UNIVERSIDADE DA BEIRA INTERIOR
Ciências

Resolubilidade de equações polinomiais

Andreia Sofia Faustino Raquel

Relatório de Estágio para obtenção do grau de mestre em
Ensino de Matemática no 3.º ciclo do Ensino Básico e no Ensino Secundário
(2.º ciclo de estudos)

Orientadora: Prof. Doutora Isabel Maria Romano Cunha

Covilhã, outubro de 2012

Agradecimentos

À professora doutora Isabel Maria Romano Cunha, que para além de orientadora tornou-se, para mim, uma amiga, sempre presente nos bons e maus momentos que passei até à conclusão deste processo. A sua orientação constante, o seu estímulo, os seus vastos conhecimentos e as suas observações críticas fizeram-me perceber que estava perante uma profissional conhecedora, exigente, sensata e justa, permitindo-me levar a bom porto a elaboração desta dissertação. A ela devo o não desistir em momentos complicados e acreditar que era possível chegar ao fim desta difícil caminhada. Por tudo isto lhe agradeço e lhe manifesto o meu sincero reconhecimento. Obrigada.

Aos meus pais pela compreensão, paciência e forma disponível com que sempre me acompanharam.

Aos restantes familiares e amigos por todo o apoio prestado.

Resumo

Neste trabalho centramo-nos na resolubilidade das equações quadráticas, cúbicas e quárticas. Enquadramos esta temática no contexto polinomial e visitamos alguns resultados suporte ao estudo apresentado.

Palavras-chave

Polinómios, Resolubilidade.

Abstract

In this report we focus on solving quadratic, cubic and quartic equations. We approach this subject in polynomial context and we visit some results which support our study.

Keywords

Polynomyals, Solvability.

Índice

Introdução

O presente Relatório integra o 2.º ciclo em Ensino de Matemática no 3.º ciclo do Ensino Básico e no Ensino Secundário. O tema *Polinómios* é, nos currículos destes níveis de ensino, central e transversal.

O desenvolvimento da Álgebra está intimamente ligado à resolução de equações polinomiais. Procurar fórmulas resolventes para equações polinomiais numa incógnita foi uma aventura de séculos. A equação quadrática, apesar de já ser manuseada no Antigo Egito, cerca de 1700 anos a.C., somente no século XII, foi posta na forma como hoje a conhecemos, graças à contribuição de Baskhara que a escreveu em versos. Para os terceiro e quarto graus as fórmulas foram descobertas por matemáticos italianos em meados do século XVI. Seguiram-se dois séculos de enorme empenho de muitos matemáticos na procura de uma fórmula para a equação quíntica, mas esses esforços não se concretizaram no sentido pretendido, mas levaram à demonstração, por Abel, no início do século XIX, que tal fórmula não existe, sendo esse resultado ampliado e explicado pelo génio francês E. Galois, que caracterizou as equações polinomiais $f(x) = 0$, com grau n, que são solúveis por radicais, por meio de uma propriedade de certo grupo de permutações de suas raizes, atualmente designado por grupo de Galois. Nasceu aí a Teoria de Grupos e concluiu-se que a equação polinomial de grau $n \geq 5$ não pode ser resolvida por radicais.

Escolhemos como tema para o nosso estudo a *Resolubilidade de equações polinomiais* e isso permitiu-nos uma revisão científica de vários tópicos no contexto polinomial.

O primeiro capítulo inclui de forma sumária alguns conceitos base referidos ao longo do trabalho, tornando deste modo a sua leitura mais auto contida.

No segundo capítulo consideramos *polinómios* com coeficientes num anel unitário e incluímos alguns resultados versando a divisão de polinómios, a fatorização, o número de raizes e a irredutibilidade.

O terceiro capítulo dedica-se ao Teorema Fundamental da Álgebra, às relações de Girard e sua ligação ao teorema fundamental dos polinómios simétricos.

No quarto capítulo constam os métodos clássicos para a resolução de equações algébricas de grau $2 \leq n \leq 4$, onde determinamos expressões para as raizes de um dado polinómio em função dos seus coeficientes, incluímos alguns exemplos, detalhes históricos e propriedades. Terminamos com uma breve referência à irresolubilidade das equações quínticas.

Capítulo 1

Preliminares

Incluímos neste capítulo conceitos importantes para o desenvolvimento do trabalho.

1.1 Estruturas

A axiomatização da Álgebra exigiu a definição de *estruturas algébricas abstratas.* Uma estrutura algébrica abstrata é formada por um conjunto não vazio X, dito o *suporte* da estrutura e uma *operação binária* em X que verifica um conjunto de suposições ou axiomas. Um dos problemas principais da Álgebra Geral é o de determinar conjuntos de axiomas que sejam suficientemente gerais para incluir muitos exemplos concretos úteis e, simultaneamente, suficientemente ricos para a obtenção de resultados interessantes. A definição que se segue corresponde à estrutura abstrata mais central da Álgebra.

Definição 1.1. Seja G um conjunto munido de uma operação binária $* : G\times \to G$. Dizemos que $G \equiv (G, *)$ é um *grupo* se satisfaz as seguintes propriedades:

1. $*$ é associativa, isto é, $g * (h * k) = (g * h) * k$, para quaisquer $g, h, k \in G$;

2. Existe $e \in G$ tal que $e * g = g * e = g$, para qualquer $g \in G$; e diz-se a *identidade* ou *elemento neutro* de G;

3. Para qualquer $g \in G$, existe $g^{-1} \in G$ verificando $g * g^{-1} = g^{-1} * g = e$; g^{-1} designa-se por *inverso* de g.

   O grupo G diz-se *abeliano* se $*$ é comutativa, ou seja:

4. $g * h = h * g$, sempre que $g, h \in G$.

Quando o conjunto G é finito, dizemos que G é *grupo finito* e representamos por $|G|$ a *ordem* (cardinalidade) de G.

Recordamos agora as definições de algumas subestruturas e de estruturas quociente com o objetivo de fixar notações. Deixamos de explicitar as operações e não distinguimos a notação para os elementos neutros dos grupos, excepto se isso der azo a alguma confusão.

Assim, se G e H são grupos, $g_1, g_2 \in G$ e $h_1, h_2 \in H$ escrevemos g_1g_2 e h_1h_2 para o produto dos elementos em G e H, apesar de estes poderem não estar de qualquer forma relacionados.

Definição 1.2. Sejam G um grupo e $H \subset G$ um conjunto não-vazio. Dizemos que H é um *subgrupo* de G (e escrevemos $H \leq G$) se $gh \in H$ e $g^{-1} \in H$, sempre que $g, h \in H$.

Se $H \leq G$ e $g \in G$ definem-se as *classes laterais* de H em G por

$$Hg = \{hg : h \in H\}$$
$$gH = \{gh : h \in H\}$$

Se H é um subgrupo de G, dizemos que H é um *subgrupo normal* de G (e escrevemos $H \trianglelefteq G$) se e só se para qualquer $h \in H$ e $g \in G$, temos $ghg^{-1} \in H$, ou equivalentemente, se $Hg = gH$, para qualquer $g \in G$. [15]

Um grupo G diz-se *simples* se não tem subgrupos normais além dos triviais, $\{e\}$ e G .

Se $H \trianglelefteq G$ define-se o *grupo quociente* G/H como o conjunto das classes laterais com operação definida por $(g_1H)(g_2H) = (g_1g_2)H$.

A cardinalidade de G/H designa-se por *índice* de H em G e representa-se por $|G : H|$.

Note-se que a aplicação $H = eH \to aH$, $h \mapsto ah$ é bijetiva e como tal todas as classes de equivalência têm o mesmo cardinal, igual a $|H|$. G é a união disjunta das classes de equivalência, logo

$$|G| = |G : H||H|.$$

Assim tem-se o

Teorema 1.3 (**Teorema de Lagrange**[1])**.** *A ordem de um grupo finito é um múltiplo da ordem de qualquer dos seus subgrupos.*

Revemos o conceito de homomorfismo.

Definição 1.4. Sejam G e H grupos. A aplicação $\varphi : G \to H$ diz-se um *homomorfismo* de grupos se para quaisquer $x, y \in G, \varphi(xy) = \varphi(x)\varphi(y)$.

Um homomorfismo φ diz-se *monomorfismo* se for injetiva, *epimorfismo* se for sobrejetiva e é um *isomorfismo* quando é uma bijeção. Os isomorfismos $\psi : G \to G$ dizem-se *automorfismos.*

São de verificação imediata as seguintes resultados.

Proposição 1.5. *Seja $\varphi : G \to H$ um homomorfismo de grupos. Então:*

(i) $\varphi(e) = e, \quad \varphi(x^{-1}) = \varphi(x)^{-1}$, *para qualquer* $x \in G$,

(ii) $\operatorname{im}\varphi = \varphi(G)$ *é um subgrupo de* G,

[1] Joseph-Louis Lagrange, 1736 - 1813

(iii) $\ker\varphi = \varphi^{-1}(e)$ *é um subgrupo normal de* G.

Teorema 1.6. *[15]*

1. *Seja* $\varphi : G \to H$ *um homomorfismo de grupos, então o grupo quociente* $G/\ker\varphi$ *é isomorfo a* $\operatorname{im}\varphi$ *através do isomorfismo*

$$\begin{array}{rccc} \bar{\varphi}: & G/\ker\varphi & \to & \operatorname{im}\varphi \\ & a\ker\varphi & \mapsto & \varphi(a). \end{array}$$

2. *Seja* N *um subgrupo normal de um grupo* G, *então a aplicação* $\pi : G \to G/N,\ a \mapsto aN$, *é um epimorfismo, dito a projeção de* G *sobre* G/N *e* $\ker\pi = N$. *Em particular, isto prova que qualquer subgrupo normal é o núcleo de algum homorfismo.*

3. *Seja* $\varphi : G \to H$ *um homomorfismo de grupos. Então* φ *é um monomorfismo se e só se* $\ker\varphi = \{e\}$ *e* φ *é um epimorfismo se e só se* $\operatorname{im}\varphi = H$.

Exemplo 1.7. Sejam G um grupo e $a \in G$. A aplicação $I_a : G \to G$ dada por $I_a(x) = axa^{-1}$ é um automorfismo, dito um *automorfismo interno*.
O conjunto $\operatorname{Aut} G$ dos automorfismos de G é um grupo para a composição de aplicações. A aplicação $I : G \to \operatorname{Aut} G$, dada por $I(a) = I_a$ é um homomorfismo cuja imagem $\operatorname{im} I$ é o subgrupo dos automorfismos internos, que representamos por $\operatorname{Int} G$. O seu núcleo é $\ker I = \{a \in G : I_a = id\} = \{a \in G : ax = xa,\ \forall x \in G\}$, dito o *centro* de G, que notamos por $Z(G)$.

Exemplo 1.8. Seja Ω um conjunto arbitrário não vazio. O conjunto

$$S(\Omega) = \{f\ : \Omega \to \Omega : f \text{ é uma aplicação bijetiva}\}$$

é um grupo para a composição de aplicações, chamado o *grupo das permutações de* Ω. Os grupos contidos em $S(\Omega)$ designam-se por *grupos de transformações de* Ω.

No caso em que $\Omega = \{1, 2, \cdots, n\}$, representamos o grupo $S(\Omega)$ por S_n e designamo-lo por *grupo simétrico de ordem* n. Os elementos de S_n podem representar-se por:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

e designam-se por *permutações*. A ordem do grupo simétrico de grau n é $|S_n| = n!$. O seu elemento neutro é a aplicação identidade: $\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$.

O resultado que segue releva a importância dos grupos simétricos.

Teorema 1.9 (Cayley [2]). *Seja* G *um grupo de ordem* n. *Então* G *é isomorfo a um subgrupo de* S_n.

[2] Arthur Cayley, 1821 - 1895

Demonstração. Identifiquemos S_n com $S(G) = \{f : G \to G : f \text{ é bijetiva}\}$ e consideremos a aplicação:

$$\begin{array}{rccccc} L: & G & \to & S(G) & & \\ & a & \mapsto & L_a: & G & \to & G \\ & & & & x & \mapsto & ax. \end{array}$$

A aplicação L_a é bijetiva, para qualquer $a \in G$, com inversa $L_{a^{-1}}$ e $L_{ab} = L_a \circ L_b$, para quaisquer $a, b \in G$. Donde, L é um homomorfismo de grupos.
Consideremos ainda $a \in \ker L$, logo $L_a = id$, isto é $ax = x$, para qualquer $x \in G$. Em particular $a = ae = e$, donde $\ker L = \{e\}$ e $G \simeq \operatorname{im} G \leq S(G)$.

□

Apresentamos, de seguida, estruturas mais complexas envolvendo duas operações.

Definição 1.10. O terno $(A, +, .)$ diz-se um *anel* se:

1. $(A, +)$ é grupo abeliano;

2. A operação . é associativa;

3. São válidas as leis da distributividade:

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

   para quaisquer $a, b, c \in A$.
   Se existir uma identidade, 1, para a multiplicação, dizemos que A é um *anel com identidade* ou *anel unitário*. Se a multiplicação for comutativa, dizemos que o *anel* é *comutativo* ou *abeliano*.
   Chamamos à (única) identidade para a soma, o *zero* do anel.

Definição 1.11. Um *domínio de integridade*, D, é um anel unitário abeliano, sem divisores de zero, ou seja, se $a \cdot b = 0$, onde $a, b \in D$, então $a = 0$ ou $b = 0$.

Seja A um anel com identidade. Representemos por A^*, o conjunto dos elementos invertíveis de A.

Definição 1.12. Um *anel de divisão* é um anel unitário K tal que $K^* = K \backslash \{0\}$. A um anel de divisão comutativo chama-se *corpo*. Portanto, um corpo é um anel comutativo com identidade onde todo o elemento diferente de 0 possui inverso.

É imediato ver que todo o corpo é um domínio de integridade. $\mathbb{Z}$ é um exemplo de domínio de integridade que não é corpo. No entanto,

Teorema 1.13. *Todo o domínio de integridade finito é um corpo.*

Demonstração. Seja $D = \{0, d_1, d_2, \ldots, d_n\}$ um domínio de integridade finito. Para cada $i \in \{1, 2, \ldots, n\}$, consideremos os produtos $d_i d_1, d_i d_2, \ldots, d_i d_n$. Eles são distintos dois a dois: $d_i d_j = d_i d_k$ se e só se $d_i(d_j - d_k) = 0$. Como D não tem divisores de zero e $d_i \neq 0$, tem-se necessariamente $d_j = d_k$. Assim, os produtos $d_i d_1, d_i d_2, \ldots, d_i d_n$ percorrem todos os elementos não nulos de D e, portanto, existe j tal que $d_i d_j = 1$. Logo, concluímos que d_i é invertível e D é um corpo.

□

Lema 1.14. *Sejam $D \neq \{0\}$ um domínio de integridade e $B = \{(a, b) : a, b \in D \text{ e } b \neq 0\}$. A relação binária em B definida por*

$$(a, b) \simeq (a', b') \Leftrightarrow ab' = a'b$$

é uma relação de equivalência.

Demonstração. A reflexividade e a simetria resultam trivialmente. A transitividade é consequência direta de D não ter divisores de zero.

□

Definição 1.15. Seja $D \neq \{0\}$ um domínio de integridade. Se $a, b \in D$ e $b \neq 0$, a *fracção* $\frac{a}{b}$ é dada por

$$\frac{a}{b} = \{(a', b') \in D \times D : b' \neq 0 \text{ e } ab' = a'b\}.$$

Designamos o conjunto de todas as fracções $\frac{a}{b}$ por $\mathrm{Frac}(D)$. Definimos a *soma* e o *produto* de fracções por

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \tag{1.1}$$

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}\ . \tag{1.2}$$

O conjunto $\mathrm{Frac}(D)$ munido destas operações algébricas é um corpo, dito *corpo das fracções* de D.

Recordamos mais alguns conceitos e estabelecemos notações.

Definição 1.16. Seja $\emptyset \neq S \subseteq A$. Dizemos que S é um *subanel* do anel A se é fechado para $+$ e $.$ e forma um anel para estas operações.
Um subanel I de A é um *ideal* de A (e escrevemos $I \trianglelefteq A$) se, para cada $a \in A$ e cada $x \in I$, $ax \in I$ e $xa \in I$.
O menor ideal de A contendo a é o *ideal principal gerado* por a :

$$\langle a \rangle = \{xa + na : x \in A, n \in \mathbb{Z}\}.$$

Se A é um anel e $I \trianglelefteq A$, construímos o *anel quociente* A/I como sendo o conjunto das classes laterais do subgrupo I no grupo aditivo $(A, +)$ com as operações definidas por:

$$(r + I) + (s + I) = (r + s) + I$$
$$(r + I).(s + I) = (r.s) + I \ .$$

Sejam $n \in \mathbb{N}$ e $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$. É imediato verificar que $n\mathbb{Z} \trianglelefteq \mathbb{Z}$. Definimos $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Prova-se que $\mathbb{Z}_n$ é um corpo se e só se n é primo [14].

Capítulo 2

Polinómios

2.1 Anel dos polinómios

Definições 2.1. Seja A um anel comutativo com unidade, 1. Um *polinómio em A na indeterminada x* [1] é uma soma formal

$$a_0 + a_1 x + \cdots + a_n x^n$$

onde $a_0, a_1, \cdots a_n \in A, \quad n \in \mathbb{N}_0$. Podemos representar o polinómio na forma

$$f = f(x) = a_0 + a_1 x + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i,$$

convencionando que $x^0 = 1$.

Os elementos $a_i \in A$ dizem-se os *coeficientes* do polinómio f.

Dois *polinómios* são *iguais* se e só se os respetivos coeficientes são iguais.

Soma e produto de polinómios - Sejam f e g polinómios em A na indeterminada x, então

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{e} \quad g(x) = \sum_{i=0}^{m} b_i x^i,$$

onde $a_i,\ b_i \in A$ e, sem perda de generalidade, consideramos $n \leq m$. Definimos a soma

$$(f+g)(x) = \sum_{i=0}^{m} (a_i + b_i) x^i$$

e o produto

$$(fg)(x) = \sum_{i=0}^{m+n} c_i x^i,$$

onde

$$c_i = \sum_{h+j=i} a_h b_j.$$

Designamos por $A[x]$ o conjunto dos polinómios em A na indeterminada x.

[1] Usamos a letra x para representar a indeterminada $(0, 1, \ldots)$ como poderíamos designá-la por uma outra letra, *e.g.* y ou t.

É imediato concluir que $A[x]$ é um anel comutativo com unidade. A identidade para a soma é o *polinómio nulo*

$$0 = 0 + 0x + \cdots \in A[x]$$

e a identidade para o produto é

$$1 = 1 + 0x + \cdots \in A[x].$$

Observações 2.2.

1. Como indicámos, omitiremos por vezes na notação para os polinómios a indeterminada, sempre que daí não resulte qualquer ambiguidade.

2. É possível também definir um polinómio como sendo uma sequência $f = (r_0, r_1, \ldots)$ de elementos $r_i \in A$ tal que para algum $n \in \mathbb{N}_0$ se tem $r_j = 0$, quando $j > n$.

3. Muitas vezes definimos os polinómios com coeficientes reais como as funções $p : \mathbb{R} \to \mathbb{R}$ da forma $p(x) = \sum_{i=0}^{n} p_i x^i$, onde os reais p_i são os coeficientes do polinómio. Não podemos definir deste modo os polinómios com coeficientes num anel A se pretendermos que polinómios com coeficientes distintos sejam distintos. De facto, se A tem mais do que um elemento $a \neq 0$ existe uma infinidade de possíveis polinómios. No entanto se A é finito, existe apenas um número finito de funções $f : A \to A$, que não podem ser usadas para definir todos os polinómios com coeficientes em A.

   Por exemplo, se $A = \mathbb{Z}_2$, existem apenas quatro funções:

$$\begin{array}{cccc} f_1 & f_2 & f_3 & f_4 \\ 0 \mapsto 0 & 0 \mapsto 0 & 0 \mapsto 1 & 0 \mapsto 1 \\ 1 \mapsto 0 & 1 \mapsto 0 & 1 \mapsto 0 & 1 \mapsto 1 \end{array}$$

   mas, por outro lado, exigindo-se que polinómios com coeficientes distintos sejam distintos, temos uma infinidade de polinómios com coeficientes em $\mathbb{Z}_2$:

$$0,\ 1,\ x,\ x^2,\ x+1,\ x^3,\ x^2+x^3,\ 1+x+x^2+x^3,\ x+x^2+x^3, 1+x^3, \ldots$$

4. Embora o polinómio $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ não seja uma função podemos definir uma *função polinomial associada a* f que, por abuso de notação, também representamos por $f : A \to A$, dada por:

$$r \mapsto f(r) = a_0 + a_1 r + \cdots + a_n r^n.$$

   Contudo dois polinómios distintos podem dar origem à *mesma função*, como no exemplo anterior, onde os polinómios x e x^2 definem ambos a função identidade em $\mathbb{Z}_2$.

5. Para somar e multiplicar polinómios, procedemos exatamente como estamos habituados com os polinómios de coeficientes reais. Por exemplo, em $\mathbb{Z}_4[x]$, para $p = 1 + x + 2x^2$ e $q = 1 + 2x^2$, temos:

$$\begin{aligned} p + q &= (1 + x + 2x^2) + (1 + 2x^2) \\ &= (1 + 1) + (1 + 0)x + (2 + 2)x^2 \\ &= 2 + x, \end{aligned}$$

$$\begin{aligned} pq &= (1 + x + 2x^2)(1 + 2x^2) \\ &= (1 + x + 2x^2)1 + (1 + x + 2x^2)2x^2 \\ &= (1 + x + 2x^2) + (2x^2 + 2x^3 + 0x^4) \\ &= 1 + x + 2x^3. \end{aligned}$$

Definição 2.3. Seja A um anel comutativo com unidade 1 e $0 \neq f \in A[x]$. O *grau* de f é o expoente da maior potência de x com coeficiente não nulo. Portanto, se

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

com $a_n \neq 0$, dizemos que f tem grau n e escrevemos $\operatorname{gr} f = n$.
O coeficiente a_n diz-se o coeficiente *principal*. Se $a_n = 1$, f diz-se um *polinómio mónico*.
Convencionamos que $\operatorname{gr} 0 = -\infty$; este é um símbolo que neste contexto tem as propriedades seguintes: $-\infty < n$, $-\infty + n = -\infty$, para $n \in \mathbb{Z}$ e $(-\infty) + (-\infty) = -\infty$.
Representaremos por $A_n[x]$ o conjunto dos polinómios de $A[x]$ cujo grau é menor ou igual do que n.

O lema que se segue será útil ao longo do texto.

Lema 2.4. *Sejam D um domínio de integridade e $f, g \in D[x]$. Então:*

(i) $\operatorname{gr}(f + g) \leq \max(\operatorname{gr} f, \operatorname{gr} g)$;

(ii) $\operatorname{gr}(fg) = \operatorname{gr} f + \operatorname{gr} g$.

Demonstração. Estas propriedades são consequência direta da definição das operações. A desigualdade em (i) deve-se à possibilidade do cancelamento de termos e (ii) resulta de D não ter divisores de zero.

□

Tem-se o seguinte resultado:

Teorema 2.5. *Se $\mathbb{K}$ é um corpo, então $\mathbb{K}[x]$ é um anel comutativo com identidade (de facto é um domínio de integridade).*
$\mathbb{K}$ pode ser realmente mergulhado em $\mathbb{K}[x]$ identificando cada elemento de $\mathbb{K}$ com o correspondente polinómio constante.
Os únicos elementos de $\mathbb{K}[x]$ com inverso multiplicativo são os elementos de $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.
$\mathbb{K}_n[x]$ é um espaço vetorial sobre $\mathbb{K}$ de dimensão $n + 1$.

Demonstração. A verificação das propriedades básicas dos anéis é elementar. É também imediato concluir que $\mathbb{K}[x]$ não tem divisores de zero, visto que se $0 \neq p \in \mathbb{K}[x]$, não pode existir $q \neq 0$ em $\mathbb{K}[x]$ verificando $p \cdot q = 0$, uma vez que $\operatorname{gr}(p \cdot q) = \operatorname{gr} p + \operatorname{gr} q$.
Seja g invertível em $\mathbb{K}[x]$. Então existe $h \in \mathbb{K}[x]$ verificando $g \cdot h = 1$. Pelo lema anterior, $\operatorname{gr} g = \operatorname{gr} h = 0$ e, como tal, $g \in \mathbb{K}$.
Por último, resulta da definição das operações de polinómios, do lema anterior e porque $\mathbb{K}$ é um corpo, que $\mathbb{K}_n[x]$ é um espaço vetorial sobre $\mathbb{K}$. O conjunto $\{1, x, x^2, \ldots, x^n\}$ constitui uma sua base, pelo que concluímos que $\dim \mathbb{K}_n[x] = n + 1$.

□

2.2 Divisibilidade e Fatorização única de Polinómios. Irredutibilidade.

A menos que seja dito o contrário, utilizaremos ao longo do texto as notações A, D e $\mathbb{K}$, para significar: anel comutativo com unidade, domínio de integridade e corpo, respetivamente.

Comecemos por estudar o algoritmo usual para a divisão de polinómios.

Teorema 2.6 (**Teorema da divisão**). *Sejam $f, g \in A[x]$, com $f \neq 0$. Então existem polinómios únicos $q, r \in A[x]$ que verificam $g = qf + r$, com $\operatorname{gr} r < \operatorname{gr} f$.*

Demonstração. Provemos a existência por indução no grau de g. Se $\operatorname{gr} g = -\infty$ então $g = 0$ e $q = r = 0$ é uma solução. Se $\operatorname{gr} g = 0$ então $g = c \in A^*$. Se também $\operatorname{gr} f = 0$ então $f = k \in A^*$ e $q = \dfrac{c}{k}$ e $r = 0$ é uma solução. No caso em que $\operatorname{gr} f > 0$ então $q = 0$ e $r = g$ é uma solução. A indução para os dois primeiros casos está provada.

Suponhamos agora que se verifica a existência para todos os polinómios cujo grau é inferior a n e seja $g \in A[x]$ tal que $\operatorname{gr} g = n > 0$. Se $\operatorname{gr} f > n$ então $q = 0$ e $r = g$ é uma solução. Se $\operatorname{gr} f \leq \operatorname{gr} g$, temos

$$f(x) = a_m x^m + \ldots + a_0$$

$$g(x) = b_n x^n + \ldots\ldots + b_0$$

onde $m \leq n$ e $a_m \neq 0 \neq b_n$. Consideremos

$$g_1(x) = b_n a_m^{-1} x^{n-m} f(x) - g(x).$$

Ora, em g_1 anulam-se os termos de ordem n, logo $\operatorname{gr} g_1 < \operatorname{gr} g$, donde, por hipótese de indução, existem polinómios q_1 e r_1 tais que $\operatorname{gr} r_1 < \operatorname{gr} f$ e

$$g_1 = q_1 f + r_1.$$

Os polinómios

$$q = b_n a_m^{-1} x^{n-m} - q_1 \quad \text{e} \quad r = -r_1$$

verificam

$$g = qf + r \quad \text{e } \operatorname{gr} r < \operatorname{gr} f$$

como pretendíamos.

Para mostrar a unicidade, suponhamos que

$$g = q_1 f + r_1 = q_2 f + r_2, \qquad \text{onde} \qquad \operatorname{gr} r_i < \operatorname{gr} f, \quad \text{para } i = 1, 2.$$

Então

$$r_2 - r_1 = (q_1 - q_2)f.$$

Ora, pelo Lema 2.4 esta igualdade só é válida quando

$$r_2 - r_1 = (q_1 - q_2)f = 0,$$

obtendo-se $r_1 = r_2$ e $q_1 = q_2$, uma vez que $f \neq 0$. Donde, q e r são únicos.

□

Os polinómios q e r designam-se, respetivamente, *quociente* e *resto* da divisão de g por f. O caso em que $r = 0$ corresponde ao caso em que f é divisor (ou factor) de g e escrevemos $f \mid g$.

Observação 2.7. O processo descrito no teorema anterior constitui o *algoritmo da divisão*. Se o grau do dividendo, $D(x)$, for menor do que o grau do divisor $d(x)$, o processo pára. Caso contrário, continua e o objetivo é "reduzir" o grau efetuando um número finito de sucessivas divisões por $d(x)$, onde intervêm *restos parciais* $r_i(x)$ dados por

$$r_1(x) = D(x) - \frac{b_m}{a_n} x^{m-n} d(x) \;\text{ e }\; r_i(x) = r_{i-1}(x) - \frac{c_l}{a_n} x^{l-n} d(x), \qquad i = 2, 3, \ldots$$

onde $b_m x^m$, $a_n x^n$ e $c_l x^l$ são os termos de maior grau de D, d e r_{i-1}, respetivamente.

Após um número finito de passos obtemos um resto $r_k(x)$ de grau inferior a n. O resto da divisão original é $r_k(x)$ e o quociente é formado coleccionando os termos obtidos em cada passo.

Exemplo 2.8. Consideremos a divisão de $D(x) = 2x^4 + x^3 - 3x^2 + 2x - 1$ por $d(x) = x^2 + 1$. Têm-se:

$$\begin{aligned} r_1(x) &= D(x) - \frac{2}{1} x^2 d(x) \\ &= (2x^4 + x^3 - 3x^2 + 2x - 1) - 2x^2(x^2 + 1) \\ &= x^3 - 5x^2 + 2x - 1 \end{aligned}$$

$$\begin{aligned} r_2(x) &= r_1(x) - \frac{1}{1}xd(x) \\ &= (x^3 - 5x^2 + 2x - 1) - x(x^2 + 1) \\ &= -5x^2 + x - 1 \end{aligned}$$

$$\begin{aligned} r_3(x) &= r_2(x) - \left(-\frac{5}{1}d(x)\right) \\ &= (-5x^2 + x - 1) - (-5)(x^2 + 1) \\ &= x + 4 \end{aligned}$$

Como $\operatorname{gr} r_3(x) < \operatorname{gr} d(x)$, o processo termina. O quociente é $q(x) = 2x^2 + x - 5$ e o resto é $r(x) = x + 4$.

É frequente dispormos todos os cálculos da seguinte forma:

$$\begin{array}{rrrrr|l} 2x^4 & +x^3 & -3x^2 & +2x & -1 & x^2+1 \\ \cline{6-6} -2x^4 & & -2x^2 & & & 2x^2+x-5 \\ \cline{1-3} & x^3 & -5x^2 & +2x & -1 & \\ & -x^3 & & -x & & \\ \cline{2-5} & & -5x^2 & +x & -1 & \\ & & 5x^2 & & +5 & \\ \cline{3-5} & & & x & +4 & \end{array}$$

Observação 2.9. A introdução do algoritmo da divisão de polinómios no Ensino Secundário fornece a oportunidade de rever o algoritmo da divisão de inteiros e levar os alunos a entender o seu funcionamento. A ideia subjacente consiste em irmos reduzindo o dividendo até que o quociente seja zero e o resto igual ao "próprio dividendo". Na divisão de polinómios reduzimos, em cada etapa, o grau do dividendo. Na divisão de inteiros reduzimos o número de algarismos do dividendo. Vejamos, por exemplo, a divisão de 3971 por 17.

$$\begin{array}{rrrr|l} 3 & 9 & 7 & 1 & 1\ 7 \\ \cline{5-5} -\ 3 & 4 & & & 2\ 3\ 3 \\ \cline{1-2} & 5 & 7 & & \\ & -\ 5 & 1 & & \\ \cline{2-3} & & 6 & 1 & \\ & & -\ 5 & 1 & \\ \cline{3-4} & & & 1 & 0 \end{array}$$

Comecemos por fazer uma estimativa do número de algarismos do quociente. Quando "baixamos as duas primeiras casas" de 3971 concluímos que terá 3 algarismos. Assim, o primeiro algarismo do quociente corresponde ao maior inteiro k tal que o produto de $k00$ por 17 seja menor do que 3971, o que equivale a determinar o maior valor de k para o qual $17k \leq 39$, que é $k = 2$. Obtemos a parcela 200 do quociente e

$$r_1 = D - 200 \times 17 = 3971 - 3400 = 571,$$

onde D designa o dividendo e r_1 o primeiro resto parcial.

Reduzimos o nosso exercício à divisão de 571 por 17. Procuramos o maior inteiro k tal que o produto de 17 por $k0$ seja menor do que 571, ou equivalentemente, que verifica $17k \leq 57$. A solução é $k = 3$ e chegámos à segunda parcela do quociente, 30, bem como a

$$r_2 = r_1 - 30 \times 17 = 571 - 510 = 61.$$

Por último, dividimos 61 por 17 e o maior inteiro k que verifica $17k \leq 61$ é $k = 3$. Assim temos

$$r_3 = 61 - 3 \times 17 = 61 - 51 = 10,$$

que já é menor do que 17. O quociente pretendido é $q = 200 + 30 + 3 = 233$ e o resto desta divisão é $r = 10$.

□

É consequência direta do teorema da divisão o resultado que se segue.

Corolário 2.10 (Teorema do Resto). *Se $p(x) \in \mathbb{K}[x]$ e $a \in \mathbb{K}$, o resto da divisão de $p(x)$ por $(x - a)$ é o polinómio constante $r(x) = p(a)$. Em particular, $(x - a) \mid p(x)$ se só se a é raiz de $p(x)$, isto é, se e só se $p(a) = 0$.*

Exibimos e fundamentamos um processo alternativo, sintético, desenvolvido por Ruffini[2], para a divisão de polinómios quando o grau do polinómio divisor é 1.

Regra de Ruffini 2.11. Consideremos o polinómio

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{K}[x]$$

de grau n e seja $c \in \mathbb{K}$. Pelo teorema da divisão em $\mathbb{K}[x]$ sabemos que existem $q(x) \in \mathbb{K}[x]$ e $r \in \mathbb{K}$, únicos, tais que

$$p(x) = q(x)(x - c) + r \quad \text{onde} \quad r = p(c).$$

Podemos escrever

$$q(x) = b_{n-1} x^{n-1} + \cdots + b_1 x + b_0 \in \mathbb{K}[x].$$

Assim, como

$$q(x)(x - c) + r = b_{n-1} x^n + (b_{n-2} - c b_{n-1}) x^{n-1} + \cdots + (b_0 - a b_1) x + (r - c b_0)$$

vem, por igualdade de polinómios,

$$\begin{aligned} a_n &= b_{n-1} \\ a_{n-1} &= (b_{n-2} - c b_{n-1}) \\ &\vdots \\ a_1 &= (b_0 - c b_1) \\ a_0 &= (r - c b_0) \end{aligned}$$

[2]Paolo Ruffini, 1765 - 1822

pelo que

$$b_{n-1} = a_n$$
$$b_{n-2} = a_{n-1} + cb_{n-1}$$
$$\vdots$$
$$b_0 = a_1 + cb_1$$
$$r = a_0 + cb_0.$$

É possivel calcular os coeficientes b_j de $q(x)$ e o resto $r = f(c)$ utilizando o seguinte esquema:

a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	a_0
	cb_{n-1}	cb_{n-2}	$\ldots$	cb_1	cb_0
b_{n-1}	b_{n-2}	b_{n-3}	$\ldots$	b_0	r

onde cada entrada na última linha corresponde à soma das duas entradas mais acima na mesma coluna.

Exemplo 2.12. Seja $p(x) = x^3 - 10000x^2 - 10002x + 9999$. Do exposto anteriormente facilmente se conclui que $p(10001) = -2$, como indica a tabela:

1	-10000	-10002	9999
	10001	10001	-10001
1	1	-1	-2

Os processos convencionais para este cálculo poderiam tornar-se trabalhosos ou eventualmente conduzir a erros numéricos, caso algum dos resultados parciais excedesse o número de dígitos significativos da calculadora utilizada.

O resultado que se segue ajuda a saber quando $f \in \mathbb{Q}[x]$ tem uma raiz racional, ou, equivalentemente, um factor em $\mathbb{Q}[x]$ de grau 1.

Lema 2.13. *Seja* $0 \neq f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ *tal que* $\frac{r}{s}$ *é uma raiz de* f*, onde* $r, s \in \mathbb{Z}$ *com* $s \neq 0$ *e* $\text{mdc}(r, s) = 1$*. Então* $r \mid a_0$ *e* $s \mid a_n$*.*

Demonstração. Como $f\left(\frac{r}{s}\right) = 0$, então

$$a_n \left(\frac{r}{s}\right)^n + \cdots + a_1 \frac{r}{s} + a_0 = 0,$$

donde

$$a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_0 s^n = 0$$

e tem-se

$$-r(a_n r^{n-1} + a_{n-1} r^{n-2} s + \cdots + a_1 s^{n-1}) = a_0 s^n.$$

Conclui-se que $r \mid a_0 s^n$, mas como $\text{mdc}(r, s) = 1$, resulta que $r \mid a_0$.
Semelhantemente se prova que $s \mid a_n$.

□

Observação 2.14. O resultado anterior é muito útil. Se quisermos, por exemplo, saber se o polinómio $2x^7 + 1 \in \mathbb{Z}_3[x]$ tem raizes no corpo $\mathbb{Z}_3$, como $\mathbb{Z}_3$ tem apenas três elementos, é possível calcular o valor da respetiva função polinomial em cada um deles, concluindo-se que 1 é a única raiz do polinómio. No entanto, se substituirmos $\mathbb{Z}_3$ por $\mathbb{Q}$, já não é possível calcular o valor da função em todos os elementos de $\mathbb{Q}$, mas esse lema reduz o nosso campo de procura a $1, -1, \frac{1}{2}$, e $-\frac{1}{2}$. É fácil ver que estes números não são raízes do polinómio e, portanto, ele não tem raízes racionais.

Uma consequência do teorema do resto é o resultado clássico sobre o número máximo de raízes de um polinómio não nulo, que é válido quando $A = D$ é um domínio de integridade.

Proposição 2.15. *Se $p \in D[x]$ e $\operatorname{gr} p = n \geq 0$, então p tem no máximo n raízes em D.*

Demonstração. Provamos por indução no grau do polinómio $p(x)$. Se $n = 0$, o polinómio $p(x)$ é constante e não nulo, logo não tem raízes.
Supondo a afirmação válida para $n \geq 0$, considere-se que $\operatorname{gr} p(x) = n + 1$ e que existe uma raiz a de $p(x)$ (se $p(x)$ não tem raízes nada há a provar). Pelo teorema do resto, $p(x) = q(x)(x-a)$, e como D é um domínio de integridade, $\operatorname{gr} q(x) = n$, logo, por hipótese de indução, concluímos que $q(x)$ tem, no máximo, n raízes. Por outro lado, se $b \in D$ é distinto de a, temos $p(b) = q(b)(b-a)$ e como D é domínio de integridade $p(b) = 0$ apenas quando $q(b) = 0$, ou seja, as restantes raízes de $p(x)$ são necessariamente raízes de $q(x)$ e, por isso, $p(x)$ tem no máximo $n + 1$ raízes.

□

Apresentamos de seguida os conceitos de divisibilidade e máximo divisor comum, essenciais na aritmética dos polinómios.

Definição 2.16. Sejam f, g polinómios com coeficientes num corpo $\mathbb{K}$.

(a) Dizemos que f *divide* g ou que f *é divisor de* g em $\mathbb{K}[x]$, e escrevemos $f \mid g$, se existe $q \in \mathbb{K}[x]$ tal que $g = qf$. Caso contrário, escrevemos $f \nmid g$.

(b) Um polinómio $d \in \mathbb{K}[x]$ é um *máximo divisor comum*(mdc) de f e g em $\mathbb{K}[x]$ se $d \mid f$ e $d \mid g$ e se sempre que $h \in \mathbb{K}[x]$ é tal que $h \mid f$ e $h \mid g$ então $h \mid d$.

(c) Dizemos que f e g são *primos entre si* se 1 é um máximo divisor comum de f e g em $\mathbb{K}[x]$.

No lema que se segue provamos que o máximo divisor comum de dois polinómios é único a menos do produto por uma constante não nula.

Lema 2.17. *Sejam $f, g \in \mathbb{K}[x]$, com $0 \neq f$ e $k \in \mathbb{K}^*$. Se d é um máximo divisor comum de f e g, então kd também é máximo divisor comum de f e g.*
Se d e e são máximos divisores comuns de f e g, então existe $\lambda \in \mathbb{K}^*$ tal que $e = \lambda d$.

Demonstração. Se $d \in \mathbb{K}[x]$ é máximo divisor comum de f e g, resulta imediatamente que para $k \in \mathbb{K}^*$, se tem $kd \mid f$ e $kd \mid g$. Seja $h \in \mathbb{K}[x]$ tal que $h \mid f$ e $h \mid g$. Então $h \mid d$, logo $h \mid kd$ e kd é máximo divisor comum de f e g.
Se d e e são máximos divisores comuns de f e g, então $e \mid d$ e $d \mid e$. Donde, existem $q_1, q_2 \in \mathbb{K}[x]$ que verificam

$$e = q_1 d \quad \text{e} \quad d = q_2 e = q_2 q_1 d.$$

Tem-se, portanto, $\operatorname{gr} q_1 = \operatorname{gr} q_2 = 0$ e $\lambda = q_1 \in \mathbb{K}^*$.

□

A existência de um máximo divisor comum é garantida pelo algoritmo que a seguir se apresenta, cuja designação se deve à generalização para polinómios do algoritmo de Euclides[3] para a divisão de naturais.

Algoritmo de Euclides 2.18. Sejam $f, g \in \mathbb{K}[x]$, polinómios não nulos. Façamos $f = r_{-1}$ e $g = r_0$. Pelo Teorema 2.6 existem polinómios únicos $q_i, r_i \in \mathbb{K}[x]$ tais que:

$$\begin{aligned}
&r_{-1} = q_1 r_0 + r_1 && \operatorname{gr} r_1 < \operatorname{gr} r_0 \\
&r_0 = q_2 r_1 + r_2 && \operatorname{gr} r_2 < \operatorname{gr} r_1 \\
&r_1 = q_3 r_2 + r_3 && \operatorname{gr} r_3 < \operatorname{gr} r_2 \\
&\quad \dots \\
&r_i = q_{i+2} r_{i+1} + r_{i+2} && \operatorname{gr} r_{i+2} < \operatorname{gr} r_{i+1} \\
&\quad \dots
\end{aligned} \tag{2.1}$$

Ora, como $\operatorname{gr} r_i \in \mathbb{N} \cup \{-\infty\}$ e $\operatorname{gr} r_i > \operatorname{gr} r_{i+1}$, existe s tal que $r_{s+2} = 0$. Assim, a lista de equações fica completa com:

$$\begin{aligned}
&r_{s-1} = q_{s+1} r_s + r_{s+1} && \operatorname{gr} r_{s+1} < \operatorname{gr} r_s \\
&r_s = q_{s+2}\ r_{s+1}, &&
\end{aligned} \tag{2.2}$$

onde r_{s+1} é o último resto não nulo.

Teorema 2.19. *Com a notação do algoritmo anterior, r_{s+1} é um máximo divisor comum de $f, g \in \mathbb{K}[x]$.*

Demonstração. Mostremos, por um raciocínio indutivo, que

$$r_{s+1} \mid r_i, \quad \text{para todo o} \quad -1 \leq i \leq s+1. \tag{2.3}$$

É claro que $r_{s+1} \mid r_{s+1}$ e $r_{s+1} \mid r_s$. Suponhamos agora que $r_{s+1} \mid r_j$, para todo o $j > i$. Então $r_{s+1} \mid q_{i+2} r_{i+1} + r_{i+2} = r_i$. Tem-se então (2.3) e, em particular, $r_{s+1} \mid f, g$.
Se h for um divisor comum de f, g prova-se, por um raciocínio indutivo no sentido contrário ao anteriormente descrito, que $h \mid r_{s+1}$. Logo, r_{s+1} é um máximo divisor comum de f, g.

□

[3] Euclides de Alexandria, aproximadamente 325 aC - aproximadamente 265 aC

É consequência direta dos três resultados anteriores o seguinte:

Corolário 2.20. *Sejam $f, g \in \mathbb{K}[x]$ com $f, g \neq 0$ e seja $d \in \mathbb{K}[x]$ um máximo divisor comum de f e g. Então existem $a, b \in \mathbb{K}[x]$ tais que $d = af + bg$.*

Exemplo 2.21. Sejam $f(x) = 2x^6 + x^3 + x^2 + 2 \in \mathbb{K}_3[x]$ e $g(x) = x^4 + x^2 + 2x \in \mathbb{K}_3[x]$. Ora,

$$\begin{aligned} 2x^6 + x^3 + x^2 + 2 &= (2x^2 + 1)(x^4 + x^2 + 2x) + (x + 2) \\ x^4 + x^2 + 2x &= (x^3 + x^2 + 2x + 1)(x + 2) + 1 \\ x + 2 &= (x + 2)1 + 0. \end{aligned}$$

Portanto $\text{mdc}(f, g) = 1$ e f e g são primos entre si.

Além disso,

$$\begin{aligned} 1 &= x^4 + x^2 + 2x - (x^3 + x^2 + 2x + 1)(x + 2) \\ &= g(x) - (x^3 + x^2 + 2x + 1)(f(x) - (2x^2 + 1)g(x)) \\ &= -(x^3 + x^2 + 2x + 1)f(x) + (1 + 2x^2 + 1)g(x) \\ &= (2x^3 + 2x^2 + x + 2)f(x) + (2x^2 + 2)g(x). \end{aligned}$$

No anel $A[x]$, os elementos invertíveis podem ser usados para obter fatorizações triviais de outros elementos. Por exemplo, o polinómio constante $a(x) = a_0$, com $a_0 \in A^*$, é invertível. Assim, existe $b(x) \in A[x]$ tal que $a(x)b(x) = 1$ e, como tal, para qualquer $p(x) \in A[x]$, tem-se $p(x) = a(x)b(x)p(x)$. Assim, se $q(x) \mid p(x)$ diremos que $q(x)$ é um *fator próprio* de $p(x)$ se e só se $p(x) = a(x)q(x)$, onde nem $a(x)$ nem $q(x)$ são invertíveis. Uma fatorização é *não trivial* se e só se inclui pelo menos um fator próprio.

Exemplo 2.22. A fatorização $2x - 4 = 2(x - 2)$ é trivial em $\mathbb{Q}[x]$ mas é não trivial em $\mathbb{Z}[x]$, onde os únicos polinómios invertíveis são $a(x) = 1$ e $b(x) = -1$.

Definição 2.23. Seja $f \in A[x]$ tal que $\text{gr}\, f \geq 1$. Diz-se que f é *redutível* em $A[x]$ se existem $g, h \in A[x]$ com $\text{gr}\, g, \text{gr}\, h < \text{gr}\, f$ tais que $f = gh$. Caso contrário, f diz-se *irredutível* em $A[x]$.

Exemplos 2.24.

1. Em qualquer anel $A[x]$, $p(x) = x$ é irredutível.

2. Num domínio de integridade D, os únicos polinómios invertíveis são os polinómios constantes.

3. Se $\text{gr}\, p \geq 2$ e p tem pelo menos uma raiz então, pelo teorema do resto, p é redutível em $D[x]$.

4. Se p é mónico e tem grau 2 ou 3, então p é redutível em $D[x]$ se e só se tem pelo menos uma raiz em D.

5. Um polinómio (de grau 4, pelo menos) pode ser redutível sobre um corpo e não ter raízes nesse corpo, como acontece com o polinómio $x^4+4 = (x^2+2x+2)(x^2-2x+2)$, em $\mathbb{Q}[x]$.

6. A redutibilidade ou irredutibilidade de um dado polinómio depende fortemente do anel em consideração. Por exemplo, o polinómio $q(x) = x^2 - 2 \in \mathbb{Q}[x]$ é irredutível em $\mathbb{Q}[x]$, mas $x^2 - 2 = (x+\sqrt{2})(x-\sqrt{2})$ é redutível em $\mathbb{R}[x] \supset \mathbb{Q}[x]$; por outro lado, $x^2 + 1$ é irredutível em $\mathbb{Q}[x]$ ou $\mathbb{R}[x]$ mas é redutível em $\mathbb{C}[x] \supset \mathbb{R}[x] \supset \mathbb{Q}[x]$.

7. É sabido da Álgebra elementar que em $\mathbb{R}[x]$ os únicos polinómios irredutíveis são os polinómios de grau 1 e os polinómios $p(x) = ax^2 + bx + c$ de grau 2 com *discriminante* $\Delta = b^2 - 4ac$ negativo. Provaremos que esta é uma consequência do Teorema Fundamental da Álgebra.

8. Em $\mathbb{Q}[x]$ a identificação dos irredutíveis é mais difícil. Neste caso apenas se conhecem condições suficientes de irredutibilidade e não se conseguem identificar explicitamente os polinómios irredutíveis.

Pretendemos, no que se segue, provar que $\mathbb{K}[x]$ é um domínio de fatorização única.

Proposição 2.25. *Seja $f \in \mathbb{K}[x]$ tal que $\operatorname{gr} f \geq 1$. Então f é um polinómio irredutível ou um produto de polinómios irredutíveis em $\mathbb{K}[x]$.*

Demonstração. Argumentemos por indução no grau de f. Se $\operatorname{gr} f = 1$, então f é irredutível. Se $\operatorname{gr} f > 1$ e f é irredutível não há nada a provar. Caso contrário, existem $g, h \in \mathbb{K}[x]$ com $\operatorname{gr} g, \operatorname{gr} h < \operatorname{gr} f$ tais que $f = gh$ e, por hipótese de indução, g e h ou são irredutíveis ou produto de irredutíveis. Donde, f é um produto de irredutíveis.

□

Lema 2.26. *Sejam f um polinómio irredutível em $\mathbb{K}[x]$ e $g, h \in \mathbb{K}[x]$ tais que $f \mid gh$. Então $f \mid g$ ou $f \mid h$.*

Demonstração. Suponhamos que $f \nmid g$. Seja d um máximo divisor comum de f e g. Então $d \mid f$ e, como f é irredutível, então $d = kf$ ou $d = k$, onde $k \in \mathbb{K}^*$. Se $d = kf$, resulta que $f \mid g$, o que é contraditório. Logo $d = k \in \mathbb{K}^*$ e conclui-se, pelo lema 2.17, que 1 é um máximo divisor comum de f e g. Como tal, pelo Corolário 2.20, existem $a, b \in \mathbb{K}[x]$ verificando $1 = af + bg$ e, por sua vez, $h = haf + hbg$. Mas $f \mid haf$ e, porque $f \mid gh$, também $f \mid hbg$. Portanto, $f \mid h$, como pretendíamos provar.

□

O teorema seguinte destaca a importância dos polinómios irredutíveis em $\mathbb{K}[x]$.

Teorema 2.27 (Unicidade da fatorização em $\mathbb{K}[x]$). *Seja $f \in \mathbb{K}[x]$ tal que $\operatorname{gr} f \geq 1$. Então f tem uma fatorização como produto de polinómios irredutíveis em $\mathbb{K}[x]$, única, a menos do produto por constantes e da ordem dos fatores.*

Demonstração. A existência da fatorização é consequência da Proposição 2.25. Mostremos a unicidade. Suponhamos que

$$f = f_1 \cdots f_r = g_1 \cdots g_s, \tag{2.4}$$

onde f_i, g_j são irredutíveis e $\operatorname{gr} f_i, \operatorname{gr} g_j \geq 1$. Assim, $f_1 \mid g_1 \cdots g_s$ e, pelo lema anterior, $f_1 \mid g_j$, para algum j, $1 \leq j \leq s$. Logo, $f_1 = k_1 g_j$, com $k_1 \in \mathbb{K}^*$, visto que g_1 é irredutível. Excluindo em (2.4) estes dois elementos temos

$$k_1 f_2 \cdots f_r = g_1 \cdots g_{j-1} g_{j+1} \cdots g_s.$$

Repetindo o argumento, obtemos por exaustão, $r = s$ e $f_i = \mu_i g_{\sigma(i)}$, para alguma permutação $\sigma \in S_r$, $\mu_i \in \mathbb{K}^*$ e $i = 1, \cdots, r$. Assim, a decomposição é única a menos do produto por constantes e da ordem pela qual se escrevem os fatores.

□

Vejamos que todo o polinómio irredutível em $\mathbb{Z}[x]$, também o é em $\mathbb{Q}[x]$.

Lema 2.28 (Gauss[4]). *Seja $f \in \mathbb{Z}[x]$. Se f é irredutível em $\mathbb{Z}[x]$ então f é irredutível em $\mathbb{Q}[x]$.*

Demonstração. Suponhamos que f é irredutível em $\mathbb{Z}[x]$ mas redutível em $\mathbb{Q}[x]$. Então existem $g, h \in \mathbb{Q}[x]$ tais que $f = gh$, com $\operatorname{gr} g, \operatorname{gr} h < \operatorname{gr} f$. Seja n o mínimo múltiplo comum dos denominadores dos coeficientes de g e h e p um fator primo de n. Assim, $nf = f'g'$, onde $n \in \mathbb{N}$ e $g', h' \in \mathbb{Z}[x]$ e se

$$g' = g_0 + g_1 x + \cdots + g_r x^r$$
$$h' = h_0 + h_1 x + \cdots + h_s x^s,$$

então $p \mid g_i$, para $i = 0, \cdots, r$ ou $p \mid h_j$, para $j = 0, \cdots, s$, visto que, caso contrário, existem valores mínimos de i, j tais que $p \nmid g_i$ e $p \nmid h_j$. Mas p divide o coeficiente de x^{i+j} em $g'h'$, que é

$$k_{i+j} = h_0 g_{i+j} + h_1 g_{i+j-1} + \cdots h_j g_i + \cdots + h_{i+j} g_0.$$

Logo $p \mid h_j g_i$. Por outro lado, dada a escolha de i e j, p divide todas as parcelas excepto $h_j g_i$, o que é uma contradição.
Sem perda de generalidade, podemos assumir que $p \mid g_i$, para g_i, $(i = 0, \cdots, r)$ e então $g' = pg''$, onde $g'' \in \mathbb{Z}[x]$ tem o mesmo grau de g' (ou g). Escrevendo $n = pn_1$, resulta $pn_1 f = pg''h'$ e $n_1 f = g''h'$. Continuando assim, cortamos todos os factores primos de n

[4]Carl Friedrich Gauss, 1777-1855, foi um dos grandes matemáticos de Göttingen.

até chegar a uma equação do tipo $f = \bar{g}\bar{h}$, onde $\bar{g}, \bar{h} \in \mathbb{Z}[x]$. Mas isto é absurdo visto que, por hipótese, f é irredutível em $\mathbb{Z}[x]$. Logo, f é irredutível em $\mathbb{Q}[x]$, como pretendíamos provar.

□

O Critério que se segue deve-se a Eisenstein [5], prodigioso aluno de Gauss, e permite-nos obter vários exemplos de polinómios irredutíveis em $\mathbb{Q}[x]$.

Teorema 2.29 (**Critério de Eisenstein**). *Seja*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

um polinómio de grau n. Se existe um primo $p \in \mathbb{Z}$ tal que

1. $p \nmid a_n$
2. $p \mid a_i, \quad i = 0, 1, \cdots, n-1$
3. $p^2 \nmid a_0$,

então f é irredutível em $\mathbb{Q}[x]$.

Demonstração. De acordo com o lema de Gauss, basta provar que f é irredutível em $\mathbb{Z}[x]$. Suponhamos, por absurdo, que existem $g, h \in \mathbb{Z}[x]$, com $\leq \operatorname{gr} g, \operatorname{gr} h < \operatorname{gr} f$ tais que $f = gh$. Assim temos

$$g = b_r x^r + \cdots + b_1 x + b_0 \qquad\qquad h = c_s x^r + \cdots + c_1 x + c_0,$$

com $r + s = n$ e $g_0 h_0 = a_0$. Logo, por *2*, $p \mid g_0$ ou $p \mid h_0$, mas por *3*, não divide ambos. Podemos, sem perda de generalidade, assumir que $p \mid g_0$, mas $p \nmid h_0$. Se $p \mid g_i$, para $i = 0, 1, \cdots, r$, então $p \mid a_n$, o que é impossível por *1*. Seja b_j o primeiro coeficiente de g que não é divisível por p. Então

$$a_j = b_j c_0 + \cdots + b_0 c_j,$$

onde $j < n$. Isto implica que p divide c_0, porque p divide $a_j, b_0, \ldots, b_{j-1}$ mas não divide b_j, o que é uma contradição. Portanto, f é irredutível em $\mathbb{Z}[x]$.

□

Exemplos 2.30.

1. Para qualquer $p \in \mathbb{Z}$ primo e $n \geq 1$, $f(x) = x^n - p$ é irredutível em $\mathbb{Z}[x]$ e em $\mathbb{Q}[x]$.
2. Seja $f(x) = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3} \in Q[x]$. O polinómio $f(x)$ é irredutível se e só

$$9f(x) = 2x^5 + 15x^4 + 9x^3 + 3$$

é irredutível sobre $\mathbb{Q}$. Pelo critério de Eisenstein, para $p = 3$, $f(x)$ é irredutível sobre $\mathbb{Q}$.

[5] Ferdinand Gotthold Max Eisenstein, 1823-1852.

3. Sejam p um número primo e $f(x) = 1 + x + \cdots + x^{p-1} \in \mathbb{Z}[x]$. Designemos por

$$\mathbb{Q}(x) = \left\{ \frac{g}{h} : g, h \in \mathbb{Q}[x],\ h \neq 0 \right\}$$

o corpo das fracções de $\mathbb{Q}[x]$. Como um elemento em $\mathbb{Q}(x)$, $f(x) = \dfrac{x^p - 1}{x - 1}$. De modo que

$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1}.$$

Como $p, \binom{p}{2}, \cdots, \binom{p}{p-1}$ são múltiplos de p e $\binom{p}{p-1}$ não é múltiplo de p^2, então $f(x+1)$ é irredutível em $\mathbb{Z}[x]$. Mas o homomorfismo de anéis $\psi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ que é a identidade em $\mathbb{Z}$ e transforma x em $x-1$ é um isomorfismo. Assim, $f(x) = \psi(f(x+1))$ é irredutível, visto que a imagem de um elemento irredutível por um isomorfismo é também um elemento irredutível.

Este exemplo mostra que o Critério de Eisenstein pode ser utilizado em algumas situações onde não se aplica diretamente, como no caso de $f(x) = x^6 + x^3 + 1$, em que

$$\begin{aligned} f(x+1) &= (x+1)^6 + (x+1)^3 + 1 \\ &= x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3 \end{aligned}$$

é irredutível em $\mathbb{Q}[x]$ e, como tal, f é irredutível em $\mathbb{Q}[x]$.

□

Em qualquer anel de polinómios, os polinómios $x - a$ são irredutíveis. Verificaremos que existem corpos onde os únicos polinómios irredutíveis são da forma $x - a$.

Capítulo 3

Teorema Fundamental da Álgebra. Raízes e coeficientes.

3.1 Teorema fundamental da Álgebra

Esta secção está dedicada ao teorema fundamental da Álgebra. Não obstante a sua importância no desenvolvimento histórico da Matemática, abrindo o caminho para o reconhecimento geral dos números complexos, a sua prova quase sempre pouco tem a ver com a Álgebra. Grandes nomes deram o seu contributo neste assunto desde Gauss, Cauchy [1], Liouville [2] e Laplace [3]. Muitas demonstrações têm sido apresentadas (um artigo de Netto e Le Vasseur[4], por exemplo, lista perto uma centena delas) e de tempos em tempos surgem outras. O resultado[5] foi estabelecido por D'Alembert[6] nos finais do século XVIII, mas era já pressentido por Girard [7] e Descartes [8], nos princípios do século XVII. A primeira demonstração integralmente aceite é atribuída a Gauss e aparece na sua tese de doutoramento em 1799. A demonstração que apresentamos é elegante e uma das mais curtas. Deve-se essencialmente a Argand[9] (em 1814) e baseia-se numa anterior, mas falhada, de d'Alembert (em 1746).

Definição 3.1. O corpo $\mathbb{K}$ diz-se *algebricamente fechado* se e só se qualquer polinómio não constante $f \in \mathbb{K}[x]$ tem pelo menos uma raiz em $\mathbb{K}$.

Teorema 3.2 (Teorema Fundamental da Álgebra). $\mathbb{C}$ *é algebricamente fechado.*

[1] Augustin Louis Cauchy, 1789 - 1857

[2] Joseph Liouville, 1809 - 1882

[3] Pierre-Simon Laplace, 1749 - 1827

[4] E. Netto and R. Le Vavasseur: *Les fonctions rationelles,* Enc. Sciences Math. Pures Appl. **I 2** (1907), 1-232

[5] *"Toda a equação algébrica de grau n de coeficientes complexos admite precisamente n raízes complexas."*

[6] Jean Le Rond d'Alembert, 1717 - 1783

[7] Pierre Simon Girard, 1765 - 1836

[8] René Descartes, 1596 - 1650

[9] Jean Robert Argand, 1768 - 1822

Demonstração. Basta provar que qualquer $f(x) \in \mathbb{C}[x]$ com $\operatorname{gr} f(x) \geq 1$ tem uma raiz em $\mathbb{C}$, porque depois o resultado segue por indução no grau de f, visto que se $\alpha \in \mathbb{C}$ é uma raiz, então $f(x) = (x-\alpha)g(x)$.

Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{C}[x]$, $a_n \neq 0$, $n \geq 1$ e consideremos a correspondente função polinomial $f : \mathbb{C} \to \mathbb{C}$, $z \mapsto f(z)$.

Para $z \in \mathbb{C}$ com $|z|$ suficientemente grande

$$f(z) = a_n z^n \left(1 + \frac{a_{n-1}}{a_n z} + \cdots + \frac{a_0}{a_n z^n}\right),$$

onde $\left(1 + \frac{a_{n-1}}{a_n z} + \cdots + \frac{a_0}{a_n z^n}\right) \to 1$ e $|a_n z^n| \to \infty$ quando $|z| \to \infty$.

Assim, para $C = |a_0| = |f(0)|$, existe um número real $R > 0$ tal que $|f(z)| > C$, para todo o $z \in \mathbb{C}$ verificando $|z| > R$.

Por outro lado, a função $|f(z)|$ é contínua, logo atinge mínimo absoluto no conjunto fechado e limitado $A = \{z \in \mathbb{C} : |z| \leq R\}$. Seja $z_0 \in A$ um ponto no qual esse mínimo é atingido. Então $|f(z_0)| \leq |f(0)| = C$ e, portanto, $|f(z_0)| \leq |f(z)|$, para qualquer $z \in \mathbb{C}$, o que significa que $|f(z)|$ tem em z_0 um mínimo absoluto. Resta agora provar que $f(z_0) = 0$. Suponhamos, por absurdo, que $f(z_0) \neq 0$. Chegaremos a uma contradição ao encontrar um elemento $z_1 \in \mathbb{C}$ tal que $|f(z_1)| < |f(z_0)|$.

É possível escrever

$$f(x) = c_0 + c_1(x - z_0) + \cdots + c_n(x - z_0)^n ,$$

com $c_0 = f(z_0) \neq 0$. Sejam $t = x - z_0$ e $m > 1$ tais que $c_1 = \cdots = c_{m-1} = 0$ mas $c_m \neq 0$ (tal m existe visto que $\operatorname{gr} f(x) \geq 1$). Então $f(x) = c_0 + c_m t^m + t^{m+1} g(t)$, com $g(t) \in \mathbb{C}[t]$. Consideremos $\alpha \in \mathbb{C}$ tal que $\alpha^m = -\frac{c_0}{c_m}$ e seja $\beta = \lambda\alpha$, com $\lambda \in \mathbb{R}$ e $0 \leq \lambda \leq 1$. Assim,

$$\begin{aligned} f(z_0 + \beta) &= c_0 + c_m\beta^m + \beta^{m+1} g(\beta) \\ &= c_0 + \lambda^m c_m \alpha^m + \lambda^{m+1}\alpha^{m+1} g(\lambda\alpha) \\ &= c_0(1 - \lambda^m + \lambda^{m+1} c_0^{-1}\alpha^{m+1} g(\lambda\alpha)) . \end{aligned}$$

Consideremos a função contínua

$$\begin{aligned} \varphi : [0,1] &\to \mathbb{R} \\ \lambda &\mapsto |\lambda^{m+1} c_0^{-1}\alpha^{m+1} g(\lambda\alpha)| . \end{aligned}$$

Como φ é contínua e $[0,1]$ é compacto, existe um $1 < k \in \mathbb{R}$ tal que $|\varphi(\lambda)| < k$, para todo o $\lambda \in [0,1]$. Donde,

$$\begin{aligned} |f(z_0 + \lambda\alpha)| &\leq |c_0|(|1 - \lambda^m| + \lambda^{m+1}|c_0^{-1}\alpha^{m+1} g(\lambda\alpha)|) \\ &\leq |c_0|(1 - \lambda^m + \lambda^{m+1} k) \\ &= |c_0|(1 - \lambda^m(1 - \lambda k)) . \end{aligned}$$

Logo, em particular,

$$|f\left(z_0 + \frac{1}{2k}\alpha\right)| \leq |c_0|\left(1 - \left(\frac{1}{2k}\right)^m \frac{1}{2}\right) < |c_0| = |f(z_0)| ,$$

o que é uma contradição. Concluímos portanto que $f(z_0) = 0$, como pretendíamos provar.

□

Como é conhecido, dado um complexo $z = a + ib$, com $a, b \in \mathbb{R}$ e $i^2 = -1$, designamos por *conjugado de* z o complexo que representamos por $\overline{z} = a - ib$. É de verificação imediata o seguinte lema:

Lema 3.3. *Sejam* $z, w \in \mathbb{C}$. *Então:*

1. $\overline{z + w} = \overline{z} + \overline{w}$;
2. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$;
3. z *é real se e só se* $\overline{z} = z$.

É consequência do Teorema Fundamental da Álgebra o:

Corolário 3.4. *Os polinómios mónicos irredutíveis em* $\mathbb{R}[x]$ *são precisamente os polinómios* $x - a$, $a \in \mathbb{R}$ *e* $x^2 + bx + c$ *com* $b, c \in \mathbb{R}$ *verificando* $b^2 - 4c < 0$.

Demonstração. Suponhamos que $p(x) \in \mathbb{R}[x]$ é mónico e irredutível. Seja $\alpha \in \mathbb{C}$ uma raiz de $p(x)$. Se:

- $\alpha = a \in \mathbb{R}$, então $(x - a) \mid p(x)$ e por irredutibilidade, $p(x) = x - a$.
- $\alpha \in \mathbb{C} \setminus \mathbb{R}$ então $\overline{\alpha}$ também é raiz de $p(x)$, visto que $p(\overline{\alpha}) = \overline{p(\alpha)} = 0$. Sejam $b = -(\alpha + \overline{\alpha})$ e $c = \alpha\overline{\alpha}$. Então $b, c \in \mathbb{R}$ e $x^2 + bx + c = (x - \alpha)(x - \overline{\alpha}) \mid p(x)$ em $\mathbb{C}[x]$. Ora, o algoritmo da divisão de $p(x)$ por $x^2 + bx + c$ dá sempre coeficientes reais, logo $x^2 + bx + c \mid p(x)$ em $\mathbb{R}[x]$. Por irredutibilidade, $p(x) = x^2 + bx + c$ e, como não tem raízes reais, $b^2 - 4c < 0$.

□

3.2 Relações entre raízes e coeficientes

A resolução das equações conheceu um rápido desenvolvimento por volta de metade do século XVI até princípios do século XVII. A solução das equações cúbicas e quárticas constituiu um importante marco dando origem à álgebra simbólica, desencadeando procuras de notações eficientes e levando à criação de um novo objeto matemático: os polinómios. Entre outros, nesta evolução, destacam-se os trabalhos de Simon Stevin[10] ("L'Aritmetique", 1585), de François Viète [11] ("In Artem Analyticem Isagoge", 1591, "De Recognitione Aequationum", 1615, publicado postumamente), de René Descartes[12] ("La Geometrie", 1637) e de Albert Girard[13] ("Invention nouvelle en l'algebre", 1629). Estes avanços constituíram

[10] 1548-1620
[11] 1540-1603
[12] 1596-1650
[13] 1595-1632

um conhecimento mais profundo da natureza das equações em alguns pontos importantes como o número de raízes e as relações entre raízes e coeficientes de uma equação.

Girard mostrou que, sendo $x_1, x_2, \cdots, x_n$ soluções de

$$x^n - s_1 x^{n-1} + s_2 x^{n-2} - \ldots + (-1)^n s_n = 0 \ , \tag{3.1}$$

se tinha

$$\begin{aligned} s_1 &= x_1 + \ldots + x_n \\ s_2 &= x_1 x_2 + \ldots + x_{n-1} x_n \\ s_3 &= x_1 x_2 x_3 + \ldots + x_{n-2} x_{n-1} x_n \\ &\ldots \\ s_n &= x_1 x_2 \ldots x_n \end{aligned} \tag{3.2}$$

e fazendo $\sigma_k = \sum_{i=1}^{n} x_i^k$, para qualquer inteiro k, então

$$\begin{aligned} \sigma_1 &= s_1 \\ \sigma_2 &= s_1^2 - 2s_2 \\ \sigma_3 &= s_1^3 - 3s_1 s_2 + 3s_3 \\ \sigma_4 &= s_1^4 - 4s_1^2 s_2 + 4s_1 s_3 - 2s_2^2 - 4s_4. \end{aligned} \tag{3.3}$$

Repare-se que este resultado era mais um postulado do que um teorema porque afirmava a existência de raízes de polinómios, "impossíveis", da forma $a + b\sqrt{-1}$, mas Girard não explicava o que tinha em mente:[14]

> *One could say of what use are these solutions which are impossible, I answer for three things, for the certitude of the general rule, because there is no other solution, for its utility.*

Teria sido interessante compreender como Girard encontrou as relações (3.2) porque, apesar de elas resultarem prontamente da identificação dos coeficientes em

$$x^n - s_1 x^{n-1} + s_2 x^{n-2} - \ldots + (-1)^n s_n = (x - x_1)(x - x_2) \cdots (x - x_n) \ ,$$

esta igualdade não era, provavelmente, conhecida de Girard.

Em meados do século XVIII o facto do número de soluções de uma equação ser igual ao seu grau tornou-se conhecimento comum como uma "tradição" matemática, aceite sem demonstração e inquestionável. Isto constituiu, pelo menos, uma boa hipótese de trabalho e os matemáticos começaram a fazer cálculo formalmente com raízes de equações sem se preocuparem com a sua natureza, levando à descoberta de algumas relações entre coeficientes de um polinómio e respetivas raízes.

Para traduzirmos adequadamente os resultados deste período precisamos de alguns conceitos.

[14] A. Girard, *Invention Nouvelle en l'Algèbre*, réimpression par D. Bierens De Haan, Muré Frères, Leiden, 1884

Como vimos anteriormente, se D é um domínio de integridade e x é uma indeterminada, $D[x]$ é também um domínio de integridade. Podemos então continuar este processo. Se $x_1, x_2, \cdots, x_n$ forem indeterminadas distintas, podemos definir, recursivamente, os domínios de integridade

$$D[x_1], (D[x_1])[x_2], \cdots, (\cdots (D[x_1]) \cdots [x_{n-1}])[x_n] \ .$$

Cada elemento em $(\cdots (D[x_1]) \cdots [x_{n-1}])$ pode ser escrito na forma

$$\sum r_{\alpha_1, \cdots, \alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

onde $r_{\alpha_1, \cdots, \alpha_n} \in D$ e $\alpha_i \in \mathbb{N}_0$. Prova-se [17] que se nesta construção permutarmos os x_i, os anéis que resultam são isomorfos. Escreveremos então

$$D[x_1, \cdots, x_n] \ ,$$

para representar o anel dos polinómios sobre D nas indeterminadas $x_1, \cdots, x_n$, que comutam entre si.

Introduzimos agora a seguinte:

Definição 3.5. Sejam $\mathbb{K}$ um corpo e $x_1, x_2, \cdots, x_n$ indeterminadas. Um polinómio p em $\mathbb{K}[x_1, x_2, \ldots, x_n]$ diz-se *simétrico* se não é alterado quando as indeterminadas permutam arbitrariamente entre si, isto é, se para qualquer $\pi \in S_n$,

$$p(x_{\pi(1)}, \cdots, x_{\pi(n)}) = p(x_1, \cdots, x_n).$$

Os *polinómios simétricos elementares* em $\mathbb{K}[x_1, x_2, \cdots, x_n]$ são

$$\begin{aligned} s_1 &= x_1 + \ldots + x_n = \sum_i x_i \\ s_2 &= x_1x_2 + x_1x_3 \ldots + x_1x_n + x_2x_3 + \cdots x_{n-1}x_n = \sum_{i<j} x_ix_j \\ &\cdots \\ s_n &= x_1x_2 \ldots x_n. \end{aligned} \tag{3.4}$$

Os polinómios simétricos elementares geram o subanel dos polinómios simétricos. Exibimos, sem demonstração, o seguinte:

Teorema 3.6 (**Teorema fundamental dos polinómios simétricos**, [14]). *Seja* $\mathbb{K}$ *um corpo. Então cada polinómio simétrico em* $\mathbb{K}[x_1, x_2, \ldots, x_n]$ *pode ser escrito como um polinómio sobre* $\mathbb{K}$ *nos polinómios simétricos elementares* s_i , $i = 1, \cdots, n$.

Exemplo 3.7. O polinómio $x_1^3 + x_2^3 + x_3^3 \in \mathbb{Q}[x_1, x_2, x_3]$ é simétrico, logo, pode ser expresso como um polinómio em $s_1 = x_1+x_2+x_3$, $s_2 = x_1x_2+x_1x_3+x_2x_3$ e $s_3 = x_1x_2x_3$. Considerações sobre o grau permitem concluir que existem racionais a_1, a_2 e a_3 tais que

$$x_1^3 + x_2^3 + x_3^3 = a_1(x_1 + x_2 + x_3)^3 + a_2(x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) + a_3x_1x_2x_3.$$

Escolhendo convenientemente valores para $x_1, x_2\ x_3$, obtemos:

$$\begin{aligned} 3 &= 27a_1 + 9a_2 + a_3 && (x_1 = x_2 = x_3 = 1) \\ 2 &= 8a_1 + 2a_2 && (x_1 = x_2 = 1, x_3 = 0) \\ 1 &= a_1 && (x_1 = 1, x_2 = x_3 = 0). \end{aligned}$$

A solução deste sistema é $a_1 = 1, a_2 = -3, a_3 = 3$. Assim,

$$x_1^3 + x_2^3 + x_3^3 = (x_1 + x_2 + x_3)^3 - 3(x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) + 3x_1x_2x_3.$$

□

Os polinómios simétricos elementares em $\alpha_1, \ldots, \alpha_n$ escrevem-se em termos dos coeficientes do polinómio cujas raízes são $\alpha_1, \ldots, \alpha_n$. O lema que se segue, cuja demonstração não incluímos, pode ser consultada, por exemplo, em [3] ou [14].

Lema 3.8. *Seja* $\mathbb{K}$ *um corpo e seja* $f(x) = x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{K}[x]$. *Então existe um corpo (*extensão de $\mathbb{K}$, corpo de decomposição de f *)* $L \supseteq \mathbb{K}$ *tal que* $\alpha_1, \ldots, \alpha_n \in L$ *são as raízes de* f, *pelo que* $f(x) = (x - \alpha_1) \ldots (x - \alpha_n) \in L[x]$ *e, portanto,*

$$a_i = (-1)^i s_i(\alpha_1, \ldots, \alpha_n).$$

Corolário 3.9. *Sejam* f, $\alpha_1, \ldots, \alpha_n$, $\mathbb{K}$ *e* L *como nas condições do lema anterior e seja* $p(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \cdots, x_n]$ *um polinómio simétrico. Então* $p(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}$.

Demonstração. Do teorema fundamental dos polinómios simétricos conclui-se que $p(x_1, \ldots, x_n) \in \mathbb{K}[s_1, \ldots, s_n]$. Pelo lema anterior, $s_i(\alpha_1, \ldots, \alpha_n) = (-1)^i a_i \in \mathbb{K}$.

□

Repare-se que as propriedades acima referidas nos permitem obter relações entre as raízes de uma equação polinomial, mesmo sem a resolver, ou obter uma equação polinomial conhecidas as suas raízes.

Exemplo 3.10. As raízes $x_1,\ x_2,\ x_3$ da equação $2x^3 - 4x^2 + 6x + 7 = 0$, ou, equivalentemente, $x^3 - 2x^2 + 3x + \dfrac{7}{2} = 0$, satifazem:

$$\begin{aligned} &x_1 + x_2 + x_3 = 2 \\ &x_1x_2 + x_1x_3 + x_2x_3 = 3 \\ &x_1x_2x_3 = -\frac{7}{2}. \end{aligned}$$

Exemplo 3.11. Sabendo que as raízes de uma dada equação polinomial são $1,\ 1,\ \dfrac{1}{2}$ e -1 é possível obtê-la visto que, tendo grau 4, pode ser escrita como

$$x^4 - s_1x^3 + s_2x^2 - s_3x + s_4 = 0,$$

onde

$$
\begin{aligned}
s_1 &= 1 + 1 + \frac{1}{2} - 1 = \frac{3}{2} \\
s_2 &= 1 \cdot 1 + 1 \cdot \frac{1}{2} + 1 \cdot (-1) + 1 \cdot \frac{1}{2} + 1 \cdot (-1) = -\frac{1}{2} \\
s_3 &= 1 \cdot 1 \cdot \frac{1}{2} + 1 \cdot 1 \cdot (-1) + 1 \cdot \frac{1}{2} \cdot (-1) + 1 \cdot \frac{1}{2} \cdot (-1) = -\frac{3}{2} \\
s_4 &= 1 \cdot 1 \cdot \frac{1}{2} \cdot (-1) = -\frac{1}{2}.
\end{aligned}
$$

A equação pretendida é

$$x^4 - \frac{3}{2}x^3 - \frac{1}{2}x^2 + \frac{3}{2}x - \frac{1}{2} = 0$$

ou, equivalentemente,

$$2x^4 - 3x^3 - x^2 + 3x - 1 = 0.$$

Capítulo 4

Soluções por radicais de equações algébricas

No capítulo anterior provámos a existência de raízes para qualquer equação polinomial com coeficientes complexos, mas não mostrámos como calcular essas raízes efetivamente. Incluiremos de seguida as resoluções clássicas das equações quadráticas, cúbicas e quárticas e apresentaremos alguns pormenores da sua história.

Chamaremos *equação algébrica de grau n* a uma equação do tipo

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = 0 \tag{4.1}$$

onde os coeficientes $a_0,\ a_1,\ \ldots, a_n,\ \ (a_0 \neq 0)$ representam números reais (ou complexos)[1].

Resolver a equação (4.1) é determinar as suas *soluções* (as *raízes* do polinómio na variável x que constitui o primeiro membro), *i. e.*, é encontrar os valores de x que transformam a equação numa identidade verdadeira. Obviamente, essas soluções são funções dos coeficientes $a_0,\ a_1,\ \ldots, a_n$.
A pesquisa do número de soluções duma equação algébrica e da sua determinação foi objeto do trabalho dos matemáticos ao longo dos séculos.
A equação do primeiro grau

$$a_0x + a_1 = 0 \quad (a_0 \neq 0)$$

tem uma só solução $\quad x = -\dfrac{a_1}{a_0}$.

[1]Mais geralmente poderíamos considerar coeficientes num corpo K qualquer, mas não é esse o objetivo neste capítulo do trabalho.

4.1 A equação quadrática

A solução de uma equação quadrática era já conhecida pelos matemáticos da Babilónia que sabiam como "completar o quadrado" e foi popularizada no mundo ocidental durante o Renascimento. Sabemos que a equação do segundo grau

$$a_0x^2 + a_1x + a_2 = 0 \quad (a_0 \neq 0) \tag{4.2}$$

tem soluções dadas pela fórmula

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_0}.$$

As duas soluções α_1 e α_2 da equação (4.2) verificam

$$\alpha_1 + \alpha_2 = -\frac{a_1}{a_0}, \quad \alpha_1\alpha_2 = \frac{a_2}{a_0}\ .$$

4.2 A equação cúbica

Será possível encontrar uma fórmula semelhante para resolver equações do terceiro grau

$$a_0x^3 + a_1x^2 + a_2x + a_3 = 0 \quad (a_0 \neq 0)? \tag{4.3}$$

E de grau superior? Existirá um processo geral para calcular as raízes de equações de grau superior a dois, a partir dos coeficientes, aplicando um número finito de vezes as operações racionais (adição, subtração, multiplicação e divisão) e a extração de raízes? As soluções assim obtidas designam-se *soluções por radicais*.

Reparemos que na procura das soluções da equação (4.1) podemos supor, sem perda de generalidade, $a_0 = 1$. Além disso basta considerar o caso $a_1 = 0$, visto que supondo já $a_0 = 1$, a mudança de variável

$$x = y - \frac{a_1}{n}$$

transforma o polinómio no primeiro membro num polinómio em y, cujo coeficiente de y^{n-1} é zero, sendo as raízes do primeiro polinómio facilmente calculáveis a partir das raízes deste novo polinómio.

A equação cúbica (4.3) é equivalente a $x^3 + \frac{a_1}{a_0}\,x^2 + \frac{a_2}{a_0}\,x + \frac{a_3}{a_0} = 0$. Se na equação

$$x^3 + ax^2 + bx + c = 0.$$

fizermos a substituição $x = y - \frac{a}{3}$

$$\left(y - \frac{a}{3}\right)^3 + a\,\left(y - \frac{a}{3}\right)^2 + b\,\left(y - \frac{a}{3}\right) + c = 0$$

obtemos uma nova equação desprovida do termo do segundo grau:

$$y^3 + \left(b - \frac{a^2}{3}\right) y + \frac{2a^3}{27} - \frac{ab}{3} + c = 0. \tag{4.4}$$

Basta, portanto estudar as equações do terceiro grau do tipo

$$x^3 + px + q = 0. \tag{4.5}$$

Para encontrarmos as soluções desta equação, façamos $x = u + v$ em (4.5) e obtemos

$$u^3 + v^3 + 3u^2v + 3uv^2 + p(u + v) + q = 0$$

ou seja,

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0.$$

Se existirem números u, v que verifiquem

$$\begin{cases} u^3 + v^3 = -q \\ uv = -\dfrac{p}{3}, \end{cases}$$

isto é, tais que

$$\begin{cases} u^3 + v^3 = -q \\ u^3v^3 = -\dfrac{p^3}{27}, \end{cases}$$

então $x = u + v$ será solução de (4.5).

Pretendemos, pois, calcular u^3 e v^3 conhecendo a sua soma e o seu produto. Assim, u^3 e v^3 são as raízes da equação de segundo grau

$$w^2 + qw - \frac{p^3}{27} = 0$$

e, portanto,

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \qquad \text{e} \qquad v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Como consequência têm-se as três raízes da equação (4.5), na fórmula devida a Tartaglia:

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \tag{4.6}$$

Se a cada raiz somarmos $-\dfrac{a_1}{3a_0}$, obtemos todas as soluções de (4.3).

□

Observação 4.1. A existência de uma fórmula resolvente para a equação do 3.º grau não corresponde a uma situação completamente satisfatória do ponto de vista prático, visto que muitas vezes as expressões fornecidas pelas fórmulas "escondem" as raízes. Com efeito, se considerarmos, por exemplo, a equação

$$x^3 - 13x - 12 = 0,$$

de acordo com a fórmula obtida, as raízes são dadas por

$$x = \sqrt[3]{6 + i\frac{35}{\sqrt{27}}} + \sqrt[3]{6 - i\frac{35}{\sqrt{27}}},$$

que nada adianta em termos práticos. Contudo, como se pode ver diretamente, a equação dada tem como soluções -3, -1 e 4.

Observação 4.2. Note-se que conhecidas u_1 e v_1, raízes cúbicas de u^3 e v^3, respetivamente, tais que

$$u_1 v_1 = -\frac{p}{3},$$

então, utilizando a notação polar $e^{i\theta} = \cos\theta + i\,\mathrm{sen}\,\theta$, sendo $\omega = e^{2\pi i/3}$ uma das raízes cúbicas da unidade, temos também

$$(u_1\omega)(v_1\omega^2) = (u_1\omega^2)(v_1\omega) = -\frac{p}{3}.$$

Deste modo, temos as três raízes de (4.5) dadas por:

$$u_1 + v_1, \quad u_1\omega + v_1\omega^2, \quad u_1\omega^2 + v_1\omega.$$

□

Consideremos agora

$$g(x) = x^3 + px + q \in \mathbb{R}[x].$$

Explicaremos a natureza das raízes de $g(x)$, a partir do sinal do discriminante

$$D = \frac{p^2}{4} + \frac{p^3}{27}.$$

Veremos que se $D > 0$, a equação $g(x) = 0$ tem uma raiz real e duas raízes complexas conjugadas; se $D = 0$, tem uma ou duas raízes reais e se $D < 0$, como acontece no exemplo referido na observação 4.1 , têm-se três raízes reais simples. Este caso é por muitos considerado um *aspecto paradoxal* da fórmula de Ferro e Tartaglia, chamado tradicionalmente "caso irredutível", porque ao tentarmos eliminar os radicais recaímos noutra equação de terceiro grau, como detalharemos adiante.

Estudemos então a natureza das raízes do polinómio cúbico. Consideremos:

i) D > 0

Neste caso $\sqrt{D} \in \mathbb{R}$ e podemos escolher as raízes cúbicas reais

$$u_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{D}} = r_1 \in \mathbb{R} \qquad \text{e} \qquad v_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{D}} = r_2 \in \mathbb{R}.$$

A raiz $x_1 = r_1 + r_2$ é real,

$$x_2 = r_1\omega + r_2\omega^2 \qquad \text{e} \qquad x_3 = r_1\omega^2 + r_2\omega$$

são raízes complexas conjugadas com parte imaginária não nula, visto que

$$\overline{\omega} = \omega^2, \qquad \overline{x_2} = \overline{r_1\omega + r_2\omega^2} = x_3 \qquad \text{e} \qquad r_1 \neq r_2.$$

ii) D = 0

Aqui $g(x)$ tem uma raiz tripla, $x = 0$, quando $q = 0$. Se $q \neq 0$, o polinómio $g(x)$ admite duas raízes reais, uma simples:

$$x_1 = 2\sqrt[3]{-\frac{q}{2}}$$

e outra

$$x_2 = x_3 = -\sqrt[3]{-\frac{q}{2}},$$

com multiplicidade dois.

iii) D < 0

Nesta situação tem-se $p < 0$ e escrevendo

$$\sqrt{D} = i\sqrt{-D},$$

podemos considerar dois complexos não reais conjugados

$$-\frac{q}{2} + i\sqrt{-D} = ae^{i\alpha} \qquad \text{e} \qquad -\frac{q}{2} - i\sqrt{-D} = ae^{-i\alpha},$$

onde $-\pi < \alpha < \pi$ e $a > 0$ é tal que $a^2 = -\left(\frac{p}{3}\right)^3 > 0$.

Sejam agora $u_1 = \sqrt[3]{a}e^{i\alpha/3}$ e $v_1 = \sqrt[3]{a}e^{-i\alpha/3}$, onde $\sqrt[3]{a}$ é a raiz cúbica real de $a \in \mathbb{R}$. Então

$$x_1 = u_1 + v_1, \quad x_2 = u_1\omega + v_1\omega^2, \quad x_3 = u_1\omega^2 + v_1\omega$$

são raízes reais de $g(x)$, visto que u_1 e v_1 são complexos conjugados, assim como ω e ω^2. Um cálculo direto permite concluir que elas são distintas.

□

Exemplo 4.3. A equação

$$x^3 - 6x - 4 = 0$$

tem $D = \frac{16}{4} - \frac{216}{2} = -4 < 0$. Existem, portanto, três raízes reais simples. Ora,

$$u^3 = 2 + 2i = \sqrt{8}e^{i\pi/4} \quad \text{e} \quad v^3 = 2 - 2i = \sqrt{8}e^{-i\pi/4}.$$

Escolhendo uma das três raízes cúbicas de $2 + 2i$, $u_1 = \sqrt{2}e^{i\pi/12}$ e o valor correspondente $v_1 = \sqrt{2}e^{-i\pi/12}$, obtém-se

$$x_1 = u_1 + v_1 = 2\sqrt{2}\cos\left(\frac{\pi}{12}\right) = 1 + \sqrt{3}.$$

As restantes raízes são

$$x_2 = \sqrt{2}e^{i\pi/12}e^{2\pi i/3} + \sqrt{2}e^{-i\pi/12}e^{4\pi i/3} = -2$$

e

$$x_3 = \sqrt{2}e^{i\pi/12}e^{4\pi i/3} + \sqrt{2}e^{-i\pi/12}e^{2\pi i/3} = 1 - \sqrt{3}.$$

Observações 4.4.

1. O chamado **caso irredutível** é muito interessante do ponto de vista histórico. Quando $D < 0$ existem três raízes reais mas a Fórmula de Cardano exibe estas raízes como somas de números complexos não reais. O termo *irredutível* não tem nada a ver com a irredutibilidade de polinómios, mas prende-se com a dificuldade deste caso que não só precisa do conceito de número imaginário, que teve uma aceitação quase nula no século XVI, demorando a sua consagração até ao século XIX, como também dá lugar a cálculos circulares. Vejamos:

   Sejam $s, t \in \mathbb{R}$ com $t \neq 0$. Procuremos $a, b \in \mathbb{R}$ que verifiquem

   $$(a + ib)^3 = s + it.$$

   Desenvolvendo a expressão no primeiro membro e, por igualdade de complexos obtemos

   $$a^3 - 3ab^2 = s \quad \text{e} \quad 3a^2b - b^3 = t$$

   e, dado que $t \neq 0$ também $b \neq 0$. Efetuando alguns cálculos e tomando $w = \frac{a}{b}$, vem:

   $$w^3 - 3w = \frac{s}{b^3}$$

   e

   $$3w^2 - 1 = \frac{t}{b^3},$$

   donde concluímos que

   $$w^3 - \frac{3s}{t}w^2 - 3w + \frac{s}{t} = 0.$$

Se tomarmos y tal que $w = y + \dfrac{s}{t}$, temos a equação cúbica reduzida

$$y^3 - 3ky - 2\frac{sk}{t} = 0, \quad \text{com} \quad k = 1 + \frac{s^2}{t^2} \in \mathbb{R}^+.$$

Resolvendo esta equação como indicámos no início desta secção e escrevendo $\sqrt{D} = ik$, vem

$$u = \sqrt[3]{sk/t + ki} = \sqrt[3]{k/t} \cdot \sqrt[3]{s + it}.$$

Como o nosso propósito era exprimir $\sqrt[3]{s + it}$ na forma $a + ib$, estas manobras nada adiantaram.

2. **Resolução trigonométrica**

É possível achar aproximações das soluções de uma equação cúbica no *caso irredutível* com a ajuda de uma tabela de cossenos. Esta resolução é devida a F. Viète.

Seja $g(x) = x^3 + px + q \in \mathbb{R}[x]$ e suponhamos que $D = \left(\dfrac{q}{2}\right)^2 + \left(\dfrac{p}{3}\right)^3 < 0$; então g tem todas as suas raízes reais e resulta também que

$$p < 0 \qquad \text{e} \qquad 0 < \frac{27q^2}{-4p^3} < 1\ . \tag{4.7}$$

Ora, atendendo a que:

i) $\cos 3\theta = 4\cos^3\theta - 3\cos\theta, \quad \forall\theta \in \mathbb{R},$

ii) $\cos 3\theta = \cos(3\theta + 2\pi) = \cos(3\theta + 4\pi),$

concluímos que $\cos\theta, \quad \cos(\theta + \dfrac{2\pi}{3})$ e $\cos(\theta + \dfrac{4\pi}{3})$ são as raízes reais de

$$f_\theta(t) = t^3 - \frac{3}{4}t - \frac{1}{4}\cos 3\theta \in \mathbb{R}[t].$$

O objetivo é tentar transformar $g(x)$ de modo a assumir o aspeto de $f_\theta(t)$, para θ conveniente. Como as raízes de f_θ são limitadas por -1 e 1, façamos $x = kt$, com $0 \neq k \in \mathbb{R}$ e, para encontrarmos as raízes de $g(x)$, basta calcularmos as raízes de

$$h(t) = t^3 + \frac{p}{k^2}t + \frac{q}{k^3}\ .$$

Sejam $k = \sqrt{-4p/3} \in \mathbb{R}$ e $\theta \in \mathbb{R}$ tal que $\cos 3\theta = -\dfrac{-4q}{k^3}$ (existe por (4.7)) e temos

$$h(t) = f_\theta(t).$$

Donde, as raízes de $h(t)$ são as raízes de $f_\theta(t)$. Encontrando uma aproximação de $3\theta = \arccos(-4q/k^3)$ (por exemplo com recurso a uma tabela de cosenos),obtêm-se também aproximações às três raízes: $\cos\theta, \quad \cos(\theta + \dfrac{2\pi}{3})$ e $\cos(\theta + \dfrac{4\pi}{3})$ e, por fim, as aproximações das raízes de $g(x)$.

□

Vejamos alguns exemplos retirados do livro de Álgebra de Euler, escrito em 1770.

Exemplo 4.5. A equação $x^3 - 6x - 9 = 0$ tem $D = \frac{81}{4} - \frac{216}{27} = \frac{49}{4} > 0$, logo admite uma raiz real e um par de raízes complexas. A raiz real resulta de (4.6) e é

$$x_1 = \sqrt[3]{\frac{9}{2} + \frac{7}{4}} + \sqrt[3]{\frac{9}{2} - \frac{7}{4}} = 2 + 1 = 3.$$

Atendendo a que $x^3 - 6x - 9 = (x - 3)(x^2 + 3x + 3)$, conclui-se que as raízes complexas são $x_2 = -\frac{3}{2} + i\frac{\sqrt{2}}{2}$ e $x_3 = -\frac{3}{2} - i\frac{\sqrt{2}}{2}$.

Exemplo 4.6. Seja $x^3 - 3x - 2 = 0$. Neste caso $D = 0$ e por aplicação da fórmula (4.6), ou por inspeção (com base nos divisores do termo independente), tem-se a raiz $x = 2$. Como $x^3 - 3x - 2 = (x-2)(x+1)^2$, resulta que -1 é a outra raiz do trinómio, com multiplicidade igual a 2.

A fórmula desenvolvida pelos matemáticos italianos Ferro e Tartaglia e publicada por Cardano, para além do seu valor histórico, explica também algumas propriedades interessantes, como por exemplo, o facto de a expressão

$$\sqrt[3]{20 + 14\sqrt{2}} + \sqrt[3]{20 - 14\sqrt{2}}$$

em $\mathbb{R}$ representar um número inteiro.

Exemplo 4.7. A equação $x^3 - 6x - 40 = 0$ tem $D = 392 > 0$ e, testando os divisores de 40, verificamos que 4 é uma sua raiz. Logo, de

$$x^3 - 6x - 40 = (x - 4)(x^2 + 4x + 10)$$

surgem as duas outras raízes do trinómio: 4 e $-2 \pm i\sqrt{6}$. Concluímos assim que

$$\sqrt[3]{20 + 14\sqrt{2}} + \sqrt[3]{20 - 14\sqrt{2}} = 4.$$

Nem sempre a utilização da fórmula para as equações cúbicas se revela necessária, como atestam os exemplos anteriores onde as raízes reais poderiam ser obtidas por simples inspeção. Contudo, noutros casos é essencial, caso não queiramos utilizar métodos numéricos de resolução.

Exemplo 4.8. A equação $x^3 + 3x + 2 = 0$, com $D = 2 > 0$, tem um par de raízes complexas e uma raiz real r dada pela fórmula (4.6),

$$r = \sqrt[3]{-1 + \sqrt{2}} + \sqrt[3]{-1 - \sqrt{2}} = \sqrt[3]{-1 + \sqrt{2}} - \sqrt[3]{1 + \sqrt{2}}.$$

4.3 A equação quártica

Consideremos a equação

$$x^4 + bx^3 + cx^2 + dx + e = 0 \tag{4.8}$$

com b, c, d, e em $\mathbb{R}$ ou $\mathbb{C}$, de onde se tem

$$x^4 + bx^3 = -cx^2 - dx - e.$$

"Completando o quadrado" no primeiro membro, temos

$$\left(x^2 + \frac{1}{2}\, bx\right)^2 = \left(\frac{1}{4}\, b^2 - c\right) x^2 - dx - e.$$

Introduzamos uma nova variável, y :

$$\left(x^2 + \frac{1}{2}\, bx + \frac{1}{2}\, y\right)^2 = \left(\frac{1}{4}\, b^2 - c + y\right) x^2 + \left(\frac{1}{2}\, by - d\right) x + \left(\frac{1}{4}\, y^2 - e\right). \tag{4.9}$$

O segundo membro da igualdade anterior é um quadrado perfeito se e só se

$$\left(\frac{1}{2}\, by - d\right)^2 - 4\left(\frac{1}{4}\, b^2 - c + y\right)\left(\frac{1}{4}\, y^2 - e\right) = 0,$$

ou seja se e só se y é raiz de

$$f_r(x) = x^3 - cx^2 + (bd - 4e)x - (d^2 + e(b^2 - 4c)) = 0. \tag{4.10}$$

Designemos $f_r(x)$ por *polinómio cúbico resolvente* e seja y_1 uma sua qualquer raiz, que pode eventualmente ser determinada com recurso à fórmula de Cardan. Para este y_1, o segundo membro de (4.9) tem a forma $(mx+n)^2$, onde m, n são determinados a partir dos coeficientes b, c, d, e e da raiz y_1. Assim, de (4.9) resulta

$$x^2 + \left(\frac{1}{2}\, b - m\right) x + \left(\frac{1}{2}\, y_1 - n\right) = 0 \tag{4.11}$$

ou

$$x^2 + \left(\frac{1}{2}\, b + m\right) x + \left(\frac{1}{2}\, y_1 + n\right) = 0. \tag{4.12}$$

As quatro raízes das últimas equações quadráticas são as quatro raízes da equação (4.8).

□

Exemplo 4.9. A equação

$$x^4 + 4x^3 + 2x^2 + 4x + 1 = 0$$

tem polinómio cúbico resolvente dado por

$$f_r(x) = x^3 - 2x^2 + 12x - 24,$$

que admite 2 como uma das raízes. As equações do segundo grau correspondentes

$$x^2 + 1 = 0 \quad \text{e} \quad x^2 + 4x + 1 = 0$$

dão as raízes da equação quártica dada: $\pm i$ e $-2 \pm \sqrt{3}$.

Observação 4.10. Sendo x_1, x_2, x_3, x_4 as raízes da equação quártica em (4.8) e y_1 uma raiz do polinómio cúbico resolvente, têm-se as relações $x_1x_2 = \frac{1}{2}\, y_1 - n$ e $x_3x_4 = \frac{1}{2}\, y_1 + n$, donde se deduz que $y_1 = x_1x_2 + x_3x_4$. O resultado seguinte estabelece as relações ente as raízes da equação quártica e as restantes raízes do respetivo polinómio cúbico resolvente.

Proposição 4.11. *Sejam* x_1, x_2, x_3, x_4 *as raízes do polinómio* $f(x) = x^4 + bx^3 + cx^2 + dx + e \in \mathbb{R}[x]$ *e* y_1, y_2, y_3 *dadas por*

$$y_1 = x_1x_2 + x_3x_4, \qquad y_2 = x_1x_3 + x_2x_3, \qquad y_3 = x_1x_4 + x_2x_3.$$

Então y_1, y_2, y_3 *são as raízes do polinómio cúbico resolvente em (4.10).*

Demonstração. Como x_1, x_2, x_3, x_4 são as raízes do polinómio $f(x)$, então tem-se pelo Teorema fundamental dos polinómios simétricos

$$\begin{aligned} -b &= x_1 + x_2 + x_3 + x_4 \\ c &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ -d &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ e &= x_1x_2x_3x_4. \end{aligned}$$

Cálculos diretos comprovam que:

$$\begin{aligned} &y_1 + y_2 + y_3 = c\ , \\ &y_1y_2 + y_1y_3 + y_2y_3 = bd - 4e, \\ &y_1y_2y_3 = d^2 + e(b^2 - 4c), \end{aligned}$$

tendo-se portanto

$$(x - y_1)(x - y_2)(x - y_3) = x^3 - cx^2 + (bd - 4e)x - (d^2 + e(b^2 - 4c)),$$

o que nos permite concluir que y_1, y_2, y_3 são as raízes do polinómio cúbico resolvente em (4.10).

4.4 Irresolubilidade de equações gerais de quinto grau

Como vimos, a solução de uma equação quadrática era conhecida pelos matemáticos da Babilónia e foi popularizada no mundo ocidental durante o Renascimento. Em 1545, a publicação da *Ars Magna* de Geronimo Cardano (1501-1576), também conhecido por Cardan, inclui fórmulas para a resolução de equações do terceiro e quarto graus, atribuídas pelo autor, respetivamente, a Niccolo Tartaglia (1500-1565) e Ludovico Ferrari (1522-1565). Estas soluções constituíram um forte estímulo na procura de fórmulas para resolução de equações algébricas de graus mais elevados.

Entre os matemáticos que fizeram investigações incluem-se Tschirnhaus (1651-1708), Euler (1707-1783), Vandermonde (1735-1796) e Lagrange(1736-1813). Vandermonde publicou expressões para as 11-ésimas raízes da unidade em $\mathbb{C}$. Lagrange analisou os truques

utilizados nos polinómios de grau 2,3 e 4 e mostrou que nas resoluções existe uma ideia comum subjacente, nomeadamente a definição de funções das raízes que permanecem invariantes sob certas permutações das raízes e provou que esta abordagem falha no caso de um polinómio de grau 5.

Em 1799, Paollo Ruffini publicou uma demonstração, hoje considerada incompleta, que pretendia provar a inexistência de uma fórmula geral para resolver uma equação polinomial de grau 5. Em 1824, Niels Henrik Abel (1802-1829) mostrou que:

existem equações polinomiais do quinto grau cujas soluções não podem ser obtidas por radicais.

Inspirado pela demonstração de Abel da impossibilidade de resolução de grau cinco, Évariste Galois (1811-1832) iniciou o estudo de equações algébricas de grau arbitrário, e mostrou não só a impossibilidade de resolução da equação algébrica geral de grau maior ou igual a cinco, como deu ainda um critério para decidir se uma equação particular pode ser resolvida e, em caso afirmativo, um método de resolução. Este matemático, com uma vida breve e aventurosa, que morreu num duelo depois de ter escrito a sua resolução numa carta a um amigo, é considerado o criador da Álgebra Moderna e o seu trabalho teve consequências muito para além do problema original da resolução de equações algébricas por radicais. Tendo em vida visto gorada a publicação dos seus trabalhos nos círculos científicos de Paris, foi em 1843 que Joseph Liouville apresentou o trabalho de Galois à Academia das Ciências em Paris.

Galois associou a um polinómio $f(x) \in \mathbb{Q}[x]$ um certo grupo, dito *grupo de Galois*, $\Gamma(f)$, de permutações das raízes de f. Galois mostrou que $f(x) = 0$ é resolúvel por radicais se e só se $\Gamma(f)$ é um grupo *solúvel*, ou seja se e só se é possível estabelecer uma cadeia de subgrupos distintos de $\Gamma(f)$, em que cada um é normal no que se lhe segue, isto é, existem subgrupos normais $H_m,\ H_{m-1}, \ldots, H_1, H_0$ verificando

$$H_m \trianglelefteq H_{m-1} \trianglelefteq \cdots H_1 \trianglelefteq H \trianglelefteq \Gamma(f) \tag{4.13}$$

tais que $|H_m| = 1$ e os números $\dfrac{|H_{m-1}|}{|H_m|}, \cdots, \dfrac{|H|}{|H_1|}, \dfrac{|G|}{|H|}$ são todos primos. [11]

Uma consequência deste resultado é a inexistência de uma fórmula resolvente para todas as equações polinomiais de grau 5. Repare-se que S_5 é tal que $|S_5| = 120$ e admite apenas dois subgrupos normais, com ordens 60 e 1. Ora, $\frac{120}{60} = 2$ é primo, mas $\frac{60}{1}$ não.

Também a partir desse resultado é fácil verificar que uma equação quártica é resolúvel por radicais: o seu grupo de Galois tem ordem vinte e quatro e é possível obter uma sequência de subgrupos normais nas condições de (4.13) com doze, quatro, dois e um elementos. Como

$$\frac{24}{12} = 2,\ \frac{12}{4} = 3,\ \frac{4}{2} = 2,\ \frac{2}{1} = 2$$

são primos, a conclusão é imediata. Deduz-se ainda que uma fórmula deste tipo se constrói juntando uma raiz quadrada, uma raiz cúbica e mais duas raízes quadradas, como se con-

firma na secção 4.3. Estes e outros resultados da Teoria de Galois podem ser aprofundados em [3], [8], [14], [1], entre muitos outros.

As conclusões de Galois não impedem a existência de algoritmos resolventes para algumas equações polinomiais de grau superior a 4. Afirmam a impossibilidade da existência de uma fórmula resolvente para todas. Este facto não se traduziu numa completa impossibilidade de obtenção de soluções exatas destas equações polinomiais. Nos séculos XVIII e XIX várias ferramentas altamente sofisticadas, que ultrapassam as limitações da Teoria de Galois, foram desenvolvidas com esse propósito, envolvendo: séries (Lambert (1757), Euler (1770), Chebychev (1838), e Eisenstein (1844)), equações diferenciais (Cockle (1860) e Harley (1862)), funções teta (Hermite (1858)) e hipergeométricas (Clausen (1828)),... Esses resultados, contudo, transcendem o âmbito deste trabalho.

Bibliografia

[1] Alberto Elduque. *Groups and Galois Theory.* Course Notes, 2009 - 2011

[2] Carl B. Boyer. *História da Matemática.* Edgard Blucher, 1996.

[3] E. Artin. *Galois Theory*,

[4] Elon L. Lima, Paulo C. P. Carvalho, Eduardo Wagner, Augusto C. Morgado. *A Matemática do Ensino Médio - Volume 1.* Sociedade Brasileira de Matemática, 9.ª edição, 2006

[5] Elon L. Lima, Paulo C. P. Carvalho, Eduardo Wagner, Augusto C. Morgado. *A Matemática do Ensino Médio - Volume 3.* Sociedade Brasileira de Matemática, 6.ª edição, 2006

[6] Elon L. Lima. *Meu Professor de Matemática e outras histórias.* Sociedade Brasileira de Matemática, 5.ª edição, 2006

[7] Garrett Birkhoff, Saunders Mac Lane. *A Survey of Modern Algebra.* A K Peters, 5.ª edição, 1997

[8] Ian Stewart. *Galois Theory.* Chapmann & Hall, 1998

[9] J. Eurico Nogueira, Suzana Nápoles, António Monteiro, José A. Rodrigues, M. Adelaide Carreira. *Contar e Fazer Contas.* SPM e Gradiva, 1.ª edição, 2004

[10] J. Silva Oliveira. *As equações algébricas de 3.º, 4.º e 5.º grau*

[11] Jean-Pierre Tignol. *Galois' Theory of Algebraic Equations.* World Scientific, 2001

[12] Jorge Picado. *Corpos e equações algébricas,* 2007

[13] Martin Aigner, G. M. Ziegler. *Proofs from the Book,* 4.ª ed., Springer, 2010

[14] Owen J. Brison. *Teoria de Galois.* Textos de Matemática, Volume 6, Departamento de Matemática da Faculdade de Ciências da Universidade de Lisboa, 4.ª edição, 2003

[15] Rui L. Fernandes e M. Ricou. *Introdução à Álgebra.* IST Press, 2004

[16] Pedro J. Freitas. *Polinómios*. Textos de Matemática, Volume 20, Departamento de Matemática da Faculdade de Ciências da Universidade de Lisboa, 2010

[17] B. L. van der Warden. *Algebra*, Vol. I, Springer-Verlag, New York, 1991