



João Luís
da Costa Nunes

Zeros de polinómios: localização, fórmulas
resolventes e aplicações



**João Luís
da Costa Nunes**

Zeros de polinómios: localização, fórmulas resolventes e aplicações

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestrado em Matemática, realizada sob orientação científica de Paulo José Fernandes Almeida, Professor Auxiliar do Departamento de Matemática da Universidade de Aveiro.

Mais uma vez, à minha M-estrela que teria feito, neste ano, 100 anos! O seu brilho não parou de brilhar e insiste em contagiar-me e inspirar-me em fazer sempre mais, sem grandes pausas. Às outras que a ela se foram juntando e que também brilham, contribuindo para mais luz!

O júri / The jury

Presidente / President

Professora Doutora Andreia Oliveira Hall

Professora Associada da Universidade de Aveiro

Vogais / Committee

Professor Doutor Paulo José Fernandes Almeida

Professor Auxiliar da Universidade de Aveiro (orientador)

Professor Doutor Pedro Jorge Santos Freitas

Professor Auxiliar da Universidade de Lisboa

Agradecimentos / Acknowledgements

Agradeço ao Professor Paulo Almeida o acolhimento humano, a capacidade humilde e rigorosa com que tratou a minha sugestão inicial, transformando-a em algo mais rico e mais completo. Agradeço a forma dedicada, pronta e rigorosa, bem como o estímulo e reforços positivos com que pautou a sua presença neste trabalho. Agradeço a todos aqueles que me ouviram falar sobre o assunto aqui tratado, em especial àquele que mais me ouve nos últimos tempos, em tudo. Agradeço ainda aos alunos que me têm, ao longo dos anos, e em especial nos dois últimos, acompanhado e/ou provocado «encontros» que me obrigam a ir mais além. Uma palavra de reconhecimento aos Matemáticos que nesta dissertação são mencionados pelo seu trabalho e por me terem possibilitado esta pequena «viagem» a um universo que desconhecia.

Palavras-chave

Polinómios, número de zeros, localização de zeros, fórmulas resolventes, construções com régua e compasso

Resumo

Nesta dissertação apresentamos deduções das fórmulas resolventes das equações de graus inferiores a cinco e os trabalhos de Abel e de Galois, concorrentes para a prova da não existência de fórmulas congêneres para as equações de grau superior, usando radicais.

Tratamos, usando fundamentos algébricos envolvendo o grau de uma extensão de um corpo, a impossibilidade de algumas construções geométricas usando apenas régua e compasso. Apresentamos ainda algumas regras para a determinação do número de zeros reais de um polinómio e sua localização. Sobre este assunto, propomos um guião de uma tarefa aplicada a alunos do 11º ano de Ciências e Tecnologias como aplicação/extensão de conteúdos abordados no Programa da disciplina de Matemática A do Ensino Secundário.

Keywords

Polynomials, number of roots, location of roots, resolvent formulas, constructions with ruler and compass

Abstract

In this dissertation we present deductions of the resolvent formulas for the equations of degrees below five and the works of Abel and Galois, competing for the proof of the non-existence of similar formulas for higher degree, using radicals. Using algebraic foundations involving the degree of a field extension, we show, the impossibility of several geometric constructions with only ruler and compass. We also present some rules for computing the number of polynomial real roots as well as their location. On this subject, we propose a script of a task for students of the «11^o ano, Ciências e Tecnologias» as an application/extension of the contents of the «Matemática A» course Program.

Conteúdo

1	Introdução	1
2	Preliminares	3
2.1	Noções básicas de Álgebra abstrata	3
2.2	Noções básicas de Análise	6
3	Fórmulas resolventes	9
3.1	Equações lineares e do 2º grau	9
3.2	Equações cúbicas	10
3.3	Equações do 4º grau	17
4	Equações do 5º grau	21
4.1	Introdução	21
4.2	Resolubilidade de equações do 5º grau através de radicais	22
5	Construções com régua e compasso	27
5.1	Os problemas dos gregos	27
5.1.1	A duplicação do cubo	27
5.1.2	A trisseção do ângulo	28
5.1.3	A quadratura do círculo	28
5.1.4	A construção de um heptágono regular numa circunferência dada	28
5.2	As regras impostas pelos gregos	29
5.3	A solução algébrica dos problemas	30
6	Número e localização de zeros reais de um polinómio	39
6.1	Número de zeros reais de um polinómio	41
6.1.1	Regra de Budan-Fourier	41
6.1.2	Regra dos sinais de Descartes	42
6.1.3	Teorema de Sturm	44
6.2	Localização dos zeros de um polinómio	47
7	Conclusões	51
A	Roteiro da tarefa de grupo	57
A.1	Enquadramento e introdução	57
A.2	Descrição da tarefa	59
A.3	Soma e produto das soluções de uma equação do 2º grau	59
A.4	Número e localização de zeros reais de um polinómio	60

A.4.1	Regra dos sinais de Descartes	60
A.4.2	Regra de Budan-Fourier	62

Lista de Figuras

5.1	Construção de um segmento de reta de comprimento $\sqrt{\alpha}$	30
5.2	Construção de um ângulo de amplitude $\frac{\pi}{3}$ radianos	34
6.1	Gráfico da função polinomial definida por $p(x) = x^4 - 13x^3 + 3x^2 + 124x + 36$.	49

Capítulo 1

Introdução

Em maio de 2019, numa aula de Matemática A da turma do 10^o CT4 da Escola Secundária Lima-de-Faria- Cantanhede, surgia casualmente o primeiro contributo para o tema desta dissertação. Tratávamos o tema “Polinómios” e numa breve introdução histórica ao capítulo, os autores do Manual adotado (*Novo Espaço, Matemática A*, B. Costa e E. Rodrigues, Porto Editora) faziam uma referência muito breve à Regra de Descartes (1596-1650) para determinação do número de soluções de uma equação. Não muito tempo depois, alguém, exterior a esta realidade do Ensino Secundário, questionava o autor desta dissertação se os alunos deste nível de ensino conheciam a referida Regra!

Foi este o segundo contributo para a escolha do tema: gostaríamos que a dissertação visasse polinómios, nomeadamente o estudo de regras (que desconhecêssemos) que permitissem a determinação do número dos seus zeros e os localizassem.

Se este objetivo fosse cumprido, dar-se-ia cumprimento, achávamos nós, aos objetivos deste Mestrado: contribuir para a formação contínua sólida, orientada para a resolução de problemas reais sentidos pelos professores na sua prática letiva, bem como para o aprofundamento de conceitos fundamentais.

Com esta dissertação, pretendemos, para além de dar resposta à questão levantada do conhecimento de regras para a determinação do número e localização de zeros de polinómios, conhecer as fórmulas resolventes de equações de grau inferior a 5 e explorar as razões que levam à não existência de uma congénere para as do quinto grau ou superior. Analisamos também, como estes contributos algébricos justificam a impossibilidade de algumas construções geométricas usando régua e compasso, famosas e muito antigas, como é o caso da quadratura do círculo, por exemplo.

Organizámos o presente texto, da seguinte forma:

No capítulo dois apresentamos e revemos alguns conceitos e resultados básicos mas importantes, de domínios variados, necessários a uma melhor compreensão do trabalho aqui desenvolvido e que a ele servirão de apoio.

No capítulo três deduzimos as fórmulas resolventes das equações do segundo, terceiro e quarto graus. Aqui, temos a oportunidade de ter contacto com saberes tão distintos quanto aqueles que eram conhecidos quinze séculos a.C. (para as equações de grau um e dois) e aqueles que foram desenvolvidos e disputados no século XVI por Scipione del Ferro (1465-1526), Nicolo Tartaglia (1500-1557), Girolamo Cardano (1501-1576), entre outros. Referimo-nos à resolução de equações de grau três e quatro.

No capítulo quatro abordamos as equações do quinto grau, pauta-nos a prova do Teorema de Abel (1802-1829)-Ruffini (1765-1833) e percorremos de forma especial e

imprescindível, os trabalhos de Évariste Galois (1811-1832), o responsável pela prova da impossibilidade de resolver, de uma forma geral, uma equação de grau superior a 5, usando radicais. Refira-se que, já antes, com apenas 19 anos, Abel havia provado que não existia fórmula resolvente para equações do quinto grau. Neste capítulo, são abordados de forma sumária e utilitária algumas noções e resultados acerca de *extensões de corpos*, necessários à prova pretendida.

No capítulo cinco analisamos como é que o *grau de uma extensão de um corpo* é uma ferramenta útil na prova da irresolubilidade geométrica, usando apenas régua e compasso, de alguns problemas colocados pelos matemáticos gregos antigos: duplicação do cubo, trisseção do ângulo, quadratura do círculo e inscrição de um heptágono regular numa dada circunferência.

No capítulo seis apresentamos algumas regras (descobertas entre o século XVI e XIX) que nos dão informação a respeito do número e localização dos zeros reais de um polinómio, a saber: Regra de Budan (1761-1840)-Fourier (1768-1830), Regra dos sinais de Descartes, Teorema de Sturm (1803-1855), Regra de Cauchy (1789-1857) e Regra de Lagrange (1736-1813).

No apêndice A anexamos o roteiro da tarefa proposta aos alunos de duas turmas do 11^o ano do curso de Ciências e Tecnologias relacionada com alguns dos assuntos abordados nesta dissertação e que se coadunam com alguns domínios por si estudados nos anos de escolaridade já frequentados.

Capítulo 2

Preliminares

Neste capítulo apresentamos alguns conceitos e resultados úteis para o trabalho desenvolvido. Podem ser encontrados de forma mais detalhada com exemplos, demonstrações e resultados associados em [5], [7], [13], [14] e [15].

2.1 Noções básicas de Álgebra abstrata

Nesta secção elencamos, em especial, as definições de algumas estruturas e subestruturas algébricas (grupo, anel, corpo, por exemplo). Apresentamos ainda as noções de relação de equivalência, de classe, de permutação e de alguns morfismos.

Definição 2.1.1 (*Grupo*) Um grupo é um par $(G; *)$, constituído por um conjunto G e uma operação binária $*$: $G * G \rightarrow G$, que satisfaz os seguintes axiomas:

- *Associatividade*: se a, b, c são elementos de G então $a * (b * c) = (a * b) * c$
- *Elemento neutro*: existe um elemento e em G tal que $a * e = e * a = a$, para todo o elemento a de G
- *Inversos*: para todo o elemento a de G existe um elemento a' em G tal que $a * a' = a' * a = e$

Se, além disso, $a * b = b * a$, para todos os elementos a e b de G , o grupo $(G; *)$ diz-se **abeliano** ou **comutativo**.

Definição 2.1.2 (*Subgrupo*) Subgrupo de um grupo G é um subconjunto não vazio de G que tem, ele próprio, estrutura de grupo relativamente à operação que define o grupo G .

Definição 2.1.3 (*Relação de equivalência*) Seja A um conjunto e seja R uma relação entre pares de elementos de A , isto é, R é um subconjunto de $A \times A$. Quando, para a e $b \in A$, se tem $(a, b) \in R$, escreve-se aRb .

R é uma relação de equivalência em A se se verificam, para quaisquer $a, b, c \in A$:

- aRa (*reflexiva*)
- Se aRb então bRa (*simétrica*)
- Se aRb e bRc então aRc (*transitiva*)

Definição 2.1.4 (*Classes de conjugação*) Dois elementos x e y de um grupo G são conjugados se $gxg^{-1} = y$, para algum $g \in G$. A relação de conjugação é uma relação de equivalência cujas classes de equivalência se designam por classes de conjugação.

Definição 2.1.5 (Subgrupo normal) Um subgrupo H de G diz-se normal se H é reunião de classes de conjugação.

Definição 2.1.6 (Anel) Um anel $(A, +, \cdot)$ é um conjunto A munido de duas operações binárias, que denotaremos por $+$ e \cdot , tais que:

- $(A; +)$ é um grupo abeliano (o seu elemento neutro é designado por **zero do anel** e o inverso de cada elemento, designado por **simétrico**)
- a operação \cdot é associativa; ou seja, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para quaisquer $a, b, c \in A$
- a operação \cdot é distributiva relativamente a $+$, ou seja, $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$, para quaisquer $a, b, c \in A$.

Usaremos somente A para designar um anel arbitrário $(A, +, \cdot)$.

Um anel A diz-se **comutativo** se a operação \cdot é comutativa. Chama-se **anel com identidade** (ou **anel unitário**) se a operação \cdot possui um elemento neutro (chamado identidade), ou seja, se existe um elemento 1 em A , tal que $a \cdot 1 = 1 \cdot a = a$, para qualquer $a \in A$.

Se para quaisquer $a, b \in A$, $a \cdot b = 0 \implies a = 0 \vee b = 0$, diz-se que A é um **anel sem divisores de zero**. A um anel comutativo, unitário e sem divisores de zero, chama-se um **domínio de integridade**.

Definição 2.1.7 (Subanel) Subanel de um anel A é um subconjunto não vazio de A que tem, ele próprio, estrutura de anel relativamente às operações que definem o anel A .

Definição 2.1.8 (Ideal) Um subanel I de A diz-se um ideal se, para cada $a \in A$ e cada $x \in I$, ax e xa pertencem a I .

Definição 2.1.9 (Ideal principal) O menor ideal de A contendo a é o ideal

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

designado por **ideal principal gerado por a** .

Se A for também unitário, $\langle a \rangle = \{xa : x \in A\}$.

Seja A um anel comutativo. Um ideal I de A diz-se principal se existe algum $a \in A$ tal que $I = \langle a \rangle$.

Definição 2.1.10 (Corpo) Se um domínio de integridade satisfaz a propriedade

$$\forall a \in A, a \neq 0, \exists b \in A : a \cdot b = b \cdot a = 1, \text{ então é um corpo.}$$

Definição 2.1.11 (Subcorpo) Sendo L um corpo, $K \subseteq L$ é um subcorpo de L quando K é um subconjunto não vazio de L tal que $(K, +)$ é um subgrupo de $(L, +)$ e $(K \setminus \{0\}, \cdot)$ é um subgrupo de $(L \setminus \{0\}, \cdot)$.

Definição 2.1.12 (Extensão de um corpo)

Diz-se que um corpo L é uma extensão de um corpo K , se K é um subcorpo de L . A extensão é **própria** quando $L \neq K$.

Definição 2.1.13 (Espaço vetorial) Seja V um conjunto e seja K um corpo. Diz-se que V é um espaço vetorial ou linear sobre K se estiverem definidas duas operações, uma adição $(+)$ de elementos de V e um produto escalar de elementos de K por elementos de V (\cdot) e cujo resultado é um vetor, que satisfaçam as seguintes propriedades:

- A adição é comutativa.
 - A adição é associativa.
 - Em V existe um elemento neutro para a adição.
 - Para cada elemento v de V , existe em V um simétrico de v .
 - A multiplicação de elementos de K por elementos de V é distributiva em relação à adição de elementos de V .
 - A multiplicação de elementos de K por elementos de V é distributiva em relação à adição de elementos de K .
 - O produto do elemento neutro do corpo K por qualquer elemento v de V é igual a v .
 - Para quaisquer elementos v de V e a, b de K , tem-se $a(bv) = (ab)v$.
- Sempre que $K = \mathbb{R}$, o espaço vetorial V diz-se um **espaço vetorial real**. Se $K = \mathbb{C}$ irá ser um **espaço vetorial complexo**.

Proposição 2.1.14 Se \mathbb{L} é uma extensão de \mathbb{K} então \mathbb{L} é um espaço vetorial sobre \mathbb{K} .

Demonstração: Ver [7, pp. 231] □

Definição 2.1.15 (Homomorfismo de anéis) Sejam A e A' dois anéis. Uma função $f : A \rightarrow A'$ diz-se um homomorfismo de A em A' se satisfaz as seguintes condições:

- (i) $f(x +_A y) = f(x) +_{A'} f(y), \forall x, y \in A$;
- (ii) $f(x \cdot_A y) = f(x) \cdot_{A'} f(y), \forall x, y \in A$.

De notar que se usam apenas os símbolos $+$ e \cdot para representar as operações em causa.

Se f for homomorfismo bijetivo, dizemos que f é um **isomorfismo**. Neste caso, diz-se que os anéis A e A' são **isómorfos**.

Os homomorfismos de A em A são chamados de **endomorfismos** de A , já os isomorfismos de A sobre si mesmo são chamados de **automorfismos** de A .

Definição 2.1.16 (Permutação) Seja $I_n = \{1, 2, \dots, n\}, n \geq 2$. Uma permutação σ dos elementos de I_n é qualquer bijeção de I_n em I_n .

O conjunto de todas as bijeções de I_n em I_n , munido da operação da composição de funções é um grupo denominado **grupo das permutações** sobre I_n e representa-se por S_n .

Se σ é tal que $\sigma(a_1) = a_2, \sigma(a_2) = \sigma^2(a_1) = a_3, \dots, \sigma(a_{r-1}) = \sigma^{r-1}(a_1) = a_r$ e $\sigma(a_r) = \sigma^r(a_1) = a_1$ então, σ diz-se um **ciclo** de comprimento r e representa-se por $(a_1 a_2 \dots a_r)$.

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

Definição 2.1.17 Sejam a e b dois números inteiros. Se $a \neq 0$ e existir um inteiro c tal que $b = ac$, dizemos que a divide b , e escrevemos $a \mid b$.

Se a não divide b , escrevemos $a \nmid b$.

Teorema 2.1.18 (Teorema Fundamental da Álgebra) Seja $P(t)$ um polinómio não constante sobre \mathbb{C} . Então existe pelo menos um $z \in \mathbb{C}$ tal que $P(z) = 0$. Dizemos que z é um zero de $P(t)$ ou que z é uma raiz da equação $P(t) = 0$.

Demonstração: Ver [7, pp. 265] □

Teorema 2.1.19 (Teorema de Kronecker(1823-1891)) *Seja K um corpo e $p(x) \in K[x]$ um polinómio de grau $n \geq 1$. Existe uma extensão L de K onde $p(x)$ se decompõe num produto de termos lineares da forma*

$$p(x) = (x - \theta_1)(x - \theta_2) \cdots (x - \theta_n)$$

e escreve-se $L = K(\theta_1, \dots, \theta_n)$, onde $\theta_1, \dots, \theta_n$ são os zeros de $p(x)$ em L .

Demonstração: Ver [13, pp. 87, Teorema 3.13] □

Proposição 2.1.20 *Se uma equação polinomial $a_0 + a_1x + \dots + a_nx^n = 0$, com a_i inteiros, $i = 0, \dots, n$, tem uma solução racional, digamos $\frac{p}{q}$, com p e q inteiros primos entre si, então $p \mid a_0$ e $q \mid a_n$.*

Demonstração: Seja $\frac{p}{q}$, com p e q inteiros primos entre si, solução da equação $a_0 + a_1x + \dots + a_nx^n = 0$, com a_i inteiros, $i = 0, \dots, n$.

Então, substituindo, temos $a_0 + a_1\frac{p}{q} + \dots + a_n\left(\frac{p}{q}\right)^n = 0$, com a_i inteiros, $i = 0, \dots, n$.

Multiplicando ambos os membros por q^n , temos: $a_0q^n + a_1pq^{n-1} + \dots + a_np^n = 0$, com a_i inteiros, $i = 0, \dots, n$.

Ora, todos os termos da equação, à exceção de a_np^n , são múltiplos de q , logo q divide a_np^n . Mas, p e q são primos entre si, então q divide a_n .

Por outro lado, também temos que todos os termos da equação, à exceção de a_0q^n , são múltiplos de p , logo p divide a_0q^n . Mas, p e q são primos entre si, então p divide a_0 . □

Teorema 2.1.21 (Fórmula do Binómio de Newton (1643-1727)) *Sejam x, y elementos de um anel comutativo e n um inteiro não-negativo.*

Tem-se que:

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k.$$

2.2 Noções básicas de Análise

Nesta secção, apresentamos resultados referentes a funções reais de variável real e que permitem averiguar a existência de zeros num determinado intervalo.

Incluimos ainda as fórmulas de Moivre que nos permitem determinar uma potência e as de um dado número complexo.

Teorema 2.2.1 (Teorema de Bolzano (1781-1848)) *Se f é uma função real de variável real contínua num determinado intervalo $[a, b]$ então, para qualquer valor d compreendido entre $f(a)$ e $f(b)$, existe pelo menos um valor c compreendido entre a e b tal que $f(c) = d$.*

Em particular, se $f(a) \times f(b) < 0$, então $\exists c \in]a, b[$: $f(c) = 0$, isto é, f possui pelo menos um zero no intervalo $]a, b[$.

Teorema 2.2.2 (Teorema de Rolle (1652-1719)) *Dada uma função f contínua, definida num intervalo $[a, b]$ e diferenciável em $]a, b[$, se $f(a) = f(b)$, então existe um c em $]a, b[$ tal que $f'(c) = 0$.*

Resulta deste teorema que:

1- *se I for um intervalo de \mathbb{R} e se f for uma função derivável de I em \mathbb{R} , então entre quaisquer dois zeros de f há pelo menos um zero da derivada f' .*

2- *se I for um intervalo de \mathbb{R} e se f for uma função derivável de I em \mathbb{R} , entre dois zeros consecutivos da derivada f' não pode haver mais do que um zero de f (podendo não existir nenhum).*

Definição 2.2.3 (Conjugado de um número complexo) *Seja $z = a + bi$, $a, b \in \mathbb{R}$. Chamamos conjugado de z ao complexo $a - bi$ que denotamos por \bar{z} .*

Se $z = \rho e^{i\theta} \in \mathbb{C}$, temos $\bar{z} = \rho e^{-i\theta}$.

Teorema 2.2.4 (Fórmulas de Moivre (1667-1754)) *Seja $z = \rho e^{i\theta} \in \mathbb{C}$, não nulo e seja n natural.*

Tem-se que:

1- $z^n = \rho^n e^{in\theta}$

2- $\sqrt[n]{z} = \sqrt[n]{\rho} e^{i\frac{\theta+2k\pi}{n}}, k = 0, 1, \dots, n-1.$

Capítulo 3

Fórmulas resolventes

Desde sempre, e até às descobertas de Galois, que um dos principais objetivos da Álgebra clássica foi resolver *equações polinomiais* de grau n com coeficientes reais, exprimindo as suas soluções, isto é, os zeros de um polinómio, em função dos seus coeficientes, usando um número finito de operações usuais (adição, subtração, multiplicação, divisão e radiciação). Ao longo dos tempos e recuando ao primeiro milénio da era cristã, encontramos tentativas de encontrar fórmulas que, usando as operações referidas, resolvam qualquer equação polinomial. Neste capítulo, apresentamos as conhecidas e que dizem respeito às equações de grau inferior a cinco.

3.1 Equações lineares e do 2º grau

É frequentemente afirmado que foram os babilónios os primeiros a resolver equações quadráticas, algo descabido já que estes não possuíam a noção de “equação”. O que desenvolveram foi uma abordagem algorítmica para resolver problemas que, em terminologia atual, dariam origem a uma equação quadrática. No entanto, todos os seus problemas tinham soluções positivas, já que diziam respeito, na maioria dos casos, a medidas de comprimentos.

Euclides (325 a.C. (?)– 265 a.C.) desenvolveu uma abordagem geométrica de problemas que equivalia a encontrar um comprimento que, na notação atual, era a solução de uma equação quadrática.

Matemáticos hindus e Brahmagupta (598-665) em particular, levaram os métodos dos matemáticos babilónicos mais longe e apresentaram métodos (quase atuais) que admitiam soluções negativas. Usaram abreviaturas para as incógnitas.

O árabe Muhammad al-Khwarizmi (780?-850?) classificou os diferentes tipos de equações quadráticas através de exemplos, dividindo-as em seis tipos. Estas eram compostas por três tipos de quantidades: raízes, quadrados de raízes e números, isto é, x , x^2 e números. Dividiu então as equações nos seguintes tipos:

- quadrados iguais a raízes;
- quadrados iguais a números;
- raízes iguais a números;
- quadrados e raízes iguais a números ($x^2 + 10x = 39$, p.e.);
- quadrados e números iguais a raízes ($x^2 + 21 = 10x$, p.e.);
- raízes e números iguais a quadrados ($3x + 4 = x^2$, p.e.).

Al-Khwarizmi forneceu a regra para resolver cada um dos tipos de equação, deu um exemplo aplicando essencialmente aquilo que hoje chamaríamos a fórmula resolvente para as equações do segundo grau. Apresentou a prova geométrica usando o “completamento do quadrado”. Contudo, só em 1145, a Europa viu publicado o livro de Hiyya Ha-Nasi (conhecido por Savasorda (1070-1136)) que continha a resolução completa das equações do segundo grau: *Liber embadorum* [21].

Passemos então à análise das equações de grau um.

Sejam $a, b \in \mathbb{C}$, $a \neq 0$. Temos a solução trivial: $at + b = 0 \iff t = -\frac{b}{a}$.

Já quinze séculos antes de Cristo, estas equações, bem como as do segundo grau (não reconhecidas como tal) eram resolvidas uma vez que os matemáticos sabiam como “completar um quadrado”. Este método foi dado a conhecer no Ocidente, no Renascimento, através das traduções do livro *Al-jabr wa'l muqabalah* do matemático islâmico Muhammad al-Khwarizmi, publicado na primeira metade do século IX [13, pp. 55] [21].

Relativamente às equações do segundo grau, consideremos:

$$at^2 + bt + c = 0, a, b, c \in \mathbb{C}, a \neq 0.$$

Dividindo ambos os membros por a , obtemos:

$$t^2 + b_1 t + c_1 = 0, \text{ com } b_1 = \frac{b}{a} \text{ e } c_1 = \frac{c}{a}.$$

Por “completamento do quadrado”, vem:

$$t^2 + b_1 t + \left(\frac{b_1}{2}\right)^2 = \left(\frac{b_1}{2}\right)^2 - c_1 \iff \left(t + \frac{b_1}{2}\right)^2 = \frac{b_1^2}{4} - c_1.$$

Isto é,

$$t + \frac{b_1}{2} = \pm \sqrt{\frac{b_1^2}{4} - c_1} \iff t = -\frac{b_1}{2} \pm \sqrt{\frac{b_1^2}{4} - c_1}.$$

Simplificando e substituindo b_1 e c_1 pelos valores correspondentes, obtemos a fórmula resolvente por nós conhecida, isto é,

$$t = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \quad (3.1)$$

3.2 Equações cúbicas

É preciso recuar a 1515, a Bolonha, para encontrarmos del Ferro, o primeiro a descobrir soluções para algumas equações do 3º grau, numa época em não eram ainda usados os números negativos.

De notar que as equações $x^3 + px = q$, $x^3 = px + q$ e $x^3 + q = px$, com p e q números positivos, eram vistas como diferentes tipos de equações e as últimas eram frequentemente ignoradas por terem habitualmente uma solução negativa. Estas só surgem com Tartaglia e Cardano que a elas se refere com “soluções falsas”. Foi Cardano o pioneiro, embora não os entenda e deles duvide, no uso dos números imaginários. Só em 1572, em *Algebra*, Rafael Bombelli (1526-1572) os introduz de forma consistente ao mesmo tempo que explica como lidar com os números negativos. Voltando a del Ferro, refira-se que o seu método de resolução de algumas equações cúbicas assentou na sua redução a outra sem termo de grau dois. Julga-se que assim pensou pelo facto de as outras serem muito difíceis de resolver. Conta-se que, no leito da morte (1526), del Ferro terá revelado esta solução secreta ao seu aluno Antonio Maria del Fiore (séc. XV-XVI) que veio a ser considerado um “mediocre matemático” [3]. Este terá feito saber que conhecia como resolver algumas equações cúbicas, sem no entanto revelar como.

Esta divulgação terá encorajado Tartaglia a descobrir o segredo. Em 1530, anunciou que o havia conseguido para todas as do tipo $x^3 + px = q$, quando na verdade só teria encontrado para algumas.

Del Fiore e Tartaglia encetaram assim uma “guerra” que os levou a um confronto (fevereiro de 1535) no qual cada um propôs ao outro trinta problemas: Tartaglia venceu resolvendo-os em duas horas já que (todos) eram equações do tipo $x^3 + px = q$. Del Fiore não acreditava que o seu rival as soubesse resolver... Tartaglia terá sido, depois, chamado a casa de Cardano que para além de respeitado professor em Milão e Bolonha, também era médico prestigiado, astrólogo, herege e jogador, para eventual arranjo de patrono. Refira-se que Tartaglia não possuía fonte de rendimentos, talvez devido à sua gaguez provocada por corte de sabre sofrido na tomada de Brescia (1512) pelos franceses [3].

Em 1539, Cardano pediu a Tartaglia que divulgasse o seu método de resolução das referidas equações comprometendo-se a manter segredo antes dele o publicar, coisa que nunca veio a acontecer. Tartaglia acedeu e Cardano e o seu jovem assistente Lodovico Ferrari (1522-1565), que veio a descobrir a solução para as equações do 4º grau (1541), encetaram uma análise do método que lhes foi revelado. Nessa tarefa, Cardano descobriu que del Ferro teria encontrado a solução para as equações cúbicas antes de Tartaglia. Talvez o tenha descoberto através de uns apontamentos de del Ferro que lhe terão sido cedidos pelo genro deste, Hannibal della Nave, onde estava a solução. Refira-se que del Ferro, hoje, mal é lembrado. Escudado nesta descoberta, Cardano rompeu o compromisso com Tartaglia e publicou-a a par das soluções para as equações de 4º grau no livro *Ars Magna* (1545), tido como marco do início da era moderna na Matemática e que fará do seu autor o mais competente algebrista da época [3]. Aliás, ocupando parte substancial da obra já que fez uma análise detalhada dos treze tipos de equações cúbicas às quais falta o termo do 2º grau. Já para as do 4º grau, apenas analisa algumas e apenas possíveis. Como não é de surpreender, esta revelação veio trazer uma azeda disputa com Tartaglia que acusa Cardano de traição, insultando-o a ele e a Ferrari, seu fiel discípulo. E é precisamente este que entra na “guerra” com mais emoção: através de panfletos, respondeu com as mesmas armas, defendendo o seu mestre que adota uma postura mais discreta. Tartaglia vê-se assim, de novo, envolvido numa disputa pública, desta feita com Ferrari. Decidem “confrontar-se” em agosto de 1548 em Milão: cada um propôs ao outro sessenta e dois problemas. Ferrari saiu vencedor indiscutível levando o seu rival a abandonar a cidade, logo após o primeiro dia da disputa [8].

Voltemos às equações do 3º grau e deduzamos a sua fórmula resolvente.

Qualquer equação cúbica pode ser escrita na forma

$$t^3 + at^2 + bt + c = 0, a, b, c \in \mathbb{C},$$

após termos dividido ambos os membros pelo coeficiente do termo de maior grau. Para obter uma equação equivalente da forma $t^3 + b_1t + c_1 = 0$, basta fazer $y = t + \frac{a}{3}$ (transformação de Tschirnhaus (1651-1708)), isto é, fazendo $t = y - \frac{a}{3}$. Refira-se que este matemático, conde, esperava com as suas transformações, encontrar um método geral para a resolução de equações de qualquer grau (n) eliminado todos os seus termos exceto os de grau n e zero. Tschirnhaus estudou em Leyden e fundou uma indústria de vidro em Itália a fim de poder aí realizar as suas experiências com a luz. Foi apelidado de “descobridor da porcelana” por ter contribuído para estabelecer fábricas do ramo em Dresden.

Voltando à “sua transformação” e à equação cúbica inicial, temos:

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

Usando a fórmula do Binômio de Newton, teorema 2.1.21, no desenvolvimento do cubo, vem:

$$\left(y - \frac{a}{3}\right)^3 = y^3 - ay^2 + \frac{a^2y}{3} - \frac{a^3}{27}.$$

Sendo assim, a equação inicial toma a forma:

$$y^3 - ay^2 + \frac{a^2y}{3} - \frac{a^3}{27} + ay^2 - \frac{2a^2y}{3} + \frac{a^3}{9} + by - \frac{ab}{3} + c = 0,$$

ou ainda,

$$y^3 + \left(b - \frac{a^2}{3}\right)y + \left(\frac{a^3}{9} + c - \frac{ab}{3} - \frac{a^3}{27}\right) = 0.$$

Fazendo $p = b - \frac{a^2}{3}$ e $q = \frac{a^3}{9} + c - \frac{ab}{3} - \frac{a^3}{27}$, temos que toda a equação cúbica pode ser transformada numa equação cúbica da forma

$$y^3 + py + q = 0. \quad (3.2)$$

A redução à forma (3.2) será devida a Cardano uma vez que ele, em *Ars Magna*, a usa em nove dos dez casos das equações cúbicas com termo do 2º grau, não fazendo referência a qualquer nome. Refira-se que, no décimo caso ($x^3 + d = bx^2$), Cardano usa a substituição $x = \frac{d^{\frac{2}{3}}}{y}$ uma vez que simplificaria os cálculos. Tartaglia desconheceria esta técnica uma vez que ele só se referia a equações do 3º grau sem termo do 2º grau, como se poderá comprovar em poema que ele diz ter dado a Cardano com a solução das equações cúbicas. [8, pp. 23-24].

Voltando à equação (3.2) e para evitar algumas frações, podemos escrevê-la na forma:

$$y^3 + 3b_1y + c_1 = 0. \quad (3.3)$$

Seja r uma solução desta equação.

Ora, sabemos que para a equação quadrática $t^2 - rt - b_1 = 0$, existem soluções m e n (em geral, números complexos) tais que:

$$m + n = r \wedge mn = -b_1. \quad (3.4)$$

Então, como $r^3 + 3b_1r + c_1 = 0$, vem:

$$(m + n)^3 + 3(-mn)(m + n) + c_1 = 0.$$

Pela fórmula do Binômio de Newton, teorema 2.1.21, e atendendo a (3.4) temos

$$(m + n)^3 = m^3 + n^3 - 3b_1r.$$

A equação (3.3) assume assim a forma $m^3 + n^3 + c_1 = 0$, equivalente a afirmar que

$$m^3 + n^3 = -c_1. \quad (3.5)$$

Por outro lado

$$m^3n^3 = (mn)^3 = (-b_1)^3 = -b_1^3. \quad (3.6)$$

Podemos então afirmar que m^3 e n^3 são soluções da equação quadrática

$$t^2 + c_1 t - b_1^3 = 0. \quad (3.7)$$

Pela fórmula resolvente (3.1), temos, sem perda de generalidade:

$$m^3 = \frac{-c_1 + \sqrt{c_1^2 + 4b_1^3}}{2}; \quad n^3 = \frac{-c_1 - \sqrt{c_1^2 + 4b_1^3}}{2}.$$

De notar que m^3 e n^3 são ditos “conjugados”.

Sendo assim, m é uma das raízes cúbicas de m^3 e n é uma das raízes cúbicas de n^3 . Para simplificar, denotemos

$$m = \sqrt[3]{\frac{-c_1 + \sqrt{c_1^2 + 4b_1^3}}{2}}; \quad n = \sqrt[3]{\frac{-c_1 - \sqrt{c_1^2 + 4b_1^3}}{2}}.$$

Por (3.4), temos:

$$r = \sqrt[3]{\frac{-c_1 + \sqrt{c_1^2 + 4b_1^3}}{2}} + \sqrt[3]{\frac{-c_1 - \sqrt{c_1^2 + 4b_1^3}}{2}}.$$

Sejam agora, m_1 e n_1 raízes cúbicas de m^3 e n^3 , respetivamente, tais que

$$m_1 n_1 = -b_1. \quad (3.8)$$

Ora, como as raízes cúbicas complexas da unidade são $1, \omega = e^{i\frac{2\pi}{3}}$ e $\omega^2 = e^{i\frac{4\pi}{3}}$, as raízes cúbicas de m^3 são $m_1, m_1\omega$ e $m_1\omega^2$ e as de n^3 são $n_1, n_1\omega$ e $n_1\omega^2$. De notar que, quando m^3 e n^3 são reais, então m e n são as suas raízes cúbicas reais, respetivamente.

Como $r = m + n$, temos nove (3×3) possibilidades para o seu valor:

$m_1 + n_1; m_1 + n_1\omega; m_1 + n_1\omega^2; m_1\omega + n_1; m_1\omega + n_1\omega; m_1\omega + n_1\omega^2; m_1\omega^2 + n_1; m_1\omega^2 + n_1\omega; m_1\omega^2 + n_1\omega^2$.

Contudo, só três verificam a condição $mn = -b_1$.

Vejamos:

$$m_1 n_1 = -b_1, \text{ por (3.7);}$$

$$m_1 n_1 \omega = -b_1 \omega;$$

$$m_1 n_1 \omega^2 = -b_1 \omega^2;$$

$$m_1 \omega n_1 = -b_1 \omega;$$

$$m_1 \omega n_1 \omega = -b_1 \omega^2;$$

$$m_1 \omega n_1 \omega^2 = -b_1 \omega^3 = -b_1;$$

$$m_1 \omega^2 n_1 = -b_1 \omega^2;$$

$$m_1 \omega^2 n_1 \omega = -b_1 \omega^3 = -b_1;$$

$$m_1 \omega^2 n_1 \omega^2 = -b_1 \omega^4.$$

Pelo exposto, podemos estabelecer:

Teorema 3.2.1 (Fórmula de Cardano) *Sejam $b, c \in \mathbb{C}$.*

As soluções da equação $t^3 + 3bt + c = 0$ são $m + n; m\omega + n\omega^2; m\omega^2 + n\omega$, sendo

m uma das raízes cúbicas de $\frac{-c + \sqrt{c^2 + 4b^3}}{2}$;

n uma das raízes cúbicas de $\frac{-c - \sqrt{c^2 + 4b^3}}{2}$ tais que $mn = -b$;

$\omega = e^{i\frac{2\pi}{3}}$ e $\omega^2 = e^{i\frac{4\pi}{3}}$.

Esta é então a *Fórmula de Cardano*, não por mérito de descoberta mas sim por ter sido Cardano a publicá-la. Foi este método que levou ao desenvolvimento da teoria dos números complexos, tendo sido Cardano o pioneiro na introdução dos números da forma $a + \sqrt{-b}$, com a e b , inteiros positivos. Todavia, fê-lo de forma cautelosa e com “um forte sentimento de culpa”. De notar que, no caso das equações quadráticas com binómio discriminante negativo elas eram simplesmente consideradas impossíveis mas, nas cúbicas não há como escapar aos números complexos, já que no método em causa algumas soluções reais obtêm-se passando pelos números complexos como é o caso do segundo exemplo a seguir apresentado (ver [13, pp. 57]).

Exemplo 3.2.2 *Apliquemos o método, acima descrito na dedução da **Fórmula de Cardano**, na resolução da equação $t^3 - 6t^2 + 11t - 6 = 0$, onde, usando as mesmas notações, temos: $a = -6$, $b = 11$ e $c = -6$.*

Transformemo-la na forma $y^3 + py + q = 0$, fazendo $y = t - 2$, equivalente a $t = y + 2$.

Para tal, atendendo a (3.2), basta fazer $p = 11 - \frac{(-6)^2}{3} = -1$ e $q = \frac{(-6)^3}{9} - 6 - \frac{-6 \times 11}{3} - \frac{(-6)^3}{27} = 0$.

Sendo assim, a equação dada é equivalente a $y^3 - y = 0$ (do tipo $y^3 + 3b_1y + c_1 = 0$, com $3b_1 = -1$ e $c_1 = 0$) e seja r uma sua solução. Logo, temos

$$r^3 - r = 0. \quad (3.9)$$

Por outro lado, sabemos que a equação quadrática $t^2 - rt - b_1 = 0$ terá como soluções m e n , números complexos, tais que

$$m + n = r \text{ e } mn = -b_1. \quad (3.10)$$

Substituindo em (3.8), vem: $(m + n)^3 - (m + n) = 0$. Efetuando cálculos e tendo em conta (3.9), temos

$$m^3 + n^3 - 3b_1r - r = 0,$$

equivalente a $m^3 + n^3 = 0$, uma vez que $3b_1 = -1$.

Ora, $m^3n^3 = (mn)^3 = (-b_1)^3 = \left(\frac{1}{3}\right)^3 = \frac{1}{27}$.

Então, m^3 e n^3 são soluções da equação quadrática $t^2 + 0t + \frac{1}{27} = 0$, isto é, de $t^2 + \frac{1}{27} = 0$. Tem-se então, sem perda de generalidade, que, $m^3 = \sqrt{\frac{1}{27}} i$ e $n^3 = -\sqrt{\frac{1}{27}} i$.

De notar que a equação do 2º grau em causa, caso fosse completa, por exemplo, seria resolvida pela já exposta fórmula resolvente das equações deste grau.

Sejam m_1 e n_1 , respetivamente, uma das raízes cúbicas de m e n e que denotaremos por $m_1 = \sqrt[3]{\sqrt{\frac{1}{27}} i}$ e $n_1 = \sqrt[3]{-\sqrt{\frac{1}{27}} i}$. De notar que $m_1 + n_1 = 0$ e $m_1n_1 = -b_1 = \frac{1}{3}$.

*Ora, de acordo com a **Fórmula de Cardano**, teorema 3.2.1, as soluções da equação $y^3 - y = 0$, com $b = -\frac{1}{3}$ e $c = 0$, são $m + n$, $m\omega + n\omega^2$ e $m\omega^2 + n\omega$, sendo m uma das raízes cúbicas de $\sqrt{\frac{1}{27}} i$, digamos m_1 , e n uma das raízes cúbicas de $-\sqrt{\frac{1}{27}} i$, digamos n_1 , com $mn = \frac{1}{3}$, $\omega = e^{i\frac{2\pi}{3}}$ e $\omega^2 = e^{i\frac{4\pi}{3}}$.*

$$\text{Então, } m_1 = \sqrt[3]{\sqrt{\frac{1}{27}} i} = \sqrt[3]{\frac{1}{3} e^{i\frac{\pi}{6}}} \text{ e } n_1 = \sqrt[3]{-\sqrt{\frac{1}{27}} i} = \sqrt[3]{\frac{1}{3} e^{-i\frac{\pi}{6}}}.$$

Sendo assim, $m_1 + n_1 = \sqrt[3]{\frac{1}{3}} (e^{i\frac{\pi}{6}} + e^{-i\frac{\pi}{6}}) = \frac{\sqrt{3}}{3} \times 2 \cos\left(\frac{\pi}{6}\right) = 1$, o que traduz que $y = 1$ é solução da equação $y^3 - y = 0$, logo $t = 1 + 2 = 3$ é solução da equação inicial.

Ora, $m_1\omega + n_1\omega^2 = \sqrt{\frac{1}{3}}e^{i\frac{\pi}{6}}e^{i\frac{2\pi}{3}} + \sqrt{\frac{1}{3}}e^{-i\frac{\pi}{6}}e^{i\frac{4\pi}{3}} = \sqrt{\frac{1}{3}}\left(e^{i\frac{5\pi}{6}} + e^{i\frac{7\pi}{6}}\right) = -1$, o que traduz que $y = -1$ é solução da equação $y^3 - y = 0$, logo $t = -1 + 2 = 1$ é solução da equação inicial.

Finalmente, $m_1\omega^2 + n_1\omega = \sqrt{\frac{1}{3}}e^{i\frac{\pi}{6}}e^{i\frac{4\pi}{3}} + \sqrt{\frac{1}{3}}e^{-i\frac{\pi}{6}}e^{i\frac{2\pi}{3}} = \sqrt{\frac{1}{3}}\left(e^{i\frac{3\pi}{2}} + e^{i\frac{\pi}{2}}\right) = 0$, o que traduz que $y = 0$ é solução da equação $y^3 - y = 0$, logo $t = 0 + 2 = 2$ é solução da equação inicial.

Concluindo, as soluções da equação $t^3 - 6t^2 + 11t - 6 = 0$ são 1, 2 e 3.

Exemplo 3.2.3 Consideremos a equação $x^3 - 15x - 4 = 0$.

Ora, $3b = -15$, $c = -4$, e $c^2 + 4b^3 = 16 - 500 = -484$.

Sendo assim, pela **Fórmula de Cardano**, teorema 3.2.1, m é uma das raízes cúbicas de $2 + \sqrt{-121}$ e n uma das raízes cúbicas de $2 - \sqrt{-121}$. Então uma das raízes da equação é $m + n = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$ e seria considerada impossível em \mathbb{R} .

Contudo, ela possui três raízes reais: 4, $-2 + \sqrt{3}$ e $-2 - \sqrt{3}$.

Comprovemos que 4 é raiz da equação em causa.

Ora, $(2 + i)^3 = 2 + 11i$ e $(2 - i)^3 = 2 - 11i$, logo $2 + i$ e $2 - i$, são respetivamente, raízes cúbicas de $2 + 11i$ e de $2 - 11i$, por isso, $2 + i + 2 - i = 4$ é solução da equação.

De notar que estas falhas de Cardano, aliás por ele reconhecidas, vieram a ser ultrapassadas por Raphael Bombelli, por volta de 1560. Foi este matemático italiano o primeiro a usar a notação para aquilo que hoje denotamos por i a que chamou “piu di meno”(ver [13, pp. 58]).

Exemplo 3.2.4 Determinemos as três soluções da equação $y^3 + 6y + 2 = 0$.

Temos $3b = 6$, $c = 2$ e $c^2 + 4b^3 = 4 + 32 = 36$.

Logo, pela **Fórmula de Cardano**, teorema 3.2.1, a raiz cúbica real de m^3 é $m = \sqrt[3]{2}$ e a raiz cúbica real de n^3 é $n = \sqrt[3]{-4}$.

Então, uma das raízes da equação é $\sqrt[3]{2} + \sqrt[3]{-4}$.

Outra é $m\omega + n\omega^2$, igual a

$$\sqrt[3]{2}e^{i\frac{2\pi}{3}} + \sqrt[3]{-4}e^{i\frac{4\pi}{3}} = \left(-\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{4}}{2}\right) + \left(\frac{\sqrt[3]{2}\sqrt{3}}{2} + \frac{\sqrt{3}\sqrt[3]{4}}{2}\right)i.$$

A terceira é $m\omega^2 + n\omega$, igual a

$$\sqrt[3]{2}e^{i\frac{4\pi}{3}} + \sqrt[3]{-4}e^{i\frac{2\pi}{3}} = \left(-\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{4}}{2}\right) + \left(-\frac{\sqrt[3]{2}\sqrt{3}}{2} - \frac{\sqrt{3}\sqrt[3]{4}}{2}\right)i.$$

Exemplo 3.2.5 Determinemos as três soluções da equação $y^3 - 6y + 2 = 0$.

Temos $3b = -6$, $c = 2$ e $c^2 + 4b^3 = 4 - 32 = -28$.

Logo, pela **Fórmula de Cardano**, teorema 3.2.1, uma das raízes cúbicas de m^3 é $m = \sqrt[3]{-1 + i\sqrt{7}}$ e uma das raízes cúbicas de n^3 é $n = \sqrt[3]{-1 - i\sqrt{7}}$.

Ora, $m^3 = -1 + \sqrt{7}i = \sqrt{8}e^{i\theta}$, sendo θ tal que $\cos \theta = -\frac{1}{\sqrt{8}}$ e $\sin \theta = \frac{\sqrt{7}}{\sqrt{8}}$.

Uma vez que n^3 é o conjugado de m^3 , temos $n^3 = \sqrt{8}e^{-i\theta}$.

Então, uma das raízes da equação é

$$m + n = \sqrt[3]{\sqrt{8}e^{i\theta}} + \sqrt[3]{\sqrt{8}e^{-i\theta}} = \sqrt{2}e^{i\frac{\theta}{3}} + \sqrt{2}e^{-i\frac{\theta}{3}} = 2\sqrt{2}\cos\left(\frac{\theta}{3}\right).$$

Notemos que $mn = 2 = -b$.

As outras duas serão $m\omega + n\omega^2$ e $m\omega^2 + n\omega$.

Comprovemos que $m + n$ é, de facto, solução da equação dada.

Temos que,

$(m + n)^3 - 6(m + n) + 2 = (2\sqrt{2})^3 \cos^3\left(\frac{\theta}{3}\right) - 6 \times 2\sqrt{2} \cos\left(\frac{\theta}{3}\right) + 2$, o que simplifica para

$$4\sqrt{2} \left(4 \cos^3\left(\frac{\theta}{3}\right) - 3 \cos\left(\frac{\theta}{3}\right) \right) + 2. \quad (3.11)$$

Sabemos que

$\cos(3\alpha) = \cos(2\alpha + \alpha) = \cos(2\alpha) \cos \alpha - \sin(2\alpha) \sin \alpha =$
 $(\cos^2 \alpha - \sin^2 \alpha) \cos \alpha - 2 \sin^2 \alpha \cos \alpha =$
 $\cos^3 \alpha - (1 - \cos^2 \alpha) \cos \alpha - 2(1 - \cos^2 \alpha) \cos \alpha =$
 $\cos^3 \alpha - \cos \alpha + \cos^3 \alpha - 2 \cos \alpha + 2 \cos^3 \alpha = 4 \cos^3 \alpha - 3 \cos \alpha$, qualquer que seja o valor de α . Isto é, $\cos(3\alpha) = 4 \cos^3 \alpha - 3 \cos \alpha$.

Sendo assim, a expressão (3.10) toma a forma

$$4\sqrt{2} \cos \theta + 2 = 4\sqrt{2} \left(-\frac{1}{\sqrt{8}} \right) + 2 = 0, \text{ como queríamos mostrar.}$$

Exemplo 3.2.6 Consideremos a equação $y^3 + 3y - 36 = 0$ que admite 3 como solução óbvia ($3^3 + 3 \times 3 - 36 = 0$). Temos $3b = 3$, $c = -36$ e $c^2 + 4b^3 = 1296 + 4 = 1300$.

Logo, pela **Fórmula de Cardano**, teorema 3.2.1, uma das raízes da equação é $\sqrt[3]{18 + \sqrt{325}} + \sqrt[3]{18 - \sqrt{325}}$ que parece longe do valor 3, ... mas não está. Senão vejamos: substituindo na equação em causa, vem:

$$\left(\sqrt[3]{18 + \sqrt{325}} + \sqrt[3]{18 - \sqrt{325}} \right)^3 + 3 \left(\sqrt[3]{18 + \sqrt{325}} + \sqrt[3]{18 - \sqrt{325}} \right) - 36 = 0.$$

Pela fórmula do Binómio de Newton, teorema 2.1.21, temos

$$18 + \sqrt{325} + 3\sqrt[3]{(18 + \sqrt{325})^2 (18 - \sqrt{325})} + 3\sqrt[3]{(18 + \sqrt{325}) (18 - \sqrt{325})^2} \\ + 18 - \sqrt{325} + 3 \left(\sqrt[3]{18 + \sqrt{325}} + \sqrt[3]{18 - \sqrt{325}} \right) - 36 = 0.$$

Equivalentemente, temos

$$36 + 3\sqrt[3]{(18^2 - 325) (18 + \sqrt{325})} + 3\sqrt[3]{(18^2 - 325) (18 - \sqrt{325})} + \\ 3 \left(\sqrt[3]{18 + \sqrt{325}} + \sqrt[3]{18 - \sqrt{325}} \right) - 36 = 0.$$

De onde vem:

$$36 + 3\sqrt[3]{324 - 325} \left(\sqrt[3]{18 + \sqrt{325}} + \sqrt[3]{18 - \sqrt{325}} \right) + \\ 3 \left(\sqrt[3]{18 + \sqrt{325}} + \sqrt[3]{18 - \sqrt{325}} \right) - 36 = 0.$$

Finalmente, obtemos o pretendido:

$$36 - 3\sqrt[3]{18 + \sqrt{325}} - 3\sqrt[3]{18 - \sqrt{325}} + 3\sqrt[3]{18 + \sqrt{325}} + 3\sqrt[3]{18 - \sqrt{325}} - 36 = 0,$$

que é uma afirmação verdadeira.

3.3 Equações do 4º grau

Cardano, na sua obra-prima *Ars Magna*, lista vinte tipos de equações do 4º grau para as quais encontrou solução: dez casos não têm termo de grau três e os dez restantes, não têm termo de grau um. Exemplifica, indicando que, quatro do primeiro tipo e duas do segundo, são resolúveis pelo método de Ferrari. Apresenta ainda um único exemplo com termos do 1º e 3º grau, $x^4 + 2x^3 = x + 1$, que é resolvida reduzindo-a à sucessão de duas equações quadráticas. No método apresentado na obra de Cardano para a resolução destas equações, não é usada a transformação que as reduz a equações sem termo de grau três, como foi feito, de forma análoga para as cúbicas, eliminando o termo de grau dois. Se tal tivesse sido feito, juntamente com o método desenvolvido por Ferrari, teríamos encontrado a solução para todas as equações do 4º grau. Sendo assim, pode instalar-se a dúvida acerca do autor da ideia da redução da equação à forma em causa e da consequente solução de qualquer equação do 4º grau: Cardano, Ferrari ou outro? Contudo, encontramos a afirmação de Cardano, em *Ars Magna*, que “é devida a Ferrari, que a inventou a meu pedido”[[3], pp. 196]. Como afirmámos, o trabalho destes dois matemáticos teve como base a equação escrita de forma a não ter termo de grau três usando processo distinto do usado nas equações do 3º grau, contudo mais tarde, Lagrange fez notar que o método desenvolvido antes podia ser aplicado a uma equação do 4º grau completa que se resolve à custa de uma do 3º [8].

Refira-se ainda que, em 1637, Descartes, apresentou outro método de resolução de equações do 4º grau baseado na fatorização do polinómio na forma

$(y^2 + ky + l)(y^2 + my + n)$ e cujos coeficientes obedecem às condições: $k + m = 0$; $km + l + n = p$; $kn + lm = q$ e $ln = r$ [8].

Deduzamos agora a fórmula resolvente para as equações do 4º grau. Sejam $a, b, c, d \in \mathbb{C}$. Qualquer equação do 4º grau pode ser escrita na forma

$$t^4 + at^3 + bt^2 + ct + d = 0,$$

após termos dividido ambos os membros pelo coeficiente do termo de maior grau. Fazendo $y = t + \frac{a}{4}$ (transformação de Tschirnhaus), vem:

$$\left(y - \frac{a}{4}\right)^4 + a\left(y - \frac{a}{4}\right)^3 + b\left(y - \frac{a}{4}\right)^2 + c\left(y - \frac{a}{4}\right) + d = 0.$$

Pela fórmula do Binómio de Newton, teorema 2.1.21, temos

$$y^4 + \left(\frac{3a^2}{8} - \frac{3a^2}{4} + b\right)y^2 + \left(-\frac{a^3}{16} + \frac{3a^3}{16} - \frac{ab}{2} + c\right)y + \left(\frac{a^4}{256} - \frac{a^4}{64} + \frac{a^2b}{16} - \frac{ac}{4} + d\right) = 0.$$

Simplificando, vem

$$y^4 + \left(b - \frac{3a^2}{8}\right)y^2 + \left(c - \frac{ab}{2} + \frac{a^3}{8}\right)y + \left(d - \frac{ac}{4} + \frac{a^2b}{16} - \frac{3a^4}{256}\right) = 0.$$

Fazendo $p = b - \frac{3a^2}{8}$, $q = c - \frac{ab}{2} + \frac{a^3}{8}$ e $r = d - \frac{ac}{4} + \frac{a^2b}{16} - \frac{3a^4}{256}$, temos que toda a equação de grau quatro é da forma

$$y^4 + py^2 + qy + r = 0, \tag{3.12}$$

equivalente a $y^4 + py^2 = -qy - r$.

“Completando o quadrado”, temos:

$$y^4 + py^2 + \left(\frac{p}{2}\right)^2 = -qy - r + \left(\frac{p}{2}\right)^2.$$

Ou seja,

$$\left(y^2 + \frac{p}{2}\right)^2 = -qy - r + \frac{p^2}{4}. \quad (3.13)$$

Introduzindo um parâmetro u , observamos que:

$$\left(y^2 + \frac{p}{2} + u\right)^2 = \left(y^2 + \frac{p}{2}\right)^2 + 2\left(y^2 + \frac{p}{2}\right)u + u^2.$$

Usando (3.13) no segundo membro desta igualdade, vem:

$$\begin{aligned} \left(y^2 + \frac{p}{2} + u\right)^2 &= -qy - r + \frac{p^2}{4} + 2y^2u + pu + u^2 \\ &= 2uy^2 - qy + \left(-r + \frac{p^2}{4} + pu + u^2\right) \end{aligned}$$

Seja u de modo que a última expressão obtida seja um quadrado perfeito, isto é, da forma $(m - n)^2$.

Sendo assim, temos:

$$2uy^2 = m^2, \text{ isto é, } m = y\sqrt{2u}$$

e

$$2mn = qy, \text{ isto é, } n = \frac{qy}{2m}.$$

Substituindo nesta última expressão o valor de m , obtemos:

$$\begin{aligned} n &= \frac{qy}{2y\sqrt{2u}} \\ &= \frac{q}{2\sqrt{2u}}. \end{aligned}$$

Assim, $n^2 = \frac{q^2}{8u}$ e teremos $\frac{q^2}{8u} = -r + \frac{p^2}{4} + pu + u^2$.

Se $u \neq 0$, vem que $q^2 = -8ru + 2p^2u + 8pu^2 + 8u^3$, ou seja, obtemos a equação do 3º grau em u :

$$8u^3 + 8pu^2 + (2p^2 - 8r)u - q^2 = 0. \quad (3.14)$$

cujas soluções (u) podem ser encontradas pela **Fórmula de Cardano**, teorema 3.2.1.

Encontrados os valores de u , para encontrar as soluções da equação em y (3.12), basta ter em conta que $\left(y^2 + \frac{p}{2} + u\right)^2 = \left(y\sqrt{2u} - \frac{q}{2\sqrt{2u}}\right)^2$.

Daqui, vem que:

$y^2 + \frac{p}{2} + u = \pm\left(y\sqrt{2u} - \frac{q}{2\sqrt{2u}}\right)$, que são equações do 2º grau em y , logo de fácil determinação das respectivas soluções.

Para resolver a equação inicial $t^4 + at^3 + bt^2 + ct + d = 0$ em ordem a t , basta fazer $t = y - \frac{a}{4}$.

Se $u = 0$ não teríamos obtido (3.14) mas teríamos $q = 0$, logo (3.12) seria uma equação biquadrada, podendo ser resolvida pela fórmula resolvente das equações do 2º grau. Assim, de novo, conseguimos resolver equações através de operações com radicais.

Exemplo 3.3.1 Apliquemos o método acima descrito na resolução da equação $t^4 + t^3 + t^2 + t + 1 = 0$, onde, usando as mesmas notações, temos: $a = b = c = d = 1$. Transformemo-la na forma $y^4 + py^2 + qy + r = 0$, fazendo $y = t + \frac{1}{4}$, equivalente a $t = y - \frac{1}{4}$.

Para tal, atendendo a (3.12), basta fazer $p = 1 - \frac{3 \times 1^2}{8} = \frac{5}{8}$, $q = 1 - \frac{1 \times 1}{2} + \frac{1^3}{8} = \frac{5}{8}$ e $r = 1 - \frac{1 \times 1}{4} + \frac{1^2 \times 1}{16} - \frac{3 \times 1^4}{256} = \frac{205}{256}$. Sendo assim, a equação dada é equivalente a $y^4 + \frac{5}{8}y^2 + \frac{5}{8}y + \frac{205}{256} = 0$, ou seja, $y^4 + \frac{5}{8}y^2 = -\frac{5}{8}y - \frac{205}{256}$.

“Complemando o quadrado”, temos

$$\left(y^2 + \frac{5}{16}\right)^2 = -\frac{5}{8}y - \frac{45}{64}. \quad (3.15)$$

Introduzindo um parâmetro u , vem

$$\left(y^2 + \frac{5}{16} + u\right)^2 = \left(y^2 + \frac{5}{16}\right)^2 + 2\left(y^2 + \frac{5}{16}\right)u + u^2.$$

Atendendo a (3.15) e reordenando, temos $\left(y^2 + \frac{5}{16} + u\right)^2 = 2uy^2 - \frac{5}{8}y - \frac{45}{64} + \frac{5}{8}u + u^2$.

Seja u de modo que a última expressão obtida seja um quadrado perfeito, isto é, da forma $(m - n)^2$. Sendo assim, temos: $m^2 = 2uy^2$, logo $m = y\sqrt{2u}$. Por outro lado, temos $2mn = \frac{5}{8}$, logo $n = \frac{5}{16\sqrt{2u}}$, depois de termos substituído o valor de m obtido. Então, temos $n^2 = \frac{25}{512u}$, o que implica que $\frac{25}{512u} = -\frac{45}{64} + \frac{5}{8}u + u^2$. Obtemos assim, para u não nulo, a equação do 3º grau $512u^3 + 320u^2 - 360u - 25 = 0$, equivalente a $u^3 + \frac{5}{8}u^2 - \frac{45}{64}u - \frac{25}{512} = 0$ cujas soluções podem ser encontradas pela **Fórmula de Cardano**, teorema 3.2.1. São elas: $u = \frac{5}{8}$, $u = -\frac{5}{8} - \frac{\sqrt{5}}{4}$ e $u = -\frac{5}{8} + \frac{\sqrt{5}}{4}$.

Para encontrar as soluções da equação (3.12) em y , basta ter em conta que

$$\left(y^2 + \frac{5}{16} + \frac{5}{8}\right)^2 = \left(y\sqrt{\frac{5}{4}} - \frac{5}{16\sqrt{\frac{5}{4}}}\right)^2$$

que são equações do 2º grau em y , logo de fácil determinação das respectivas soluções.

As equações em causa são:

$$y^2 - \frac{\sqrt{5}}{2}y + \frac{15}{16} + \frac{\sqrt{5}}{8} = 0 \text{ e } y^2 + \frac{\sqrt{5}}{2}y + \frac{15}{16} - \frac{\sqrt{5}}{8} = 0.$$

Aplicando a fórmula resolvente das equações do 2º grau, obtemos:

$$y = \frac{\sqrt{5}}{4} - \frac{\sqrt{2(5+\sqrt{5})}}{4}i; y = \frac{\sqrt{5}}{4} + \frac{\sqrt{2(5+\sqrt{5})}}{4}i; y = -\frac{\sqrt{5}}{4} - \frac{\sqrt{10-2\sqrt{5}}}{4}i \text{ e } y = -\frac{\sqrt{5}}{4} + \frac{\sqrt{10-2\sqrt{5}}}{4}i.$$

Para resolver a equação inicial $t^4 + t^3 + t^2 + t + 1 = 0$ em ordem a t , basta fazer $t = y - \frac{1}{4}$, obtendo assim as soluções $\frac{\sqrt{5}-1}{4} \pm \frac{\sqrt{2(5+\sqrt{5})}}{4}i$ e $y = -\frac{\sqrt{5}}{4} \pm \frac{\sqrt{10-2\sqrt{5}}}{4}i$.

Capítulo 4

Equações do 5º grau

4.1 Introdução

Sejam $a, b, c, d, e \in \mathbb{C}$. Qualquer equação do 5º grau pode ser escrita na forma

$$t^5 + at^4 + bt^3 + ct^2 + dt + e = 0,$$

após termos dividido ambos os membros pelo coeficiente do termo de maior grau. Usando a transformação de Tschirnhaus, $y = t + \frac{a}{5}$, a equação dada é equivalente a $y^5 + py^3 + qy^2 + ry + s = 0$. Contudo, usando métodos semelhantes ao usados para as de grau inferior, não houve sucesso na obtenção de uma fórmula resolvente que use radicais, embora tenha surgido matéria matemática muito interessante neste percurso.

No princípio do século XIX, Abel usando trabalhos de Lagrange e de Ruffini, provou que existem equações do 5º grau cujas soluções não podem ser obtidas através de operações com radicais. Esta conclusão levantou o problema de como as reconhecer.

Foi Galois quem obteve conclusões acerca do assunto e ainda sobre a impossibilidade de resolver, por radicais, uma equação de grau superior ou igual a 5.

Consideremos a equação

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{C}.$$

O conjunto dos elementos que se podem obter a partir dos coeficientes a_i através de adições, subtrações, multiplicações e divisões forma um corpo $\mathbb{K} = \mathbb{Q}(a_0, \dots, a_n)$.

O objetivo do método da obtenção de soluções através de radicais é estender o corpo \mathbb{K} por junção de radicais até obter um corpo \mathbb{L} que contenha as raízes x_1, \dots, x_n da equação dada.

Por exemplo, na equação $x^2 + a_1 x + a_0 = 0$, as raízes x_1 e x_2 estão na extensão $\mathbb{Q}(a_0, a_1) = \mathbb{Q}(x_1 x_2, x_1 + x_2)$ por junção do radical

$$\begin{aligned} \Delta &= \sqrt{a_1^2 - 4a_0} = \sqrt{(x_1 + x_2)^2 - 4x_1 x_2} = \\ &= \sqrt{x_1^2 + 2x_1 x_2 + x_2^2 - 4x_1 x_2} = \sqrt{(x_1 - x_2)^2} = \pm(x_1 - x_2). \end{aligned}$$

Neste caso, a extensão (radical) $\mathbb{L} = \mathbb{Q}(a_0, a_1, \sqrt{a_1^2 - 4a_0})$ coincide com $\mathbb{Q}(x_1, x_2)$.

Galois provou que a resolubilidade de uma equação por radicais depende das propriedades dos subgrupos dos grupos que ficaram associados ao seu nome.

4.2 Resolubilidade de equações do 5º grau através de radicais

Para abordar o método de encontrar soluções de equações por radicais é necessário ter alguns conhecimentos relativos às extensões de corpos. Os conceitos e resultados necessários a esta tarefa serão apresentados à medida que forem necessários. As demonstrações da maioria dos resultados serão omitidas, mas incluem-se as referências onde poderão ser encontradas.

Teorema 4.2.1 (Abel-Ruffini) *Existem polinômios de grau cinco que não podem ser resolúveis por radicais.*

Demonstração: Ver [16, pp. 177, Teorema 15.10] □

Iremos, nesta secção, desenvolver os conceitos necessários para provar este teorema, usando um exemplo particular. De notar que a argumentação usada é válida para qualquer outro polinômio de grau cinco com as mesmas propriedades que o considerado: ter coeficientes em \mathbb{Q} , ser irredutível em \mathbb{Q} e possuir exatamente três zeros reais.

São exemplos de polinômios com estas características: $x^5 - 8x + 2$, $x^5 - 4x + 2$, $2x^5 - 10x + 5$ e $x^5 - 6x^2 + 5$.

Para provarmos a irredutibilidade de um polinômio é útil conhecer o seguinte critério:

Teorema 4.2.2 (Critério de Eisenstein (1823-1852)) *Seja $f(t) = a_0 + a_1t + a_2t^2 + \dots + a_nt^n$ um polinômio sobre \mathbb{Z} .*

Se existir um primo q tal que:

1- $q \nmid a_n$

2- $q \mid a_i, i = 0, \dots, n-1$

3- $q^2 \nmid a_0$,

então, f é irredutível em \mathbb{Q} , isto é, não é produto de polinômios de graus menores.

Demonstração: Ver [16, pp. 55-56, Teorema 3.19] □

Para a prova pretendida, isto é, para provarmos a existência de polinômios do 5º grau irresolúveis através de radicais, consideremos o polinômio $p(x) = x^5 - 8x + 2$, por exemplo.

Ora, em $p(x)$, temos $a_0 = 2, a_1 = -8, a_2 = a_3 = a_4 = 0$ e $a_5 = 1$.

Para $q = 2$, temos que:

$2 \nmid 1; 2 \mid (-8); 2 \mid 0$ e $2^2 \nmid 2$.

Sendo assim, pelo Critério de Eisenstein, teorema (4.2.2), podemos concluir que $p(x)$ é irredutível em \mathbb{Q} , isto é, não é um produto de polinômios de graus inferiores.

Analisemos a seguinte tabela de valores de $p(x)$:

x	-2	-1	0	1	2
$p(x)$	-14	9	2	-5	18

Pelo Corolário do Teorema de Bolzano, teorema 2.2.1, e uma vez que p define uma função contínua, temos que em $] -2, -1[$, em $]0, 1[$ e em $]1, 2[$, p admite zeros. Ora, a

derivada $p'(x) = 5x^4 - 8$ é positiva exceto em $\left] -\sqrt[4]{\frac{8}{5}}, \sqrt[4]{\frac{8}{5}} \right[$ (de notar que nos referimos à raiz quarta real e positiva de $\frac{8}{5}$), ou seja, entre aproximadamente, -1.1247 e 1.1247 .

Assim, pelo Teorema de Rolle, teorema 2.2.2, como entre dois zeros de p existe pelo menos um zero de p' e como p' tem dois zeros, p tem exatamente três zeros reais distintos, digamos θ_1, θ_2 e θ_3 . Tem também dois zeros complexos conjugados, digamos θ_4, θ_5 .

Do Teorema de Kronecker, teorema 2.1.19, surge a seguinte definição que nos permitirá avançar na prova em causa:

Definição 4.2.3 (Polinómio resolúvel por radicais) Um polinómio $p(x) \in \mathbb{K}[x]$ diz-se resolúvel por radicais sobre \mathbb{K} se existir uma extensão por radicais \mathbb{L} de \mathbb{K} onde $p(x)$ se decompõe em fatores lineares.

Definição 4.2.4 (Corpo de decomposição) Seja $p(x) \in \mathbb{K}[x]$. Chama-se corpo de decomposição de $p(x)$ à menor extensão \mathbb{L} de \mathbb{K} , tal que $p(x)$ se decompõe, em \mathbb{L} , num produto de termos de grau um e $\mathbb{L} = \mathbb{K}(\theta_1, \dots, \theta_n)$, com θ_i os zeros de $p(x)$ em \mathbb{L} .

Notemos que \mathbb{L} é único.

No caso do polinómio em análise, temos que $\mathbb{L} = \mathbb{Q}(\theta_1, \theta_2, \theta_3, \theta_4, \theta_5)$ é o corpo de decomposição de $p(x)$.

Definição 4.2.5 (Automorfismos de Galois) Seja \mathbb{L} uma extensão de \mathbb{K} . Um automorfismo Φ de \mathbb{L} diz-se um \mathbb{K} -automorfismo (ou de Galois) se deixa fixos os elementos de \mathbb{K} , isto é, $\Phi|_{\mathbb{K}} = \text{id}$.

O conjunto dos \mathbb{K} -automorfismos de \mathbb{L} , munido da operação usual da composição de funções, forma um grupo:

Definição 4.2.6 (Grupo de Galois de uma extensão) Chama-se grupo de Galois de uma extensão \mathbb{L} de \mathbb{K} , que se denota por $\text{Gal}(\mathbb{L}, \mathbb{K})$, ao grupo dos \mathbb{K} -automorfismos de \mathbb{L} .

Definição 4.2.7 (Grupo de Galois de um polinómio) Seja $p(x) \in \mathbb{K}[x]$. Chama-se grupo de Galois de $p(x)$ sobre \mathbb{K} (ou grupo de Galois da equação $p(x) = 0$) que se denota por $\text{Gal}(p(x), \mathbb{K})$, ao grupo $\text{Gal}(\mathbb{L}, \mathbb{K})$, com \mathbb{L} o corpo de decomposição de $p(x)$ sobre \mathbb{K} .

Teorema 4.2.8 Se $p(x) \in \mathbb{K}[x]$ tem n zeros distintos no seu corpo de decomposição \mathbb{L} , então $\text{Gal}(p(x), \mathbb{K})$ é isomorfo a um subgrupo do grupo simétrico \mathbb{S}_n , grupo de todas as permutações (funções bijetivas) que podem ser efetuadas com n símbolos de \mathbb{K} para a composição de funções.

No caso em apreço, o grupo de Galois em causa pode ser considerado um subgrupo de \mathbb{S}_5 .

Atendendo a 2.1.14, temos:

Definição 4.2.9 (Grau de uma extensão) Seja \mathbb{L} uma extensão de \mathbb{K} . O grau da extensão \mathbb{L} sobre \mathbb{K} , denotado por $[\mathbb{L} : \mathbb{K}]$ é a dimensão do espaço vetorial \mathbb{L} sobre \mathbb{K} .

Definição 4.2.10 (Elemento algébrico) Seja \mathbb{L} uma extensão de \mathbb{K} e seja $\theta \in \mathbb{L}$. Dizemos que θ é algébrico sobre \mathbb{K} se existe um polinómio (não nulo) $p(x) \in \mathbb{K}[x]$ tal que $p(\theta) = 0$. Caso contrário, θ é transcendente sobre \mathbb{K} .

Definição 4.2.11 (*Extensão gerada e Extensão simples*) *Seja \mathbb{L} uma extensão de \mathbb{K} . Se $\mathbb{S} \subseteq \mathbb{L}$, designamos por $\mathbb{K}(\mathbb{S})$ a extensão de \mathbb{K} gerada por \mathbb{S} , ou seja, o menor subcorpo de \mathbb{L} que contém $\mathbb{K} \cup \mathbb{S}$. Se $\mathbb{S} = \{\theta_1, \dots, \theta_n\}$ ou $\mathbb{S} = \{\theta\}$, escrevemos simplesmente $\mathbb{K}(\theta_1, \dots, \theta_n)$ ou $\mathbb{K}(\theta)$ em vez de $\mathbb{K}(\mathbb{S})$. Neste último caso, $\mathbb{K}(\theta)$ diz-se uma extensão simples de \mathbb{K} .*

Proposição 4.2.12 *Seja \mathbb{L} uma extensão de \mathbb{K} e seja $\theta \in \mathbb{L}$ um elemento algébrico sobre \mathbb{K} . Seja $I = \{p(x) \in \mathbb{K}[x] : p(\theta) = 0\}$ que é um ideal de \mathbb{K} , já que para cada $k \in \mathbb{K}$, $x \in I$, kx e $xk \in I$. Existe um polinómio mónico $m_\theta(x)$ (coeficiente de maior grau unitário), único, tal que $I = \langle m_\theta(x) \rangle$, isto é, ideal principal gerado pelo polinómio $m_\theta(x)$.*

Tem-se que:

- 1- $m_\theta(x)$ é irredutível sobre \mathbb{K}
- 2- Para cada $p(x) \in \mathbb{K}[x]$, $p(\theta) = 0$ se e só se $m_\theta(x) \mid p(x)$
- 3- $m_\theta(x)$ é o polinómio mónico, não nulo, em $\mathbb{K}[x]$ de menor grau, que tem θ por zero.

Demonstração: Ver [13, pp. 37, Teorema 2.7] e [13, pp. 66-67, Proposição 3.4] □

Definição 4.2.13 (*Polinómio mínimo*) *Seja \mathbb{L} uma extensão de \mathbb{K} e seja $\theta \in \mathbb{K}$.*

Ao polinómio $m_\theta(x)$ cuja existência é assegurada pela Proposição 4.2.12, chamamos polinómio mínimo de θ sobre \mathbb{K} .

Exemplo 4.2.14 $x^2 + 1$ é o polinómio mínimo de i sobre \mathbb{R} .

Exemplo 4.2.15 $x^2 - 2$ é o polinómio mínimo de $\sqrt{2}$ sobre \mathbb{Q} .

Teorema 4.2.16 *Seja θ algébrico sobre \mathbb{K} , com polinómio mínimo $m_\theta(x)$ sobre \mathbb{K} . Então, cada elemento $\lambda \in \mathbb{K}(\theta)$ tem uma expressão única na forma $\lambda = p(\theta)$, onde $p(x) \in \mathbb{K}[x]$ é tal que $\text{grau}(p(x)) < \text{grau}(m_\theta(x))$, isto é, se $\text{grau}(m_\theta(x)) = n$, então existem $a_0, a_1, \dots, a_{n-1} \in \mathbb{K}$, únicos, tais que $\lambda = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$*

Demonstração: Ver [13, pp. 67, Teorema 3.5] □

Teorema 4.2.17 *Se θ é algébrico sobre \mathbb{K} e $\text{grau}(m_\theta(x)) = n$, então*

$[\mathbb{K}(\theta) : \mathbb{K}] = n$ e $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ é uma base do espaço vetorial $\mathbb{K}(\theta)$ sobre \mathbb{K} .

Nota: O grau da extensão, $[\mathbb{K}(\theta) : \mathbb{K}]$, coincide com o grau do polinómio mínimo, $m_\theta(x)$.

Exemplo 4.2.18 *Seja p inteiro primo. Temos: $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$ e $\{1, \sqrt{p}\}$ é uma base de $\mathbb{Q}(\sqrt{p})$ sobre \mathbb{Q} . Basta observar que $x^2 - p$ é o polinómio mínimo de \sqrt{p} sobre \mathbb{Q} e que tem grau dois.*

Teorema 4.2.19 (**Teorema da Torre**) *Sejam $\mathbb{M} \supseteq \mathbb{L} \supseteq \mathbb{K}$ extensões sucessivas de um corpo \mathbb{K} . Então $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.*

Demonstração: Ver [13, pp. 63-64, Teorema 3.2] □

Exemplo 4.2.20 Considere-se a extensão $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de \mathbb{Q} . Ora, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é a extensão simples $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ de $\mathbb{Q}(\sqrt{2})$.

Ora,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

Para determinar $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$, pensemos no grau do polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2})$.

Ora, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{R}\}$.

$\sqrt{3}$ é zero de $x^2 - 3 \in \mathbb{Q}[x] \subset \mathbb{Q}(\sqrt{2})[x]$.

Será que $x^2 - 3$ é irredutível sobre $\mathbb{Q}(\sqrt{2})$?

Sim, porque os seus zeros ($\pm\sqrt{3}$) não pertencem a $\mathbb{Q}(\sqrt{2})$.

Vejamos que, para termos

$(\pm\sqrt{3}) = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$, implicaria $3 = a^2 + 2ab\sqrt{2} + 2b^2$,

isto é, teríamos $\sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$, para $a, b \neq 0$.

Se $a = 0$, viria $2b^2 = 3$, isto é, $b = \pm\sqrt{\frac{3}{2}}$.

Se $b = 0$, viria $3 = a^2$, isto é, $a = \pm\sqrt{3}$.

Obteríamos contradições em ambos os casos, já que $a, b \in \mathbb{Q}$.

Portanto, $x^2 - 3$ é o polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}(\sqrt{2})$, logo

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$, sendo $\{1, \sqrt{3}\}$ uma base de $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$.

Pelo Exemplo 4.2.18, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, logo $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \times 2 = 4$, atendendo ao Teorema da Torre, teorema 4.2.19.

Voltemos a $p(x) = x^5 - 8x + 2$ irredutível sobre \mathbb{Q} .

Temos, para qualquer zero θ de $p(x)$ que $[\mathbb{Q}(\theta) : \mathbb{Q}] = 5$.

Consequentemente, temos que $[\mathbb{L} : \mathbb{Q}]$ é um múltiplo de 5.

Sendo $\mathbb{G} = \text{Gal}(\mathbb{L}, \mathbb{K})$ o grupo de Galois, então $|\mathbb{G}|$ é um múltiplo de 5 ($|\mathbb{G}|$ representa a ordem de \mathbb{G} , isto é o número de elementos de \mathbb{G}), uma vez que:

Definição 4.2.21 (Extensão normal) Diz-se que uma extensão finita \mathbb{L} de um corpo \mathbb{K} é uma extensão normal se for um corpo de decomposição de algum polinómio de $\mathbb{K}[x]$.

Definição 4.2.22 (Extensão separável) Um polinómio $p(x) \in \mathbb{K}[x]$, irredutível sobre \mathbb{K} , diz-se separável sobre \mathbb{K} se não tiver raízes múltiplas numa extensão de decomposição, isto é, um polinómio $p(x) \in \mathbb{K}[x]$ é separável sobre \mathbb{K} se todos os seus fatores irredutíveis o forem. Um elemento algébrico numa extensão \mathbb{L} de \mathbb{K} diz-se separável sobre \mathbb{K} se o seu polinómio mínimo for separável sobre \mathbb{K} . Diz-se que uma extensão algébrica \mathbb{L} de um corpo \mathbb{K} é uma extensão separável se qualquer $\theta \in \mathbb{L}$ for separável sobre \mathbb{K} .

Definição 4.2.23 (Extensão de Galois) Diz-se que uma extensão finita \mathbb{L} de um corpo \mathbb{K} é uma extensão de Galois se for normal e separável.

Teorema 4.2.24 Seja \mathbb{L} uma extensão finita de \mathbb{K} . Então:

(1) $|\mathbb{G}(\mathbb{L}, \mathbb{K})| \leq [\mathbb{L} : \mathbb{K}]$

(2) Se \mathbb{L} é uma extensão de Galois de \mathbb{K} , então $|\mathbb{G}(\mathbb{L}, \mathbb{K})| = [\mathbb{L} : \mathbb{K}]$

Demonstração: Ver [13, pp. 104, Teorema 3.21]] □

Vejamos agora um dos teoremas de Sylow (1832-1918):

Teorema 4.2.25 *Seja p um número primo e p^m a maior potência de p que divide a ordem do grupo G . Então $|G| = p^m k$, sendo p primo com k . O grupo G contém pelo menos um subgrupo de ordem p^m .*

Demonstração: Ver [15, pp. 30, Teorema 18.1] □

Por este resultado, vem que $G \subseteq S_5$ contém um elemento de ordem 5, isto é, um ciclo (permutação cíclica) de comprimento 5.

Por outro lado, a aplicação $z \rightarrow \bar{z}$ de \mathbb{C} , induz um \mathbb{Q} -automorfismo de \mathbb{L} que mantém fixos os três zeros reais de $p(x)$ (θ_1, θ_2 e θ_3) e permuta os dois zeros complexos, a que corresponde, digamos, a permutação (45).

Conclusão: G contém um ciclo de ordem cinco e uma transposição (ciclo de comprimento dois).

Teorema 4.2.26 *Seja p um número primo. O grupo S_p pode ser gerado por um ciclo de ordem p e qualquer transposição.*

Demonstração: Ver [4, pp. 5, Corolário 2.10] □

Sendo assim, usando o teorema anterior, 4.2.26, vem que, $G = S_5$.

A questão inicial, de $p(x)$ não ser resolúvel por radicais, advém precisamente de S_5 não ser um grupo resolúvel:

Definição 4.2.27 (Grupo resolúvel) *Um grupo G diz-se resolúvel se existir uma torre de subgrupos $\{1\} = G_0 \subseteq G_1 \subseteq G_2 \cdots \subseteq G_{n-1} \subseteq G_n = G$, tal que, para cada $i \in \{1, 2, \dots, n\}$, G_{i-1} é um subgrupo normal de G_i e G_i/G_{i-1} é abeliano.*

Nota: G_{i-1} é um subgrupo normal de G_i se e só se $xG_{i-1} = G_{i-1}x, \forall x \in G_i$.

Conclusões:

- 1- Subgrupos de grupos resolúveis são resolúveis
- 2- Quocientes de grupos resolúveis são resolúveis
- 3- Dado um subgrupo normal H de G , G é resolúvel se e só se H e G/H são resolúveis.

Por exemplo, S_3 é resolúvel pois $\{id\} \subset \{id, (123), (132)\} \subseteq S_3$, mas, S_5 já não é resolúvel. (Demonstração em [2, pp. 47, Proposição 4.1.5])

Teorema 4.2.28 *$p(x) \in \mathbb{K}[x]$ é resolúvel por radicais se e só se $Gal(p(x), \mathbb{K})$ é resolúvel.*

Demonstração: Ver [2, pp. 46-47, Teorema 4.1.3] □

Concluindo, fica assim provado que o polinómio $p(x) = x^5 - 8x + 2$ não é resolúvel por radicais, ficando assim demonstrado o Teorema de Abel-Ruffini, acima enunciado, isto é, que existem polinómios do 5º grau não resolúveis por radicais.

Uma vez que S_n não é resolúvel para $n \geq 5$ (Demonstração em [2, pp. 47, Proposição 4.1.5]), fica provado que não há fórmulas resolventes para equações de grau maior ou igual a 5.

Capítulo 5

Construções com régua e compasso

Neste capítulo vamos ver que há construções geométricas que não são possíveis usando somente régua (não graduada) e compasso, uma vez que, na sua resolução algébrica, dão origem a soluções de equações cujo grau não é uma potência de base dois, como é o caso da duplicação do cubo e da trisseção do ângulo, por exemplo; ou a números não algébricos, como é caso da quadratura do círculo.

5.1 Os problemas dos gregos

Nesta secção analisamos como é que o grau de uma extensão algébrica é uma ferramenta de grande utilidade na resolução de problemas geométricos famosos criados pelos gregos, nomeadamente o da duplicação do cubo, da trisseção de um ângulo e da quadratura do círculo.

Na Grécia antiga, muitos matemáticos pretendiam exprimir geometricamente muitas das suas ideias. Para Euclides (300 a.C.), por exemplo, só a reta e a circunferência eram figuras geométricas perfeitas. Tal pressuposto limitava a dois, os instrumentos permitidos nas construções geométricas: a régua (não graduada) e o compasso.

Mesmo com as suas indiscutíveis capacidades e feitos, os matemáticos gregos da época não foram capazes de descobrir um método geométrico para construções aparentemente simples, segundo as regras impostas. Não é contudo de espantar já que se trata de construções impossíveis usando apenas os dois instrumentos permitidos: a régua não graduada e o compasso. Acresça-se o facto de não possuírem forma de o provar nem tão pouco desconfiavam de tal impossibilidade. Sabiam contudo que, sem as limitações de Platão (428/427 a.C.- 348/347 a.C.) as construções eram possíveis.

A prova da impossibilidade, obedecendo às regras de Platão, só veio a ser revelada nos finais do século XIX, exatamente com as extensões de corpos.

5.1.1 A duplicação do cubo

Este problema consiste na construção de um cubo com o dobro do volume de um cubo dado. Se tomarmos um cubo de aresta 1, pretendemos construir um outro cuja aresta tenha de comprimento $\sqrt[3]{2}$. Se tal fosse possível, então um determinado espaço vetorial teria a dimensão errada, como veremos.

Uma referência a este problema aparece num documento supostamente escrito por Eratóstenes (276-194 a.C.) ao rei Ptolomeu II onde cita o poeta Minos que dava uma sugestão errada para a construção de um novo túmulo para Glaucus (na mitologia grega, um deus do mar que se terá tornado imortal por ter comido uma erva mágica):

O túmulo que escolheste é pequeno demais para túmulo real. Duplica-o [em volume] sem lhe modificar a forma. Conseguirás isso se duplicares cada lado do túmulo [13, pp. 72].

Como sabemos, estava errado: nesse caso, o volume do novo túmulo seria 2^3 vezes maior. Este assunto tornou-se motivo de investigação entre os geómetras.

5.1.2 A trisseção do ângulo

A trisseção de um ângulo arbitrário questiona a existência de um método de divisão deste em três partes iguais. Sabemos que há alguns ângulos que podem ser trissetados. Será que todos o são?

Mostraremos adiante que, não é possível usando apenas régua e compasso, com o ângulo de amplitude 60 graus. Tal só poderia acontecer caso o ponto de coordenadas $(\cos 20, 0)$ fosse *construível*, o que não acontece já que $\cos 20$ é zero do polinómio $8x^3 - 6x - 1$ que é irredutível sobre \mathbb{Q} , como veremos mais adiante aquando da análise da resolução algébrica deste problema.

É provável que a origem deste problema esteja ligada à paixão dos gregos pela construção de polígonos regulares: a construção de um eneágono regular implica que a trisseção do ângulo seja possível.

5.1.3 A quadratura do círculo

Este problema tem a ver com a construção de um quadrado cuja área seja igual à de um círculo dado. Se partirmos de um círculo de raio 1 (cuja área é π), pretende-se a construção de um quadrado cujo lado tenha comprimento $\sqrt{\pi}$.

Encontramos informação sobre o assunto no Papiro de Rhind, o manuscrito matemático mais antigo que se conhece e que foi copiado por Ahmes (1680-1620 a.C.).

5.1.4 A construção de um heptágono regular numa circunferência dada

Em 1837, Wantzel (1814-1848) provou, para além da impossibilidade da construção de um heptágono regular inscrito numa dada circunferência, a impossibilidade dos problemas da duplicação do cubo e o da trisseção do ângulo ao provar a irredutibilidade, sobre o corpo dos números racionais, de polinómios convenientes. Em 1882, Lindemann (1852-1939) provou a impossibilidade da quadratura do círculo quando provou a transcendência de π sobre o mesmo corpo.

Antes destes, muitos matemáticos e muitos curiosos abordaram estes problemas e a eles se dedicaram. O número de tentativas de resolução foi de tal forma que, em 1775, a Academia de Paris, decretou que, mais nenhuma solução destes problemas apresentada por amadores seria analisada, evitando assim a perda de tempo dos seus funcionários.

O tempo que demorou a serem resolvidos estes problemas, depois de colocados, deveu-se ao facto de as construções em causa serem impossíveis usando apenas régua não graduada e compasso e porque a demonstração de tal impossibilidade assenta sobre argumentos

algébricos (então desconhecidos), embora os problemas sejam geométricos. Os argumentos necessários à prova só começaram a ser desenvolvidos no século XIX. Referimo-nos, como já foi dito, às extensões de corpos, nomeadamente à do corpo dos números racionais.

5.2 As regras impostas pelos gregos

Relativamente às construções geométricas em causa, as regras impostas pelos gregos eram muito restritivas:

A régua é usada como mero instrumento auxiliar para traçar linhas direitas mas não para medir ou marcar distâncias.

Regra 1: A régua pode ser usada para traçar uma nova linha, com a extensão que se pretenda, através de quaisquer dois pontos que façam (já) parte da figura

Regra 2: O compasso pode ser usado para traçar novas circunferências, de dois modos:

(a) Colocar uma das extremidades do compasso num dos pontos dados e a outra extremidade noutra dos pontos dados e traçar a circunferência ou um seu arco;

(b) Colocar o compasso como em (a) mas, de seguida, mover, sem alterar a sua abertura, uma das extremidades para um terceiro ponto da figura. Traçar aí uma circunferência (ou um seu arco) com este terceiro ponto como centro.

De notar que, primitivamente, com os géometras gregos o uso do compasso não incluía a regra 2 (b). Os gregos achavam que o compasso quando levantado, deixava de existir, não podendo por isso, ser usado para transferir comprimentos. Porém, prova-se que, qualquer construção que se possa fazer com as regras 1, 2(a) e 2(b) pode realizar-se somente usando 1 e 2(a). A diferença é que no último caso, poderá exigir mais passos.

Conhecemos muitas construções que obedecem às regras estabelecidas, como por exemplo: divisão de um segmento de reta num qualquer número de partes iguais; traçado de uma paralela ou de uma perpendicular a uma reta dada, passando por um ponto dado; bissecção de um ângulo; construção de um ângulo de amplitude 60° , dados dois pontos; inscrição de um pentágono regular numa circunferência;...

Algumas destas construções figuram nos diversos volumes dos *Elementos* de Euclides que sistematizou uma enorme variedade de construções possíveis de realizar com régua e compasso. Por exemplo, a bissecção de um ângulo dado figura no *Livro 1* (Proposição 9) e a inscrição de um pentágono regular numa dada circunferência, no *Livro 4* (Proposição 11).

Analisemos uma construção cumpridora das regras impostas e que consta de [9] (cf. [13, pp. 79]):

Exemplo 5.2.1 *Dado um segmento de reta de comprimento $\alpha > 0$, é possível construir um segmento de reta de comprimento $\sqrt{\alpha}$.*

Consideremos, em referencial cartesiano, $A = (1, 0)$ e $B = (1 + \alpha, 0)$, extremos de um segmento de reta e a origem $O = (0, 0)$.

Assinalemos o ponto de coordenadas $(1, 1)$ e o ponto médio M , do segmento de reta $[OB]$.

Construamos a circunferência de centro M e raio \overline{MB} .

Tracemos a reta vertical definida por A e por $(1, 1)$.

A interseção da circunferência e desta reta dá-nos um ponto C que dista de A , $\sqrt{\alpha}$, já que:

$\overline{AM} = \frac{1+\alpha}{2} - 1;$
 $\overline{MC} = \overline{MB} = \frac{1+\alpha}{2}$ (raio da circunferência).
 Como $\overline{AM}^2 + \overline{AC}^2 = \overline{MC}^2$, temos
 $(\frac{1+\alpha}{2} - 1)^2 + \overline{AC}^2 = (\frac{1+\alpha}{2})^2,$
 isto é, $(\frac{\alpha-1}{2})^2 + \overline{AC}^2 = (\frac{1+\alpha}{2})^2.$
 Simplificando, vem:
 $\overline{AC}^2 = \frac{1+2\alpha+\alpha^2}{4} - \frac{\alpha^2-2\alpha+1}{4},$ o que traduz que:
 $\overline{AC}^2 = \alpha,$ isto é, $\overline{AC} = \sqrt{\alpha}.$

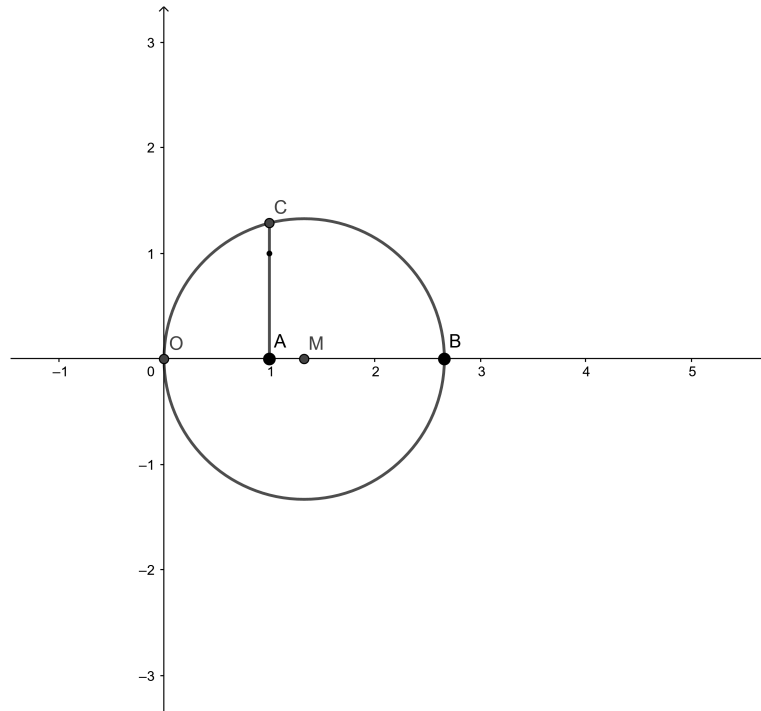


Figura 5.1: Construção de um segmento de reta de comprimento $\sqrt{\alpha}$

5.3 A solução algébrica dos problemas

Nesta secção, iremos formular em termos algébricos, a geometria das construções em causa com régua e compasso.

Consideremos o corpo \mathbb{R} dos números reais e seja \mathbb{P} uma qualquer parte do conjunto dos pontos do plano \mathbb{R}^2 de cardinal maior que um.

Definição 5.3.1 (*Ponto construível num passo*) Um ponto P do plano diz-se construível num passo a partir de \mathbb{P} se P for a intersecção de duas retas, uma reta e uma circunferência ou duas circunferências construídas a partir dos pontos de \mathbb{P} , usando régua e compasso, de acordo com as regras (1) e (2) acima estabelecidas.

Mais geralmente, um ponto P do plano diz-se construível a partir de \mathbb{P} se existirem $P_1, P_2, \dots, P_n = P$ tais que P_1 é construível num passo a partir de \mathbb{P} e, para

cada $i = 2, 3, \dots, n$, P_i é construível num passo a partir de \mathbb{P}_{i-1} , fazendo $\mathbb{P}_{i-1} = \mathbb{P} \cup \{P_1, P_2, \dots, P_{i-1}\}$.

Exemplo 5.3.2 Bisseção de um segmento de reta

Dados dois pontos A e B , construíamos o ponto médio, C , do segmento de reta de A a B que denotamos por $[AB]$.

Consideremos $\mathbb{P} = \{A, B\}$.

Método de construção:

(1) Coloquemos a ponta seca do compasso em A e estendamos a outra ponta até que esteja exatamente em B . Desenhemos a circunferência e repitamos o processo colocando a ponta seca do compasso no ponto B . Designemos por D e E os pontos de interseção das circunferências desenhadas. Ora, D e E são construíveis num passo a partir de $\mathbb{P} = \{A, B\}$.

(2) Seja $\mathbb{P}_1 = \mathbb{P} \cup \{D, E\}$. Com o auxílio da régua, tracemos o segmento de reta $[DE]$. O ponto C pretendido é o ponto de interseção de $[AB]$ (construído também com o auxílio da régua) com $[DE]$. C é assim construível num passo a partir de \mathbb{P}_1 .

Concluindo, C é assim construível em dois passos a partir de \mathbb{P} .

A estratégia para ultrapassar as limitações das construções com régua não graduada e compasso é, em cada fase da construção, associarmos o subcorpo de \mathbb{C} gerado pelas coordenadas dos pontos construídos que é também um subcorpo de \mathbb{R} .

Seja \mathbb{K}_0 o subcorpo de \mathbb{R} gerado pelo conjunto $\{x, y \in \mathbb{R} : (x, y) \in \mathbb{P}\}$, com \mathbb{P} uma qualquer parte de \mathbb{R}^2 . Para $i \geq 1$, se $P_i = (x_i, y_i)$ então definamos $\mathbb{K}_i = \mathbb{K}_{i-1}(x_i, y_i)$, isto é, juntemos ao subcorpo \mathbb{K}_{i-1} o conjunto $\{x_i, y_i\}$.

Desta construção, resulta a torre de subcorpos que acompanha a construção pretendida:

$$\mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \mathbb{K}_2 \subseteq \dots \subseteq \mathbb{K}_n \subseteq \mathbb{R}.$$

No exemplo acima, note-se que, quando $A(0, 0)$ e $B(1, 0)$, temos

$$\mathbb{P} = \{(0, 0), (1, 0)\} \text{ e } \mathbb{K}_0 = \mathbb{Q}.$$

Ora, $\mathbb{K}_1 = \mathbb{Q}(\sqrt{3}) = \mathbb{K}_2$, já que, pelo Teorema de Pitágoras, temos $D = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$, $E = \left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$ e $C = \left(\frac{1}{2}, 0\right)$.

O facto de as retas e as circunferências usadas para a construção dos pontos P_1, P_2, \dots, P_n serem definidas, em \mathbb{R}^2 , como sabemos, por equações de graus um e dois, do tipo

$ax + by + c = 0$ ($a, b, c \in \mathbb{R}$) e $x^2 + y^2 + ax + by + c = 0$ ($a, b, c \in \mathbb{R}$), respetivamente, somos conduzidos ao lema:

Lema 5.3.3 Os números reais x_i e y_i são zeros em \mathbb{K}_i de polinómios de coeficientes em \mathbb{K}_{i-1} de grau um ou dois, em particular $[\mathbb{K}_i : \mathbb{K}_{i-1}] \in \{1, 2, 4\}$.

Contudo, nunca toma o valor 4 já que x_i e y_i pertencem à mesma extensão quadrática de \mathbb{K}_{i-1} [17, pp. 79, Teorema 7.4].

Demonstração: Como $P_i = (x_i, y_i)$ é construível a partir de \mathbb{P}_{i-1} , então ou é:

- a interseção de duas retas definidas por pontos de \mathbb{P}_{i-1}
- a interseção de uma reta e de uma circunferência definidas por pontos de \mathbb{P}_{i-1}
- a interseção de duas circunferências definidas por pontos de \mathbb{P}_{i-1} .

Demonstremos apenas o segundo caso (interseção de uma reta e de uma circunferência).

Seja P_i um ponto de interseção da reta l definida pelos pontos $A = (a_1, a_2)$ e $B = (b_1, b_2)$ de \mathbb{P}_{i-1} e da circunferência de centro $C = (c_1, c_2) \in \mathbb{P}_{i-1}$ e raio r dado pela distância entre os pontos $U = (u_1, u_2)$ e $V = (v_1, v_2) \in \mathbb{P}_{i-1}$, com $U \neq V$.

A reta l pode ser definida por

$$y = \frac{b_2 - a_2}{b_1 - a_1}x + b. \quad (5.1)$$

Como $A \in l$, temos $a_2 = \frac{b_2 - a_2}{b_1 - a_1}a_1 + b$, ou seja, $b = a_2 - \frac{b_2 - a_2}{b_1 - a_1}a_1$. Substituindo em (5.1), temos: $y = (x - a_1)\frac{b_2 - a_2}{b_1 - a_1} + a_2$, ou seja, $\frac{x - a_1}{b_1 - a_1} = \frac{y - a_2}{b_2 - a_2}$, com $a_1 \neq b_1$ e $a_2 \neq b_2$.

Por outro lado, a circunferência pode ser definida por $(x - c_1)^2 + (y - c_2)^2 = r^2$.

Sendo assim, $P_i = (x_i, y_i)$ é solução do sistema

$$\begin{cases} \frac{x - a_1}{b_1 - a_1} = \frac{y - a_2}{b_2 - a_2} \\ (x - c_1)^2 + (y - c_2)^2 = r^2 \end{cases},$$

com $a_1, a_2, b_1, b_2, c_1, c_2, u_1, u_2, v_1, v_2 \in \mathbb{K}_{i-1}$.

Ora, pelo Teorema de Pitágoras, $r^2 = (v_1 - a_1)^2 + (v_2 - a_2)^2 \in \mathbb{K}_{i-1}$.

Resolvendo a primeira equação em ordem a y e substituindo na segunda, temos:

$$y = \frac{b_2 - a_2}{b_1 - a_1}(x - a_1) + a_2 \text{ e } (x - c_1)^2 + \left(\frac{b_2 - a_2}{b_1 - a_1}(x - a_1) + a_2 - c_2 \right)^2 = r^2.$$

x_i é então zero do polinómio quadrático $(x - c_1)^2 + \left(\frac{b_2 - a_2}{b_1 - a_1}(x - a_1) + a_2 - c_2 \right)^2 - r^2 \in \mathbb{K}_{i-1}[x]$.

Se este polinómio for irredutível sobre \mathbb{K}_{i-1} , então $[\mathbb{K}_{i-1}(x_i) : \mathbb{K}_{i-1}] = 2$, caso contrário, $[\mathbb{K}_{i-1}(x_i) : \mathbb{K}_{i-1}] = 1$.

Se resolvêssemos a primeira equação em ordem a x e substituíssemos, teríamos, analogamente, que y_i seria zero de um polinómio quadrático em $\mathbb{K}_{i-1}[y]$, pelo que viria também $[\mathbb{K}_{i-1}(y_i) : \mathbb{K}_{i-1}] \in \{1, 2\}$.

Nos três casos (interseção de duas retas, de uma reta e de uma circunferência e de duas circunferências), teremos $[\mathbb{K}_{i-1}(x_i) : \mathbb{K}_{i-1}]$ e $[\mathbb{K}_{i-1}(y_i) : \mathbb{K}_{i-1}]$, para $i = 1, 2, \dots, n$, a tomar os valores 1 ou 2.

Uma vez que $[\mathbb{K}_{i-1}(x_i, y_i) : \mathbb{K}_{i-1}(x_i)] \leq [\mathbb{K}_{i-1}(y_i) : \mathbb{K}_{i-1}]$, vem que

$$[\mathbb{K}_{i-1}(x_i, y_i) : \mathbb{K}_{i-1}(x_i)] \in \{1, 2\}.$$

Sendo assim, como $[\mathbb{K}_i : \mathbb{K}_{i-1}] = [\mathbb{K}_{i-1}(x_i, y_i) : \mathbb{K}_{i-1}(x_i)] [\mathbb{K}_{i-1}(x_i) : \mathbb{K}_{i-1}]$, temos que $[\mathbb{K}_i : \mathbb{K}_{i-1}] \in \{1, 2\}$. \square

Daqui resulta que:

Teorema 5.3.4 *Se o ponto $P = (x, y) \in \mathbb{IR}^2$ é construível a partir de \mathbb{P} então $[\mathbb{K}_0(x) : \mathbb{K}_0]$ e $[\mathbb{K}_0(y) : \mathbb{K}_0]$ são potências de base 2.*

Demonstração: Por definição, existe uma sequência finita de pontos de \mathbb{IR}^2 , digamos $P_1, P_2, \dots, P_n = P$, tais que para $i = 1, 2, \dots, n$ o ponto $P_i(x_i, y_i)$ é *construível* num passo a partir de \mathbb{P}_{i-1} .

Pelo lema 5.3.3, tem-se $[\mathbb{K}_i : \mathbb{K}_{i-1}] \in \{1, 2\}$.

Ora, $[\mathbb{K}_n : \mathbb{K}_0] = [\mathbb{K}_n : \mathbb{K}_{n-1}] [\mathbb{K}_{n-1} : \mathbb{K}_{n-2}] \cdots [\mathbb{K}_2 : \mathbb{K}_1] [\mathbb{K}_1 : \mathbb{K}_0]$, pelo que

$[\mathbb{K}_n : \mathbb{K}_0]$ é uma potência de base 2 (produto de potências de base 2).

Como $[\mathbb{K}_n : \mathbb{K}_0] = [\mathbb{K}_n : \mathbb{K}_0(x)] [\mathbb{K}_0(x) : \mathbb{K}_0]$; $[\mathbb{K}_n : \mathbb{K}_0] = [\mathbb{K}_n : \mathbb{K}_0(y)] [\mathbb{K}_0(y) : \mathbb{K}_0]$, vem o pretendido. \square

É este o resultado chave para a prova da impossibilidade de construção, com régua e compasso, dos problemas clássicos atrás referidos. Permitir-nos-á, assim, provar a impossibilidade da construção de muitos números a partir dos racionais.

A duplicação do cubo

Teorema 5.3.5 *O cubo não pode ser duplicado usando construções com régua e compasso.*

Demonstração: Dado um cubo de lado unitário e portanto de volume $1^3 = 1$, consideremos como uma das suas arestas o segmento de reta de extremos $(0, 0)$ e $(1, 0)$.

Um cubo de volume duplo, 2, teria uma aresta de comprimento α , tal que $\alpha^3 = 2$.

A obtenção do cubo de volume 2 corresponde à construção, a partir de $\mathbb{P} = \{(0, 0), (1, 0)\}$ de uma aresta de comprimento $\sqrt[3]{2}$, o que é equivalente à construção do ponto $(\sqrt[3]{2}, 0)$ partindo de \mathbb{P} .

Como $\mathbb{K}_0 = \mathbb{Q}$, se tal fosse possível, teríamos que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ seria uma potência de base 2. Mas, $\sqrt[3]{2}$ é zero do polinómio $x^3 - 2$, irreduzível em \mathbb{Q} , pelo Critério de Eisenstein, teorema 4.2.2, (para $q = 2$, por exemplo: $2 \nmid 1; 2 \mid 0; 2^2 \nmid (-2)$). Logo, o polinómio mínimo de $\sqrt[3]{2}$ sobre \mathbb{Q} é $x^3 - 2$, logo $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (atendendo a 4.2.17), que não é uma potência de base 2.

Sendo assim, fica provado que o cubo não pode ser duplicado. \square

A trisseção do ângulo

Teorema 5.3.6 *O ângulo de amplitude $\frac{\pi}{3}$ radianos não pode ser trissetado usando construções com régua e compasso.*

Demonstração:

Consideremos $\mathbb{P} = \{(0, 0), (1, 0)\}$ e $\mathbb{K}_0 = \mathbb{Q}$. Construamos a circunferência c de centro $O = (0, 0)$ que passa por $A = (1, 0)$. Se traçarmos arcos de raio $[OA]$ e centros em O e em A , obtemos o ponto B tal que $[OAB]$ é equilátero, isto é $\hat{AOB} = \frac{\pi}{3}$. Se fosse possível trissectar o ângulo \hat{AOB} , seria possível, a partir de \mathbb{P} , construir o ponto $C \in \mathbb{R}^2$ tal que $\hat{AOC} = \frac{\pi}{3} = \frac{\pi}{9}$, isto é, o ponto $(\cos(\frac{\pi}{9}), 0) \in [OA]$. Sendo assim, também seria possível construir o ponto $(2 \cos(\frac{2\pi}{9}), 0)$ e teríamos que $[\mathbb{Q}(2 \cos(\frac{\pi}{9})) : \mathbb{Q}]$ seria uma potência de base 2, o que é falso.

Já provámos na Secção 3.2 que: $\cos(3\theta) = 4 \cos^3 \theta - 3 \cos \theta$, qualquer que seja o valor de θ . Assim, para $\theta = \frac{\pi}{9}$, temos $\cos(\frac{3\pi}{9}) = 4 \cos^3(\frac{\pi}{9}) - 3 \cos(\frac{\pi}{9})$, isto é, $\cos(\frac{\pi}{3}) = 4 \cos^3(\frac{\pi}{9}) - 3 \cos(\frac{\pi}{9})$, isto é, $\frac{1}{2} = 4 \cos^3(\frac{\pi}{9}) - 3 \cos(\frac{\pi}{9})$.

Sendo assim, $\cos(\frac{\pi}{9})$ é zero do polinómio

$$8x^3 - 6x - 1 = 0. \quad (5.2)$$

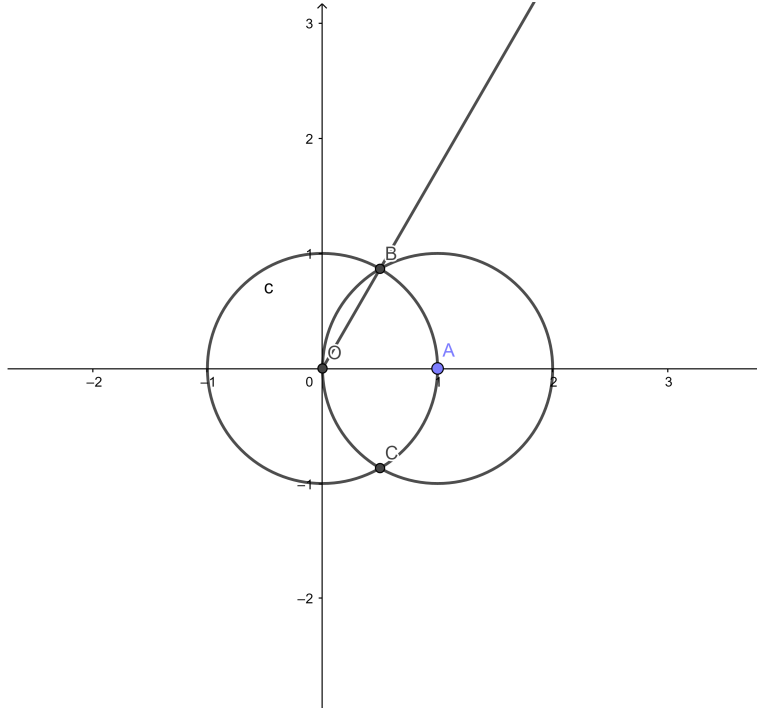


Figura 5.2: Construção de um ângulo de amplitude $\frac{\pi}{3}$ radianos

Fazendo $\beta = 2 \cos\left(\frac{\pi}{9}\right)$, temos $\cos\left(\frac{\pi}{9}\right) = \frac{\beta}{2}$ e de (5.2), vem $8\frac{\beta^3}{8} - 6\frac{\beta}{2} - 1 = 0$, ou seja, $\beta^3 - 3\beta - 1 = 0$, isto é, $2 \cos\left(\frac{\pi}{9}\right)$ é zero do polinómio $x^3 - 3x - 1$.

Mas, $x^3 - 3x - 1 \in \mathbb{Q}[x]$ é irreduzível sobre \mathbb{Q} . Se tivesse zeros racionais, eles só poderiam ser 1 ou -1 , atendendo à proposição 2.1.20, o que não acontece.

Concluindo, por 4.2.17, temos:

$[\mathbb{Q}(2 \cos(\frac{\pi}{9})) : \mathbb{Q}] = 3$ que não é uma potência de base 2, o que prova que o ângulo de amplitude $\frac{\pi}{3}$ radianos não pode ser trissetado. \square

A quadratura do círculo

Teorema 5.3.7 *Não é possível fazermos a quadratura do círculo usando construções com régua e compasso.*

Demonstração: Seja $\mathbb{P} = \{(0,0), (1,0)\}$, considerando assim um círculo de raio 1, isto é, de área π .

O objetivo seria a construção de um quadrado de área π , isto é, de medida de lado $\sqrt{\pi}$, isto é, a construção do ponto $(\sqrt{\pi}, 0)$ (ou $(0, \sqrt{\pi})$). Mas, se $(\sqrt{\pi}, 0)$ fosse *construível* então $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = 2^n$, para algum $n \in \mathbb{N}_0$. Neste caso, teríamos que $[\mathbb{Q}(\pi) : \mathbb{Q}]$ dividiria 2^n . Como $\sqrt{\pi}$ é zero do polinómio $x^2 - \pi$, então $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)] = 2$. Por outro lado, $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{\pi} : \mathbb{Q}(\pi))][\mathbb{Q}(\pi) : \mathbb{Q}]$, portanto $[\mathbb{Q}(\pi) : \mathbb{Q}]$ dividiria 2^n e teríamos π algébrico sobre \mathbb{Q} , isto é, existiria um polinómio não nulo em \mathbb{Q} que admitiria π como zero. Tal é absurdo, como provou Lindemann em 1882, π é transcendente sobre \mathbb{Q} , logo

fica demonstrado o pretendido. \square

A construção de polígonos regulares

Teorema 5.3.8 *Não é possível inscrever um heptágono regular numa circunferência usando construções com régua e compasso.*

Demonstração: Seja $\mathbb{P} = \{(0, 0), (1, 0)\}$, considerando assim uma circunferência de raio 1.

Os vértices do heptágono regular são determinados pelas raízes da equação $x^7 = 1$, isto é pelas raízes de índice 7 da unidade. Uma delas é $e^{i\frac{2\pi}{7}}$. Sendo assim, será possível inscrever um heptágono regular na circunferência, se o ponto $(\cos(\frac{2\pi}{7}), \sin(\frac{2\pi}{7}))$ for *construível* a partir de \mathbb{P} , isto é, se cada uma das coordenadas do ponto o for.

Ora, $x^7 - 1 = 0$ é equivalente a $(x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = 0$.

Assim, as demais raízes da equação $x^7 - 1 = 0$ são as da equação

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0.$$

Se dividirmos ambos os membros por x^3 , não nulo, obtemos

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

Equivalentemente, temos $x^3 + \frac{1}{x^3} + x^2 + \frac{1}{x^2} + x + \frac{1}{x} + 1 = 0$.

Adicionando quantidades adequadas, podemos ter

$$\left(x^3 + \frac{1}{x^3} + 3\left(x + \frac{1}{x}\right) - 3\left(x + \frac{1}{x}\right)\right) + \left(x^2 + \frac{1}{x^2} + 2 - 2\right) + \left(x + \frac{1}{x}\right) + 1 = 0.$$

Isto é, $(x + \frac{1}{x})^3 - 3(x + \frac{1}{x}) + (x + \frac{1}{x})^2 - 2 + (x + \frac{1}{x}) + 1 = 0$.

Simplificando, temos $(x + \frac{1}{x})^3 + (x + \frac{1}{x})^2 - 2(x + \frac{1}{x}) - 1 = 0$.

Fazendo $y = x + \frac{1}{x}$, vem $y^3 + y^2 - 2y - 1 = 0$.

Ora, sabemos que x é uma raiz de índice 7 da unidade. Seja $x = e^{i\frac{2\pi}{7}}$. Então $\frac{1}{x} = e^{-i\frac{2\pi}{7}}$.

Sendo assim, $y = x + \frac{1}{x} = 2\cos(\frac{2\pi}{7})$. Ora, se y é *construível*, então $\cos(\frac{2\pi}{7})$ também é *construível*, e reciprocamente. Por outro lado, se x é *construível*, então $y = x + \frac{1}{x}$ também o é. Logo, se provarmos que y não é *construível*, provaremos que x também não o é.

Assim, é suficiente mostrar que o polinómio $y^3 + y^2 - 2y - 1$ não tem zeros racionais. Se os tivesse, eles só poderiam ser 1 ou -1, atendendo à proposição 2.1.20, o que não acontece. Logo, o polinómio é irredutível sobre \mathbb{Q} .

Sendo assim, $[\mathbb{Q}(2\cos(\frac{2\pi}{7})) : \mathbb{Q}] = 3$, que não é potência de 2, o que prova que $2\cos(\frac{2\pi}{7})$ não é *construível*, isto é, o heptágono regular não pode ser inscrito numa circunferência usando régua e compasso [12]. \square

E quanto ao caso geral de um polígono regular com n lados? Quando é que é possível inscrever um polígono regular numa circunferência, usando apenas régua e compasso?

Definição 5.3.9 (*Polígono construível*) *Um polígono diz-se construível se todos os seus vértices são pontos construíveis de \mathbb{R}^2 .*

No caso $n = 7$, vimos que a construção passava pela construção do ponto

$$\left(\cos \left(\frac{2\pi}{n} \right), \sin \left(\frac{2\pi}{n} \right) \right).$$

Se inscrevermos um polígono regular com n lados na circunferência unitária de centro na origem do referencial (\mathbb{R}^2) e um dos vértices no ponto $(1, 0)$, então os outros vértices serão os elementos do conjunto

$$\left\{ \left(\cos \left(\frac{2\pi k}{n} \right), \sin \left(\frac{2\pi k}{n} \right) \right) : 0 < k < n \right\}.$$

Se conseguirmos construir o ponto $\left(\cos \left(\frac{2\pi}{n} \right), \sin \left(\frac{2\pi}{n} \right) \right)$, então conseguimos construir os outros a partir deste, usando régua e compasso.

Assim, o polígono é *construível* se e só se este ponto/vértice é *construível*.

Os gregos foram capazes de construir, com régua e compasso, polígonos regulares com 3, 4, 5 e 6 lados, mas, como era de prever, não o conseguiram fazer para o de 7 lados. E pararam aqui. Só em 1796, Gauss (1777-1855), com 19 anos e enquanto estudante da Universidade de Göttingen, depois de ter deixado Brunswick, avançou, construindo um polígono regular com 17 lados, o maior passo na área, desde os feitos dos matemáticos gregos. Publicou o seu resultado na Secção VII (artigo 354) da sua famosa obra *Disquisitiones Arithmeticae* dedicada à Teoria dos Números, à exceção da secção referida [6][21]. Descobriu ainda uma condição suficiente para que um polígono regular de n lados (n -gono) seja *construível* com régua e compasso:

Teorema 5.3.10 *O n -gono regular é construível com régua e compasso se*

$$n = 2^\alpha \text{ ou } n = 2^\beta p_1 \cdots p_t, \quad (5.3)$$

com $\alpha \in \mathbb{N} \setminus \{1\}$, $\beta \in \mathbb{N}_0$, $t \in \mathbb{N}$ e p_i primos ímpares distintos da forma $p_i = 2^{2^{r_i}} + 1$ ($r_i \in \mathbb{N}_0$) [13, pp. 86].

O número $F_r = 2^{2^r} + 1$, $r \in \mathbb{N}_0$ (n -ésimo número de Fermat (1601-1665)) quando primo, denomina-se um primo de Fermat.

Os cinco primeiros números primos de Fermat, por si mesmo descobertos, são:

r	$F_r = 2^{2^r} + 1$
0	3
1	5
2	17
3	257
4	65537

Fermat conjecturou que qualquer número F_r é primo mas, em 1732, foi contrariado por Euler (1707-1783) que mostrou que $F_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417$, isto é, não é primo.

Os únicos números primos de Fermat conhecidos até ao momento são os descobertos pelo próprio.

Sendo assim, só se sabe que um polígono regular com p lados (p primo) é *construível* para $p = 2, 3, 5, 17, 257, 65537$.

Refira-se que as primeiras construções consistentes de um 257-gono se deveram a Magnus Paucker (1787-1855) em 1822 e depois a Friedrich Richelot (1808-1875) em 1832 [22].

Assim, para $n \leq 100$, o n -gono regular é *construível* se e só se é um dos seguintes números:

$3(= F_0)$; $4(= 2^2)$; $5(= F_1)$; $6(= 2 \times 3)$; 8; 10; 12; 15; 16; 17; 20; 24; 30; 32; 34; 40; 48; 51; 60; 64; 68; 80; 85 e 96.

Exemplos:

$$96 = 2^5 \times 3(3 = F_0)$$

$$85 = 2^0 \times 5 \times 17(5 = F_1; 17 = F_2)$$

$$80 = 2^4 \times 5(5 = F_1)$$

$$51 = 2^0 \times 3 \times 17(17 = F_2).$$

Refira-se que o polígono regular com 18 lados não é *construível* com régua e compasso já que $18 = 2 \times 3 \times 3$ e sendo assim o número primo 3 aparece duas vezes.

Se n não tiver nenhuma das formas indicadas em (5.3), Wantzel, em 1837, provou que a construção é impossível num artigo no *Journal de Mathématiques Pures et Appliquées*, habitualmente conhecido pelo nome do seu fundador *Liouville* (1809-1889). Com este artigo, tornou-se o primeiro a publicar as provas da impossibilidade de construção, com régua e compasso, dos famosos problemas dos gregos. Mais tarde, as provas foram melhoradas por Charles Sturm, contudo sem publicação. Em 1845, Wantzel, no aprofundamento do seu trabalho no domínio da resolução de equações, apresentou nova prova da impossibilidade de resolver todas as equações algébricas por radicais. Escreveu na introdução que, embora a prova de Abel estivesse correta, entendia que era apresentada de uma forma muito complicada e vaga, por isso tão pouco apreciada. Referia ainda os estudos de Ruffini, muitos anos antes, que considerava ainda mais vaga e insuficiente. Revelava que tinha sido também da reunião das pesquisas destes dois matemáticos que havia chegado a uma prova que lhe parecia ser tão rigorosa que não deixaria margem para dúvidas sobre esta parte tão importante da resolução de equações por radicais [21].

Capítulo 6

Número e localização de zeros reais de um polinómio

Vimos, até aqui, que, para equações de grau superior a quatro, existem equações que não podem ser resolvidas por radicais (Teorema de Abel). Sendo assim, nestes casos, para além do recurso a processos gráficos, teremos de usar métodos numéricos de aproximação das raízes que exigem uma aproximação inicial de uma delas. Por isso, é de particular importância conhecer previamente o seu número, a sua localização e/ou ainda a sua separação, por exemplo, em intervalos disjuntos. Neste capítulo, abordamos alguns resultados que permitirão cumprir estes objetivos.

Para a determinação do número de zeros reais de um polinómio apresentamos:

- a Regra de Budan-Fourier que adquiriu o nome dos matemáticos contemporâneos Budan de Boislaurent e de Joseph Fourier que de forma autónoma e independente desenvolveram dois teoremas diferentes mas equivalentes que permitiam determinar o número máximo de zeros reais de um polinómio num determinado intervalo. Budan, um matemático amador, revelou-o num livro de memórias em 1803, mas só o publicou passados quatro anos. Já Fourier terá usado a regra congénere num curso que ministrou em 1797. Só após a sua morte o resultado foi publicado (1831);

- a Regra dos sinais de Descartes, por ele descrita em 1636 no livro *La Géométrie, III*, a obra a que se refere como aquela onde conseguiu demonstrar o que nas obras *Dioptrique*, *Météores* apenas tentou fazer: que o “seu” *Méthode* era melhor que o vulgar... Considerado o “pai da filosofia moderna” apresentou uma “visão científica transformada do mundo” e foi responsável por um novo ramo da Matemática que ligava a Geometria à Álgebra. O livro atrás referido é considerado uma tratado sobre a teoria elementar das equações abordando: a determinação das suas raízes racionais, o “baixar” do grau conhecida uma das raízes, entre outros, nomeadamente, a regra que aqui exploramos e que determina o número das suas raízes “verdadeiras” e “falsas”, isto é, positivas e negativas. Refira-se ainda que nesta obra apresentou a resolução algébrica de equações do 3º e 4º graus e, finalizando, defendeu que apresentou “as construções mais simples possíveis para problemas (...) em particular, a trissecção do ângulo e a duplicação do cubo (...)”.

Segundo J.F. Scott, autor de uma obra dedicada aos trabalhos de Descartes (1987), este via Geometria e Álgebra assim : *Not only can questions of solvability and geometrical possibility be decided elegantly, quickly and fully from the parallel algebra, without it they*

cannot be decided at all [3, pp. 229-237][21].

- o Teorema de Sturm publicado em 1829 no seu famoso artigo *Mémoire sur la résolution des équations numériques*. Hermite (1822-1901), que publicou a primeira prova da transcendência do número e , escreveu que este resultado teria a sorte de se tornar imediatamente um clássico e de conquistar um lugar inquestionável no ensino da Matemática e que por utilizar apenas noções elementares, era um exemplo raro de simplicidade e elegância.

Contudo Hermite estava errado. Nem as Regras de Budan e de Fourier, nem o Teorema de Sturm encontraram lugar nos livros escritos alguns anos depois de serem descobertos, o que prova que as modas na Matemática mudam e a solução de um problema que Lagrange considerava importante, não garantiu que alcançasse fama.

No que concerne a regras de localização dos zeros, abordaremos:

- a Regra de Cauchy, matemático francês considerado a “estrela” da década de 1820-30, filho de pais instruídos, estudou na École Polytechnique e na École des Ponts et Chaussées o que lhe permitiu exercer engenharia. Foi profícuo na publicação de artigos e trabalhos: terá publicado 789. Um seu biógrafo, Belhoste, em 1991, resumiu esta notável obra referindo-se a ele como tendo uma enorme criatividade científica pois apresentou estudos em todas as áreas conhecidas da Matemática. Por exemplo, terá sido ele a começar de forma definitiva a história dos determinantes com um artigo de 1812 onde era clara a sua preferência pela Matemática pura, apresentada de forma elegante e com provas muito rigorosas. Mais tarde, em 1815, num outro artigo, aplica a teoria dos determinantes a um problema de Geometria e a um de Física. Os seus contributos na área das funções de variável complexa foram notórios, sendo considerado o fundador neste domínio. Foi ilustre pedagogo na École Polytechnique, onde os seus cursos eram famosos, conhecido pela introdução ímpar do rigor nas demonstrações e o principal divulgador, na Europa, por exemplo, do diagrama de Wessel-Argand-Gauss para a representação de números complexos. Deu ainda ao cálculo elementar o carácter que tem hoje, tornou fundamental o conceito de limite dando-lhe um cariz aritmético mais preciso, definiu de forma muito clara a noção de infinitésimo e de derivada e de forma satisfatória definiu função contínua. Ser conservador valeu-lhe o exílio já que se recusou a prestar juramento de fidelidade ao rei Luís Filipe quando Carlos X foi deposto. Era muito controverso e inúmeras vezes foi preterido em concursos para lugares de professor em universidades. Abel, em 1826, escreveu: “*Cauchy está louco e não há nada que possa ser feito por ele, embora, agora, ele seja o único que sabe como a Matemática deve ser feita*” [3, pp. 353-359][21].

- a Regra de Lagrange, nascido Giuseppe Lodovico Lagrangia, em Turim e por isso reclamado italiano, embora considerado francês. Foi o mais velho de 11 filhos e teve planeada uma carreira como advogado e que era do seu agrado. Contudo, a leitura de um trabalho de Halley (1656-1742), que deu nome ao cometa, sobre o uso da álgebra em ótica, fê-lo entusiasmar-se pela Matemática. Foi um autodidata e em 1754, publicou o seu primeiro trabalho matemático assinado com o nome de Luigi De la Grange Tournier. Nele sentiu-se, de certa forma, o seu trabalho isolado, sem supervisão matemática. Terá, todavia, enviado previamente os resultados a Euler (seu dileto conselheiro) e constatou com desagrado, no mês seguinte à publicação, que eles apareciam descritos na correspondência entre Johann Bernoulli (1667-1748) e Leibniz (1646-1716). Com apenas 19 anos foi nomeado professor na Escola Real de Artilharia, em Turim, revelando assim o reconhecimento da originalidade e profundidade na abordagem da grande variedade dos temas que tratava. D’Alembert (1717-1783), todavia, achava que Turim possuía (em

Lagrange) um tesouro cujo valor talvez não soubesse. Em 1770, quando trabalhava em Berlim, Lagrange apresentou o trabalho *Reflexões sobre a resolução algébrica das equações* dedicado às razões que justificam a resolubilidade, através de radicais das equações de grau igual ou inferior a quatro [21].

6.1 Número de zeros reais de um polinómio

As regras a seguir apresentadas permitem provar, para um dado polinómio, a existência de um determinado número de zeros em \mathbb{R} ou num seu subconjunto. Esta informação vai permitir também localizá-los.

Consideremos um qualquer polinómio $p(x)$ com coeficientes reais. Se este possuir zeros complexos, sabemos que estes serão em número par, já que os zeros complexos conjugados aparecem aos pares: se $\alpha = a + bi \in \mathbb{C}$ é um zero de um polinómio $p(x)$ com coeficientes reais também $\bar{\alpha} = a - bi$ é zero de $p(x)$.

Sendo assim, se $p(x)$ for de grau n , ímpar, então terá um número ímpar de zeros reais. Se, por outro lado, $p(x)$ for de grau par, o número de zeros reais será par.

Seja $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, com $a_i \in \mathbb{R}, i = 0, 1, \dots, n$ e $a_n \neq 0$.

Definição 6.1.1 *Seja V_+ o número de variações de sinal dos coeficientes não nulos de $p(x)$, seja V_- o número de variações de sinal dos coeficientes não nulos de $q(x) = p(-x)$, seja N_+ o número de zeros reais positivos de $p(x)$ e N_- o número de zeros reais negativos de $p(x)$.*

6.1.1 Regra de Budan-Fourier

Esta Regra aplica-se a um intervalo aberto e limitado e, com ela, ficaremos a saber o número de zeros reais do polinómio nesse intervalo.

Sejam $a, b \in \mathbb{R}$ e consideremos as sucessões de derivadas:

$p(a), p'(a), p''(a), \dots, p^{(n)}(a)$, com $p(a) \neq 0$

$p(b), p'(b), p''(b), \dots, p^{(n)}(b)$, com $p(b) \neq 0$.

Seja V_a o número de variações de sinal da primeira sucessão e V_b o número de variações de sinal da segunda.

Teorema 6.1.2 (Regra de Budan-Fourier) *O número N de zeros reais do polinómio $p(x)$ no intervalo $]a, b[$ não excede o valor $V_a - V_b$ e $(V_a - V_b) - N$ é par.*

Demonstração: Ver [11, pp. 244-246] (cf. [10, pp. 114])

□

Exemplo 6.1.3 *Seja $p(x) = x^4 - 13x^3 + 3x^2 + 124x + 36$.*

Como $p(x)$ é de grau 4, pelo Teorema Fundamental da Álgebra, teorema 2.1.18, possui quatro zeros complexos, incluindo as suas multiplicidades. Como $p(x)$ é de grau 4 (par), então terá um número par de zeros reais: 0, 2 ou 4.

Aplicação da Regra de Budan-Fourier no intervalo $]-4, 5[$, já que $p(-4) \neq 0$ e $p(5) \neq 0$.

	Sinal em $a = -4$	Sinal em $a = 5$
$p(x) = x^4 - 13x^3 + 3x^2 + 124x + 36$	+	-
$p'(x) = 4x^3 - 39x^2 + 6x + 124$	-	-
$p''(x) = 12x^2 - 78x + 6$	+	-
$p'''(x) = 24x - 78$	-	+
$p^{(4)}(x) = 24$	+	+
	$V_{-4} = 4$	$V_5 = 1$

Ora, $V_{-4} - V_5 = 4 - 1 = 3$. Logo, o número N de zeros reais de $p(x)$ em $] -4, 5[$ não excede 3, isto é, N é igual a 0, 1, 2 ou 3. Mas, uma vez que $(V_{-4} - V_5) - N$ tem de ser par e $V_{-4} - V_5 = 3$, N terá de ser 1 ou 3, já que só $(V_{-4} - V_5) - 1 = 2$ e $(V_{-4} - V_5) - 3 = 0$ representam números pares.

Portanto:

- 1) temos um zero real no intervalo e um ou três fora do intervalo $] -4, 5[$
ou
- 2) temos três zeros reais no intervalo e um fora do intervalo $] -4, 5[$.

6.1.2 Regra dos sinais de Descartes

Esta Regra relaciona o número de zeros reais de um polinômio com o número de variações de sinal dos seus coeficientes.

Teorema 6.1.4 (Regra dos sinais de Descartes) *Seja $p(x)$ um polinômio de coeficientes reais. Então:*

- (a) o número N_+ de $p(x)$ não excede o número V_+ de $p(x)$ e $V_+ - N_+$ é par
- (b) o número N_- de $p(x)$ não excede o número V_- de $q(x) = p(-x)$ e $V_- - N_-$ é par.

Demonstração: Ver [11, pp. 247-249] (cf. [10, pp. 114]) □

Esta Regra é uma generalização da de Budan-Fourier e permite contabilizar os zeros reais em intervalos da forma $] -\infty, 0[$ e $] 0, +\infty[$.

Exemplo 6.1.5 *Consideremos de novo $p(x) = x^4 - 13x^3 + 3x^2 + 124x + 36$.*

Em $p(x)$, o número de variações, V_+ , dos sinais dos coeficientes é 2.

Logo, $N_+ \leq 2$ e $V_+ - N_+$ é par.

Assim, como $V_+ = 2$, temos, $N_+ = 2$ ou $N_+ = 0$, isto é, $p(x)$ ou tem dois zeros reais positivos ou nenhum zero real positivo.

Por outro lado, como $q(x) = p(-x) = x^4 + 13x^3 + 3x^2 - 124x + 36$, temos $V_- = 2$, donde $N_- \leq 2$ e $V_- - N_-$ é par, isto é,

$2 - N_-$ é par, logo $N_- = 2$ ou $N_- = 0$.

Resumindo a informação obtida, $p(x)$ verifica um dos seguintes casos:

- terá dois zeros reais positivos e dois zeros reais negativos
- terá dois zeros reais positivos e dois zeros complexos conjugados
- terá dois zeros reais negativos e dois zeros complexos conjugados
- terá quatro zeros complexos conjugados dois a dois.

Conjuguemos estas informações com as obtidas na aplicação da Regra de Budan-Fourier: o polinómio terá um zero real no intervalo $] -4, 5[$ e um ou três zeros reais fora dele ou terá três zeros reais no intervalo $] -4, 5[$ e um zero real fora dele.

Procuremos tirar conclusões a respeito do número e sinal dos zeros no intervalo $] -4, 5[$. Para tal, será útil a aplicação da Regra de Budan-Fourier no intervalo $] -4, 0[$, por exemplo.

Ora, o número de variações de sinal da sucessão das derivadas $p(0)$, $p'(0)$, $p''(0)$, $p'''(0)$, $p^{(4)}(0)$ é $V_0 = 2$.

Logo, o número N de zeros reais de $p(x)$ em $] -4, 0[$ não excede $V_{-4} - V_0 = 4 - 2 = 2$, isto é, N terá de ser 0, 1 ou 2. Como $2 - N$ tem de ser par, temos $N = 0$ ou $N = 2$, isto é, em $] -4, 0[$ teremos nenhum ou dois zeros reais.

Contudo, pela Regra de Budan-Fourier aplicada no intervalo $] -4, 5[$, concluimos que, neste intervalo há pelo menos um zero real, logo, no intervalo $] -4, 0[$ terão de estar dois zeros reais.

Como $p(x)$ é um polinómio do 4º grau, terá então dois zeros reais em $] -4, 0[$ (negativos, portanto) e nenhum zero real fora dele ou dois zeros reais em $] -4, 0[$ e dois zeros reais fora dele.

Só o último caso pode ocorrer atendendo às conclusões tiradas da aplicação da Regra dos sinais de Descartes, isto é, o polinómio $p(x)$ terá dois zeros reais em $] -4, 0[$, portanto, dois zeros reais negativos e dois fora dele. Vejamos que estes dois últimos são positivos.

Na aplicação da Regra de Budan-Fourier no intervalo $] -4, 5[$, concluimos que, neste intervalo, $p(x)$ teria um ou três zeros reais. Isto traduz que, em $] 0, 5[$, existirá um zero real, isto é, um zero positivo, o que obriga, segundo a Regra de Descartes, a que o outro também o seja e o que traduz que $p(x)$ terá dois zeros reais negativos e dois zeros reais positivos.

Exemplo 6.1.6 Vejamos que a Regra dos sinais de Descartes se aplica a polinómios do 1 e do 2 graus.

Seja $a(x) = a_0 + a_1x$, $a_0, a_1 \in \mathbb{R} \setminus \{0\}$. Sabemos que o único zero real é $-\frac{a_0}{a_1}$. Este será positivo se e só se o número de variações de sinal dos coeficientes de $a(x)$ for 1, isto é, se a_0 e a_1 tiverem sinais contrários.

Seja $b(x) = a_0 + a_1x + a_2x^2$, $a_0, a_1, a_2 \in \mathbb{R} \setminus \{0\}$.

Se $a_0 > 0, a_1 > 0, a_2 > 0$ (ou $a_0 < 0, a_1 < 0$ e $a_2 < 0$), $V_+ = 0$, logo, $N_+ = 0$, isto é, $b(x)$ não terá zeros reais positivos. Ora $b(-x) = a_0 - a_1x + a_2x^2$, donde $V_- = 2$, por isso N_- será 0 ou 2, isto é, $b(x)$ terá nenhum ou dois zeros reais negativos. Tal acontece, como sabemos, se $a_1^2 - 4a_0a_2 < 0$ ou se $a_1^2 - 4a_0a_2 > 0$, respetivamente. No caso de $a_1^2 - 4a_0a_2 = 0$, o polinómio terá um zero real negativo duplo.

Se $a_0 < 0$ e $a_2 > 0$ (ou $a_0 > 0$ e $a_2 < 0$), independentemente do sinal de a_1 , temos que $V_+ = 1$, logo $N_+ \leq 1$. Para $V_+ - N_+$ ser par, como $V_+ = 1$, vem $N_+ = 1$. Assim, $b(x)$ terá um zero real positivo. Analogamente, temos que $b(x)$ terá também um zero real negativo.

Se $a_0 > 0, a_1 < 0$ e $a_2 > 0$ (ou $a_0 < 0, a_1 > 0$ e $a_2 < 0$), temos que $V_+ = 2$, logo $N_+ \leq 2$ e $2 - N_+$ é par. Sendo assim, $b(x)$ terá nenhum zero real positivo, caso $a_1^2 - 4a_0a_2 < 0$; dois zeros reais positivos, caso $a_1^2 - 4a_0a_2 > 0$ ou um zero real positivo duplo, se $a_1^2 - 4a_0a_2 = 0$.

De notar que, neste caso, uma vez que $V_- = 0$, não podem existir zeros reais negativos.

Notemos ainda que: se $a_2 = 0$, temos um polinómio de grau 1 e se $a_0 = 0$, temos sempre dois zeros reais distintos ou um duplo, no caso de $a_1 = 0$.

Exemplo 6.1.7 Seja $c(x) = x^{11} + x^8 - 3x^5 + x^4 + x^3 - 2x^2 + x - 2$.

Temos $V_+ = 5$. Logo, $N_+ \leq 5$, isto é, $N_+ = 0, 1, 2, 3, 4, 5$. $5 - N_+$ é par quando, ou $N_+ = 1$, ou $N_+ = 3$ ou $N_+ = 5$. Assim sendo, $c(x)$ terá um, ou três ou cinco zeros reais positivos.

Como $c(-x) = -x^{11} + x^8 + 3x^5 + x^4 - x^3 - 2x^2 - x - 2$, temos $V_- = 2$. Logo, $N_- \leq 2$, isto é, $N_- = 0, 1, 2$. $2 - N_-$ é par quando, ou $N_- = 0$, ou $N_- = 2$.

Assim sendo, $c(x)$ terá nenhum ou dois zeros reais negativos.

Em suma, o polinómio $c(x)$ poderá ter: um zero real positivo e nenhum negativo; um zero real positivo e dois negativos; três zeros reais positivos e nenhum negativo; três zeros reais positivos e dois negativos ou ainda, cinco zeros reais positivos e nenhum negativo ou cinco zeros reais positivos e dois negativos.

Uma vez que o número máximo de zeros reais é sete e o grau do polinómio $c(x)$ é onze, podemos concluir que $c(x)$ terá pelo menos quatro zeros complexos não reais.

6.1.3 Teorema de Sturm

A regra de Budan-Fourier embora prática e de simples aplicação tem a desvantagem de se comportar de forma muito semelhante para polinómios do tipo $p(x)$ e $p(x) + c$ (c constante), uma vez que têm derivadas iguais, contudo os zeros de ambos podem diferir demasiado.

Um método mais preciso foi proposto por Sturm (1829) onde as derivadas sucessivas são substituídas pelos restos das divisões de p por p' (derivada de p) com algumas modificações. A regra de Sturm conduzir-nos-á à determinação do número exato de zeros reais de um polinómio num certo intervalo, usando o número de variações de sinal dos valores de uma sucessão que definiremos mais adiante.

O algoritmo da divisão de polinómios

Teorema 6.1.8 Sejam $a(x), b(x) \in \mathbb{R}[x]$. Então existem polinómios únicos, $q(x)$ e $r(x)$ tais que

$$a(x) = q(x)b(x) + r(x),$$

com $r(x) = 0$ ou $\text{grau}(r(x)) < \text{grau}(b(x))$.

Ao polinómio $r(x)$ chamamos polinómio resto da divisão de $a(x)$ por $b(x)$.

Demonstração: Ver [1, pp. 27-28, Teorema 7.1]

□

O algoritmo de Sturm

Seja $a(x) \in \mathbb{R}[x]$. A **sucessão de Sturm** irá ser construída usando o algoritmo da divisão de polinómios, a partir de $a(x)$ e será do tipo, digamos $(d_0(x), d_1(x), d_2(x), \dots)$ e dar-nos-á informação a respeito dos zeros de $a(x)$ a partir da variação de sinais dos polinómios que a constituem.

Definição 6.1.9 (Sucessão de Sturm) A sucessão de Sturm é definida por:

- $d_0(x) = a(x)$
- $d_1(x) = a'(x)$
- $d_2(x) = -r_1(x)$, sendo $r_1(x)$ o resto da divisão de $d_0(x)$ por $d_1(x)$
- $d_{i+2}(x) = -r_{i+1}(x)$, sendo $r_{i+1}(x)$ o resto da divisão de $d_i(x)$ por $d_{i+1}(x)$.

É claro que, $\text{grau}(d_0(x)) > \text{grau}(d_1(x)) > \text{grau}(d_2(x)) > \dots$, o que traduz que a sucessão é finita.

Exemplo 6.1.10 Seja $d_0(x) = x^3 - x + 1 = a(x)$. Assim, $d_1(x) = 3x^2 - 1$. Dividamos $d_0(x)$ por $d_1(x)$. Obtemos:

$$x^3 - x + 1 = \frac{1}{3}x(3x^2 - 1) + \left(-\frac{2}{3}x + 1\right)$$

Temos assim que $d_2(x) = \frac{2}{3}x - 1$.

Repetindo o processo (d_1 por d_2), vem:

$$3x^2 - 1 = \left(\frac{9}{2}x + \frac{27}{4}\right)\left(\frac{2}{3}x - 1\right) + \frac{23}{4}.$$

Assim:

$$d_3(x) = -\frac{23}{4}.$$

A sucessão de Sturm é, então: $(x^3 - x + 1, 3x^2 - 1, \frac{2}{3}x - 1, -\frac{23}{4})$.

Será, como veremos mais adiante, determinando a diferença do número de variações de sinal que esta sucessão assume nos extremos de um intervalo que estaremos aptos a encontrar, a menos da sua multiplicidade, o número de zeros reais de um polinômio.

Exemplo 6.1.11 Seja $d_0(x) = x^3 - 3x + 2 = a(x)$.

Ora, $d_1(x) = 3x^2 - 3$.

Procedendo como no exemplo anterior, temos:

$$x^3 - 3x + 2 = (3x^2 - 3)\left(\frac{1}{3}x\right) + (-2x + 2).$$

Sendo assim, $d_2(x) = 2x - 2$.

Prosseguindo, obtemos $3x^2 - 3 = (2x - 2)\left(\frac{3}{2}x + \frac{3}{2}\right) + 0$, o que traduz que $d_3(x) = 0$.

A sucessão de Sturm é: $(x^3 - 3x + 2, 3x^2 - 3, 2x - 2, 0)$.

O Teorema de Sturm e o número de zeros de um polinômio em determinado intervalo

Teorema 6.1.12 (Teorema de Sturm) Seja $a(x) \in R[x]$ e $x_0 < x_1$.

Suponhamos que $a(x_0) \neq 0 \neq a(x_1)$.

Então, o número de zeros reais de $a(x)$ no intervalo $]x_0, x_1[$, sem contar com a sua multiplicidade, é dado por:

$$V(d_0(x_0), d_1(x_0), d_2(x_0), \dots) - V(d_0(x_1), d_1(x_1), d_2(x_1), \dots),$$

onde $V(b_0, b_1, b_2, \dots)$ é o número de variações de sinal da sequência (b_0, b_1, b_2, \dots) e d_0, d_1, d_2, \dots os termos da sucessão de Sturm, definida em 6.1.9.

Demonstração: Ver [1, pp. 29-30, Teorema 7.7]

□

Exemplo 6.1.13 Aplicação do Teorema de Sturm a polinómios do 2º grau

Consideremos $a(x) = ax^2 + bx + c = d_0(x)$ ($a > 0$).

Ora, $a'(x) = 2ax + b = d_1(x)$.

Dividindo $a(x)$ por $a'(x)$, temos

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

Portanto,

$$d_0(x) = ax^2 + bx + c, \quad d_1(x) = 2ax + b, \quad d_2(x) = -r(x) = \frac{b^2}{4a} - c.$$

De notar que $\frac{b^2}{4a} - c = \frac{b^2 - 4ac}{4a}$.

Sendo assim, como $a > 0$, o sinal de $\frac{b^2}{4a} - c$ é o mesmo do binómio discriminante que, tal como sabemos, é $\Delta = b^2 - 4ac$.

Para $M > 0$, suficientemente grande, temos, uma vez que $a > 0$:

$$d_0(-M) > 0 \text{ e } d_0(M) > 0$$

$$d_1(-M) < 0 \text{ e } d_1(M) > 0.$$

Sendo assim,

(1) $V(d_0(-M), d_1(-M), d_2(-M))$ é 1 ou 2, dependendo se o binómio discriminante (Δ) é negativo ou não, respetivamente.

Por outro lado,

(2) $V(d_0(M), d_1(M), d_2(M))$ é 1 ou 0, dependendo se o binómio discriminante é negativo ou não, respetivamente.

Concluindo, se $\Delta > 0$, a diferença entre (1) e (2) é $2 - 0 = 2$, o que confirma o que conhecemos do sinal do binómio discriminante: $a(x)$ tem 2 zeros reais se e só se $b^2 - 4ac > 0$. Por outro lado, se $\Delta < 0$, a diferença entre (1) e (2) é $1 - 1 = 0$, confirmando que, quando o sinal do binómio discriminante é negativo, o polinómio não tem zeros reais.

Analogamente se prova para $a < 0$.

Exemplo 6.1.14 Apliquemos o algoritmo de Sturm ao polinómio $a(x) = x^3 + 3x^2 - 1$.

Dividindo $d_0(x) = x^3 + 3x^2 - 1$ por $d_1(x) = 3x^2 + 6x$, temos

$$x^3 + 3x^2 - 1 = \left(\frac{1}{3}x + \frac{1}{3}\right)(3x^2 + 6x) + (-2x - 1).$$

Prosseguindo nas divisões, temos: $3x^2 + 6x = \left(\frac{3}{2}x + \frac{9}{4}\right)(2x + 1) + \left(-\frac{9}{4}\right)$.

Sendo assim a sucessão de Sturm é:

$$(x^3 + 3x^2 - 1, 3x^2 + 6x, 2x + 1, \frac{9}{4}).$$

Estudemos a variação de sinal destes polinómios em $]-\infty, +\infty[$.

Temos, $d_0(-\infty) < 0$, $d_1(-\infty) > 0$, $d_2(-\infty) < 0$ e $d_3(-\infty) > 0$.

Logo, há três variações de sinal.

Temos ainda, $d_0(+\infty) > 0$, $d_1(+\infty) > 0$, $d_2(+\infty) > 0$ e $d_3(+\infty) > 0$, dando lugar a zero variações de sinal.

Então, pelo Teorema de Sturm, $a(x) = x^3 + 3x^2 - 1$ tem três zeros reais.

Para localizarmos estes três zeros, basta atender a:

$$V(d_0(-3), d_1(-3), d_2(-3), d_3(-3)) = 3 \quad (-, +, -, +)$$

$V(d_0(-2), d_1(-2), d_2(-2), d_3(-2)) = 2 \quad (+, 0, -, +)$, uma vez que ocorre variação de sinal do primeiro para o terceiro termo da sequência e deste para o quarto, já que o segundo é nulo

$$V(d_0(-1), d_1(-1), d_2(-1), d_3(-1)) = 2 \quad (+, -, -, +)$$

$$V(d_0(0), d_1(0), d_2(0), d_3(0)) = 1 \quad (-, 0, +, +)$$

$$V(d_0(1), d_1(1), d_2(1), d_3(1)) = 0 (+, +, +, +).$$

Por isso, concluímos que um dos zeros reais está no intervalo $] -3, -2[$, outro em $] -1, 0[$ e o outro em $] 0, 1[$.

6.2 Localização dos zeros de um polinómio

Apresentamos agora alguns resultados que nos permitirão localizar e separar os zeros de um polinómio.

Teorema 6.2.1 (Regra de Cauchy) *Consideremos um qualquer polinómio de coeficientes reais*

$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, a_0 \neq 0$. Todos os zeros $x_j \in \mathbb{C}, j = 1, \dots, n$ de $p(x)$, verificam:

$$\left(1 + \max_{1 \leq k \leq n} \left| \frac{a_k}{a_0} \right| \right)^{-1} \leq |x_j| \leq 1 + \max_{1 \leq k \leq n-1} \left| \frac{a_k}{a_n} \right|.$$

Demonstração: Ver [20, pp. 146-147, lema 7] □

Teorema 6.2.2 (Regra de Lagrange) *Seja $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, um qualquer polinómio de coeficientes reais no qual $a_n > 0, a_{n-1} \geq 0, \dots, a_{m+1} \geq 0, a_m < 0$, isto é, a_m é o primeiro coeficiente negativo na sequência a_n, a_{n-1}, \dots, a_0 .*

Então, os zeros reais positivos (r) do polinómio $p(x)$ são majorados por

$$r \leq 1 + \max_{a_k < 0} \left| \frac{a_k}{a_0} \right|^{\frac{1}{n-m}}.$$

Demonstração: Ver [19, pp. 7-8, Teorema II.2] □

Analogamente, esta regra podem ser usada para encontrar limites superiores para zeros negativos. Para tal, basta aplicá-la ao polinómio $p(-x)$. Para limitar inferiormente, aplicamos as regras a $p\left(\frac{1}{x}\right)$, para os zeros positivos e a $p\left(-\frac{1}{x}\right)$, para os zeros negativos.

Exemplo 6.2.3 *Seja $p(x) = x^4 - 13x^3 + 3x^2 + 124x + 36$.*

Aplicação da Regra de Cauchy:

$$a_4 = 1, a_3 = -13, a_2 = 3, a_1 = 124, a_0 = 36.$$

Ora,

$$\max_{1 \leq k \leq 4} \left| \frac{a_k}{a_0} \right| = \max \left\{ \frac{124}{36}, \frac{3}{36}, \frac{13}{36}, \frac{1}{36} \right\} = \frac{124}{36},$$

$$\max_{1 \leq k \leq 3} \left| \frac{a_k}{a_4} \right| = \max \left\{ \frac{36}{1}, \frac{124}{1}, \frac{3}{1} \right\} = 124.$$

Pela Regra de Cauchy, temos que todos os zeros (r) de $p(x)$ verificam:

$(1 + \frac{124}{36})^{-1} \leq |r| \leq 1 + 124 \iff \frac{9}{40} \leq |r| \leq 125$, isto é, todos os zeros do polinómio p estão situados, no plano complexo, na coroa circular definida pelas circunferências de raio interior $\frac{9}{40}$ e raio exterior 125, centradas na origem.

Aplicação da Regra de Lagrange:

Localizemos os zeros positivos (r^+) do polinómio $p(x)$.

Determinemos, em primeiro lugar, o seu limite superior:

$$a_4 = 1 (> 0)$$

$a_3 = -13$ (primeiro coeficiente negativo de $p(x)$).

$$\text{Ora, } \max_{a_k < 0} \left| \frac{a_k}{a_4} \right| = \max \left\{ \frac{13}{1} \right\} = 13.$$

$$1 + 13^{\frac{1}{4-3}} = 1 + 13 = 14.$$

Sendo assim,

$$r^+ \leq 14. \quad (6.1)$$

Para determinar o limite inferior para os zeros positivos de $p(x)$, procedemos de forma análoga aplicando a Regra a $p\left(\frac{1}{x}\right)$, isto é, a

$$\left(\frac{1}{x}\right)^4 - 13\left(\frac{1}{x}\right)^3 + 3\left(\frac{1}{x}\right)^2 + 124\frac{1}{x} + 36 = \frac{1}{x^4} - \frac{13}{x^3} + \frac{3}{x^2} + \frac{124}{x} + 36 = 36x^4 + 124x^3 + 3x^2 - 13x + 1.$$

Temos assim:

$$a_4 = 36, a_3 = 124, a_2 = 3, a_1 = -13, a_0 = 1.$$

Ora, $a_4 = 36 (> 0)$.

$a_1 = -13$ é primeiro coeficiente negativo de $p\left(\frac{1}{x}\right)$.

Então,

$$\max_{a_k < 0} \left| \frac{a_k}{a_4} \right| = \max \left\{ \frac{13}{36} \right\} = \frac{13}{36}.$$

Mas,

$$\left(1 + \left(\frac{13}{36}\right)^{\frac{1}{4-1}}\right)^{-1} = 0,584. \quad (6.2)$$

Logo, de (6.1) e (6.2), temos $0,584 \leq r^+ \leq 14$.

Analogamente se prova que $-6 \leq r^- \leq -0,225$, aplicando as regras a $p(-x) = x^4 + 13x^3 + 3x^2 - 124x + 36$ e a $p\left(-\frac{1}{x}\right) = 36x^4 - 124x^3 + 3x^2 + 13x + 1$.

Uma outra forma de localizar zeros de polinómios, uma vez que estes definem funções contínuas, é a aplicação do Teorema de Bolzano, teorema 2.2.1.

Tendo em conta alguns valores de $p(x)$, podemos confirmar as conclusões apresentadas, isto é, que os zeros reais positivos pertencem ao intervalo $]0,584; 14[$ e os negativos a $]-6; -0,225[$.

x	$p(x)$
-3	123
-2	-80
-1	-71
0	36
1	151
3	165
5	-269
12	228

Podemos afirmar que em cada um dos intervalos $]-3; -2[,]-1; 0[,]3; 5[$ e $]5; 12[$ existe um único zero real, o que é confirmado ainda pela análise do gráfico da função polinomial definida por $p(x)$.

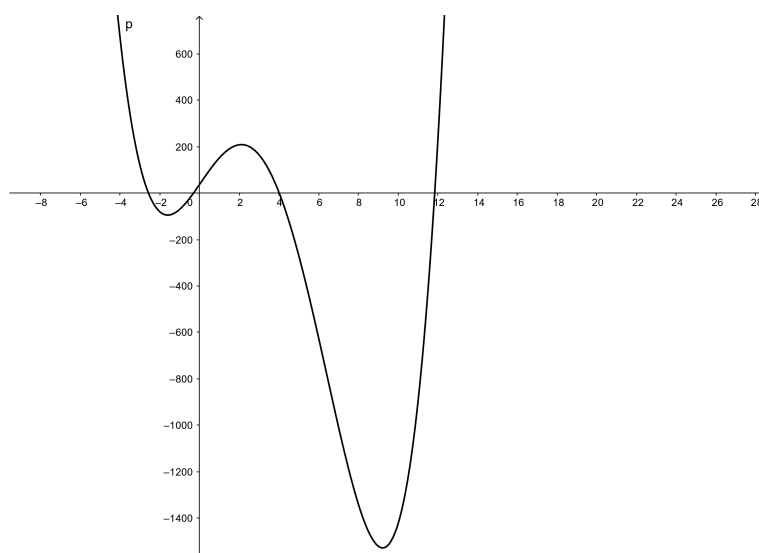


Figura 6.1: Gráfico da função polinomial definida por $p(x) = x^4 - 13x^3 + 3x^2 + 124x + 36$.

Capítulo 7

Conclusões

A primeira e principal conclusão desta dissertação terá de ser o enriquecimento pessoal do seu autor, surgido da oportunidade de contactar com assuntos que envolvem uma vastíssima área de estudo, ainda por cima milenar. Sabemos que descobrir zeros de polinómios vem de longe e terá sido a razão do nascimento da Álgebra. O aumento do grau do polinómio trouxe problemas acrescidos e a tentativa de encontrar os seus zeros atravessou eras sucessivas de matemáticos em domínios tão importantes e úteis como é o caso da resolução de equações.

A análise da temática foi uma mais-valia para quem tem interesse no aprofundamento, no conhecimento e na investigação da Matemática. No caso, acresce-se (ainda) o facto de ter sido trazida durante a prática letiva. Constituiu por isso, mais uma vez, a oportunidade de estudar um tema novo, passados quase trinta anos da conclusão de uma licenciatura e longe da realidade, por vezes rotineira, dos Programas curriculares. Contudo, o tema pode ser visto como uma extensão (apetecível e natural) destes. Refira-se ainda a necessidade de utilizar o sistema LaTeX, uma novidade agradável que poderá vir a ser útil no futuro, também na prática letiva.

Tivemos oportunidade de revisitar as fórmulas resolventes das equações de grau inferior a cinco e com particular interesse analisar as disputas entre Tartaglia, Cardano e seus discípulos, na defesa dos seus feitos e méritos. Interessante foi também conjugar os contributos dados pelos diferentes matemáticos no mesmo sentido, como foi o caso de Cardano, Ferrari, Descartes e Lagrange na resolução das equações do quarto grau.

A questão da inexistência de fórmula resolvente para equações de grau igual ou superior a cinco, foi para nós, neste trabalho, o maior desafio. A necessidade de possuir conhecimentos acerca das *extensões de corpos* e dos *grupos de Galois*, por exemplo, exigiu-nos delinear um plano de demonstração do *Teorema de Abel-Ruffini* com fases bem definidas e bem colocadas. Para esta prova, foi necessário envolver mais de vinte definições, teoremas e proposições que envolviam conceitos desconhecidos ou há muito esquecidos. Não desvalorizando o resultado de Abel, assente no trabalho de Ruffini e de Lagrange, chamou-nos particular atenção (porque desconhecíamos) a teoria do jovem Galois que permitiu distinguir as equações de grau igual ou superior a cinco resolúveis (ou não) por radicais. Refira-se que as ideias de Galois só foram completamente divulgadas após a sua morte, com tiro no estômago, depois de um duelo com pistolas, defendendo a honra de uma *coquette*, conhecida por Stéphanie-Felicie Poterin *du Motel*, *respeitável* filha de um médico. Uns dias antes, antevendo a sua morte, escreve a dois amigos, e confessa: “Morro vítima de uma infame coquete. É numa rixa miserável que a minha vida se ex-

tingue. Oh! Porquê morrer por uma coisa tão trivial, por uma coisa tão desprezível?”. Deixa também uma carta a Chevalier, esta de teor matemático, na qual afirma: “Fiz algumas descobertas em análise. (...) Peça publicamente a Jacobi ou Gauss que dêem a sua opinião (...) da importância destes teoremas. Mais tarde, haverá, espero eu, quem tirará vantagens de decifrar toda esta embrulhada”. Deve-se a Liouville, em julho de 1843, a publicação dos trabalhos de Galois também em documento dirigido à Academia das Ciências de Paris.

A “embrulhada” a que Galois se referia veio a revelar-se fundamental na criação da teoria de grupos. Na tentativa de descobrir método que decidisse quais as equações do 5º grau resolúveis por radicais, descobre que “Tudo depende das *simetrias* da equação”, isto é, das permutações dos conjuntos das suas soluções[18].

Depois da (pessoalmente exigente) incursão na *teoria dos corpos*, revelou-se de particular interesse a visita aos problemas clássicos dos gregos e a prova da impossibilidade da sua resolução usando apenas régua e compasso. Nesta prova apenas foram utilizados argumentos algébricos centrados no conceito de grau de uma *extensão de um corpo*. Foi deveras curioso conhecer que, as condições impostas pelos matemáticos gregos nas construções aparentemente simples mas impossíveis, só vieram a ter resposta no final do século XIX. Isto é, eles não tinham como saber as razões da impossibilidade!

Relativamente ao número e localização dos zeros de um polinómio, ponto-chave motivador do que se veio a tornar o tema deste trabalho, tudo foi descoberta.

É claro que hoje nos parece óbvio que uma primeira abordagem deste problema passará pela observação do gráfico da função polinomial associada, por exemplo. Contudo, só teremos acesso ao número de zeros reais num determinado intervalo e sabemos que tal pode não ser nem o desejado nem o suficiente. Sendo assim, concluímos que existem métodos, como os aqui abordados que são fáceis de trabalhar e que dão resultados aceitáveis. Entendemos que eram resultados em tudo aplicáveis como extensão aos alunos do Ensino Secundário com quem trabalhávamos há dois anos consecutivos (10º e 11º anos) e que acabavam de estudar derivadas de funções polinomiais, entre outras.

Por assim ser, foi de particular relevância a realização da tarefa de grupo proposta aos alunos (Apêndice A). Todos os alunos (cerca de 50) fizeram parte de um grupo e apenas um não foi avaliado por não ter cumprido o prazo de entrega. Analisando os relatórios entregues julgamos ter havido interesse e empenho, refletidos nas classificações obtidas: a média final situou-se entre 15 e 16 valores, repetindo-se o panorama no domínio dos *Conhecimentos e Procedimentos*, avaliados na tarefa. A classificação mínima obtida foi 6,3 e a máxima 18,8 valores. Nesta tarefa tiveram oportunidade de aprender métodos/resultados para determinar o número e localizar os zeros reais de um polinómio/raízes de uma equação, investigar a respeito da biografia dos matemáticos envolvidos (algo que costuma ser do seu agrado), bem como usar tecnologia e software didáticos adequados e por si escolhidos (calculadora gráfica, GeoGebra, Python) para confirmação de resultados obtidos por via algébrica. De todos os domínios avaliados nesta tarefa, mostraram pior desempenho na *Comunicação Matemática* onde obtiveram média pouco superior a 10 valores. Revelaram, sem grande surpresa, dificuldade em transmitir/defender ideias usando convenientemente linguagem matemática e/ou linguagem corrente.

Na tarefa proposta, nenhum dos grupos aceitou a sugestão adicional e que visava o uso do *Teorema de Sturm*, outra ferramenta para encontrar o número e localizar os zeros de um polinómio. Teria sido interessante revisitar o algoritmo da divisão inteira de polinómios, lecionado no 10º ano, dando-lhe uma utilidade prática que serviria de fator

de motivação ao uso de algo que não apreciam muito.

Nas suas conclusões ou na sua autoavaliação de final de período, os grupos ou os alunos a título individual, referiram, a título de exemplo (sic):

- “(...) *serviu de um grande exemplo em como se nos for dado as instruções corretas é possível aprender matérias totalmente novas por nossa inteira responsabilidade e de forma autónoma*”;
- “(...) *(foi uma) forma de aprendermos mais sobre aquilo que não aparece no (...) programa (...) e que de outra forma provavelmente não teríamos conhecimento (...) e que pode vir a ser útil no futuro*”;
- “(...) *enquadra-se bem no nosso ano de escolaridade. Foi bastante pertinente, já que explorámos mais aplicações concretas de conteúdos (...) tivemos oportunidade de descobrir, raciocinar e comunicar Matemática*”;
- “(...) *oportunidade de explorar uma aplicação de conteúdos conhecidos, por exemplo, derivadas das funções polinomiais, experienciamos outras metodologias de ensino e fomos também capazes de usar tecnologia para encontrar respostas (...)*”;
- “(...) *proporcionar um momento de reflexão e de aprendizagem diferente de outros por ser um aprofundamento de uma matéria curiosa (...) ultrapassando as Aprendizagens Essenciais*”;
- “(...) *saímos um pouco da nossa área de conforto e isto é muito importante na nossa vida de estudante*”.

Refira-se que esta tarefa foi proposta no meio do mês de maio do presente ano letivo: as aulas de Matemática A, em virtude do estado de calamidade, decorriam de forma síncrona ou assíncrona e os grupos terão desenvolvido o seu trabalho à distância. Faz por isso sentido valorizar o comentário feito por um dos grupos (sic):

- “(...) *útil, interessante, (...) oportunidade de ajudar uns aos outros. O grupo (estava) unido mesmo estando separado*”.

Das avaliações feitas pelos alunos a esta tarefa, não encontramos comentários negativos. Talvez, como já foi dito, porque a maioria dos alunos em causa, é de facto muito empenhada, interessada e adere com facilidade às propostas do professor. Aqueles que acharam algo de desinteressante na tarefa, julgamos não terem tido coragem de o incluir no relatório, que era de grupo.

Importa talvez referir que, neste ciclo de dois anos (10^o e 11^o ano) estes alunos tiveram a oportunidade de desenvolver outras tarefas (de grupo) do mesmo tipo e por isso, a proposta no presente ano não constituiu absoluta novidade na modalidade.

No 10^o ano, aquando do início do estudo das funções, realizaram atividade experimental relacionada com a quantidade de vela de aniversário ardida ao longo do tempo, com vista a encontrar o modelo linear que melhor se lhe ajustasse. No 11^o ano, foi-lhes proposta uma atividade com o GeoGebra para dedução das razões trigonométricas, através de uma situação real (ângulo que uma escada encostada a uma parede forma com o chão). Logo a seguir e para complementar a sugerida no 10^o ano, encontraram um modelo trigonométrico para outra situação real (distância de uma corda ao chão quando esta é rodada por duas pessoas e uma terceira a ela salta).

Fica assim claro que tem sido intenção do autor deste trabalho proporcionar aos alunos momentos diversificados de aprendizagem e de avaliação. Desta experiência fica a sensação de que a faceta investigativa nela incluída foi usada e conseguida. A intervenção dos alunos ultrapassou as rotinas (também úteis) contempladas nos Programas e nas Aprendizagens Essenciais da disciplina, muitas vezes insuficientes e limitativas para uma

aprendizagem séria e abrangente da Matemática.

Corroboramos assim as palavras de Carlos A. Braumann, professor durante décadas da Universidade de Évora, no artigo de 2002, *Divagações sobre investigação matemática e o seu papel na aprendizagem da Matemática*:“(...) (...)”.

Esta foi também a intenção com a proposta apresentada aos alunos e julgamos que o seu potencial matemático ficou algo mais musculado e as suas capacidades em enfrentar desafios, enriquecidas.

Tudo isto vem, em pleno, ao encontro do estabelecido nos pressupostos e diretivas do Ministério da Educação no âmbito da definição das *Aprendizagens Essenciais* em articulação com o *Perfil do aluno* à saída do Ensino Secundário, em particular na disciplina de Matemática A.

Destacamos:

- “(...) desenvolver competências matemáticas complexas pode requerer estratégias de ensino diferentes(...)”;
- “Os estudantes devem ter oportunidades de descobrir, raciocinar, provar e comunicar Matemática. Para isso é fundamental que (...) se envolvam em discussões e atividades estimulantes (...)” .

Por último, a execução deste trabalho e a natural partilha de alguns dos conteúdos nele abordados com dois ou três colegas de profissão, contribuiu para que o autor pedisse entretanto a sua acreditação como formador ao Conselho Científico-Pedagógico da Formação Contínua. Julga poder vir a preparar e a sugerir uma Ação de Formação sobre a temática abordada nesta Dissertação, para professores de Matemática do Ensino Secundário a um qualquer Centro de Formação. Presentemente e nos últimos tempos, a formação no âmbito específico da Matemática tornou-se algo repetitiva ou rara, desmotivando muitas vezes a sua frequência por vontade espontânea. Julgamos poder assim contribuir de forma humilde para a diversificação, fomentando assim (também) a possibilidade aos professores de saírem dos Programas e das Aprendizagens Essenciais. A metodologia que se pretende usar é a da partilha e mais uma vez, citamos Braumann que no ano 2000 afirmou:

“Aprender matemática sem forte intervenção da sua faceta investigativa é como querer aprender a conduzir um automóvel com um instrutor que apenas nos explica como se conduz e nos deixa olhar para ele enquanto conduz. Isto não chega.”

Bibliografia

- [1] Carlos d'Andrea, *Cálculo de raízes reais de polinômios*, Departament d'Àlgebra e Geometria, Universitat de Barcelona, 2006.
- [2] Gabriela Barreiros, *Grupos e Extensões de Galois*, Tese de Mestrado, Departamento de Matemática Pura, Faculdade de Ciências da Universidade do Porto, 2005.
- [3] Carl Boyer, *História da Matemática*, Revista por Uta Merzbam, 2^a edição, tradução de Elza Gomide, Editora Edgard Blücher Lda, Brasil, 1996.
- [4] Keith Conrad, *Generating sets*.
- [5] Karina Cruz, *Introdução à Teoria de Galois*, Trabalho de conclusão de curso, Centro de Ciências Exatas e de Tecnologia, Departamento de Matemática, Universidade Federal de São Carlos, Brasil, 2014.
- [6] Carl Gauss, *Disquisitiones Arithmeticae*, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo 1986 (reprint of the 1966 edition by Yale University).
- [7] Thomas Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York, 2003 (reprint of the 1974 original).
- [8] Svante Janson, *Roots of polynomials of degrees 3 and 4*, Department of Mathematics - Uppsala University, 2010.
- [9] Arthur Jones, Sidney Morris e Kenneth Pearson, *Abstract and Famous Impossibilities*, Springer, 1994.
- [10] Gabriela Jesus, *Aproximação numérica de valores próprios de matrizes reais*, Apêndice A, Dissertação de Mestrado, Departamento de Matemática, Universidade de Aveiro, 2012.
- [11] Aleksandr Kurosh, *Higher Algebra*, Translated from Russian by George Yankovsky, 4.th printing, Moscow: Mir Publishers, 1984.
- [12] Mário Miguel, *Construções com régua e compasso*, Dissertação de Mestrado, Departamento de Matemática da Universidade Federal e Rural de Pernambuco, Recife, 2018.
- [13] Jorge Picado, *Corpos e Equações Algébricas*, Textos de Apoio, Departamento de Matemática, Universidade de Coimbra, 2011.

- [14] Ana Santana, João Queiró, *Álgebra Linear e Geometria Analítica*, Departamento de Matemática da Universidade de Coimbra, 2003.
 - [15] Manuela Sobral, *Grupos e Simetrias*, Notas do curso, Sumários alargados, Departamento de Matemática, Universidade de Coimbra, 2013.
 - [16] Ian Stewart, *Galois Theory*, Chapman Hall Book, USA, 2015 (Fourth edition).
 - [17] Ian Stewart, *Galois Theory*, Chapman Hall/ CRC Mathematics, USA, 2004 (Third edition).
 - [18] Ian Stewart, *Os Problemas da Matemática*, Gradiva, Lisboa, 1996 (2ª edição).
 - [19] Panagiotis Vigklas, *Upper bounds on the values of the positive roots of polynomials*, Dissertation for the degree of Doctor of Philosophy, University of Thessaly, Volos, Greece 2010.
 - [20] Chee Yap, *Fundamental Problems of Algorithmic Algebra*, Oxford University Press, 2000.
 - [21] <https://mathshistory.st-andrews.ac.uk/>, consultado no dia 7/7/2020.
 - [22] <https://en.wikipedia.org/wiki/257-gon>, consultado no dia 16/8/2020
-

Apêndice A

Roteiro da tarefa de grupo

A proposta de trabalho de grupo a seguir apresentada foi aplicada a duas turmas do 11º ano do curso de Ciências e Tecnologia (CT) da Escola onde o autor desta dissertação leciona há mais de dez anos. As turmas em causa, 11ºCT2 e 11º CT4, são constituídas por 22 e 26 alunos, respetivamente e no 10º ano tiveram o mesmo professor. A maioria dos alunos revela motivação e interesse na disciplina que justificaram a adequação/pertinência da tarefa, mesmo envolvendo conteúdos que não fazem parte do Programa da disciplina de Matemática A do Ensino Secundário.

Escola Secundária Lima-de-Faria- Cantanhede

Tarefa de grupo Matemática A- 11º CT maio 2020

Zeros reais de polinómios: número e localização.

A.1 Enquadramento e introdução

No 10º ano, precisamente há um ano (para a maioria) tratávamos o tema "Polinómios".

Nestas aulas, surgiram duas curiosidades:

C1- por que é que alguém, aparentemente sem cálculo algum, afirmava que, por exemplo, a equação $x^2 - 5x + 6 = 0$ tinha 2 e 3 como soluções?

C2- alguém reparou que, na página 94 do Volume 1 do Manual adotado (*Novo Espaço, Matemática A, 10º ano, B. Costa e E. Rodrigues, Porto Editora*), se encontrava uma referência histórica a Descartes (1596-1650) e a uma regra com o seu nome e que anunciava determinar o número de soluções da equação $x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_n = 0$, por observação apenas dos sinais dos coeficientes dos seus termos ...

Juntando estes dois “incidentes” à pergunta que me foi feita, pela mesma altura, se os alunos do Ensino Secundário conheciam a *Regra de Descartes*, decidi aprofundar o assunto da determinação do número e localização dos zeros reais de um polinómio. À custa desta intenção, foi-me proposto também, analisar a existência de fórmulas resolventes para equações polinomiais de grau superior a dois.

Veremos, nesta atividade, como podem, por exemplo, os sinais dos coeficientes dos termos de um polinómio, fornecer informações a respeito dos seus zeros reais. Refira-se que, nesta tarefa, apenas nos dedicaremos a estes (reais): aprenderá, no 12^o ano, que há polinómios com zeros não reais (complexos) quando conhecer o conjunto dos números complexos \mathbb{C} . Vai, por exemplo, conhecer os zeros complexos do polinómio $x^2 + 1$ que são i e $-i$, sendo i a **unidade imaginária** que verifica: $i^2 = -1$.

Entenderemos assim a informação dada no Manual já referido que citamos: “A equação $x^4 - 4x^3 - 19x^2 + 106x - 120 = 0$ tem a sequência de sinais dos coeficientes: $+, -, -, +, -$. Há assim três alternâncias de sinais, por isso, ela tem três soluções reais positivas e uma permanência de sinal, por isso tem uma solução real negativa...”.

Também conheceremos uma Regra (de Budan-Fourier) que nos dará informação a respeito da localização dos zeros de um polinómio num intervalo de números reais aberto e limitado, isto é, permite-nos saber entre que valores se encontram. Esta última, permitir-nos-á conhecer uma aplicação das derivadas das funções polinomiais recentemente abordadas.

Com esta tarefa, ficam assim cumpridos os objetivos:

- aprofundar alguns conhecimentos fora do Programa da disciplina de Matemática A, constituindo assim uma oportunidade de estendê-lo a um assunto oportuno;
 - explorar (mais) uma aplicação concreta de conteúdos conhecidos, como é o caso das derivadas das funções polinomiais;
 - diversificar metodologias de ensino (in *AE/Articulação com o perfil dos alunos*, doc. ME);
 - fomentar oportunidades de descobrir, raciocinar e comunicar Matemática (também em grupo) (idem);
-

- usar tecnologia para encontrar/comprovar/complementar informação e respostas.
- (ibidem)

A.2 Descrição da tarefa

2.1 Modalidade A tarefa será realizada em grupo. 11ºCT2: 3 grupos de 4 alunos e 2 grupos de 5 alunos. 11ºCT4: 4 grupos de 4 alunos e 2 grupos de 5 alunos.

2.2 Prazo e modo de entrega Cada grupo cumpre as tarefas propostas no presente guião, depois de ter analisado os resultados e exemplos expostos, podendo/devendo proceder a investigações complementares (cuja referências inclui) e colocar dúvidas ao professor. Elabora depois, respostas completas e fundamentadas que inclui num relatório único que enviará ao professor, em formato pdf, até às **12 horas do dia 15 de junho**.

2.3 Avaliação Esta tarefa será avaliada, de acordo com os critérios de avaliação em vigor, nos domínios: *Conhecimentos e compreensão de conceitos e procedimentos matemáticos* (CP-135 pontos); *Raciocínio Matemático* (RM-10 pontos); *Resolução de problemas* (RP-15 pontos); *Comunicação Matemática* (CM-20 pontos) e *Matemática e Tecnologia* (MT-20 pontos).

A.3 Soma e produto das soluções de uma equação do 2º grau

Nesta parte da tarefa, pretendemos dar resposta à acima denominada *Curiosidade 1* (C1). Não fazendo parte do Programa da disciplina de Matemática do 9º ano, não é raro encontrar em Manuais deste nível de escolaridade, alusão ao assunto. Por exemplo, no Manual *Matemática 9, Parte 1*, M^a A. Neves e outros, Porto Editora, podemos encontrar:

Considere a equação $(x - 1)(x + 3) = 0$, equivalente a $x^2 + 2x - 3 = 0$. A equação tem como soluções $x_1 = 1$ e $x_2 = -3$.

Repare que:

$$S = x_1 + x_2 = 1 + (-3) = -2 \text{ e } P = x_1 \times x_2 = 1 \times (-3) = -3.$$

Sendo assim, em $x^2 + 2x - 3 = 0$ temos $x^2 - Sx + P = 0$. Isto é, o coeficiente do termo de grau 1 é o simétrico da soma das soluções e o termo independente, o produto delas.

De uma forma geral, tem-se, para $a \neq 0$,

$$ax^2 + bx + c = 0 \Leftrightarrow x^2 + \frac{b}{a}x + \frac{c}{a} = 0, \text{ onde } S = -\frac{b}{a} \text{ e } P = \frac{c}{a}.$$

Esta propriedade aparece nos Manuais do 9º ano, especialmente pela sua utilidade na verificação das soluções de uma equação do 2º grau encontradas pela aplicação da fórmula resolvente.

Proposta 1

Usando a propriedade atrás apresentada, resolva os seguintes exercícios. Indique todos os cálculos que efetuar e todas as justificações necessárias.

1.1. (10 pontos) Comente a afirmação: *A equação $-x^2 - x + 20 = 0$ admite (-5) e 4 como soluções.*

1.2. Escreva uma equação do 2º grau que admita as soluções:

1.2.1. (10 pontos) (-1) e $\frac{1}{2}$.

1.2.2. (10 pontos) (-1) e 0.

A.4 Número e localização de zeros reais de um polinómio

A.4.1 Regra dos sinais de Descartes

Esta Regra relaciona o número de zeros reais de um polinómio com o número de variações de sinal dos seus coeficientes.

Seja $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, com $a_i \in \mathbb{R}, i = 0, 1, \dots, n$ e $a_n \neq 0$.

Definição A.4.1 *Seja V_p o número de variações de sinal dos coeficientes não nulos de $p(x)$, seja N_+ o número de zeros reais positivos de $p(x)$ e N_- o número de zeros reais negativos de $p(x)$.*

Exemplo A.4.2 *Se $p(x) = x^4 - 13x^3 + 3x^2 + 124x + 36$, então $V_p = 2$ (a sequência de sinais dos coeficientes é: $+, -, +, +, +$). Há por isso, duas mudanças de sinal: do 1º para o*

2^o e do 2^o para o 3^o).

Exemplo A.4.3 Se $p(x) = x^4 - 4x^3 - 19x^2 + 106x - 120$, então $V_p = 3$ (a sequência de sinais dos coeficientes é: +, -, -, +, -. Há por isso, três mudanças de sinal: do 1^o para o 2^o; do 3^o para o 4^o e do 4^o para o 5^o).

Teorema A.4.4 Regra dos sinais de Descartes

Seja $p(x)$ um polinómio de coeficientes reais. Então:

- (a) o número N_+ de $p(x)$ não excede o número V_p e $V_p - N_+$ é par
- (b) o número N_- de $p(x)$ não excede o número V_q , com $q(x) = p(-x)$ e $V_q - N_-$ é par.

[2, pp. 114]

Proposta 2 (10 pontos)

Elabore um pequeno texto (máximo de 10 linhas) no qual apresente uma nota biográfica de Descartes incluindo algo sobre o seu estudo no domínio no qual esta Regra se enquadra.

Aplicação da Regra dos sinais de Descartes

Exemplo A.4.5 Seja $p(x) = x^4 - 13x^3 + 3x^2 + 124x + 36$.

Já vimos atrás que $V_p = 2$.

Logo, $N_+ \leq 2$ e $V_p - N_+$ é par. Isto é, N_+ pode tomar os valores 0, 1 ou 2. Mas, para $2 - N_+$ ser par, N_+ só pode ser 0 ou 2, o que quer dizer que $p(x)$ ou não tem qualquer zero real positivo ou tem dois zeros reais positivos.

Por outro lado, como $q(x) = p(-x) = x^4 + 13x^3 + 3x^2 - 124x + 36$, temos $V_q = 2$. Analogamente ao feito para $p(x)$, temos que N_- só pode ser 0 ou 2, isto é, $p(x)$ ou não tem qualquer zero real negativo ou tem dois zeros reais negativos.

Resumindo a informação obtida relativamente ao número de **zeros reais** de $p(x)$, podemos afirmar que se verificará um dos seguintes casos:

- não terá zeros reais nem positivos nem negativos ($N_+ = 0$ e $N_- = 0$);
- não terá zeros reais positivos e terá dois zeros reais negativos ($N_+ = 0$ e $N_- = 2$);

- terá dois zeros reais positivos e não terá zeros reais negativos ($N_+ = 2$ e $N_- = 0$);
- terá quatro zeros reais: dois positivos e dois negativos ($N_+ = 2$ e $N_- = 2$).

Proposta 3: Aplicação da Regra dos sinais de Descartes a polinómios do 1º e 2º graus ($4 \times 10 = 40$ pontos)

Para cada um dos polinómios a seguir indicados:

- 1- determine os seus zeros reais;
- 2- confirme os seus resultados usando a Regra dos sinais de Descartes.

3.1 $a(x) = 3x - 2$

3.2 $b(x) = x^2 + 2x + 1$

3.3 $c(x) = x^2 - x - 6$

3.4 $d(x) = x^2 + 4x + 5$

Proposta 4 (20 pontos) Determine o possível número de zeros reais positivos e negativos do polinómio

$$r(x) = x^{11} + x^8 - 3x^5 + x^4 + x^3 - 2x^2 + x - 2.$$

A.4.2 Regra de Budan-Fourier

A utilidade desta Regra é a mesma da de Descartes, contudo aplica-se a um intervalo aberto e limitado, isto é, permite determinar o número de zeros reais de um polinómio num intervalo $]a, b[$, $a, b \in \mathbb{R}$. Sendo assim, permite localizá-los.

Envolve as sucessivas derivadas da função polinomial que o polinómio $p(x)$ em causa define, os valores que elas tomam em a e b (extremos do intervalo) e o número de variações de sinal de cada uma.

Isto é, há que considerar as sucessões das derivadas:

(1) $p(a), p'(a), p''(a), p'''(a), \dots, p^{(n)}(a)$, com $p(a) \neq 0$;

(2) $p(b), p'(b), p''(b), p'''(b), \dots, p^{(n)}(b)$, com $p(b) \neq 0$.

Designemos por V_a e por V_b o número de variações de sinal das sucessões (1) e (2), respetivamente.

Teorema A.4.6 *Regra de Budan-Fourier*

O número N de zeros reais do polinómio $p(x)$ no intervalo $]a, b[$ não excede o valor $V_a - V_b$ e $(V_a - V_b) - N$ é par.

[2, pp. 114]

Aplicação da Regra de Budan-Fourrier

Exemplo A.4.7 Seja $p(x) = x^4 - 13x^3 + 3x^2 + 124x + 36$.

Descubra-se o número (N) de zeros reais de $p(x)$ no intervalo $] -4, 5[$, já que $p(-4) \neq 0$ e $p(5) \neq 0$.

	Sinal em $a = -4$	Sinal em $a = 5$
$p(x) = x^4 - 13x^3 + 3x^2 + 124x + 36$	+	−
$p'(x) = 4x^3 - 39x^2 + 6x + 124$	−	−
$p''(x) = 12x^2 - 78x + 6$	+	−
$p'''(x) = 24x - 78$	−	+
$p^{(4)}(x) = 24$	+	+
	$V_{-4} = 4$	$V_5 = 1$

Ora, $V_{-4} - V_5 = 4 - 1 = 3$.

Logo, o número N de zeros reais de $p(x)$ em $] -4, 5[$ não excede 3, isto é, N é igual a 0, 1, 2 ou 3.

Mas, uma vez que $(V_{-4} - V_5) - N$ tem de ser par e $V_{-4} - V_5 = 3$, N terá de ser 1 ou 3, já que só $(V_{-4} - V_5) - 1 = 2$ e $(V_{-4} - V_5) - 3 = 0$ representam números pares.

Proposta 5 (10 pontos)

Relativamente ao Exemplo 4.7, comprove o resultado obtido, usando tecnologia gráfica.

Proposta 6 (10 pontos) Elabore um pequeno texto (máximo de 10 linhas) no qual apresente notas biográficas de Budan e de Fourier. Faça uma breve alusão aos seus estudos no domínio no qual esta Regra se enquadra.

Proposta 7.1 Usando a Regra de Budan-Fourier, determine o número de zeros reais de cada um dos polinômios seguintes nos intervalos indicados.

De seguida, usando tecnologia gráfica, confirme os resultados obtidos, indicando valores aproximados às centésimas para esses zeros, caso existam:

7.1.1 (15 pontos) $a(x) = x^2 - x + 1$, no intervalo $] -1, 2[$.

7.1.2 (20 pontos) $b(x) = x^5 - x^4 - x^3 + 4x^2 - x - 1$, nos intervalos $] -2, -1[$, $] -1, 0[$ e $] 0, 1[$.

Proposta 7.2 (45 pontos) Considere o polinômio $c(x) = x^5 - 3x^4 - x^2 - 4x + 14$.

Usando as Regras de Descartes e de Budan-Fourier, determine o número de zeros reais e localize-os (caso existam) em intervalos disjuntos, de modo que, em cada um, esteja um e um só desses zeros.

Sugestão adicional facultativa Se tiver curiosidade (acrescida), investigue acerca do *Teorema/ algoritmo de Sturm*. Encontrará assim, outra regra para determinar o número de zeros de um polinômio e para os localizar. Para tal, vai também ter de rever o algoritmo da divisão de polinômios. Mais uma vez vai conhecer uma aplicação das derivadas das funções polinomiais. FIM.

O professor: João Luís da Costa Nunes, maio 2020

Bibliografia

[1] Carlos d'Andrea, *Cálculo de raízes reais de polinômios*, Departament d'Àlgebra e Geometria, Universitat de Barcelona, 2006.

[2] Gabriela Duarte Sobral de Jesus, *Aproximação numérica de valores próprios de matrizes reais*, Apêndice A, Dissertação de Mestrado, Departamento de Matemática, Universidade de Aveiro, 2012.