que E é extensão de K e $a_1,\ldots,a_n\in E$, com $n\in\mathbb{N}$, elementos algébricos sobre K. Então $K(a_1,\ldots,a_n)$ é extensão finita de K.*

Demonstração: É claro que sendo $a_{i+1}\in E$ algébrico sobre K, com $i+1\leq n$, então a_{i+1} é algébrico sobre $K(a_1,\ldots,a_i)$. Pelo Teorema 4, temos que $K(a_1,\ldots,a_{i+1})$ é extensão finita de $K(a_1,\ldots,a_i)$. Aplicando o Teorema 6 à sequência

$$K\subseteq K(a_1)\subseteq K(a_1,a_2)\subseteq\cdots\subseteq K(a_1,\ldots,a_n)$$

concluímos que $K(a_1,\ldots,a_n)$ é também uma extensão finita de K. ∎

Corolário 6.2. *Sejam E, K e F corpos tais que E é extensão algébrica de K e K é extensão algébrica de F. Então E é extensão algébrica de F.*

Demonstração: Seja $\alpha \in E$. Como E é extensão algébrica de K, existe $p(x) \in K[x]\backslash\{0\}$ tal que $p(\alpha) = 0$. Seja $p(x) = a_0 + a_1\, x + \cdots + a_n\, x^n$, onde $a_0, a_1, \ldots, a_n \in K$. Consideremos o corpo $F(a_0, \ldots, a_n)$. Como K é extensão algébrica de F, cada a_i, com $i = 0, \ldots, n$, é algébrico sobre F, logo $F(a_0, \ldots, a_n)$ é extensão finita de F, pelo Corolário 6.1. Assim, tomando

$$F \subseteq F(a_0, \ldots, a_n) \subseteq F(a_0, \ldots, a_n, \alpha)$$

temos que $F(a_0, \ldots, a_n, \alpha)$ é extensão finita de F, atendendo aos Teoremas 4 e 6. Pelo Teorema 5, sabemos que $F(a_0, \ldots, a_n, \alpha)$ é extensão algébrica de F, donde α é algébrico sobre F. Portanto, E é extensão algébrica de F. ∎

3.3 Corpo de decomposição de um polinómio

Já vimos, no Teorema II.16, que, dado um polinómio não constante com coeficientes num corpo, é possível encontrar um corpo onde ele se decompõe em factores de grau 1, veremos que um tal corpo "minimal" é único a menos de isomorfismo.

Definição. Dados K e E corpos, tais que E é extensão de K, e um polinómio $f(x) \in K[x]\backslash K$, dizemos que E é *corpo de decomposição* de $f(x)$ sobre K se

1) Em $E[x]$, o polinómio $f(x)$ decompõe-se em factores de grau 1,

$$f(x) = a\,(x - \alpha_1) \cdots (x - \alpha_n), \quad \text{com } \ a \in K, \ \ \alpha_1, \ldots, \alpha_n \in E\,;$$

2) $E = K(\alpha_1, \ldots, \alpha_n)$.

Todo o corpo de decomposição de um polinómio é, pois, um seu corpo de ruptura.

Exemplo.

Consideremos $f(x) = x^4 - 5\,x^2 + 6 \in \mathbb{Q}[x]$. Então $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é corpo de decomposição de $f(x)$ sobre $\mathbb{Q}$, pois

$$f(x) = (x^2 - 2)\,(x^2 - 3) = (x - \sqrt{2})\,(x + \sqrt{2})\,(x - \sqrt{3})\,(x + \sqrt{3})$$

e tem-se

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3})$$

e o corpo $\mathbb{Q}(\sqrt{2})$ é apenas um corpo de ruptura de $f(x)$. O polinómio $f(x)$ também se decompõe em factores lineares em $\mathbb{R}[x]$, mas $\mathbb{R}$ não é corpo de decomposição de $f(x)$ sobre $\mathbb{Q}$, uma vez que $\mathbb{R} \neq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Sejam K um corpo e $f(x) \in K[x]\backslash K$. Supondo que o grau n de $f(x)$ é maior ou igual a 1, pelo Teorema II.16, existem um corpo Ω e $\alpha_1, \ldots, \alpha_n \in \Omega$ tais que

$$f(x) = a\,(x - \alpha_1) \cdots (x - \alpha_n), \quad \text{com} \;\; a \in K$$

Então, o subcorpo $K(\alpha_1, \ldots, \alpha_n)$ de Ω é corpo de decomposição de $f(x)$ sobre K, e de facto é único a menos de isomorfismo como vamos provar.

Note que se $f(x)$ se decompõe em factores lineares em K e E é corpo de decomposição de $f(x)$ sobre K, então $E = K$.

Teorema 7. *Dados K um corpo e $f(x) \in K[x]\backslash K$ existe, a menos de isomorfismo, um único corpo de decomposição de $f(x)$ sobre K.*

Demonstração: Resta provar a unicidade, a menos de isomorfismo, do corpo $K(\alpha_1, \ldots, \alpha_n)$.

Pretendemos provar que dados E_1 e E_2 corpos de decomposição de $f(x)$ sobre K existe um isomorfismo $\bar{\theta} : E_1 \to E_2$ que deixa fixos os elementos de K, isto é tal que $\bar{\theta}(a) = a$, para $a \in K$.

a) Começamos por demonstrar um resultado mais geral do que o enunciado:
Sejam $\theta : F_1 \to F_2$ um isomorfismo de corpos e $f(x) \in F_1[x]$. Dados

E_1 um corpo de decomposição de $f(x)$ sobre F_1 e E_2 um corpo de decomposição de $\theta(f(x)) \in F_2[x]$ sobre F_2, existe um isomorfismo $\bar{\theta} : E_1 \to E_2$ que estende θ.
Faremos a demonstração por indução sobre a dimensão $n = [E_1 : F_1]$. Se $[E_1 : F_1] = 1$, então $E_1 = F_1$ pelo que $f(x)$ se decompõe em factores lineares em F_1 e, portanto, o mesmo sucede a $\theta(f(x))$ sobre F_2, donde $E_2 = F_2$. Tomemos então $\bar{\theta} = \theta$.
Admitamos que o resultado é válido para p tal que $1 \leq p < n$ e demonstremo-lo para n. Suponhamos pois que $[E_1 : F_1] = n$.

Atendendo a que E_1 é corpo de decomposição de $f(x)$ sobre F_1, $f(x)$ se decompõe num produto da factores irredutíveis em $F_1[x]$ e que $E_1 \neq F_1$, concluímos que um desses factores irredutíveis, digamos $g(x)$, tem grau maior do que 1 e tem uma raiz α em $E_1 \backslash F_1$. Então o polinómio $\theta(g(x))$ é irredutível em $F_2[x]$. Ora $\theta(\alpha)$ é uma raiz de $\theta(g(x))$ pelo que $\theta(\alpha) \in E_2$. Por outro lado, $\theta(\alpha) \notin F_2$ pois $\alpha \notin F_1$ e θ é um isomorfismo. Observemos agora que $F_1 \subsetneqq F_1(\alpha) \subseteq E_1$ donde, pelo Teorema da Torre, $[E_1 : F_1(\alpha)] < [E_1 : F_1] = n$.

Supondo $g(x) = a_0 + a_1 x + \ldots + a_r x^r \in F_1[x]$, sabemos que

$$F_1(\alpha) = \{b_0 + b_1\alpha + \ldots + b_{r-1}\alpha^{r-1} \in E_1 : b_0, \ldots, b_{r-1} \in F_1\}$$

com $g(\alpha) = 0$, e que analogamente

$$F_2(\theta(\alpha)) = \{c_0 + c_1\theta(\alpha) + \cdots + c_{r-1}\theta(\alpha)^{r-1} \in E_2 : c_0, \ldots, c_{r-1} \in F_2\}$$

com $\theta(g(\alpha)) = 0$. Ora θ é um isomorfismo entre F_1 e F_2, donde

$$F_2(\theta(\alpha)) = \{\theta(b_0) + \theta(b_1)\theta(\alpha) + \ldots + \theta(b_{r-1})\theta(\alpha)^{r-1} \in E_2 :$$

$$b_0, \ldots, b_{r-1} \in F_1\}$$

e, portanto, é fácil verificar que

$$\begin{array}{rcl} \bar{\theta} : F_1(\alpha) & \to & F_2(\theta(\alpha)) \\ b_0+b_1\alpha+\ldots+b_{r-1}\alpha^{r-1} & \mapsto & \theta(b_0)+\theta(b_1)\theta(\alpha)+\ldots+\theta(b_{r-1})\theta(\alpha)^{r-1} \end{array}$$

é um isomorfismo que estende θ. (Recorde a demonstração do Teorema 3.a) e a descrição do corpo quociente da Secção 2.6.) Considerando agora $f(x)$ como polinómio sobre $F_1(\alpha)[x]$ o corpo E_1 é um seu corpo de decomposição sobre $F_1(\alpha)$ e E_2 é corpo de decomposição de $\theta(f(x))$

sobre $F_2(\theta(\alpha))$. Como $[E_1 : F_1(\alpha)] < n$, por hipótese de indução existe um isomorfismo $\overline{\overline{\theta}}$: $E_1 \to E_2$ que estende $\bar{\theta}$, e portanto estende θ. O resultado fica demonstrado para qualquer $n \in \mathbb{N}$ atendendo ao princípio da indução.

b) Sejam E_1 e E_2 extensões de K que são corpos de decomposição de $f(x) \in K[x]$. Na alínea a), tomemos $F_1 = K = F_2$ e θ o isomorfismo identidade de F_1 em F_2. Então existe $\bar{\theta} : E_1 \to E_2$ um isomorfismo que estende θ, isto é tal que $\bar{\theta}(a) = \theta(a) = a$, para qualquer $a \in K$, como pretendido. ∎

Definição. Dado um conjunto W de polinómios não constantes com coeficientes num corpo K, uma extensão E de K diz-se um *corpo de decomposição de* W sobre K se qualquer $f(x) \in W$, se decompõe em $E[x]$ num produto de factores lineares e E é gerado por K e pelas raízes de todos os polinómios de W.

Exemplo.

Consideremos $f_1(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ e $f_2(x) = x^2 + 1 \in \mathbb{Q}[x]$. Então $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$ é corpo de decomposição de $\{f_1(x), f_2(x)\}$ sobre $\mathbb{Q}$.

3.4 Corpos algebricamente fechados

Nesta secção, temos por objectivo demonstrar a existência do fecho algébrico de um corpo.

Definição. Um corpo E tal que qualquer polinómio $f(x) \in E[x] \backslash E$ se decompõe em factores de grau 1 em $E[x]$ diz-se *algebricamente fechado*.

É claro que um corpo E é algebricamente fechado se e só se todo o polinómio não constante de $E[x]$ tiver uma raiz em E.

Exemplo.

Atendendo ao Teorema Fundamental de Álgebra, $\mathbb{C}$ é um corpo

algebricamente fechado. O corpo $\mathbb{R}$ não é algebricamente fechado.

Em geral, um subcorpo de um corpo algebricamente fechado não é algebricamente fechado. Como exemplo, basta tomarmos o corpo $\mathbb{C}$ e o seu subcorpo $\mathbb{R}$.

Sejam K um corpo e E uma sua extensão. Designamos por $\overline{K}_E$ o conjunto dos elementos de E algébricos sobre K. Temos $K \subseteq \overline{K}_E \subseteq E$.

Teorema 8. *Sejam K e E corpos tais que E é extensão de K. Então $\overline{K}_E$ é extensão algébrica de K. Além disso, se E for algebricamente fechado, $\overline{K}_E$ também é algebricamente fechado.*

Demonstração: Começamos por provar que $\overline{K}_E$ é um subcorpo de E. Como $0, 1 \in K$, então $0, 1 \in \overline{K}_E$. Sejam $a, b \in \overline{K}_E$. Pelos Teoremas 4 e 5, sabemos que $K(a)$ é extensão algébrica de K e $K(a, b)$ é extensão algébrica de $K(a)$. Então, pelo Corolário 6.2, o corpo $K(a, b)$ é extensão algébrica de K, donde $a - b \in \overline{K}_E$ e $ab^{-1} \in \overline{K}_E$ quando $b \neq 0$. Logo $\overline{K}_E$ é subcorpo de E, pelo Critério 2 de subcorpo.

Por definição, é claro que $\overline{K}_E$ é uma extensão algébrica de K.

Suponhamos que E é algebricamente fechado e $f(x) \in \overline{K}_E[x] \backslash \overline{K}_E$. Consideremos $f(x)$ como polinómio de coeficientes em E. Como E é algebricamente fechado, existe $\alpha \in E$ tal que $f(\alpha) = 0$. Então α é algébrico sobre $\overline{K}_E$. Tomemos a sequência

$$K \subseteq \overline{K}_E \subseteq \overline{K}_E(\alpha)$$

Pelos Corolários 5.1 e 6.2, o corpo $\overline{K}_E(\alpha)$ é extensão algébrica de K, donde α é algébrico sobre K. Então $\alpha \in \overline{K}_E$ e, portanto, $f(x)$ tem uma raiz em $\overline{K}_E$. Logo $\overline{K}_E$ é algebricamente fechado. ∎

Exemplo.

De $\mathbb{Q} \subseteq \mathbb{C}$, concluímos que $\overline{\mathbb{Q}}_{\mathbb{C}}$ é algebricamente fechado.

Definição. Dados um corpo K e uma sua extensão E, o corpo

$\overline{K}_E$ diz-se o *fecho algébrico de K em E*.

O teorema seguinte completa o anterior, garantindo-nos a unicidade de uma extensão algébrica e algebricamente fechada de um corpo K numa sua extensão E algebricamente fechada.

Teorema 9. *Sejam K e E corpos tais que E é extensão algebricamente fechada de K. Então $\overline{K}_E$ é o único subcorpo de E algebricamente fechado que é extensão algébrica de K.*

Demonstração: Seja $\mathcal{L}$ um subcorpo de E algebricamente fechado e extensão algébrica de K. Então todo o elemento de $\mathcal{L}$ é algébrico sobre K, donde $\mathcal{L} \subseteq \overline{K}_E$. Tomemos $\alpha \in \overline{K}_E$. Existe $f(x) \in K[x] \backslash K$ tal que $f(\alpha) = 0$, por definição de $\overline{K}_E$. Logo $f(x) \in \mathcal{L}[x] \backslash \mathcal{L}$ e, como $\mathcal{L}$ é algebricamente fechado, se grau $f(x) = n$, existem $a, \alpha_1, \ldots, \alpha_n \in \mathcal{L}$ tais que

$$f(x) = a\,(x - \alpha_1) \cdots (x - \alpha_n)$$

Então a raiz $\alpha \in E$ é um dos α_i, com $i = 1, \ldots, n$, e, portanto, $\alpha \in \mathcal{L}$. Logo $\mathcal{L} = \overline{K}_E$. ∎

Dado um corpo K, se considerarmos extensões algebricamente fechadas de K distintas, obtemos fechos algébricos não isomorfos? A resposta a esta questão é negativa. De facto, vamos provar que dado um corpo K, por um lado, existe uma sua extensão algébrica Ω que é corpo algebricamente fechado; por outro, se tivermos outro corpo E algebricamente fechado que seja extensão algébrica de K, então E é isomorfo a Ω. Mais ainda, podemos construir um isomorfismo entre E e Ω que fixa os elementos de K.

Definição. Uma extensão algébrica E de um corpo K que seja algebricamente fechada diz-se um *fecho algébrico* de K.

Tenhamos também presente o seguinte resultado.

Lema 10. *Sejam K e E corpos tais que E é extensão algébrica de K. Então $\#E \leq \max(\aleph_0, \#K)$.*

Demonstração: Temos $\#K[x] = \#K \cdot \aleph_0$ (Exercício 22 de Apêndice). Seja

$$\mathrm{MIrr}(K[x]) = \{f \in K[x] : f \text{ é um polinómio mónico e irredutível}\}.$$

Obviamente, temos $\#\mathrm{MIrr}(K[x]) \leq \#K[x] = \#K \cdot \aleph_0$. Dado $f(x) \in \mathrm{MIrr}(K[x])$, consideremos o conjunto das suas raízes distintas em E. Ordenemos este conjunto, o qual é finito podendo ser vazio.

Dado $\alpha \in E$, como E é extensão algébrica de K, podemos considerar $f_\alpha(x) \in K[x]$ o seu polinómio mínimo sobre K, o qual está em $\mathrm{MIrr}(K[x])$.

Tomemos então

$$\begin{aligned} \psi\colon\ E &\longrightarrow \mathrm{MIrr}(K[x]) \times \mathbb{N} \\ \alpha &\longmapsto (f_\alpha(x), i_\alpha) \end{aligned}$$

sendo i_α a posição de α no conjunto das raízes distintas de $f_\alpha(x)$ em E. É claro que ψ é uma aplicação injectiva, donde

$$\#E \leq (\#K \cdot \aleph_0) \cdot \aleph_0 = \#K \cdot (\aleph_0 \cdot \aleph_0) = \#K \cdot \aleph_0 = \max(\#K, \aleph_0). \blacksquare$$

Teorema 11. *Todo o corpo admite um fecho algébrico, que é único a menos de isomorfismo.*

Demonstração: Existência.

Seja K um corpo. Fixemos um conjunto A com cardinal infinito não numerável tal que $K \subseteq A$ e $\#K < \#A$ (ver Exercício 28 de Apêndice).

Seja $\mathcal{F} = \{E : E \text{ é extensão algébrica de } K,\ E \subseteq A \text{ e } \#E < \#A\}$. Temos $\mathcal{F} \neq \emptyset$, visto que $K \in \mathcal{F}$.

Em $\mathcal{F}$ definimos uma relação de ordem parcial $\leqslant$ do seguinte modo: dados $E_1, E_2 \in \mathcal{F}$,

$$E_1 \leq E_2 \text{ se e só se } E_2 \text{ é extensão de } E_1.$$

Comecemos por mostrar que existe um elemento maximal Ω em $(\mathcal{F}, \leqslant)$.

Seja $\mathcal{C} = \{E_i\}_{i\in I}$ uma cadeia arbitrária não vazia de elementos de $(\mathcal{F}, \leqslant)$. Vejamos que $\cup_{i\in I}E_i \in \mathcal{F}$. Pelo Exercício 4, sabemos que $\cup_{i\in I}E_i$ é um corpo, que está contido em A e que é claramente uma extensão algébrica de K. Pelo lema anterior e pela construção de A, obtemos $\#\cup_{i\in I} E_i \leq \max(\#K, \aleph_0) < \#A$. Logo $\cup_{i\in I}E_i$ está em $\mathcal{F}$. Além disso, $\cup_{i\in I}E_i$ é um majorante de $\mathcal{C}$. Atendendo ao Lema de Zorn, existe um elemento maximal Ω em $(\mathcal{F}, \leqslant)$.

Vamos provar que Ω é algebricamente fechado. Como, por definição, Ω é uma extensão algébrica de K, concluiremos então que Ω é um fecho algébrico de K.

Suponhamos que Ω não é algebricamente fechado. Então existe um polinómio $f(x) \in \Omega[x]$ de grau maior do que 1 que não se decompõe em $\Omega[x]$ em factores de grau 1. Como todo o polinómio de grau maior do que 1 se decompõe num produto de factores irredutíveis em $\Omega[x]$ pelo Teorema II.13 , podemos assumir que $f(x)$ é irredutível em $\Omega[x]$. Atendendo à demonstração do Teorema II.15 e ao Teorema 3.a), existe um corpo de ruptura Ω^* de $f(x)$ cuja forma é $\Omega^* = \Omega(\alpha)$, em que α é uma raiz de $f(x)$ que não está em Ω. Pelo Corolário 5.1, o corpo Ω^* é extensão algébrica de Ω e, sendo Ω extensão algébrica de K, concluímos pelo Corolário 6.2 que $\Omega^* = \Omega(\alpha)$ é extensão algébrica de K. Atendendo de novo ao Lema 10, obtemos $\#\Omega^* < \#A$.

Temos $A = (A\backslash\Omega)\,\dot\cup\,\Omega$ e $\#\Omega < \#A$, donde $\#A = \#(A\backslash\Omega)$. Assim, $\#(\Omega(\alpha)\backslash\Omega) \leq \#\Omega(\alpha) < \#A = \#(A\backslash\Omega)$, pelo que existe uma aplicação injectiva $\xi : \Omega(\alpha)\backslash\Omega \to A\backslash\Omega$. Esta estende-se, por união com a aplicação identidade em Ω, a uma aplicação injectiva

$$\begin{aligned} \psi : \Omega(\alpha) &\longrightarrow A \\ a \in \Omega(\alpha)\backslash\Omega &\mapsto \xi(a) \\ a \in \Omega &\mapsto a \end{aligned}$$

Em $\Lambda := \operatorname{Im}\psi$, definimos operações de adição $\oplus$ e multiplicação $\odot$ de modo natural: dados $u_1, u_2 \in \Omega(\alpha)$,

$$\begin{aligned} \psi(u_1) \oplus \psi(u_2) &= \psi(u_1 + u_2) \\ \psi(u_1) \odot \psi(u_2) &= \psi(u_1 u_2) \end{aligned}$$

É uma questão de rotina provar que $(\Lambda, \oplus, \odot)$ é um corpo que, por definição, contém K e está contido em A. Além disso $\#\Lambda = \#\Omega(\alpha) <$

$\#A$. Mais ainda, $\overline{\psi} : \Omega(\alpha) \to \Lambda, u \mapsto \psi(u)$, é um isomorfismo de corpos que deixa fixos os elementos de K, isto é tal que $\overline{\psi}(k) = k$ para qualquer $k \in K$.

Como $\Omega(\alpha)$ é extensão algébrica de K, então Λ é extensão algébrica de K (ver Exercício 13). Logo $\Lambda \in \mathcal{F}$ e $\Omega \subsetneqq \Lambda$ o que é absurdo pois Ω é maximal em $\mathcal{F}$. Portanto, Ω é algebricamente fechado, como se queria provar.

Unicidade

Pretendemos demonstrar agora que dados F_1 e F_2 fechos algébricos de K existe $\sigma : F_1 \to F_2$ um isomorfismo que fixa os elementos de K.

a) Começamos por provar um resultado mais geral. Sejam F_1 e F_2 corpos arbitrários e W um conjunto de polinómios em $F_1[x]$. Seja $\theta : F_1 \to F_2$ um isomorfismo de corpos e denotemos também por θ a sua extensão natural de $F_1[x]$ em $F_2[x]$. Sejam E_1 um corpo de decomposição de W sobre F_1 e E_2 um corpo de decomposição de $\theta(W)$ sobre F_2. Vamos provar que existe um isomorfismo $\bar{\theta} : E_1 \to E_2$ que estende θ. Estende o provado na a) do Teorema 7 mas usa esse tal a). Consideremos os ternos (M_1, M_2, τ) em que M_1 e M_2 são corpos tais que $F_1 \subseteq M_1 \subseteq E_1$, $F_2 \subseteq M_2 \subseteq E_2$ e $\tau : M_1 \to M_2$ é um isomorfismo que estende θ. Observemos que (F_1, F_2, θ) é um destes ternos. No conjunto $\mathcal{A}$ de todos estes ternos, definimos uma ordem partial do seguinte modo: dados (M_1, M_2, τ_1), $(N_1, N_2, \tau_2) \in \mathcal{A}$,

$$(M_1, M_2, \tau_1) \leqslant (N_1, N_2, \tau_2) \text{ se e só se } M_1 \subseteq N_1 \; M_2 \subseteq N_2, \tau_2|_{M_1} = \tau_1$$

temos

$$\begin{array}{ccccccc} F_1 & \subseteq & M_1 & \subseteq & N_1 & \subseteq & E_1 \\ \downarrow \theta & & \downarrow \tau_1 & & \downarrow \tau_2 & & \vdots \overline{\theta} \\ F_2 & \subseteq & M_2 & \subseteq & N_2 & \subseteq & E_2 \end{array}$$

Dada uma cadeia não vazia $\{(M_{1i}, M_{2i}, \tau_i)\}_{i \in I}$ de elementos de $(\mathcal{A}, \leq)$, provamos que $(\cup M_{1i}, \cup M_{2i}, \cup \tau_i)$ é um elemento de $\mathcal{A}$ (ver Exercício 4) que é, obviamente, um majorante da cadeia. Pelo Lema de Zorn, concluímos que $\mathcal{A}$ tem um elemento maximal (U, V, π). Vamos mostrar que $U = E_1$ e $V = E_2$, o que nos permitirá tomar $\bar{\theta} = \pi$ nas condições pretendidas.
Admitamos que $U \subsetneqq E_1$. Neste caso, existe um polinómio $f(x) \in U[x]$

com todas as raízes $a_1, \ldots, a_m$ em E_1 que não se decompõe em factores lineares em $U[x]$, o que equivale a dizer que uma sua raiz não se encontra em U, donde $U(a_1, \ldots, a_m) \neq U$.
Temos $\pi : U \to V$ um isomorfismo, $U_0 = U(a_1, \ldots, a_m)$ corpo de decomposição de $f(x)$ sobre U e $V_0 = V(\pi(a_1), \ldots, \pi(a_m))$ corpo de decomposição de $\pi(f(x))$ sobre V. Então, pela alínea a) da demonstração do Teorema 7, sabemos que existe um isomorfismo $\bar{\pi} : U_0 \to V_0$ que estende π, logo que estende θ. Portanto, $(U_0, V_0, \bar{\pi}) \in \mathcal{A}$. Como $(U, V, \pi) \lneqq (U_0, V_0, \bar{\pi})$ chegamos a um absurdo. Logo $E_1 = U$.
Analogamente, tomando π^{-1}, provamos que $E_2 = V$.

b) Sejam K um corpo e $\overline{K}$ um seu fecho algébrico, isto é uma sua extensão algébrica e algebricamente fechada. Então $\overline{K}$ é um corpo de decomposição do conjunto $K[x]$ de todos os polinómios de coeficientes em K. De facto, se $f(x) \in K[x]$ então $f(x) \in \overline{K}[x]$ e portanto decompõe-se em factores lineares em $\overline{K}[x]$, donde $f(x)$ tem todas as suas raízes em $\overline{K}$. Por outro lado, se $u \in \overline{K}$, sendo $\overline{K}$ extensão algébrica de K existe $f(x) \in K[x]$ tal que u é raiz de $f(x)$. Logo $\overline{K}$ é trivialmente gerado por K e pelo conjunto dos elementos de $\overline{K}$ que são raízes de algum polinómio de $K[x]$.

c) Terminemos a demonstração da unicidade do fecho algébrico. Seja $i : K \to K$ o isomorfismo identidade. Dados $\overline{K}_1$ e $\overline{K}_2$ fechos algébricos de K, atendendo à alínea b), podemos encarar $\overline{K}_1$ como um corpo de decomposição de $K[x]$ sobre K e $\overline{K}_2$ como corpo de decomposição da imagem de $K[x]$, que também é $K[x]$, sobre K. Então, pela alínea a), existe $\bar{\theta} : \overline{K}_1 \to \overline{K}_2$ um isomorfismo que estende i, ou seja, que deixa os elementos de K fixos. ∎

Em face do demonstrado na alínea b), podemos dizer que, a menos de isomorfismo, o fecho algébrico de um corpo K é "o conjunto das raízes de todos os polinómios de $K[x]$", o qual designamos por $\overline{K}$. Além disso, se soubermos calcular o fecho $\overline{K}_E$ de K sobre um corpo E algebricamente fechado, então podemos afirmar que $\overline{K} = \overline{K}_E$, atendendo aos Teoremas 9 e 11. Vejamos, agora, alguns exemplos.

Exemplos.

1) Temos $\mathbb{R} \subseteq \mathbb{C} = \mathbb{R}(i)$ e $\mathbb{C}$ algebricamente fechado. Como $\mathbb{C}$ é ex-

tensão finita de $\mathbb{R}$, então $\mathbb{C}$ é extensão algébrica de $\mathbb{R}$. Portanto, $\mathbb{C}$ é o fecho algébrico de $\mathbb{R}$ em $\mathbb{C}$ e é, a menos de isomorfismo, a única extensão algébrica e algebricamente fechada de $\mathbb{R}$, isto é $\mathbb{C} = \overline{\mathbb{R}}$.

2) Temos $\mathbb{Q} \subseteq \mathbb{C}$. O fecho algébrico de $\mathbb{Q}$ em $\mathbb{C}$ é pois $\overline{\mathbb{Q}}$ e $\mathbb{Q} \subsetneq \overline{\mathbb{Q}} \subsetneq \mathbb{C}$, uma vez que $\sqrt{2} \in \overline{\mathbb{Q}} \backslash \mathbb{Q}$ e $\pi \in \mathbb{C} \backslash \overline{\mathbb{Q}}$, visto π não ser algébrico sobre $\mathbb{Q}$. Temos

$$\overline{\mathbb{Q}} = \left\{ \alpha \in \mathbb{C} \colon \exists\, f(x) \in \mathbb{Q}[x] \backslash \mathbb{Q},\ f(\alpha) = 0 \right\}$$

e podemos provar que $\overline{\mathbb{Q}}$ é um conjunto numerável, pelo que $\overline{\mathbb{Q}} \not\simeq \mathbb{R}$.
Notemos que $\overline{\mathbb{Q}}$ é extensão algébrica infinita de $\mathbb{Q}$ (ver Exercício 12).

3) O exemplo seguinte mostra que, dados um corpo K e uma sua extensão E, o corpo $\overline{K}_E$ pode não ser $\overline{K}$.
Consideremos $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2})$. Como $\mathbb{Q}(\sqrt{2})$ é extensão algébrica de $\mathbb{Q}$, então $\overline{\mathbb{Q}}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Q}(\sqrt{2})$ mas $\mathbb{Q}(\sqrt{2}) \subsetneq \overline{\mathbb{Q}}$ pois, por exemplo, $\sqrt{3} \in \overline{\mathbb{Q}} \backslash \mathbb{Q}(\sqrt{2})$. O corpo $\mathbb{Q}(\sqrt{2})$ não é algebricamente fechado, por exemplo $x^2 + 1 \in \mathbb{Q}(\sqrt{2})[x]$ mas não tem raízes em $\mathbb{Q}(\sqrt{2})$.

Exercícios

1. Em $S = \mathbb{R} \times \mathbb{R}$, defina uma operação binária $\oplus$ por $(a,b) \oplus (c,d) = (a+c, b+d)$, para quaisquer $(a,b),(c,d) \in S$.
   a) Definindo outra operação binária $\odot$ por $(a,b) \odot (c,d) = (ac, bd)$, será que $(S, \oplus, \odot)$ é corpo?
   b) E se definirmos $\odot$ por $(a,b) \odot (c,d) = (ac+bd, bc-ad)$, será que $(S, \oplus, \odot)$ é corpo?

2. Seja K um domínio de integridade. Mostre que a característica de K é zero ou p, sendo p um primo.

3. Sejam K um corpo e A um subconjunto de K. Mostre que
   a) A é subcorpo de K se e só se satisfaz as condições seguintes:
      (i) $0, 1 \in A$;
      (ii) $\forall x \in A,\ -x \in A$;
      (iii) $\forall x, y \in A,\ x + y \in A$;
      (iv) $\forall x \in A \setminus \{0\},\ \ x^{-1} \in A$;
      (v) $\forall x, y \in A,\ \ xy \in A$.
   b) A é subcorpo de K se e só se satisfaz as condições seguintes:
      (i) $0, 1 \in A$;
      (ii) $\forall x, y \in A,\ \ x - y \in A$;
      (iii) $\forall x \in A,\ \forall y \in A \setminus \{0\},\ \ xy^{-1} \in A$.

4. a) Seja E um corpo. Mostre que dada uma cadeia não vazia $\{M_i\}_{i \in I}$ de subcorpos de E (em relação à inclusão), a sua união é um subcorpo de E.
   b) Sejam E_1 e E_2 corpos, $\{M_i^1\}_{i \in I}$ uma cadeia de subcorpos de E_1 e $\{M_i^2\}_{i \in I}$ uma cadeia de subcorpos de E_2 tais que existem isomorfismos $\tau_i : M_i^1 \to M_i^2$, com $i \in I$ com $\tau_i = \tau_j|_{M_i}$ quando $M_i \subseteq M_j$. Prove que existe um isomorfismo $\tau : \cup_{i \in I} M_i^1 \to \cup_{i \in I} M_i^2$.

5. Descreva os corpos $\mathbb{R}(e)$; $\mathbb{R}(2i)$; $\mathbb{Q}(\sqrt[3]{3})$; $\mathbb{Q}(\sqrt[5]{2})$.

6. Sejam F, K, E corpos tais que K é extensão de F e E é extensão de K. Mostre que

   a) Se $[K : F] = 1$, então $K = F$;

   b) Se $[E : F] = p$, com p natural primo, então $K = F$ ou $K = E$.

7. Determine

   a) $[\mathbb{Q}(\sqrt[7]{3}) : \mathbb{Q}]$;

   b) $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, onde $\alpha \in \mathbb{R}$ é raiz do polinómio $x^3 - x - 1$;

   c) $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$;

   d) $[\mathbb{Q}(\sqrt{5}, \sqrt{11}) : \mathbb{Q}]$, indicando bases de $\mathbb{Q}(\sqrt{5})$ sobre $\mathbb{Q}$, de $\mathbb{Q}(\sqrt{5}, \sqrt{11})$ sobre $\mathbb{Q}(\sqrt{5})$ e de $\mathbb{Q}(\sqrt{5}, \sqrt{11})$ sobre $\mathbb{Q}$.

8. a) Mostre que $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

   b) Determine $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}]$.

9. Determine o corpo de decomposição de $f(x) = x^4 - 5x^2 + 4 \in \mathbb{Q}[x]$ sobre $\mathbb{Q}$.

10. Mostre que

    a) se K_1, K_2 e E são corpos tais que $K_1 \subseteq K_2 \subseteq E$ e E é algebricamente fechado, então

       (i) $\overline{K_1} \subseteq \overline{K_2}$;

       (ii) $\overline{\overline{K_1}} = \overline{K_1}$.

    b) $\overline{\mathbb{R}} = \mathbb{C}$;

    c) $\overline{\overline{\mathbb{Q}}} = \overline{\mathbb{Q}}$;

    d) $\overline{\mathbb{Q}} = \overline{\mathbb{Q}(\sqrt[3]{5}, \sqrt{2})}$.

11. a) Seja $m \in \mathbb{N}$, com $m \geq 2$.
    (i) Determine $[\mathbb{Q}(\sqrt[m]{2}) : \mathbb{Q}]$.
    ii) Justifique que $\mathbb{Q}(\sqrt[m]{2}) \subseteq \overline{\mathbb{Q}}$.

    b) Use a alínea anterior para concluir que $\overline{\mathbb{Q}}$ não é extensão finita de $\mathbb{Q}$, embora seja algébrica.

12. Sejam K um corpo, F uma sua extensão e σ um automorfismo de F que deixa os elementos de K fixos. Dados $f(x) \in K[x]$ e $u \in F$ uma sua raiz, mostre que $\sigma(u)$ é raiz de $f(x)$.

13. Sejam K um corpo e E_1 e E_2 extensões de K. Mostre que se E_1 é extensão algébrica de K e existe um isomorfismo $\theta : E_1 \to E_2$ que deixa os elementos de K fixos então E_2 também é extensão algébrica de K.

14. a) Sejam K um corpo algebricamente fechado e F um subcorpo de K. Mostre que o corpo F é algebricamente fechado se e só se todo o elemento de K que é algébrico sobre F pertence a F.

    b) Sejam K um corpo e E uma sua extensão algébrica. Mostre que E é fecho algébrico de K se e só se para toda a extensão algébrica A de K existe um morfismo injectivo $\theta : A \to E$ que fixa os elementos de K.

15. Sejam K um corpo e F uma sua extensão. Mostre que o conjunto $\mathrm{Aut}_K F$ dos automorfismos de F que deixam os elementos de K fixos, ditos *K-automorfismos* constitui um grupo, que se chama o *grupo de Galois* de F sobre K.

16. a) Prove que não existe um número racional b tal que $2b^2 = 3$.

    b) Mostre que $[\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}]$.

    c) Determine uma base de $\mathbb{Q}(\sqrt{3}, \sqrt{2})$ sobre $\mathbb{Q}$ e as coordenadas de $(\sqrt{2} + \sqrt{6})^{-1}$ nessa base.

17. Sejam F_1, F_2 e E corpos tais que $\mathbb{Q} \subseteq F_1 \subseteq E$ e $\mathbb{Q} \subseteq F_2 \subseteq E$. Suponha que $F_1 = \mathbb{Q}[x]/\langle x^3 + 2x^2 + 1\rangle$ e $F_2 = \mathbb{Q}(\alpha)$, com $\alpha \in \mathbb{C}\backslash\mathbb{R}$ raiz do polinómio $x^3 + x^2 + 9x + 9$, e ainda que E é extensão finita de $\mathbb{Q}$. Determine o valor mínimo de $[E : \mathbb{Q}]$.

18. Considere um corpo K e uma sua extensão Ω de grau 7. Mostre que $K(\alpha) = K(\alpha^2)$, para qualquer $\alpha \in \Omega$.

19. Seja K um corpo e $\alpha, \beta \in \overline{K}$ com $\alpha \neq \beta$. Seja A o subconjunto de $K[x]$ formado pelos polinómios $f(x)$ tais que $f(\alpha) = f(\beta) = 0$. Mostre que

    a) (i) A é ideal de $K[x]$;
    (ii) Se $\alpha, \beta \in K$, então A é o ideal de $K[x]$ gerado por $h(x) = (x - \alpha)(x - \beta)$.

    b) A é ideal primo se e só se α e β têm o mesmo polinómio mínimo sobre K.

20. **Corpos Finitos.** Na parte A) deste exercício provamos que existem corpos de cardinalidade p^n, para quaisquer p primo e $n \in \mathbb{N}$. Na parte B), mostramos que todo o corpo finito tem cardinal da forma p^n.

    A) Seja $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$, com p primo e $n \in \mathbb{N}$. Mostre que

        a) Existe uma extensão E de $\mathbb{Z}_p$ em que

        $$f(x) = x(x - t_1) \cdots (x - t_{p^n - 1})$$

        para certos $t_1, \ldots, t_{p^n-1} \in E$;

        b) $c(E) = p$ e que se $i \neq j$, com $i, j \in \{1, \ldots, p^n - 1\}$, então $t_i \neq t_j$; mais ainda, $t_i \neq 0$, qualquer que seja $i \in \{1, \ldots, p^n - 1\}$;
        Sugestão. Considere o polinómio $f'(x) \in E[x]$.

        c) $T = \{0, t_1, \ldots, t_{p^n-1}\}$ é um subcorpo de E;

        d) Conclua que, dados um primo p e $n \in \mathbb{N}$, existe um corpo finito de cardinal p^n.

B) Seja E um corpo finito.

a) Mostre que existe p primo tal que $\mathbb{Z}_p$ é subcorpo de E, a menos de isomorfismo.

b) Considere E como espaço vectorial sobre $\mathbb{Z}_p$. Prove que E admite uma base finita $(a_1, \ldots, a_n)$ sobre $\mathbb{Z}_p$.

c) Conclua que $\sharp E = p^n$.

Capítulo 4

Construções com régua e compasso

Neste capítulo, mostraremos como alguns dos resultados algébricos sobre extensões de corpos, que acabámos de estudar, permitem responder a certas questões de natureza puramente geométrica.

Por exemplo, todos sabemos como bissectar um ângulo usando uma régua e um compasso. Poderemos, usando os mesmo instrumentos, trissectar um ângulo qualquer? Esta foi uma das muitas questões discutidas pelos geómetras gregos (Séc. V a.c.) e a que vamos responder pela negativa, provando que tal é, em geral, impossível; por exemplo, mostraremos que é impossível trissectar o ângulo $\frac{\pi}{3}$.

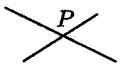
Com uma régua sem escala e um compasso, dado um conjunto de pontos $\mathcal{P}_0$ no plano euclidiano $\mathbb{R}^2$, podemos determinar novos pontos aplicando as seguintes operações:

1) Usando a régua, traçar a recta que une dois pontos P e Q de $\mathcal{P}_0$;

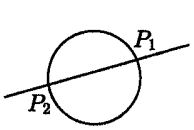
2) Usando o compasso, traçar a circunferência de centro num ponto O de $\mathcal{P}_0$ e que passa por outro ponto P de $\mathcal{P}_0$.

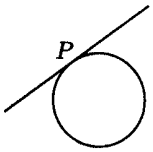
Neste contexto, dizemos que um ponto de $\mathbb{R}^2$ é *construtível num passo a partir de* $\mathcal{P}_0$ se pode ser obtido por um dos seguintes processos:

a) Como intersecção de duas rectas distintas,

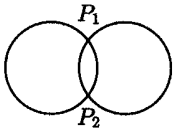


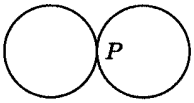
b) Como intersecção de uma recta com uma circunferência,





c) Como intersecção de duas circunferências distintas,





sendo as rectas e as circunferências em causa construídas a partir de $\mathcal{P}_0$, usando as operações 1) ou 2).

Um ponto P de $\mathbb{R}^2$ diz-se *construtível a partir de* $\mathcal{P}_0$ se pertence a $\mathcal{P}_0$ ou se existem pontos $R_1, \ldots, R_n$ em $\mathbb{R}^2$, para algum $n \in \mathbb{N}$, tais que

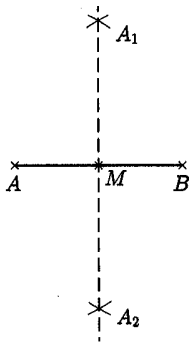
- R_1 é construtível num passo a partir de $\mathcal{P}_0$;
- o ponto R_{i+1}, com $i = 1, \ldots, n-1$ é construtível num passo a partir de $\mathcal{P}_0 \cup \{R_1, \ldots, R_i\}$;
- $R_n = P$.

Uma *recta* r diz-se *construtível* a partir de $\mathcal{P}_0$ se contiver dois pontos distintos P_1 e P_2 construtíveis a partir de $\mathcal{P}_0$, o que equivale a afirmar que r pode ser obtida aplicando a operação 1) a pontos P_1 e P_2 construtíveis a partir de $\mathcal{P}_0$. Analogamente, uma *circunferência* $\mathcal{C}$ de centro O diz-se *construtível* a partir de $\mathcal{P}_0$ se O é construtível a partir de $\mathcal{P}_0$ e se $\mathcal{C}$ contém um ponto construtível a partir de $\mathcal{P}_0$.

4.1 Algumas construções geométricas

Recordemos algumas construções com régua e compasso.

1. Vamos construir a recta perpendicular ao meio do segmento $[AB]$, sendo A e B pontos distintos:



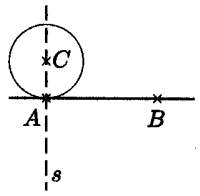
1) Traçamos $\mathcal{C}(A;B)$, circunferência de centro A que passa por B;

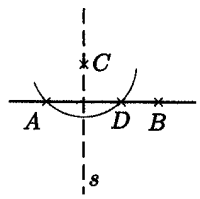
2) Traçamos $\mathcal{C}(B;A)$;

3) Achamos $A_1, A_2 \in \mathcal{C}(A;B) \cap \mathcal{C}(B;A)$;

4) $\overline{A_1A_2}$ é a recta perpendicular ao segmento $[AB]$ que passa pelo seu ponto médio M.

2. Dados dois pontos A e B distintos e um ponto C, construímos a recta s perpendicular à recta $\overline{AB}$ que passa pelo ponto C do seguinte modo:



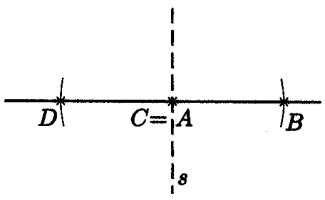


a) Se $C \neq A$,

1) Traçamos $\mathcal{C}(C;A)$;

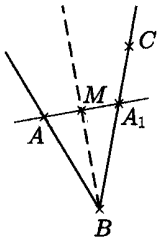
2) Se $\mathcal{C}(C;A) \cap \overline{AB} = \{A\}$, então $s = \overline{CA}$;

3) Se $\mathcal{C}(C;A) \cap \overline{AB} = \{A, D\}$, com $D \neq A$, então traçamos a recta perpendicular ao segmento $[AD]$ que passa pelo seu ponto médio, esta é a recta s;



b) Se $C = A$, traçamos $\mathcal{C}(C; B)$ e obtemos $\mathcal{C}(C; B) \cap \overline{AB} = \{B, D\}$ com $D \neq B$; em seguida traçamos a recta perpendicular ao segmento $[DB]$ que passa pelo seu ponto médio, esta é a recta s.

3. Dados A, B e C distintos e não colineares, a bissectriz do ângulo $\widehat{ABC}$ constrói-se do seguinte modo:



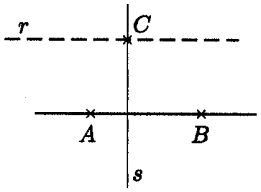
1) Traçamos $\mathcal{C}(B; A)$;

2) Temos $\mathcal{C}(B; A) \cap \dot{B}C = \{A_1\}$, com $\dot{B}C$ a semi-recta que passa por B e C e tem origem em B;

3) Construímos o ponto médio M do segmento $[AA_1]$;

4) $\dot{B}M$ é a bissectriz do ângulo.

4. Dados A, B e C distintos e não colineares, vamos construir a recta paralela a $\overline{AB}$ que passa por C:

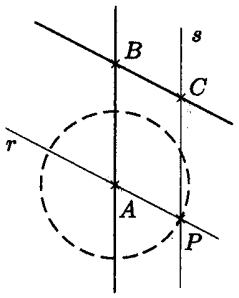


1) Traçamos $s \perp \overline{AB}$ tal que $C \in s$;

2) Traçamos $r \perp s$ tal que $C \in r$. Esta recta r é a recta pretendida.

5. Dados A, B e C distintos, vamos construir uma circunferência $\mathcal{C}(A; |BC|)$ de centro A e raio igual ao comprimento $|BC|$ do segmento $[BC]$.

a) Suponhamos que A, B e C não são colineares:



1) Traçamos $\overline{AB}$ e $\overline{BC}$;

2) Traçamos a recta $r \parallel \overline{BC}$ tal que $A \in r$;

3) Traçamos a recta $s \parallel \overline{AB}$ tal que $C \in s$;

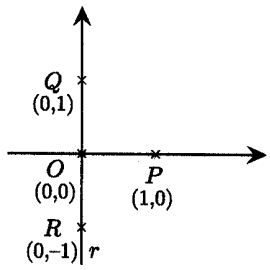
4) Seja P o ponto de intersecção de r com s, temos $|AP| = |BC|$;

5) $\mathcal{C}(A; P)$ é a circunferência pretendida.

b) Se A, B e C são colineares:

Traçamos $\mathcal{C}(B; C)$; seja $D \in \mathcal{C}(B; C) \backslash \overline{BC}$; aplicando a), traçamos $\mathcal{C}(A; |BD|)$.

6. Vejamos que, dados dois pontos distintos O e P, podemos construir um referencial (ortonormado) de $\mathbb{R}^2$ com origem O e em que a unidade de medida é o comprimento do segmento $[OP]$:



1) Traçamos $\overline{OP}$ que será o eixo $\overline{XX}$ das abcissas;

2) Traçamos $r \perp \overline{OP}$ com $O \in r$; r será o eixo $\overline{YY}$ das ordenadas;

3) Traçamos $\mathcal{C}(O; P)$;

4) $r \cap \mathcal{C}(O; P) = \{Q, R\}$;

5) $(O, \overrightarrow{OP}, \overrightarrow{OQ})$ é o referencial procurado.

Um ponto arbitrário P do plano $\mathbb{R}^2$ representa-se pelas suas coordenadas (a, b) num referencial ortonormado, em que $a, b \in \mathbb{R}$, e escrevemos $P_{\frown}(a, b)$. Dados $(a, b), (c, d) \in \mathbb{R}^2$, recordemos que a distância entre (a, b) e (c, d) é dada por $d((a, b), (c, d)) = \sqrt{(a-c)^2 + (b-d)^2}$.

Naturalmente, podemos perguntarmo-nos se todos os pontos de $\mathbb{R}^2$ são construtíveis a partir de dois pontos fixos O e P? Responderemos à frente a esta questão.

Definição. Fixados pontos O e P no plano $\mathbb{R}^2$, um número real α diz-se *construtível* se $|\alpha|$ é igual à distância entre dois pontos P_1 e P_2 construtíveis a partir de O e P.

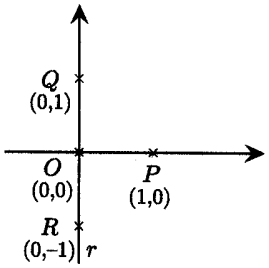
É claro que, se $\alpha \in \mathbb{R}$ é construtível, então $-\alpha$ também o é.

No que se segue, estaremos sempre a supor que partimos de dois pontos O e P sobre os quais construímos um referencial ortonormado de $\mathbb{R}^2$. Falar em construtível significará construtível a partir destes pontos.

Observemos que se existem pontos P_1 e P_2 construtíveis tais que $|\alpha| = d(P_1, P_2)$, então, usando a construção 5, podemos construir $C(O, |\alpha|)$, pelo que existem pontos R e S construtíveis tais que $|\alpha| = d(O, R) = d(O, S)$, $R \in d$, onde d designa a bissectriz do 1º quadrante, e $S \in \overline{XX}$, com $S \underset{\curvearrowright}{} (|\alpha|, 0)$.

Exemplos.

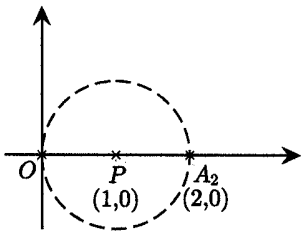
1) O real $\sqrt{2}$ é construtível, pois $\sqrt{2} = d(P, Q)$ no referencial ortonormado



2) Se $m \in \mathbb{Z}$, então m é construtível.

Demonstração: Se $m = 0$, temos $m = d(O, O)$ e se $m = 1$, então $m = d(O, P)$. Tomemos $m = 2$. Com a construção seguinte

provamos que 2 é construtível:



1) Traçamos $\mathcal{C}(P;O)$;

2) Tomamos $A_2 \in \overline{XX} \cap \mathcal{C}(P,O)$ e $A_2 \neq O$;

3) Temos $A_2 \frown (2,0)$ e $d(O,A_2) = 2$, donde 2 é construtível.

Por indução, provamos que, para qualquer $m \in \mathbb{N}$, existe um ponto A_m construtível com coordenadas $(m,0)$ tal que $d(O,A_m) = m$. Portanto, m é construtível.

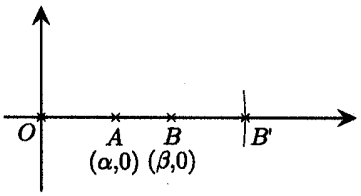
Se $m < 0$, então $-m > 0$. Ora $-m$ é construtível e, portanto, m também o é. ∎

Denotamos por K_0 o *conjunto de todos os reais construtíveis*. O Exemplo 2) mostra que $\mathbb{Z} \subseteq K_0$.

Teorema 1. *O conjunto K_0 constitui um subcorpo de $\mathbb{R}$.*

Demonstração: Já sabemos que $0, 1 \in K_0$. Por definição de real construtível, temos que, se $\alpha \in K_0$ então $-\alpha \in K_0$. Sejam $\alpha, \beta \in K_0$. Provemos que $\alpha + \beta \in K_0$.

Suponhamos que $\alpha, \beta \geq 0$. Consideremos $A \frown (\alpha, 0)$ e $B \frown (\beta, 0)$.

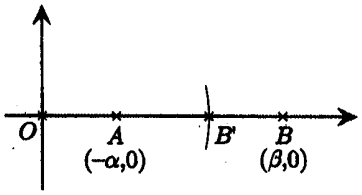


Tracemos $\mathcal{C}(A; d(O,B))$ e tomemos B' como sendo o ponto resultante da intersecção de $\mathcal{C}$ com o semieixo positivo dos $\overline{XX}$. Então $d(O,B') = \alpha + \beta$. Logo $\alpha + \beta \in K_0$.

(Neste esquema estamos a admitir, sem perda de generalidade, que $\alpha \leq \beta$.)

Se $\alpha, \beta < 0$, então $-\alpha, -\beta > 0$, donde $(-\alpha) + (-\beta) \in K_0$, pelo que $\alpha + \beta \in K_0$.

Se $\alpha < 0$ e $\beta > 0$, com $\alpha + \beta > 0$, temos $-\alpha < \beta$.

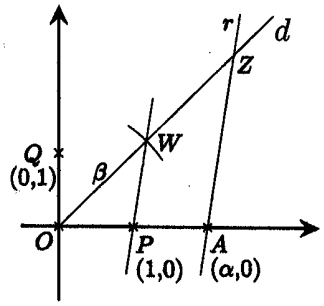


Tracemos $\mathcal{C}(O; d(A,B))$ e tomemos B' como atrás. Então $B' \curvearrowright (\alpha+\beta, 0)$. Logo $\alpha + \beta \in K_0$.

Os outros casos possíveis reduzem-se a um estudo semelhante aos anteriores. Portanto, $\alpha + \beta \in K_0$. Provemos agora que $\alpha\,\beta \in K_0$.

Se $\alpha = 0$ ou $\beta = 0$, então $\alpha\,\beta = 0$, donde $\alpha\,\beta \in K_0$.

Suponhamos $\alpha, \beta > 0$.



Consideremos:

1) Ponto $Q \curvearrowright (0,1)$;

2) Bissectriz d do 1º quadrante;

3) $\mathcal{C} = \mathcal{C}(O; \beta)$;

4) $W \in d \cap C$ no 1º quadrante;

5) $\overline{WP}$;

6) $r \parallel \overline{WP}$ tal que $A \in r$;

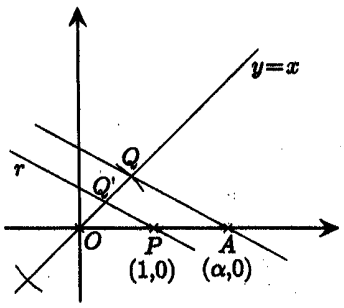
7) $\{Z\} = d \cap r$.

Temos, pelo Teorema de Thales, $\frac{|OW|}{|OP|} = \frac{|OZ|}{|OA|}$. Logo $\frac{\beta}{1} = \frac{|OZ|}{\alpha}$, donde $|OZ| = \beta\,\alpha$ e, portanto, $\alpha\,\beta \in K_0$.

Se $\alpha < 0$ ou $\beta < 0$, então $|\alpha|, |\beta| > 0$ e $|\alpha|, |\beta|$ estão em K_0. Pelo caso anterior, $|\alpha|\,|\beta| \in K_0$, donde $|\alpha\,\beta| \in K_0$ e, portanto, $\alpha\,\beta \in K_0$.

Se $\alpha \in K_0 \backslash \{0\}$, vamos mostrar que $\frac{1}{\alpha} \in K_0$.

Suponhamos $\alpha > 0$.



Consideremos:

1) A bissectriz d do 1º quadrante;

2) $\mathcal{C}(O,1)$;

3) $Q \in \mathcal{C}(O,1) \cap d$, com Q no 1º quadrante;

4) $\overline{AQ}$;

5) $r \parallel \overline{AQ}$ e tal que $P \in r$;

6) $Q' \in r \cap d$.

Temos $\frac{|OQ|}{\alpha} = \frac{|OQ'|}{1}$, logo $|OQ'| = \frac{1}{\alpha}$, pelo que $\frac{1}{\alpha} \in K_0$.

Se $\alpha < 0$, então $-\alpha > 0$, donde $\frac{1}{-\alpha} \in K_0$ e, portanto, $\frac{1}{\alpha} \in K_0$.

Concluímos, pois, que K_0 é um subcorpo de $\mathbb{R}$. ∎

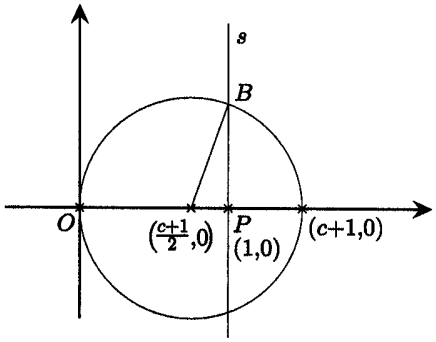
Nota. Sendo K_0 subcorpo de $\mathbb{R}$ e $\mathbb{Q}$ o subcorpo primo de $\mathbb{R}$, temos $\mathbb{Q} \subseteq K_0$, mas $K_0 \neq \mathbb{Q}$, pois $\sqrt{2} \in K_0 \backslash \mathbb{Q}$.

Exemplo.

Seja $c \in K_0$ e $c \geq 0$. Então $\sqrt{c} \in K_0$.

Demonstração: Se $c = 0$, então $\sqrt{c} = 0 \in K_0$. Se $c = 1$, então $\sqrt{1} = 1 \in K_0$.

Admitamos $c > 0$, $c \neq 1$ e $c \in K_0$. Então $\frac{c+1}{2} > \frac{1}{2}$ e temos $c+1, \frac{c+1}{2} \in K_0$.



Consideremos:

1) $(c+1,0)$ e $(\frac{c+1}{2},0)$;

2) $\mathcal{C} = \mathcal{C}((\frac{c+1}{2},0);(c+1,0))$;

3) $s \perp \overline{XX}$ tal que $P \in s$;

4) $B \in s \cap \mathcal{C}$.

(Neste esquema admitimos $\frac{c+1}{2} < 1$, mas a resolução é válida para $\frac{c+1}{2} > 1$)

Temos $\mathcal{C}$ com raio $\frac{c+1}{2}$, donde

$$\begin{aligned} d(P,B) &= \sqrt{\left(\frac{c+1}{2}\right)^2 - \left|1 - \frac{c+1}{2}\right|^2} \\ &= \sqrt{\frac{c^2+2\,c+1-(1-c)^2}{4}} \\ &= \sqrt{\frac{c^2+2\,c+1-1+2\,c-c^2}{4}} \;=\; \sqrt{c} \end{aligned}$$

Logo $\sqrt{c} \in K_0$. ∎

Observação. Seja F um subcorpo de $\mathbb{R}$ que contém x_1, y_1, x_2 e y_2 sendo (x_1, y_1) e (x_2, y_2) distintos. Num referencial ortonormado de $\mathbb{R}^2$, consideremos os pontos $P_1 \curvearrowright (x_1, y_1)$ e $P_2 \curvearrowright (x_2, y_2)$. A recta que passa por P_1 e P_2 é definida pela equação

$$(y_2 - y_1)\,x + (x_1 - x_2)\,y + \Big((y_1 - y_2)\,x_1 + (x_2 - x_1)\,y_1\Big) = 0$$

Tomando

$$a = y_2 - y_1\,, \qquad b = x_1 - x_2\,, \qquad c = (y_1 - y_2)\,x_1 + (x_2 - x_1)\,y_1$$

temos $a, b, c \in F$ e a recta admite a equação $ax + by + c = 0$.

A circunferência de centro P_1 que passa por P_2 fica definida pela equação

$$x^2+y^2+(-2\,x_1)\,x+(-2\,y_1)\,y+\Big(x_1^2+y_1^2-(x_1-x_2)^2-(y_1-y_2)^2\Big)=0$$

Considerando

$$d=-2\,x_1\,,\qquad e=-2\,y_1\,,\qquad f=x_1^2+y_1^2-(x_1-x_2)^2-(y_1-y_2)^2$$

temos $d, e, f \in F$ e a circunferência admite a equação $x^2+y^2+dx+ey+f=0$.

Notemos que as equações, acima mencionadas, deduzem-se, respectivamente, das equações da recta

$$(x_2-x_1)\,(y-y_1)=(y_2-y_1)\,(x-x_1)$$

e da circunferência

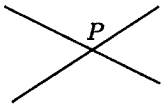
$$(x-x_1)^2+(y-y_1)^2=r^2,\qquad \text{em que}\quad r=d(P_1,P_2)$$

Lema 2. *Seja $P \curvearrowright (u,v)$ um ponto de $\mathbb{R}^2$ construtível num passo, a partir de um subconjunto $\mathcal{P}_0$ de pontos construtíveis. Seja Ω o subcorpo de $\mathbb{R}$ gerado pelas coordenadas dos pontos de $\mathcal{P}_0$. Então, se $\beta \in \{u,v\}$, temos*

$$\Omega(\beta)=\Omega(\sqrt{c}),\qquad \textit{para algum}\quad c\in\Omega\quad e\quad c>0\ .$$

Demonstração: Temos três casos a considerar:

a) Obtivemos P como ponto de intersecção de duas rectas construídas sobre pontos de $\mathcal{P}_0$.



Então (u,v) é a única solução de um sistema de equações

$$\begin{cases} a\,x+b\,y+c=0 \\ a'\,x+b'\,y+c'=0 \end{cases}$$

em que $a, b, c, a', b', c' \in \Omega$ pela observação anterior.

Portanto, u e v escrevem-se à custa de $a, b, c, a', b', c' \in \Omega$ através das operações $+$ e $\cdot$, logo $u, v \in \Omega$. Neste caso, $\Omega(\beta) = \Omega = \Omega(\sqrt{1})$.

b) Sem perda de generalidade, tomemos $\beta = u$. Obtivemos P como ponto de intersecção de uma recta com uma circunferência construídas sobre pontos de $\mathcal{P}_0$.

Então as coordenadas de P são solução de um sistema

$$\begin{cases} a\,x + b\,y + c = 0 & (1) \\ x^2 + y^2 + d\,x + e\,y + f = 0 & (2) \end{cases}$$

com $a, b, c, d, e, f \in \Omega$, de novo pela observação anterior.

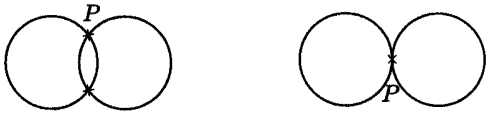
Se $b = 0$, então $a \neq 0$ e temos $u = -\frac{c}{a}$, logo $u \in \Omega$. Neste caso, $\Omega(\beta) = \Omega = \Omega(\sqrt{1})$.

Se $b \neq 0$, tirando o valor de y de (1) e substituindo em (2), concluímos que $\beta = u$ é solução de uma equação $a_1\,x^2 + a_2\,x + a_3 = 0$, com $a_1 \neq 0$ e $a_1, a_2, a_3 \in \Omega$. Então temos $a_2^2 - 4\,a_1\,a_3 \geq 0$.

Se $a_2^2 - 4\,a_1\,a_3 = 0$, tem-se $\beta = -\frac{a_2}{2\,a_1} \in \Omega$. Neste caso, obtemos $\Omega(\beta) = \Omega = \Omega(\sqrt{1})$.

Se $a_2^2 - 4\,a_1\,a_3 > 0$, então $\beta = \frac{-a_2 \mp \sqrt{a_2^2 - 4\,a_1\,a_3}}{2\,a_1}$, donde $\beta \in \Omega(\sqrt{a_2^2 - 4\,a_1\,a_3})$. Logo $\Omega(\beta) \subseteq \Omega(\sqrt{c})$, com $c = a_2^2 - 4\,a_1\,a_3 \in \Omega$. Como $\sqrt{c} = \mp(2\,a_1\,\beta + a_2)$, temos $\sqrt{c} \in \Omega(\beta)$ e, portanto, $\Omega(\beta) = \Omega(\sqrt{c})$.

c) Obtivemos P como um ponto de intersecção de duas circunferências distintas, construídas sobre pontos de $\mathcal{P}_0$.



Neste caso, (u, v) é solução de um sistema

$$\begin{cases} x^2 + y^2 + a\,x + b\,y + c = 0 \\ x^2 + y^2 + d\,x + e\,y + f = 0 \end{cases}$$

com $a, b, c, d, e, f \in \Omega$, em que $d \neq a$ ou $e \neq b$ (por serem circunferências distintas que se intersectam). Logo (u, v) é solução do sistema

$$\begin{cases} x^2 + y^2 + a\,x + b\,y + c = 0 \\ (d-a)\,x + (e-b)\,y + (f-c) = 0 \end{cases}$$

com $a, b, c, d-a, e-b, f-c \in \Omega$. Estamos, então, no caso da alínea b) e, portanto, $\Omega(\beta) = \Omega(\sqrt{c})$, para algum $c \in \Omega$ e $c > 0$. ∎

Observação. Analisando a demonstração do lema anterior, concluímos que, de um modo geral, se Ω é um subcorpo de $\mathbb{R}$ e $P \curvearrowright (u, v)$ é um ponto de $\mathbb{R}^2$ construído num passo a partir de rectas e circunferências que admitem equações cartesianas de coeficientes em Ω, então, dado $\beta \in \{u, v\}$, temos $\Omega(\beta) = \Omega(\sqrt{c})$, para algum $c \in \Omega$ tal que $c > 0$.

Notemos também que, nas condições do lema anterior, se $\Omega(u) = \Omega(\sqrt{c_1})$, com $c_1 \in \Omega$ e $c_1 > 0$, e $\Omega(v) = \Omega(\sqrt{c_2})$, com $c_2 \in \Omega$ e $c_2 > 0$, então

$$\begin{aligned} \Omega(u, v) &= \Omega(u)(v) = \Omega(\sqrt{c_1})(v) = \Omega(\sqrt{c_1}, v) \\ &= \Omega(v)(\sqrt{c_1}) = \Omega(\sqrt{c_2})(\sqrt{c_1}) = \Omega(\sqrt{c_1}, \sqrt{c_2}) \end{aligned}$$

Teorema 3. *Um número real α é construtível se e só se existir uma cadeia de subcorpos $\mathbb{Q} = \Omega_0 \subseteq \Omega_1 \subseteq \Omega_2 \subseteq \cdots \subseteq \Omega_n$ de $\mathbb{R}$ tais que*

1) $\alpha \in \Omega_n$;

2) $\Omega_{i+1} = \Omega_i(\sqrt{c_i})$, *onde* $c_i > 0$, $c_i \in \Omega_i$, *com* $i \in \{0, \ldots, n-1\}$.

Demonstração: Suponhamos que α é construtível e $\alpha \geq 0$. Então existem pontos construtíveis $P_0 = O\overset{\frown}{}(0,0)$, $P_1 = P\overset{\frown}{}(1,0)$, $P_2\overset{\frown}{}(x_2, y_2)$, $\ldots$, $P_{s-1} = (x_{s-1}, y_{s-1})$, $P_s = (\alpha, 0)$ tais que P_{i+1} é construtível por um passo a partir de $\{P_0, \ldots, P_i\}$, com $1 \leq i \leq s-1$, sendo $\alpha = d(P_0, P_s)$.

Consideremos a seguinte cadeia de subcorpos de $\mathbb{R}$:

$$\mathbb{Q} \subseteq \mathbb{Q}(x_2) \subseteq \mathbb{Q}(x_2, y_2) \subseteq \mathbb{Q}(x_2, y_2, x_3)\,\mathbb{Q}(x_2, y_2, x_3, y_3) \subseteq$$
$$\subseteq \cdots \subseteq \mathbb{Q}(x_2, y_2, \ldots, x_{s-1}, y_{s-1}) \subseteq \mathbb{Q}(x_2, y_2, \ldots, x_{s-1}, y_{s-1}, \alpha)$$

Atendendo ao Lema 2 e à última observação, cada um destes subcorpos, que designamos por Ω_{i+1}, é da forma $\Omega_i(\sqrt{c_i})$, para algum $c_i \in \Omega_i$ e $c_i > 0$, sendo α elemento do último subcorpo desta cadeia. Se $\alpha < 0$, então $-\alpha > 0$. Estamos assim nas condições anteriores. Obtemos Ω_n tal que $-\alpha \in \Omega_n$, pelo que $\alpha \in \Omega_n$.

Reciprocamente, admitamos que existe uma cadeia de subcorpos nas condições 1) e 2) do enunciado. Pretendemos provar que $\alpha \in K_0$.

Notemos que, de um modo geral, se F é um subcorpo de K_0, $c \in F$ e $c > 0$, então $F(\sqrt{c}) \subseteq K_0$, visto que $\sqrt{c} \in K_0$.

Assim, $\Omega_1 = \Omega_0(\sqrt{c_0}) = \mathbb{Q}(\sqrt{c_0}) \subseteq K_0$, donde $\Omega_2 = \Omega_1(\sqrt{c_1}) \subseteq K_0$. Sucessivamente, obtemos $\Omega_n \subseteq K_0$. Como $\alpha \in \Omega_n$, concluímos que $\alpha \in K_0$. ∎

Corolário 3.1. *Se* $\alpha \in \mathbb{R}$ *é construtível, então* α *é algébrico sobre* $\mathbb{Q}$ *e existe* $\ell \in \mathbb{N}_0$ *tal que* $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^\ell$.

Demonstração: Suponhamos que $\alpha \in \mathbb{R}$ é construtível. Consideremos uma cadeia do tipo da garantida pelo teorema anterior

$$\mathbb{Q} = \Omega_0 \subseteq \Omega_1 \subseteq \cdots \subseteq \Omega_n$$

com $\Omega_{i+1} = \Omega_i(\sqrt{c_i})$, $c_i \in \Omega_i$, $c_i > 0$, $\alpha \in \Omega_n$. Como $x^2 - c_i \in \Omega_i[x]$ e o polinómio $x^2 - c_i$ é anulador de $\sqrt{c_i}$, temos $[\Omega_{i+1} : \Omega_i] = 2^{k_i}$, em

que $k_i \in \{0, 1\}$. Portanto,

$$[\Omega_n : \mathbb{Q}] = [\Omega_n : \Omega_{n-1}] \cdots [\Omega_1 : \Omega_0] = 2^t$$

para algum $t \leq n$. Logo $[\Omega_n : \mathbb{Q}]$ é finita. Como

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \Omega_n$$

concluímos que $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ é finita e, além disso, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divide 2^t. Logo $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^\ell$, para algum ℓ tal que $0 \leq \ell \leq t$. Sendo $\mathbb{Q}(\alpha)$ extensão finita de $\mathbb{Q}$, então α é algébrico sobre $\mathbb{Q}$. ∎

4.2 Problemas

1. Duplicação do cubo

Dado um cubo, podemos construir, usando apenas régua e compasso, a aresta de um outro cubo cujo volume é o dobro do volume do primeiro?

Este problema reduz-se ao seguinte: dado um segmento de comprimento 1, podemos construir um segmento de comprimento a tal que $a^3 = 2$? De outro modo, existe algum número real a construtível tal que $a^3 = 2$?

Corolário 4. *O problema da duplicação do cubo não é resolúvel, usando apenas régua e compasso.*

Demonstração: Suponhamos que existe $a \in \mathbb{R}$ tal que $a^3 = 2$ e a é construtível. Então, pelo Corolário 3.1, temos $[\mathbb{Q}(a) : \mathbb{Q}] = 2^\ell$, para algum $\ell \in \mathbb{N}_0$. Ora a é raiz do polinómio $x^3 - 2 \in \mathbb{Q}[x]$, o qual é irredutível em $\mathbb{Q}[x]$, donde $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. Assim, obtemos $3 = 2^\ell$ para algum $\ell \geq 0$, o que é absurdo. Logo o problema não é resolúvel. ∎

2. Quadratura do círculo

É possível construir, com régua e compasso, o lado de um quadrado com área igual à área de um círculo dado?

Este problema reduz-se ao seguinte: dado um segmento de comprimento 1, podemos construir um segmento de comprimento a tal que $a^2 = \pi$? Ou seja, existe um número real a construtível tal que $a^2 = \pi$?

Corolário 5. *O problema da quadratura do círculo não é resolúvel, usando apenas régua e compasso.*

Demonstração: Suponhamos que existe $a \in \mathbb{R}$ construtível tal que $a^2 = \pi$. Então a^2 é construtível, donde π é construtível. Então, pelo Corolário 3.1, o real π é algébrico sobre $\mathbb{Q}$, o que, como já sabemos, é falso. Logo o problema não é resolúvel. ∎

3. Trissecção de um ângulo

É possível dividir um ângulo em três partes iguais, usando apenas régua e compasso?

Corolário 6. *O ângulo $\frac{\pi}{3}$ não pode ser trissectado usando apenas régua e compasso.*

Demonstração: Esta questão equivale a provar que o ponto $A\,\overset{\frown}{}\,(\cos\frac{\pi}{9}, \operatorname{sen}\frac{\pi}{9})$ não é construtível. Observemos que se tal ponto fosse construtível, então $(\cos\frac{\pi}{9}, 0)$ também o seria e, portanto, $\cos\frac{\pi}{9}$ seria um real construtível. Mostremos que $\cos\frac{\pi}{9}$ não é construtível.

Comecemos por recordar que $\cos(3\,z) = 4\cos^3 z - 3\cos z$, para qualquer $z \in \mathbb{R}$. Em particular, tomando $z = \frac{\pi}{9}$ obtemos

$$\cos\frac{\pi}{3} = 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9}$$

e, como $\cos\frac{\pi}{3} = \frac{1}{2}$, obtemos $1 = 8\cos^3\frac{\pi}{9} - 6\cos\frac{\pi}{9}$, donde $2\cos\frac{\pi}{9}$ é raiz do polinómio $x^3 - 3\,x - 1 \in \mathbb{Q}[x]$. Ora, se este polinómio de grau 3 tivesse raízes racionais elas seriam 1 ou -1, o que não se verifica. Portanto, $x^3 - 3\,x - 1$ é irredutível em $\mathbb{Q}[x]$ e $\left[\mathbb{Q}\left(2\cos\frac{\pi}{9}\right) : \mathbb{Q}\right] = 3$. Assim, concluímos, pelo Corolário 3.1, que $2\cos\frac{\pi}{9}$ não é construtível, pelo que $\cos\frac{\pi}{9}$ também o não é (uma vez que 2 é construtível). Logo,

não é possível trissectar o ângulo $\frac{\pi}{3}$ com régua e compasso. ∎

É claro que podemos trissectar alguns ângulos com régua e compasso.

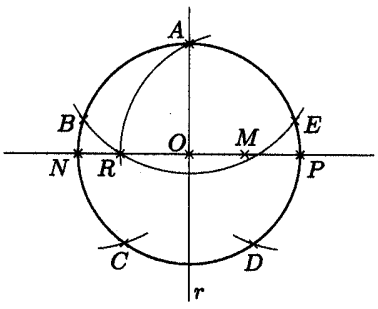
Exemplos.

1) O ângulo $\frac{\pi}{2}$ pode ser trissectado. Uma vez que $\operatorname{sen}\frac{\pi}{6} = \frac{1}{2}$, trissectar o ângulo $\frac{\pi}{2}$ corresponde a determinar os pontos de intersecção da circunferência com centro na origem e raio 1 com a recta paralela ao eixo dos $\overline{XX}$ que passa pelo ponto $(0, \frac{1}{2})$.

2) O ângulo de 27° pode ser trissectado. De facto, podemos provar que o pentágono regular é construtível, pelo que podemos obter o ângulo de 72°. Bissectando, sucessivamente, obtemos os ângulos de 36°, 18° e 9°.

Construção geométrica do pentágono regular

Consideremos



1) $\mathcal{C} = \mathcal{C}(O; P)$;
2) diâmetro $[NP]$ de $\mathcal{C}$;
3) ponto médio M de $[OP]$;
4) $r \perp \overline{NP}$ com $O \in r$;
5) $A \in \mathcal{C} \cap r$;
6) $\mathcal{C}(M; A)$;
7) $R \in [NO] \cap \mathcal{C}(M; A)$;
8) $\mathcal{C}(A; R)$;
9) $E, B \in \mathcal{C} \cap \mathcal{C}(A; R)$;
10) $\mathcal{C}(B; \text{raio} = |AR|)$;
11) $\mathcal{C}(E; \text{raio} = |AR|)$;
12) $C \in \mathcal{C} \cap \mathcal{C}(B; \text{raio} = |AR|)$;
13) $D \in \mathcal{C} \cap \mathcal{C}(E; \text{raio} = |AR|)$.

Prova-se que o pentágono fica determinado pelos pontos A, B, C, D, E. ∎

Sendo o pentágono regular construtível, o ângulo de 72° também o é, já que esta é a medida de $\widehat{AOE}$.

Nota. Não é possível construir com régua e compasso um polígono regular com um número n arbitrário de lados. Por exemplo, tal não é possível se tomarmos $n = 7$. (Justifique este facto, provando que $2\cos\frac{2\pi}{7}$ é raiz do polinómio $x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$.)

Podemos efectuar, usando régua e compasso, uma divisão *aproximada* da circunferência num número arbitrário de n partes iguais, mas nem sempre é possível efectuar uma divisão exacta: tal é o caso quando $n = 7$.

De facto, Gauss provou o seguinte resultado, cuja demonstração aqui omitimos (ver Stewart, Brison).

Teorema 7. *Um polígono regular com n lados é construtível com régua e compasso se e só se $n = 2^r\, p_1 \cdots p_s$, onde $r, s \in \mathbb{N}_0$ e $p_1, \ldots, p_s$ são primos distintos da forma $p_i = 2^{2^{r_i}} + 1$, com $r_i \in \mathbb{N}_0$ $(i = 1, \ldots, s)$.* ∎

Observemos a seguinte tabela:

r_i	p_i
0	3
1	5
2	17
3	257
⋮	⋮

Verificamos que 7 não se pode escrever na forma dada pelo teorema, confirmando que não podemos construir com régua e compasso um heptágono regular. Podemos, no entanto, construir por exemplo um hexágono regular já que $6 = 2 \cdot 3$.

Exercícios

1. Indique, justificando, quais dos seguintes números reais são construtíveis:

   a) $1/\pi$

   b) $\sqrt[3]{2}+5$

   c) $\sqrt[3]{2+\sqrt[3]{6}}$

   d) $\sqrt[4]{5}-\sqrt{7}$

   e) $\frac{\sqrt[3]{7}}{\sqrt{10}}$

   f) $\sqrt[3]{-27}$

   g) $\sqrt{3}+e$

   h) $3\,\mathrm{sen}\,\frac{2\pi}{9}$

   i) $\sqrt[4]{\sqrt[6]{4}+\sqrt[4]{3+\sqrt{2}}+7-\sqrt[3]{2}}$.

2. O ângulo $\frac{19\pi}{6}$ pode ser trissectado usando apenas régua e compasso?

3. Mostre que $\alpha = \mathrm{sen}\,\frac{2\pi}{3}$ é algébrico sobre $\mathbb{Q}$ e calcule $[\mathbb{Q}(\alpha):\mathbb{Q}]$. Diga, justificando, se α é construtível.

4. Considere o polinómio $f(x) = x^5 + \frac{3}{2}x^4 + 6x^2 + 6$.

   a) Mostre que $\mathbb{Q}[x]/\langle f(x)\rangle$ é um corpo.

   b) Prove que existe $\alpha \in \mathbb{R}$ tal que o corpo $\mathbb{Q}(\alpha)$ é isomorfo a $\mathbb{Q}[x]/\langle f(x)\rangle$.

   c) Indique uma base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.

   d) Será que $\sqrt{3}+\frac{2}{3}\alpha$ é um número real construtível?

5. Considere um referencial ortonormado de $\mathbb{R}^3$ e os pontos $A \curvearrowright (2, b, 0)$, $B \curvearrowright (-2, -b, 0)$ e $C \curvearrowright (0, 0, b)$.

   a) Determine o volume $V(b)$ do cone de vértice C e cuja base tem diâmetro $|AB|$.

   b) Verifique se existe $b \in \mathbb{R}$ construtível tal que $V(b) = 2\pi$.

Apêndice

Este apêndice é dedicado a um breve estudo de alguns conceitos e resultados da Teoria dos Conjuntos e, em particular, dos Cardinais.

Começamos por recordar algumas definições básicas e enunciar os Axiomas da Escolha, da Boa Ordenação e o Lema de Zorn.

Sejam A e B conjuntos. O *produto cartesiano* $A \times B$ de A por B é o conjunto dos pares ordenados (a, b) em que $a \in A$ e $b \in B$.

Uma *relação binária* R em A é uma parte do produto cartesiano $A \times A$. Dados $x, y \in A$ por vezes escrevemos $x\,R\,y$ em vez de $(x, y) \in R$. Uma tal relação diz-se uma *equivalência* se é *reflexiva*, isto é $x\,R\,x$ para qualquer $x \in A$; *simétrica*, ou seja $x\,R\,y$ implica $y\,R\,x$ para qualquer $x, y \in A$; e também *transitiva*, isto é $x\,R\,y$ e $y\,R\,z$ implicam $x\,R\,z$ para quaisquer $x, y, z \in A$. Se R é uma equivalência em A, dado $x \in A$ designamos por *classe de equivalência* de x o conjunto $\{y \in A : x\,R\,y\}$ dos elementos R-relacionados com x. Representamos a classe de x por $[x]_R$ ou apenas por $[x]$ se não houver ambiguidade. Uma *ordem parcial* em A é uma relação binária $\leq$ que é reflexiva, transitiva e *anti-simétrica*, isto é $x \leq y$ e $y \leq x$ implicam $x = y$, para quaisquer $x, y \in A$. Uma ordem parcial em A diz-se *total* se quaisquer elementos $x, y \in A$ são *comparáveis*, significando $x \leq y$ ou $y \leq x$, neste caso $(A, \leq)$ diz-se uma *cadeia*.

Seja A um conjunto com uma relação de ordem parcial $\leq$. Dado $A' \subseteq A$ dizemos que $a_0 \in A'$ é *elemento mínimo* [*máximo*] de A' se $a_0 \leq a'$ [$a' \leq a_0$], para qualquer $a' \in A'$. Dizemos também que A' tem um *minorante* $m \in A$ [*majorante*] se $m \leq a'$ [$a' \leq m$] para

qualquer $a' \in A'$. Um elemento $a \in A$ diz-se *minimal* [*maximal*] se $x \leq a$ [$a \leq x$] implica $x = a$, para qualquer $x \in A$.

Uma relação de ordem parcial num conjunto A tal que qualquer parte não vazia tem elemento mínimo diz-se uma *boa ordem*. Neste caso, A diz-se a um *conjunto bem ordenado*. Por exemplo, com a relação $\leq$ usual, o conjunto $\mathbb{N}$ é um conjunto bem ordenado mas o mesmo não acontece com $\mathbb{R}$ embora $(\mathbb{R}, \leqslant)$ seja uma cadeia. É claro que todo o conjunto bem ordenado é uma cadeia.

Uma *aplicação* f de A em B pode ser definida como sendo um subconjunto de $A \times B$ em que para qualquer $a \in A$ existe um único $b \in B$ tal que $(a, b) \in f$. Escrevemos $f : A \to B$, $a \mapsto b$ e, dado $a \in A$, denotamos b por $f(a)$ designando $f(a)$ por *imagem* de a. Dada $f : A \to B$, o conjunto das imagens de todos os elementos de A designa-se por $f(A)$. Uma aplicação $f : A \to B$ diz-se *injectiva* se, para quaisquer $a_1, a_2 \in A$,

$$f(a_1) = f(a_2) \;\Rightarrow\; a_1 = a_2$$

Neste caso, escrevemos $f : A \hookrightarrow B$. Dizemos que f é *sobrejectiva* se

$$\forall\, b \in B, \quad \exists\, a \in A, \quad b = f(a)$$

caso em que escrevemos $f : A \twoheadrightarrow B$. Uma aplicação diz-se *bijectiva* se for injectiva e sobrejectiva.

Dados conjuntos A e B, designamos por A^B o conjunto das aplicações de B em A. Temos $\emptyset^\emptyset = \{\emptyset\}$, $A^\emptyset = \{\emptyset\}$ e $\emptyset^A = \emptyset$ se $A \neq \emptyset$.

Proposição 1. *Se A e B são conjuntos não vazios, existe uma aplicação injectiva de A para B se e só se existe uma aplicação sobrejectiva de B para A.*

Demonstração: Seja $f\colon A \hookrightarrow B$ injectiva. Fixemos $a \in A \neq \emptyset$. Como f é injectiva, podemos definir a aplicação

$$\begin{aligned} g\colon\ & B \longrightarrow\!\!\!\!\!\rightarrow A \\ & b \in \operatorname{Im} f \mapsto f^{-1}(b), \text{ único elemento de } A \text{ que se aplica em } b \text{ por } f, \\ & b \notin \operatorname{Im} f \mapsto a\ . \end{aligned}$$

Esta aplicação g é sobrejectiva.

Reciprocamente, seja $g\colon B \twoheadrightarrow A$ sobrejectiva. Consideremos a família $\{g^{-1}(a)\}_{a\in A}$ de subconjuntos de B, sendo

$$g^{-1}(a) = \{b \in B\colon g(b) = a\} \text{ a pré-imagem de } a \text{ por } g\ .$$

Como g é sobrejectiva, cada $g^{-1}(a)$ é não vazio. Então, podemos fixar *simultaneamente* elementos $b_a \in g^{-1}(a)$, para cada $a \in A$. Definimos agora a aplicação

$$\begin{aligned} f\colon\ & A \hookrightarrow B \\ & a \mapsto b_a \end{aligned}$$

Esta aplicação f é injectiva. ∎

O que permite garantir que nesta demonstração podemos fixar simultaneamente elementos b_a, para cada $a \in A$? O Axioma da Escolha, também conhecido por Axioma de Zermelo!

Axioma da escolha. *Se A é um conjunto não vazio e $(X_i)_{i\in I}$ é uma família de subconjuntos não vazios de A indexada num conjunto I, então podemos fixar simultaneamente um elemento x_i em cada X_i, ou seja, existe uma aplicação*

$$\varphi\colon I \to \bigcup X_i$$

tal que $\varphi(i) \in X_i$, para qualquer $i \in I$.

Este axioma é de facto equivalente a outras proposições nomeadamente ao Axioma da Boa Ordenação e ao Lema de Zorn [ver Ferreira, Halmos, Monteiro, Ramalho].

Axioma da boa ordenação. *Todo o conjunto A admite uma boa ordem.*

Lema de Zorn. *Se A é um conjunto não vazio parcialmente ordenado no qual toda a cadeia não vazia tem majorante, então A tem elemento maximal.*

É também frequente ver-se o Lema de Zorn enunciado do seguinte modo: Se A é um conjunto parcialmente ordenado no qual toda a cadeia tem majorante, então A tem elemento maximal. Estas versões são equivalentes.

Teorema 2. *O Axioma da Escolha, o Axioma da Boa Ordenação e o Lema de Zorn são equivalentes.*

Chamamos a atenção do leitor para o facto de, neste texto, usarmos livremente o Axioma da Escolha.

Cardinais

Dados conjuntos A e B, dizemos que A e B têm a *mesma cardinalidade*, ou que são *equipotentes*, se existe uma bijecção entre A e B. Neste caso, escrevemos $A \sim B$.

No que se segue, vamos admitir o *Axioma dos Cardinais* (também conhecido por *Hipótese de Cantor*) como verdadeiro.

Axioma dos cardinais. *Para qualquer conjunto A, existe um conjunto, chamado* cardinal *de A e denotado por $\#A$, tal que*

$$\#A \sim A$$
$$\#A = \#B \iff A \sim B$$

É usual, também, denotar $\#A$ por $\text{card}(A)$ ou por $|A|$.

Prova-se que o Axioma dos Cardinais é consequência de outros axiomas da Teoria dos Conjuntos, mas tal facto sai do âmbito desta disciplina [ver Ferreira, Halmos, Oliveira].

Com o devido cuidado e para simplificar a escrita, se $A = \{1, \ldots, n\}$ denotamos $\#A$ por n e se $A = \emptyset$ denotamos $\#A$ por 0.

É fácil verificar que a relação de equipotência $\sim$ é uma equivalência na classe de todos os conjuntos. Note-se que falamos na classe de todos os conjuntos e não no conjunto de todos os conjuntos porque tal classe não é um conjunto.

Paradoxo de Russell. *É absurdo falar no conjunto de todos os conjuntos.*

Demonstração: Admitamos que existe o conjunto de todos os conjuntos, digamos $\mathcal{A}$. Seja $\mathcal{B} = \{x \in \mathcal{A} : \ x \notin x\}$.

Se $\mathcal{A}$ é conjunto, como $x \notin x$ é uma condição, pelo Axioma da Separação da Teoria dos Conjuntos [ver Halmos, Ferreira] concluímos que $\mathcal{B}$ é um conjunto. Logo $\mathcal{B} \in \mathcal{B}$ ou $\mathcal{B} \notin \mathcal{B}$. Se $\mathcal{B} \in \mathcal{B}$ então, por definição de $\mathcal{B}$, temos $\mathcal{B} \notin \mathcal{B}$. Se $\mathcal{B} \notin \mathcal{B}$ então, outra vez por definição de $\mathcal{B}$, obtemos $\mathcal{B} \in \mathcal{B}$. A contradição resulta do facto de termos admitido que $\mathcal{A}$ é um conjunto. ∎

Definição. Dados conjuntos A e B, dizemos que $\#A$ é *menor ou igual* a $\#B$, e escrevemos $\#A \leq \#B$, se existe uma aplicação injectiva de A em B.

Escrevemos $\#A < \#B$ quando $\#A \leq \#B$ e $\#A \neq \#B$.

Observemos que, para qualquer conjunto B, existe sempre uma aplicação injectiva de $\emptyset$ para B, que é a aplicação vazia, pelo que $0 \leq \#B$.

Atendendo à Proposição 1, é claro que

Proposição 3. *Se A e B são conjuntos não vazios, então $\#A \leq \#B$ se e só se existe uma aplicação sobrejectiva de B em A.*

No que se segue, é fundamental ter presente o resultado seguinte [ver Ferreira, Halmos, Monteiro, Oliveira, Ramalho].

Lema de Schröder–Bernstein. (Anti-simetria) *Dados conjuntos A e B, tem-se*

$$\#A \leq \#B \ \text{ e } \ \#B \leq \#A \quad \text{ se e só se } \quad \#A = \#B \ .$$

O teorema seguinte é conhecido por propriedade tricotómica da relação $\leq$ entre cardinais [ver Ferreira, Monteiro] e permite-nos con-

cluir que a relação $\leq$ é uma ordem total na classe dos cardinais, de facto, prova-se que é mesmo uma boa ordem.

Teorema 4. (Tricotomia) *Quaisquer cardinais α e β são comparáveis, isto é,*

$$\alpha = \beta \;\; ou \;\; \alpha < \beta \;\; ou \;\; \beta < \alpha \; .$$

Este último teorema é equivalente ao Axioma da Escolha.

Designamos por $\mathcal{P}(A)$ o conjunto dos subconjuntos de um conjunto A.

Teorema de Cantor. *Dado um conjunto A, tem-se*

$$\#\{0,1\}^A = \#\mathcal{P}(A) \quad e \quad \#A < \#\mathcal{P}(A).$$

Demonstração: Para provarmos que $\#\{0,1\}^A = \#\mathcal{P}(A)$ basta vermos que a *aplicação característica*

$$\begin{array}{rl} \chi : \mathcal{P}(A) \longrightarrow \{0,1\}^A & \\ A' \longmapsto \chi_{A'} : & \begin{array}{ccc} A & \longrightarrow & \{0,1\} \\ x \in A' & \mapsto & 1 \\ x \notin A' & \mapsto & 0 \end{array} \end{array}$$

é uma bijecção (os elementos de A com imagem 1 por $\chi_{A'}$ são exactamente os que estão em A' e toda a aplicação $f : A \to \{0,1\}$ fica perfeitamente definida pelo conjunto $1f^{-1}$ imagem inversa de 1). Observemos, em particular, o caso em que $A = \emptyset$. Temos $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\{0,1\}^{\emptyset} = \{\emptyset\}$ sendo $\chi_{\emptyset} : \emptyset \to \{\emptyset\}$ a aplicação vazia.

Provemos que $\#A < \#\mathcal{P}(A)$. Em primeiro lugar, observemos que $\#A \leq \#\mathcal{P}(A)$ pois a aplicação $f : A \to \mathcal{P}(A)$, $x \mapsto \{x\}$, é injectiva. Admitamos agora que $\#A = \#\mathcal{P}(A)$. Então existe $g : A \to \mathcal{P}(A)$ bijecção. Seja $A' = \{a \in A : a \notin g(a)\}$. Como g é sobrejectiva, existe $b \in A$ tal que $g(b) = A'$. Se $b \in A'$ temos $b \notin g(b)$ o que é absurdo,

e se $b \notin A'$ então $b \in g(b)$ novamente absurdo. Assim, g não existe. Portanto, $\#A \neq \#\mathcal{P}(A)$. ∎

Embora não tenhamos ainda definido conjuntos infinitos, nesta altura, é conveniente chamar a atenção do leitor para o seguinte facto: dado um conjunto infinito A apesar de se ter $\#A < \#\mathcal{P}(A)$, pelo Teorema de Cantor, tem-se $\#A = \#\mathcal{P}_F(A)$, em que $\mathcal{P}_F(A)$ designa o conjunto dos subconjuntos finitos de A [ver Ferreira, Halmos].

Exemplos.

1) Seja $\mathbb{P}$ o conjunto dos números naturais pares. Então $\#\mathbb{N} = \#\mathbb{P}$, pois $\theta\colon \mathbb{N} \to \mathbb{P}$, $n \mapsto 2\,n$, é uma bijecção.

2) Analogamente, $\#\mathbb{N} = \#\mathbb{I}$, em que $\mathbb{I}$ designa o conjunto dos números naturais ímpares.

3) Temos $\#[0,1] = \#[a,b]$, para quaisquer $a, b \in \mathbb{R}$ tais que $a < b$, pois a aplicação $\theta\colon [0,1] \to [a,b]$, $x \mapsto a + x(b-a)$, é uma bijecção.

Definição. Um conjunto A tal que $\#A = \#\mathbb{N}$ diz-se *numerável*.

O cardinal de $\mathbb{N}$ representa-se por $\aleph_0$. (Recorde-se que $\aleph$ é a primeira letra do alfabeto hebraico.)

Definição. Um conjunto A diz-se *finito* se é vazio ou é equipotente a $\{1, \ldots, n\}$, para algum $n \in \mathbb{N}$. Um conjunto diz-se *infinito* se não for finito.

Admitiremos como conhecidos alguns resultados referentes a conjuntos finitos [ver Ferreira], nomeadamente:

a) Dados $n, p \in \mathbb{N}$,

$$\{1, \ldots, n\} \sim \{1, \ldots, p\} \quad \text{se e só se} \quad n = p\ ;$$

b) Se A é um conjunto finito e $A' \subseteq A$ é tal que $A' \sim A$, então $A = A'$, isto é equivalente a dizer que se A é equipotente a

uma sua parte própria então A é infinito;

c) Toda a parte de um conjunto finito é finita, o que equivale a dizer que se um conjunto contém uma parte infinita, então é infinito;

d) Se A é um conjunto finito, então $\#A \leq \aleph_0$, pelo que $n \leq \aleph_0$, para qualquer $n \in \mathbb{N}$;

e) Dado $n \in \mathbb{N}$, não existe uma aplicação injectiva de $\mathbb{N}$ em $\{1, \ldots, n\}$, donde $\aleph_0 \not\leq n$ e portanto $n < \aleph_0$.

Exemplo.

Os conjuntos $\mathbb{N}$ e $\mathbb{P}$ são infinitos, atendendo à afirmação e) e ao facto de termos $\#\mathbb{P} = \#\mathbb{N}$.

Proposição 5. *Seja A um conjunto infinito. Então $\#\mathbb{N} \leq \#A$.*

Demonstração: Definimos, por recorrência, a seguinte aplicação

$$\begin{aligned} f\colon\ & \mathbb{N} \to A \\ & 1 \mapsto a_1, \quad \text{elemento escolhido em } A, \\ & 2 \mapsto a_2, \quad \text{elemento escolhido em } A\backslash\{a_1\}, \\ & n \mapsto a_n, \quad \text{elemento escolhido em } A\backslash\{a_1, \ldots, a_{n-1}\}. \end{aligned}$$

Note-se que $A \neq \emptyset$ porque A é infinito e que $A\backslash\{a_1\} \neq \emptyset$ pois, caso contrário, $A = \{a_1\}$, donde A seria finito. Admitindo $f(i)$ definido, para qualquer $i \leq n$, definimos $f(n+1)$ como sendo um elemento escolhido em $A\backslash\{f(1), \ldots, f(n)\}$, conjunto também não vazio pois, caso contrário, teríamos mais uma vez A finito.

É claro que f é injectiva e, portanto, $\#\mathbb{N} \leq \#A$. ∎

De facto, a condição recíproca da proposição anterior também se verifica.

Teorema 6. *Seja A um conjunto. Então*

$$A \text{ é infinito } \textit{ se e só se } \ \#\mathbb{N} \leq \#A\ .$$

Demonstração: Suponhamos que $\#\mathbb{N} \leq \#A$. Neste caso, existe uma aplicação $f\colon \mathbb{N} \hookrightarrow A$ injectiva. Logo $A \neq \emptyset$.

Admitamos que A é finito. Existe $n \in \mathbb{N}$ tal que $A \sim \{1, \ldots, n\}$ pelo que podemos tomar uma bijecção g de A em $\{1, \ldots, n\}$. A composição $g \circ f$ é pois uma aplicação injectiva de $\mathbb{N}$ em $\{1, \ldots, n\}$, o que é absurdo pelo Resultado e). Portanto A é infinito. ∎

Exemplos.

1) O conjunto $\mathbb{N}\times\mathbb{N}$ é infinito. Mais ainda, $\#(\mathbb{N}\times\mathbb{N}) = \#\mathbb{N}$.

2) Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ e $\mathcal{P}(\mathbb{N})$ também são infinitos.

Com o objectivo de definir operações entre cardinais, recordemos, agora, algumas propriedades entre conjuntos. Ao escrevermos $A \dot\cup B$ estamos a indicar que a união é disjunta, isto é, $A \cap B = \emptyset$.

Sejam A, B, C e D conjuntos tais que $A \sim C$ e $B \sim D$. Então

a) Se $A \cap B = \emptyset$ e $C \cap D = \emptyset$, temos $A \dot\cup B \ \sim \ C \dot\cup D$;

b) $A\times B \sim C\times D$;

c) $A^B \sim C^D$.

Notemos também que dados conjuntos A e B, podemos sempre considerar conjuntos A' e B' equipotentes a A e B, respectivamente, tais que $A' \cap B' = \emptyset$. Basta, por exemplo, tomar $A' = A\times\{1\}$ e $B' = B\times\{2\}$.

Face a estas propriedades é possível definir operações de adição, multiplicação e potenciação entre cardinais.

Definição. Sejam α e β cardinais. Definimos

a) $\alpha + \beta = \#(A \dot\cup B)$, em que $\alpha = \#A$, $\beta = \#B$ e $A \cap B = \emptyset$;

b) $\alpha\beta = \#(A\times B)$, em que $\alpha = \#A$ e $\beta = \#B$;

c) $\alpha^\beta = \#A^B$, em que $\alpha = \#A$ e $\beta = \#B$.

O Teorema de Cantor diz-nos, pois, que $\alpha < 2^\alpha$, para qualquer cardinal α.

Nos Exercícios 5 e 6 estão descritas as propriedades destas operações as quais devemos ter presentes no que se segue.

Uma *sucessão* $(a_i)_{i\in I}$ de elementos a_i, com $i \in I$, diz-se *numerável* se I é um conjunto numerável.

Teorema 7. *Seja $(A_i)_{i\in I}$ uma sucessão numerável de conjuntos numeráveis A_i, com $i \in I$. Então $\bigcup_{i\in I} A_i$ é numerável.*

Demonstração: Seja $i \in I$. Como A_i é numerável, A_i é equipotente a $\mathbb{N}$ e podemos escrever

$$A_i = \Big\{a_{i1}, a_{i2}, \ldots, a_{in}, \ldots\Big\}$$

em que $a_{ik} \neq a_{i\ell}$ sempre que $k \neq \ell$, para quaisquer $k, \ell \in \mathbb{N}$.

Seja

$$f\colon I\times\mathbb{N} \to A = \bigcup_{i\in I} A_i, \;\; (i,n) \mapsto a_{in}$$

Então f é uma aplicação sobrejectiva, donde $\#A \leq \#(I\times\mathbb{N})$. Ora, $\#(I\times\mathbb{N}) = \#I\#\mathbb{N} = \#\mathbb{N}\#\mathbb{N} = \#(\mathbb{N}\times\mathbb{N}) = \#\mathbb{N}$, donde $\#A \leq \#\mathbb{N}$.

Por outro lado, como $A_i \subseteq A$, obtemos $\#\mathbb{N} = \#A_i \leq \#A$. Logo, pelo Lema de Schröder–Bernstein, $\#A = \#\mathbb{N}$. ∎

Já observámos que $\#(\mathbb{N}\times\mathbb{N}) = \#\mathbb{N}$, queremos agora mostrar que, para qualquer conjunto infinito A, também se tem $\#(A\times A) = \#A$.

Comecemos por enunciar um lema, que o leitor poderá provar facilmente.

Lema 8. **a**) *Se α é um cardinal, $\alpha+\alpha = 2\,\alpha$ e $\alpha+\alpha+\alpha = 3\,\alpha$.*

b) *Se α, β e γ são cardinais tais que $\alpha < \beta$, então*

$$\alpha+\gamma \leq \beta+\gamma \quad e \quad \alpha\,\gamma \leq \beta\,\gamma$$

Teorema 9. *Seja A um conjunto infinito. Então $\#(A\times A) = \#A$.*

Demonstração: Nesta prova vamos usar o Lema de Zorn. Consideremos o conjunto

$$\mathcal{F} = \Big\{ f\colon\ X\times X \hookrightarrow X\colon\ \ X \subseteq A \ \text{ e } \ X \text{ é infinito} \Big\}$$

Começamos por mostrar que $\mathcal{F} \neq \emptyset$. Como A é infinito, pelo Teorema 6, temos $\#\mathbb{N} \leq \#A$. Assim, existe uma aplicação injectiva $g\colon\ \mathbb{N} \hookrightarrow A$. Tomemos $X_0 = g(\mathbb{N})$. Então $\#X_0 = \#\mathbb{N}$, donde X_0 é um subconjunto infinito de A e

$$\#(X_0\times X_0) = \#X_0\#X_0 = \#\mathbb{N}\#\mathbb{N} = \#(\mathbb{N}\times\mathbb{N}) = \#\mathbb{N} = \#X_0$$

Logo, existe uma bijecção $g_0 :\ X_0\times X_0 \hookrightarrow\!\!\!\!\rightarrow X_0$. Temos $g_0 \in \mathcal{F}$ e, portanto, $\mathcal{F} \neq \emptyset$.

Em $\mathcal{F}$, introduzimos uma relação de ordem parcial $\leq$ definida por: dados $f, g \in \mathcal{F}$,

$$f \leq g \quad \text{ se e só se } \ g \text{ é extensão de } f$$

Dados $f, g \in \mathcal{F}$, dizer que g é extensão de f significa que, sendo $g\colon\ X\times X \hookrightarrow X$ e $f\colon\ Y\times Y \hookrightarrow Y$, temos $Y \subseteq X$ e $f(a,b) = g(a,b)$, para qualquer $(a,b) \in Y\times Y$.

Vamos provar que $\mathcal{F}$ tem um elemento maximal $\theta\colon\ M\times M \hookrightarrow M$, sendo M um subconjunto infinito de A.

Seja $\mathcal{C} \neq \emptyset$ uma cadeia em $(\mathcal{F}, \leq)$. Suponhamos que $\mathcal{C} = \{f_\alpha\}_{\alpha\,\in\,I}$, com $f_\alpha : X_\alpha \times X_\alpha \hookrightarrow X_\alpha$.

Tomemos $\mathcal{X} = \bigcup_{\alpha\in I} X_\alpha$. Pretendemos definir uma aplicação de $\mathcal{X}\times\mathcal{X}$ em $\mathcal{X}$. Sejam $a \in X_\alpha$ e $b \in X_\beta$. Como $\mathcal{C}$ é uma cadeia, temos $f_\alpha \leq f_\beta$ ou $f_\beta \leq f_\alpha$. Admitamos, sem perda de generalidade,

que $f_\alpha \leq f_\beta$. Neste caso, $X_\alpha \subseteq X_\beta$ pelo que $a, b \in X_\beta$ e $f_\beta(a,b)$ está definido. Notemos que se $\gamma \in I$ é tal que $a, b \in X_\gamma$, então $f_\gamma(a,b)$ também está definido e, como $f_\beta \leq f_\gamma$ ou $f_\gamma \leq f_\beta$, temos $f_\gamma(a,b) = f_\beta(a,b)$. Estas observações permitem definir a aplicação

$$\begin{aligned} f\colon\ & \mathcal{X}\times\mathcal{X} \to \mathcal{X} \\ & (a,b) \mapsto f_\alpha(a,b), \quad \text{em que } \ \alpha \in I \ \text{ e } \ a,b \in X_\alpha \end{aligned}$$

Provemos que f é injectiva. Suponhamos que $(a,b),(c,d) \in \mathcal{X}\times\mathcal{X}$ são tais que $f(a,b) = f(c,d)$. Sejam $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in I$ tais que $a \in X_{\alpha_1}$, $b \in X_{\alpha_2}$, $c \in X_{\alpha_3}$ e $d \in X_{\alpha_4}$. Como $\mathcal{C}$ é cadeia, entre os quatro elementos $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ existe um, que denotaremos por β, tal que $f_{\alpha_i} \leq f_\beta$, com $i \in \{1,2,3,4\}$. Então $a, b, c, d \in X_\beta$, $f(a,b) = f_\beta(a,b)$ e $f(c,d) = f_\beta(c,d)$. Como f_β é injectiva, concluímos que $(a,b) = (c,d)$.

Uma vez que dado $\alpha \in I$, o conjunto X_α é infinito, temos $\mathcal{X}$ infinito. Portanto, $f \in \mathcal{F}$.

Observemos agora que $f_\alpha \leq f$, para qualquer $\alpha \in I$, pelo que f é um majorante de $\mathcal{C}$. Então, pelo Lema de Zorn, podemos garantir que $\mathcal{F}$ tem pelo menos um elemento maximal $\theta\colon\ M\times M \hookrightarrow M$.

Como θ é injectiva, $\#(M\times M) \leq \#M$. Por outro lado, $\#M \leq \#(M\times M)$ e, portanto, pelo Lema de Schröder–Bernstein, obtemos $\#(M\times M) = \#M$.

É nosso objectivo demonstrar que $\#A = \#M$.

Comecemos por provar que $\#(A\backslash M) < \#M$. Pelo Teorema 4, temos $\#(A\backslash M) < \#M$ ou $\#M \leq \#(A\backslash M)$.

Admitamos que $\#M \leq \#(A\backslash M)$. Então existe $Y \subseteq A\backslash M$ tal que $Y \sim M$. Logo $\#Y = \#M$. Como M é infinito, $Y \neq \emptyset$.

Consideremos os conjuntos $M\times Y$, $Y\times M$ e $Y\times Y$. Como $Y \subseteq A\backslash M$, estes conjuntos são disjuntos dois a dois. Seja

$$W = (M\times Y) \,\dot\cup\, (Y\times M) \,\dot\cup\, (Y\times Y)$$

De $\#Y = \#M$ e $\#(M\times M) = \#M$, concluímos que os conjuntos $M\times Y$, $Y\times M$ e $Y\times Y$ têm cardinal $\#M$ e, portanto,

$$\#W = \#M + \#M + \#M \ .$$

Pelo Lema 8.a), obtemos $\#W = 3\,\#M$

Agora, como $\#M$ é infinito, temos $3 < \#M$, pelo que $3\,\#M \leq \#M\,\#M$, pelo Lema 8.b). Então $3\,\#M \leq \#M$ e, como $\#M \leq 3\,\#M$, pelo Lema de Schröder–Bernstein obtemos $3\,\#M = \#M$. Portanto, $\#W = \#M = \#Y$.

Seja $g\colon W \rightarrowtail Y$ uma bijecção. Notemos que

$$(M \dot\cup Y)\times(M \dot\cup Y) = (M\times M) \dot\cup W$$

Definamos a seguinte aplicação

$$\begin{aligned}\psi\colon\ (M \dot\cup Y)\times(M \dot\cup Y) &\to M \dot\cup Y\\ (a,b) \in W &\mapsto g(a,b)\\ (a,b) \in M\times M &\mapsto \theta(a,b)\end{aligned}$$

É claro que ψ é uma aplicação injectiva, $M \dot\cup Y \subseteq A$ e $M \dot\cup Y$ é infinito, pelo que $\psi \in \mathcal{F}$. Atendendo à construção de ψ, temos $\theta \leq \psi$, com $\theta \neq \psi$ pois $Y \neq \emptyset$. Chegamos a uma contradição visto θ ser um elemento maximal de $\mathcal{F}$. Portanto $\#(A\backslash M) < \#M$.

Mostremos que $\#M = \#A$. É claro que $\#M \leq \#A$. Por outro lado, temos $A = M \dot\cup (A\backslash M)$, donde $\#A = \#M + \#(A\backslash M)$. Mas, $\#(A\backslash M) < \#M$, pelo que

$$\#A \leq \#M + \#M = 2\,\#M$$

pelo Lema 8.b). Tal como acima $2\#M = \#M$. Logo $\#A \leq \#M$. Portanto, $\#A = \#M$.

Finalmente, podemos concluir que $\#(A\times A) = \#A$. De facto, como $\#A = \#M$ e $\#(M\times M) = \#M$, temos

$$\#(A\times A) = \#A\,\#A = \#M\,\#M = \#(M\times M) = \#M = \#A$$

como queríamos demonstrar. ∎

Corolário 9.1. *Se α é um cardinal infinito, então $\alpha\,\alpha = \alpha$.*

Demonstração: Seja A um conjunto infinito tal que $\alpha = \#A$. Então $\alpha\,\alpha = \#A\times\#A = \#(A\times A) = \#A = \alpha$. ∎

Mais geralmente, podemos afirmar o seguinte.

Teorema 10. *Sejam A e B conjuntos tais que A é infinito, $B \neq \emptyset$ e $\#B \leq \#A$. Então*

$$\#(A \times B) = \#A$$

Demonstração: Como $\#B \leq \#A$, existe $f\colon B \hookrightarrow A$ injectiva. Então $g\colon A \times B \hookrightarrow A \times A$, $(a, b) \mapsto (a, f(b))$, é também uma aplicação injectiva, pelo que

$$\#(A \times B) \leq \#(A \times A)$$

Pelo Teorema 9, obtemos $\#(A \times B) \leq \#A$.

Fixemos $b \in B$. Então $h : A \hookrightarrow A \times B$, $a \mapsto (a, b)$, é uma aplicação injectiva e, portanto, $\#A \leq \#(A \times B)$. Assim, pelo Lema de Schröder–Bernstein, temos $\#(A \times B) = \#A$. ∎

Exemplos.

1) $\#\mathbb{N}\#\mathbb{R} = \#(\mathbb{N} \times \mathbb{R}) = \#\mathbb{R}$

2) $\#(\mathbb{N} \times \{1, \ldots, n\}) = \#\mathbb{N}$, para $n \in \mathbb{N}$.

Corolário 10.1. *Sejam α um cardinal infinito e β um cardinal não nulo tal que $\beta \leq \alpha$. Então $\alpha\,\beta = \alpha$.*

Demonstração: Atendendo ao teorema anterior, basta tomar conjuntos A e B tais que $\alpha = \#A$ e $\beta = \#B$. ∎

É claro que neste último resultado não podemos dispensar a condição de α ser infinito, por exemplo, $2 \leq 3$ e $2.3 \neq 3$.

Estudemos agora algumas propriedades da adição de cardinais.

Teorema 11. *Sejam A e B conjuntos tais que A é infinito e $\#B \leq \#A$. Então*

$$\#(A \cup B) = \#A$$

Demonstração: Como $A \subseteq A \cup B$, temos $\#A \leq \#(A \cup B)$. Seja $C = B \backslash A$. Então $A \cup B = A \,\dot\cup\, C$. De $C \subseteq B$, concluímos que

$\#C \leq \#B \leq \#A$, donde existe $f\colon C \hookrightarrow A$ injectiva. Seja

$$\begin{aligned} g\colon\ & A \dot\cup C \hookrightarrow A \times \{1,2\} \\ & x \in A \mapsto (x,1) \\ & x \in C \mapsto (f(x),2) \end{aligned}$$

Então g é também uma aplicação injectiva e obtemos

$$\#(A \cup B) = \#(A \dot\cup C) \leq \#(A \times \{1,2\})$$

Como $\#(A \times \{1,2\}) = \#A$, obtemos $\#(A \cup B) \leq \#A$. Portanto, $\#(A \cup B) = \#A$. ∎

Corolário 11.1. *Se α é um cardinal infinito e β é um cardinal tal que $\beta \leq \alpha$, então $\alpha + \beta = \alpha$. Em particular, $\alpha + \alpha = \alpha$.*

Demonstração: Sejam A e B tais que $\alpha = \#A$, $\beta = \#B$ e $A \cap B = \emptyset$. Temos

$$\alpha + \beta = \#A + \#B = \#(A \dot\cup B)$$

sendo $\#(A \dot\cup B) = \#A$, pelo teorema anterior. Portanto, $\alpha + \beta = \alpha$. ∎

Exemplos.

$\aleph_0 + \aleph_0 = \aleph_0$ e $\aleph_0 + n = \aleph_0$, para $n \in \mathbb{N}$.

Corolário 11.2. *Sejam α e β cardinais tais que α é infinito e $\beta \neq 0$. Então*

$$\alpha + \beta = \alpha\,\beta = \max\{\alpha, \beta\}$$

Demonstração: Pelo Teorema 4, temos $\alpha \leq \beta$ ou $\beta \leq \alpha$. Se $\beta \leq \alpha$ então, pelos Corolários 10.1 e 11.1, $\alpha\,\beta = \alpha = \alpha + \beta$. Se $\alpha \leq \beta$, como α é infinito, β também o é. Observando que $\alpha \neq 0$, pelos mesmos corolários, concluímos que $\alpha\,\beta = \beta = \alpha + \beta$. Assim,

$$\alpha\,\beta = \alpha + \beta = \max\{\alpha, \beta\}$$

como se pretendia. ∎

Exemplos.

1) Pelo Corolário 11.2, temos $\#\mathbb{N}\#\mathbb{R} = \#\mathbb{N} + \#\mathbb{R} = \#\mathbb{R}$.

2) Vejamos que $\#[0,1] = \#\mathbb{R}$. Começamos por observar que

$$\begin{aligned} \operatorname{tg}\colon\,]-\tfrac{\pi}{2},\tfrac{\pi}{2}[&\to \mathbb{R} \\ x &\mapsto \operatorname{tg} x \end{aligned}$$

é uma aplicação bijectiva, pelo que $\#\,]-\frac{\pi}{2},\frac{\pi}{2}[\, = \#\mathbb{R}$. Aplicando o Teorema 11, obtemos

$$\begin{aligned} \#\mathbb{R} &= \#\,]-\tfrac{\pi}{2},\tfrac{\pi}{2}[= \#\Big(]-\tfrac{\pi}{2},\tfrac{\pi}{2}[\,\dot\cup\,\{-\tfrac{\pi}{2},\tfrac{\pi}{2}\}\Big) \\ &= \#[-\tfrac{\pi}{2},\tfrac{\pi}{2}] = \#[0,1] \end{aligned}$$

3) É fácil provar que $\#\mathbb{Q} = \#\mathbb{Z} = \#\mathbb{N}$.

Teorema 12. $\#\mathbb{R} = 2^{\aleph_0}$.

Demonstração: Seja $f\colon\, \mathbb{R} \to \mathcal{P}(\mathbb{Q})$, $a \mapsto \{x \in \mathbb{Q}\colon\, x < a\}$. Trata-se de uma aplicação que é injectiva. De facto, se $a<b$ existe $q\in\mathbb{Q}$ tal que $a<q<b$, pelo que $q\in f(b)$ e $q\notin f(a)$, donde $f(a)\neq f(b)$. Logo, $\#\mathbb{R} \leq \#\mathcal{P}(\mathbb{Q}) = 2^{\#\mathbb{Q}} = 2^{\aleph_0}$.

Reciprocamente, tomemos $g\colon \{0,1\}^{\mathbb{N}} \to [0,1]$, $h \mapsto 0{,}h(1)h(2)\ldots$. Observemos que $0{,}h(1)h(2)\ldots$ é uma dízima em 0 e 1. É claro que g é injectiva, pelo que $2^{\aleph_0} \leq \#[0,1] = \#\mathbb{R}$. Portanto, $\#\mathbb{R} = 2^{\aleph_0}$. ∎

Completamos esta secção com a demonstração de outra caracterização de conjunto infinito. Certos autores usam esta segunda caracterização como definição de conjunto infinito, definindo conjunto finito como sendo um que não é infinito.

Teorema 13. *Seja A um conjunto. Então A é infinito se e só se é equipotente a uma sua parte própria.*

Demonstração: Tendo em conta o Resultado b), enunciado atrás, resta-nos provar a implicação directa. Suponhamos que A é

infinito. Pela Proposição 5, existe uma aplicação $f : \mathbb{N} \hookrightarrow A$ injectiva. Então $f(\mathbb{P}) \subsetneqq f(\mathbb{N}) \subseteq A$ e $f(\mathbb{P}) \sim \mathbb{P} \sim \mathbb{N} \sim f(\mathbb{N})$. De $A = f(\mathbb{N}) \dot{\cup} (A \backslash f(\mathbb{N}))$ obtemos

$$\begin{aligned} \#A &= \#f(\mathbb{N}) + \#(A \backslash f(\mathbb{N})) = \#f(\mathbb{P}) + \#(A \backslash f(\mathbb{N})) \\ &= \#(f(\mathbb{P}) \dot{\cup} (A \backslash f(\mathbb{N}))) \end{aligned}$$

em que $f(\mathbb{P}) \dot{\cup} (A \backslash f(\mathbb{N})) \subsetneqq A$. ∎

Sobre a Hipótese do Contínuo

Por fim, umas breves palavras sobre a Hipótese do Contínuo.

O Teorema de Cantor garante-nos que $\aleph_0 < 2^{\aleph_0}$, pelo que podemos afirmar que existem cardinais estritamente maiores do que $\aleph_0$.

A *Hipótese do Contínuo Generalizada* afirma que não existe um cardinal β tal que

$$\#X < \beta < \#\mathcal{P}(X)$$

para qualquer X infinito. Quando X é numerável estamos perante a *Hipótese do Contínuo*: não existe um cardinal β tal que

$$\aleph_0 < \beta < 2^{\aleph_0}$$

Definindo $\aleph_{n+1}$, para $n \geqslant 0$, como sendo o menor cardinal estritamente maior do que $\aleph_n$ (o qual existe pois $\leq$ é uma boa ordem e pelo menos $2^{\aleph_n}$ é estritamente maior que $\aleph_n$ [ver Ferreira]), da *Hipótese do Contínuo Generalizada* decorre $\aleph_{n+1} = 2^{\aleph_n}$.

Observemos que a Hipótese do Contínuo Generalizada implica o Axioma da Escolha e que a Hipótese do Contínuo é um axioma independente dos outros axiomas da Teoria dos Conjuntos (este último facto foi provado por P. Cohen em 1963).

Exercícios

1. Mostre que $f : \mathbb{Q} \to \mathbb{R}$, $n \mapsto 2n + 5$, é uma aplicação injectiva não sobrejectiva.

2. a) Existe a aplicação inversa de $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2 + x + 1$?
   b) Qual é a aplicação inversa de $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto 3x + 2$?

3. Sejam A, B, C, D conjuntos tais que $A \sim C$ e $B \sim D$. Mostre que
   a) se $A \cap B = C \cap D = \emptyset$, então $A \cup B \sim C \cup D$;
   b) $A \times B \sim C \times D$;
   c) $A^B \sim C^D$.

4. Diga justificando se é verdadeira ou falsa a seguinte proposição, para quaisquer conjuntos A e B,
$$\#A = \#B = \#\mathbb{N} \Rightarrow \#(A \cap B) = \#\mathbb{N}$$

5. Sejam α, β, γ cardinais. Mostre que
   a) $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$;
   b) $\alpha \leq \beta \Rightarrow \alpha\gamma \leq \beta\gamma$;
   c) $\alpha \leq \beta \Rightarrow \alpha^\gamma \leq \beta^\gamma$.

6. Sejam α, β, γ cardinais. Mostre que
   a) $\alpha + \beta = \beta + \alpha$;
   b) $\alpha\beta = \beta\alpha$;
   c) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$;
   d) $(\alpha\beta)\gamma = \alpha(\beta\gamma)$;

e) $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$;

f) $\alpha^{\beta+\gamma}=\alpha^{\beta}\alpha^{\gamma}$;

g) $(\alpha^{\beta})^{\gamma}=\alpha^{\beta\gamma}$;

h) $(\alpha\beta)^{\gamma}=\alpha^{\gamma}\beta^{\gamma}$.

7. Considere os cardinais $2,3,5,6$ e 8 e um cardinal arbitrário λ. Mostre que

a) $2+3=5,\ 2\cdot 3=6,\ 2^3=8$;

b) $2\lambda=\lambda+\lambda$;

c) $3\lambda=\lambda+\lambda+\lambda$.

8. Considere os cardinais $2,3,\aleph_0$ e $2^{\aleph_0}$. Prove que

a) $2+\aleph_0=\aleph_0=2\aleph_0=3\aleph_0=3+\aleph_0$;

b) $2^{\aleph_0}=3^{\aleph_0}=(2^{\aleph_0})^{\aleph_0}$;

c) $\aleph_0+2^{\aleph_0}=2^{\aleph_0}$.

9. Mostre que

a) $f:\mathbb{N}\times\mathbb{N}\to\mathbb{N},\ (m,n)\mapsto\frac{(m+n-2)(m+n-1)}{2}+m$, é uma aplicação bijectiva;

b) $\#\mathbb{N}=\#(\mathbb{N}\times\mathbb{N})$.

10. Prove que se A e B são conjuntos numeráveis, então $A\times B$ é numerável.

11. Mostre que

a) $\#\mathbb{Z}=\#\mathbb{N}$;

b) $\#\mathbb{Q}=\#\mathbb{N}$;

c) $\#\mathbb{R}=\#\mathbb{C}$.

12. Mostre que o conjunto de todas as rectas do plano que passam pela origem é equipotente a $\mathbb{R}$.

13. Mostre que o conjunto dos inteiros positivos cujo conjunto de factores primos é $\{5, 7\}$ é numerável.

14. Seja C o conjunto dos inteiros múltiplos ímpares de 3. Mostre que C é numerável.

15. Prove que

    a) A união de um número finito de conjuntos numeráveis é numerável;
    b) A união de um conjunto numerável de conjuntos finitos ou numeráveis é numerável;
    c) Sendo α um cardinal tal que $\aleph_0 < \alpha$, então o cardinal da união de um conjunto numerável de conjuntos com cardinal α é α;
    d) Em particular, o cardinal da união de um conjunto numerável de conjuntos com cardinal $2^{\aleph_0}$ é $2^{\aleph_0}$.

16. Seja A um conjunto numerável.

    a) Mostre que o conjunto das sucessões finitas de elementos de A ainda é numerável.
    b) Conclua que A é equipotente ao conjunto das suas partes finitas, $\mathcal{P}_F(A)$.

17. Seja $n \in \mathbb{N}_0$. Mostre que o conjunto $\mathbb{Q}_n[x]$ dos polinómios de grau n de $\mathbb{Q}[x]$ é numerável.

18. Mostre que $\mathbb{Q}[x]$ é numerável.

19. Mostre que $\mathcal{M} = \{A \subseteq \mathbb{N} : \#A \geq 2\}$ não é numerável. Qual o seu cardinal?

20. a) Mostre que $\#\mathbb{R} = \#\left([0,1] \times \mathbb{N}\right) = \#\left(\{0,1\} \times \mathbb{R}\right)$.
    b) Seja $C = \{\frac{1}{n} : n \in \mathbb{N}\}$. Mostre que $\#([0,1] \backslash C) = \#[0,1]$.

21. Sejam C um conjunto infinito e $\mathcal{F}$ o conjunto das aplicações de $\{0,1\}$ em C. Mostre que $\#\mathcal{F} = \#C$.

22. Seja $n \in \mathbb{N}$. Mostre que
    a) Todo o espaço vectorial de dimensão n sobre $\mathbb{Q}$ é numerável;
    b) O cardinal do conjunto $\mathbb{R}_n[x]$ dos polinómios de $\mathbb{R}[x]$ com grau menor ou igual a n é $2^{\aleph_0}$;
    c) O cardinal do conjunto de polinómios $\mathbb{R}[x]$ é $2^{\aleph_0}$;
    d) Em geral, sendo K um corpo, o cardinal do conjunto de polinómios $\mathbb{K}[x]$ é igual a $\max\{\aleph_0, \#K\}$.

23. Usando o facto de um conjunto A ser infinito se e só se for equipotente a uma sua parte própria, dê exemplos de conjuntos infinitos.

24. Mostre que $\#\mathbb{R}^{\mathbb{Q}} < \#\mathbb{R}^{\mathbb{R}}$.

25. Os conjuntos $\mathbb{R}[x] \times \mathbb{Q}[x]$ e $\mathcal{P}(\mathbb{Z} \backslash \{x \in \mathbb{R} : 2x + 1 > 0\})$ são equipotentes?

26. Calcule o cardinal de
$$X = \mathcal{P}_{\text{fin}}(\mathbb{Q}[x]) \times \left(\mathbb{R} \backslash \left\{\frac{3n+1}{n} : n \in \mathbb{N}\right\}\right) \times \mathcal{P}([-\pi, \pi]^{\mathbb{Z}_{17}} \times \mathbb{R}^{\mathbb{R}})$$

27. Mostre que o cardinal do conjunto $(\mathbb{Q} \backslash \{\frac{5n+2}{3n} : n \in \mathbb{N}\})^{\mathcal{P}(\mathbb{Z}[x])}$ é $2^{2^{\aleph_0}}$.

28. Dado um conjunto K, mostre que $A = K \dot{\cup} \mathcal{P}(K \times \mathbb{N})$ é um conjunto infinito não numerável tal que $K \subseteq A$ e $\#K < \#A$.

Bibliografia

[1] Allenby, R.B.J.T. – *Rings, Fields and Groups*, Edward Arnold, London, 1991.

[2] Blyth, T.S. e Robertson, E.F. – *Essential Student Algebra*, Vol. 1 e 3, Chapman and Hall, London, 1986.

[3] Brison, O.J. – *Teoria de Galois*, Textos de Matemática 6, 4ª edição, Departamento de Matemática, FCUL, 2003.

[4] Cameron, P.J. – *Introduction to Algebra*, Oxford University Press, Oxford, 1998.

[5] Cohn, P.M. – *Algebra*, Vol. 1 e 2, Wiley, London, 1974, 1977.

[6] Fernandes, R.L. e Ricou, M. – *Introdução à Álgebra*, IST Press, 2004.

[7] Ferreira, F. – *Princípios de Teoria dos Conjuntos*, Cadernos de Lógica e Computação, Vol. 9, College Publications 2021.

[8] Fraleigh, J.B. – *A First Course in Abstract Algebra*, Addison Wesley, 2003.

[9] Freitas, P. – *Polinómios*, Textos de Matemática 20, Departamento de Matemática, FCUL, 2010.

[10] Halmos, P.R. – *Naive Set Theory*, van Nostrand, New York, 1960.

[11] Hernstein, I.N. – *Topics in Algebra*, Wiley, New York, 1975.

[12] Howie, J.M. – *Fields and Galois Theory*, Springer, 2006.

[13] Howie, J.M. – *Complex Analysis*, Springer, 2003.

[14] Hungerford, T.W. – *Algebra*, Springer-Verlag, New York, 1972.

[15] Jacobson, N. – *Basic Algebra*, Vol. 1 e 2, Freeman, San Francisco, 1974, 1980.

[16] Jacobson, N. – *Lectures in Abstract Algebra*, Vol. 1 e 2, Van Nostrand, Princeton, NJ, 1951, 64.

[17] Lang, S. – *Algebra*, Addison-Wesley, Reading, 1993.

[18] Monteiro, A. e Matos, I.T. – *Álgebra, um primeiro curso*, Escolar Editora, Lisboa, 2ª edição, 2001.

[19] Oliveira, A. – *Teoria dos Conjuntos, Intuitiva e Axiomática*, Escolar Editora, Lisboa, 1982.

[20] Ramalho, M. – *Álgebra I*, Notas de Curso, Departamento de Matemática, FCUL, 1999.

[21] Sobral, M. – *Álgebra*, Universidade Aberta, 1996.

[22] Stewart, I. – *Galois Theory*, Chapman and Hall, London, 1989.

Índice Remissivo