Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática
em Rede Nacional PROFMAT

PROFMAT

UFPB

Equações Polinomiais e Matrizes Circulantes †

por

Pedro Jerônimo Simões de Oliveira Júnior

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT-CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Julho / 2015
João Pessoa - PB

†O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

Equações Polinomiais e Matrizes Circulantes

por

Pedro Jerônimo Simões de Oliveira Júnior

Dissertação apresentada ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva -UFPB (Orientador)

Prof. Dr. João Bosco Batista Lacerda - UFPB

Prof. Dr. Turíbio José Gomes dos Santos - UNIPÊ

Julho / 2015

Agradecimentos

A Deus, pela vida e por todos os dons dados a mim.

Aos meus pais, Avani e Pedrinho, por todos os sacrifícios feitos para que eu pudesse estudar numa boa escola e chegasse até aqui.

Aos meus dois filhos Arthur Hendricks e Augusto César pela compreensão da falta de atenção em alguns momentos.

A minha esposa Ana Paula pela compreensão nas minhas faltas bem como pelo seu empenho familiar para que tudo corresse bem.

Ao meu amigo Marcos Aurélio Mendes de Moraes pela paciência e insistência em ter me ensinado matemática quando eu tinha 14 anos. Além disso despertou curiosidade e sede de aprender.

Ao meu orientador Professor Dr. Antônio de Andrade e Silva pela confiança em mim depositada e horas dedicadas ao meu ensinamento. Agradeço, também, pelos momentos de descontração juntos, mostrando-me, além das palavras de sabedoria, ser possível fazer as duas coisas: estudar e se divertir.

Aos professores e amigos Nacib e Lenimar.

Ao amigo Marcelo Dantas pelo incetivo constante para que eu pudesse concluir meu mestrado.

Ao amigo Ivo Filho pelas correções do português em algumas partes deste trabalho.

Aos demais colegas, pelos momentos compartilhados.

"O homem lúcido me espanta
mas gosto dele na lírica
A verdade metafísica
modela o verbo e a garganta.
O homem lúcido verifica
que a existência não se estanca
põe a baba ao pé da planta
eis que a planta frutifica.
O homem lúcido como quer,
seja lá onde estiver
ele está, sem aquarela.
Sabe que a vida é viscosa
sabe que entre a náusea e a rosa
foi que a ostra faz a pérola"

Sonetilha Existencial,
Leão de Formosa

Dedicatória

Dedico este trabalho aos meus pais Pedrinho e Avani, aos meus filhos, Arthur Hendricks e Augusto César por estarem incondicionalmente ao meu lado nos casos e acasos da vida.

Resumo

Neste trabalho abordamos via matrizes circulantes a resolução de equações polinomiais de grau $n \leq 4$, $n \in \mathbb{N}^*$, destacando uma nova perspectiva para obtenção das fórmulas de Cardano-Tartaglia. Além disso, ele oportuniza uma nova maneira de olhar para questões conexas, incluindo a eliminação do termo de grau $(n-1)$ e a caracterização de equações reais com todas as raízes reais. O método é baseado na busca de uma matriz circulante cujo polinômio característico seja idêntico ao das raízes que queremos encontrar. Essa metodologia nos fornece um método simples e unificado para todas equações até quarto grau.

Palavras–chave: Matrizes de permutações. Matrizes circulantes. Equações polinomiais.

Abstract

In this work we discuss the procedures for solving polynomials equations of degree $n \leq 4$, $n \in \mathbb{N}^*$ via circulant matrices, highlighting a new perspective to obtain the Cardano-Tartaglia formulae. This brings up a new look on connected subjects, including the elimination of the term of degree $(n-1)$ and the characterization of real polynomials with all real roots. The method is based on searching a circulant matrix whose characteristic polynomial is identical to the one with the same roots we desire to find. This approach provides us a simple and unified method for all equations through degree four.

Keywords: Permutation matrices, Circulant matrices, Polynomial equations.

Sumário

Introdução

Histórico

Há algo fascinante sobre os procedimentos para a resolução de equações polinomiais com grau $n \leq 4$, $n \in \mathbb{N}^*$. Por um lado, todos sabem que, enquanto soluções gerais (usando radicais) são impossíveis para equações polinomiais de grau maior do que ou igual a cinco, elas têm sido encontradas para quadráticas, cúbicas e quárticas. Por outro lado, as soluções canônicas para a cúbica e a quártica são complicadas, e os métodos parecem ad hoc. Como é que alguém pode lembrar-se delas? Assim, é razoável pensar em obter um método simples (de fácil memorização) e unificado para todas as equações de graus até quatro.

As abordagens para a unificação têm sido algo tão longo quanto as próprias soluções. Cardano, em 1545, publicou soluções tanto para a equação cúbica quanto para equação quártica, atribuindo o primeiro mérito para Tartaglia e o segundo para Ferrari. Depois de várias tentativas subsequentes e sem êxito em resolver equações de grau maior do que ou igual a cinco, Lagrange, em 1770, apresentou uma análise detalhada para explicar por que os métodos de resolverem equações cúbicas e quárticas são bem sucedidos. A partir daquele momento até o presente, esforços têm sido apresentados para clarear as soluções de equações cúbicas e quárticas, confira Ungar [13].

Neste trabalho, apresentaremos uma abordagem unificada com base em matrizes circulantes. A ideia é construir uma "matriz circulante" C com um dado polinômio característico tal que suas raízes sejam os autovalores de C que são trivialmente encontrados para matrizes circulantes.

Esta abordagem via matrizes circulantes proporciona um belíssimo método unificado para obter as soluções de equações cúbicas e quárticas, de modo que seja facilmente lembradas. Além disso, ela mostra outra compreensão e conexão entre as matrizes e polinômios, bem como aplicações à Teoria de Interpolação e Transformada de Fourier Discreta.

Descrição

No primeiro capítulo faremos uma breve revisão sobre matrizes, determinantes, autovalores e autovetores, os quais são prerrequisitos que alicerçam a teoria sobre à qual dissertaremos.

No segundo capítulo discorreremos sobre as matrizes circulantes e suas propriedades dentre as quais poderemos destacar que cada matriz circulante C possui dois polinômios naturalmente associados a ela: o seu representante

$$q_C(W) = C$$

e seu polinômio característico

$$p_C(x) = \det(xI - C).$$

Os "circulantes" foram introduzidas pela primeira vez em 1846 por Catalan [3] em [4]

Os circulantes de ordem 2 e 3 (polinômios homogêneos de graus 2 e 3) são

$$\begin{vmatrix} X_0 & X_1 \\ X_1 & X_0 \end{vmatrix} = X_0^2 - X_1^2 = (X_0 + X_1)(X_0 - X_1)$$

e

$$\begin{aligned} \begin{vmatrix} X_0 & X_1 & X_2 \\ X_2 & X_0 & X_1 \\ X_1 & X_2 & X_0 \end{vmatrix} &= X_0^3 + X_1^3 + X_2^3 - 3X_0X_1X_2 \\ &= (X_0 + X_1 + X_2)(X_0 + \omega X_1 + \omega^2 X_2)(X_0 + \omega^2 X_1 + \omega X_2), \end{aligned}$$

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

No terceiro capítulo nos prenderemos a essência do trabalho começando com uma seção histórica a respeito das equações de grau pequeno. Em seguida, mostraremos

[3]Eugène Charles Catalan foi um matemático belga, que se distinguiu pelos seus estudos sobre a teoria dos números.

como resolver equações polinomiais usando o método circulante, chegando às fórmulas de Cardano-Tartaglia. Finalizaremos este trabalho com uma discussão sobre quais critérios as equações cúbicas e quárticas com coeficientes reais devem possuir para que todas as raízes sejam reais.

Capítulo 1

Matrizes

Ao trabalhar com um sistema de equações lineares, somente os coeficientes e suas respectivas posições são importantes. Também, ao reduzir o sistema à forma escalonada, é essencial manter as equações cuidadosamente alinhadas. Assim esses coeficientes podem ser eficientemente arrumados numa disposição retangular chamada **matriz**.

A menos que seja declarado o contrário, todos os **elementos** em nossas matrizes pertencem a algum corpo $\mathbb{K}$, arbitrário mas fixo. (Confira apêndice B.6) Esses elementos de $\mathbb{K}$ são chamados **escalares**. Nada essencial é perdido se o leitor supõe que $\mathbb{K}$ é o corpo real $\mathbb{R}$ ou o corpo complexo $\mathbb{C}$. O leitor interessado em mais detalhes pode consultar Hoffman, Lipschutz e/ou Silva [8, 11, 12].

1.1 Matrizes

Seja $\mathbb{K}$ um corpo arbitrário. Uma disposição retangular da forma

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix}$$

onde os a_{ij} são elementos de $\mathbb{K}$, é chamada **matriz** sobre $\mathbb{K}$ ou, simplesmente **matriz**, se $\mathbb{K}$ está implícito.

As n-uplas horizontais são as **linhas** da matriz e as m-uplas verticais são as **colunas**. Note que o elemento a_{ij}, chamado termo geral que aparece na i-ésima linha e j-ésima coluna. A matriz com m linhas e n colunas é chamada uma matriz do tipo m por n $(m \times n)$, descrevendo, desse modo, sua forma.

Uma matriz com o mesmo número de linhas e colunas é denominada **matriz quadrada**. Diz-se que uma matriz quadrada com n linhas e n colunas é de ordem n. A diagonal principal de uma matriz quadrada $A = (a_{ij})$ de ordem n, corresponde aos elementos de A quando $i = j$.

Sejam $A = (a_{ij})_{m \times n}$ e $B = (b_{ij})_{m \times n}$ duas matrizes. Dizemos que A é igual a B, em símbolos $A = B$, se, e somente se,

$$a_{ij} = b_{ij}, \quad 1 \leq i \leq m \quad \text{e} \quad 1 \leq j \leq n.$$

Denomina-se **matriz diagonal**, a toda matriz quadrada em que $a_{ij} = 0$, para $i \neq j$, isto é, os elementos que não estão na "diagonal principal" são nulos.

Uma matriz quadrada é denominada **identidade** se $a_{ij} = 1$, para $i = j$, e $a_{ij} = 0$, para $i \neq j$. A matriz identidade (que indicaremos por I) é um importante exemplo de matriz diagonal que merece destaque na teoria das matrizes por exercer o papel de elemento neutro na multiplicação de matrizes, ou seja,

$$A \cdot I = I \cdot A = A,$$

para toda matriz A.

A **soma** de matrizes $A_{m \times n} = (a_{ij})$ e $B_{m \times n} = (b_{ij})$ é uma matriz $m \times n$, que denotaremos $A + B$, cujos elementos são somas dos elementos correspondentes, isto é, elementos de mesma posição, de A e B. Isto é,

$$A + B = (a_{ij} + b_{ij})_{m \times n}.$$

Note que, da forma como foi definida, a adição de matrizes possui as mesmas propriedades que a adição dos números reais.

A operação que definiremos a seguir é à multiplicação de uma matriz por um escalar chamada **multiplicação por escalar**.

Sejam $A = (a_{ij})_{m\times n}$ e $k \in \mathbb{K}$. Definimos uma nova matriz

$$k \cdot A = (ka_{ij})_{m\times n}.$$

Dada uma matriz $A = (a_{ij})_{m\times n}$, podemos obter uma outra matriz $A^T = (b_{ij})_{n\times m}$, cujas linhas são as colunas de A, isto é, $b_{ij} = a_{ji}$. Neste caso, diremos que A^T é **transposta** de A.

Uma matriz é denominada **simétrica** se, e somente se, ela for igual à sua transposta, isto é, $A = A^T$.

Dadas as matrizes $A = (a_{ij})_{m\times n}$ e $B = (b_{rs})_{n\times p}$, definimos a **multiplicação** das matrizes A por B, ou seja, $AB = (c_{uv})_{m\times p}$, da seguinte forma:

$$c_{uv} = \sum_{k=1}^{n} a_{uk}b_{kv} = a_{u1}b_{1v} + \cdots + a_{un}b_{nv}.$$

Observação 1.1. *Em relação ao produto de duas matrizes podemos notar que:*

1. *Só podemos efetuar o produto de duas matrizes $A_{m\times n}$ e $B_{l\times p}$ se o número de colunas da primeira for igual ao número de linhas da segunda, isto é, $n = l$. Além disso, a matriz $C = AB$ será de ordem $m \times p$.*

2. *O elemento c_{ij} (i-ésima linha e j-ésima coluna da matriz produto) é obtido, multiplicando os elementos da i-ésima linha da primeira matriz pelos elementos correspondentes da j-ésima coluna da segunda matriz, e somando estes produtos.*

Sejam A e B matrizes quaisquer. Em geral,

$$AB \neq BA$$

(podendo mesmo um dos membros está definido ou não). Note, ainda, que podemos ter $AB = 0$, sem que $A = 0$ ou $B = 0$.

Diz-se que uma matriz quadrada A é **invertível** se existe uma matriz B tal que

$$A \cdot B = B \cdot A = I.$$

A matriz B é única, pois as igualdades

$$AB_1 = B_1A = I \text{ e } AB_2 = B_2A = I$$

implicam que

$$B_1 = B_1I = B_1(AB_2) = (B_1A)B_2 = IB_2 = B_2.$$

Denominaremos tal matriz B a inversa de A e denotamos por A^{-1}. Observe que a relação acima é simétrica; isto é, se B é a inversa de A, então A é à inversa de B.

Exemplo 1.1. *Calculemos, agora, a inversa de uma matriz genérica,* 2×2*,*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Procuramos escalares x, y, z, w *tais que*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad ou \quad \begin{pmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

o que se reduz a resolver os seguintes sistemas de equações lineares:

$$\begin{cases} ax + bz = 1 \\ cx + dz = 0 \end{cases} \quad e \quad \begin{cases} ay + bw = 0 \\ cy + dw = 1 \end{cases}$$

Se $ad - bc \neq 0$*, então*

$$x = \frac{d}{ad-bc}, \quad y = \frac{-b}{ad-bc}$$
$$z = \frac{-c}{ad-bc}, \quad w = \frac{a}{ad-bc}$$

e tais soluções são únicas. Note que, fazendo $|A| = ad - bc$*, obtemos*

$$A^{-1} = \begin{pmatrix} \frac{d}{|A|} & -\frac{b}{|A|} \\ -\frac{c}{|A|} & \frac{a}{|A|} \end{pmatrix} = \frac{1}{|A|}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

1.2 Determinantes

Já em 250 a.C. havia exemplos da resolução de sistemas de equações através de matrizes, no livro chinês *Nove Capítulos sobre a Arte Matemática*, cujo autor é desconhecido. Também algumas noções ligadas a determinantes, o assunto que será objeto de estudo neste seção, já eram conhecidas na China antiga.

Mas, se por um lado já se utilizava a noção de determinante no mundo Oriental há tanto tempo, no Ocidente este assunto começou a ser tratado esporadicamente a partir do século XVII. Nesta época surgem trabalhos de G. W. Leibniz (1646 – 1716), e G. Cramer (1704 – 1752) que desenvolve um método de resolução de sistemas através de determinantes, conhecida por "Regra de Cramer" e foi publicado em 1750 (provavelmente já conhecido por C. Maclaurin (1698 – 1746)) em 1729, e alguns resultados simétricos de J. L. Lagrange (1736 – 1813).

Só no século XIX é que os determinantes passaram a ser estudados mais sistematicamente, a começar pelo longo tratado de A. L. Cauchy (1789 – 1857) em 1812, tendo sido realizados, em seguida, trabalhos de C. G. Jacobi (1804 – 1851).

A partir de então, o uso de determinantes difundiu-se muito e este conceito de um número associado a uma matriz quadrada mostrou-se extremamente útil para caracterizar muitas situações, como a de saber se uma matriz é inversível e se um sistema admite ou não solução.

A toda matriz quadrada A sobre um corpo $\mathbb{K}$ está associado um único elemento de $\mathbb{K}$ chamado **determinante** de A, usualmente representado por

$$\det(A) \text{ ou } |A|.$$

A função determinante foi descoberta pela primeira vez na investigação de sistemas de equações lineares. Salientamos que a definição de determinante e a maior parte de suas propriedades também funcionam no caso em que os elementos da matriz pertencem a um anel (confira apêndice B.1).

Sejam A e B conjuntos arbitrários. Suponhamos que, para cada $a \in A$, está associado a um único elemento de $f(a) \in B$ por meio de uma correspondência f. A correspondência f é denominada *função* ou *transformação* de A em B e escrita

$$f : A \longrightarrow B \text{ ou } A \xrightarrow{f} B.$$

Escrevemos $f(a)$, leia "f de a", para o elemento de B que f associa a $a \in A$; $f(a)$ é chamado o *valor* de f em a ou a *imagem* de a sob f.

Uma transformação $f : A \longrightarrow B$ é *injetora*, se elementos distintos de A produzem imagens distintas em B, isto é,

$$x \neq x' \Rightarrow f(a) \neq f(a')$$

ou, equivalentemente,

$$f(a) = f(a') \Rightarrow a = a'.$$

Uma função $f : A \longrightarrow B$ é *sobrejetora*, se cada $y \in B$ é imagem de ao menos um $x \in A$. Além disso, uma função que é injetora e sobrejetora, denomina-se *bijetora*.

Uma função bijetora σ do conjunto $\{1, 2, 3, \ldots, n\}$ sobre si mesmo é chamada uma *permutação*. Denotamos σ por

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix} \quad \text{ou} \quad \sigma = (j_1 j_2 \cdots j_n), \text{ em que } j_i = \sigma(i).$$

Observe que como σ é injetora e sobrejetora, a sequência $(j_1, j_2, \ldots, j_n)$ é simplesmente um rearranjo dos números $1, 2, \ldots, n$. O número de tais permutações é n! e o conjunto de todas as permutações é denotada por S_n. Também observamos que se $\sigma \in S_n$, então a transformação inversa $\sigma^{-1} \in S_n$; e, se $\sigma, \tau \in S_n$, então a transformação composta $\sigma \circ \tau \in S_n$. Em particular, a transformação identidade

$$\epsilon = \sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma$$

pertence a S_n.

Consideremos uma permutação arbitrária σ em

$$S_n : \sigma = (j_1 j_2 \cdots j_n).$$

Diremos que σ é *par* ou *ímpar*, conforme exista um número par ou ímpar de pares (i, k), para os quais

$$i > j, \text{ mas } i \text{ precede } k \text{ em } \sigma.$$

Então, definimos o *sinal* ou paridade de σ, escrito $\operatorname{sgn} \sigma$, por

$$\operatorname{sgn}\sigma = \begin{cases} 1, & \text{se} \quad \sigma \quad \text{é} \quad \text{par} \\ -1, & \text{se} \quad \sigma \quad \text{é} \quad \text{ímpar.} \end{cases}$$

O *determinante* de uma matriz quadrada $A = (a_{ij})$ de ordem n, é a soma efetuada sobre todas as permutações $\sigma = (j_1 j_2 \cdots j_n)$ em S_n, isto é,

$$\det(A) = \sum_{\sigma \in S_n} (\operatorname{sgn}\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$$

Consideremos uma matriz quadrada $A = (a_{ij})$ de ordem n. Representaremos por M_{ij} a submatriz quadrada de ordem $(n-1)$ de A, obtida suprimindo-se sua i-ésima linha e j-ésima coluna. O determinante $\det(M_{ij})$ é denominado o *menor complementar* do elemento a_{ij} de A e definimos o cofator de a_{ij}, denotado por A_{ij}, como

$$A_{ij} = (-1)^{i+j} \cdot \det(M_{ij}).$$

Com estes cofatores podemos formar uma nova matriz $\bar{A}$, denominada *matriz dos cofatores de A*.

$$\bar{A} = [A_{ij}].$$

A partir destas considerações o determinante de uma matriz quadrada $A = (a_{ij})$ pode ser definido da seguinte forma,

$$\det(A) = \sum_{j=1}^{n} a_{ij}A_{ij} \text{ ou } \det(A) = \sum_{i=1}^{n} a_{ij}A_{ij}.$$

As fórmulas supracitadas, denominam-se desenvolvimento de Laplace, sobre uma matriz quadrada $A = (a_{ij})$ de ordem n, segundo a i-ésima linha e j-ésima coluna, respectivamente, oferecem um método de simplificar o cálculo do $\det(A)$.

Consideremos uma matriz quadrada $A = (a_{ij})$ de ordem n sobre um corpo $\mathbb{K}$. Denomina-se *adjunta* de A, a transposta da matriz dos cofatores dos elementos a_{ij} de A, representada por adj A, à matriz

$$\text{adj}\, A = \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix} = \bar{A}^T$$

Teorema 1.1. *Para qualquer matriz quadrada A,*

$$A \cdot (adj\, A) = (adj\, A) \cdot A = det\,(A) \cdot I.$$

Assim, se $det\,(A) \neq 0$, então

$$A^{-1} = \frac{1}{det\,(A)} \cdot (adj\, A).$$

1.3 Autovalores e Autovetores

Autovalores e autovetores são conceitos importantes de matemática, com aplicações práticas em áreas diversificadas como mecânica quântica, processamento de imagens, análise de vibrações, mecânica dos sólidos, estatística etc.

Sejam V e U *espaços vetoriais* sobre o mesmo corpo $\mathbb{K}$. Uma transformação $F : V \longrightarrow U$ denomina-se *transformação linear* (ou homomorfismo)[1] se satisfaz as duas condições seguintes:

1. Para quaisquer $v, w \in V$, $F(v + w) = F(v) + F(w)$.

2. Para qualquer $k \in \mathbb{K}$ e $v \in V$, $F(kv) = kF(v)$.

Em outras palavras, $F : V \longrightarrow U$ é linear se "preserva" as duas operações básicas de um espaço vetorial, isto é, adição de vetores e multiplicação por escalar.

Substituindo $k = 0$ na condição (2) acima obtemos $F(0) = 0$. Isto é, toda transformação linear leva o vetor nulo no vetor nulo.

Para quaisquer $a, b \in \mathbb{K}$ e vetores $v, w \in V$ obtemos, aplicando as duas condições de linearidade, que

$$F(av + bw) = F(av) + F(bw) = aF(v) + bF(w).$$

[1](ver apêndice B.8)

Seja A uma matriz $m \times n$ sobre um corpo $\mathbb{K}$. Então A determina uma única transformação $T : \mathbb{K}^n \longrightarrow \mathbb{K}^m$ pela associação $v \longmapsto Av$. Afirmamos que T é linear, pois pelas propriedades de matrizes, temos

$$T(v + w) = A(v + w) = Av + Aw = T(v) + T(w)$$

e

$$T(kv) = A(kv) = k(Av) = kT(v),$$

onde, $v, w \in \mathbb{K}^n$ e $k \in \mathbb{K}$.

Seja $F : V \longrightarrow U$ uma transformação linear. A *imagem* de F, em símbolos

$$\mathrm{Im}F,$$

é o conjunto dos pontos imagens de U:

$$\mathrm{Im}F = \{u \in U : F(v) = u, \text{ para algum } v \in V\}.$$

O *núcleo* de F, em símbolos $\mathrm{Ker}F$, é o conjunto dos elementos em V, que são transformados em $0 \in U$:

$$\mathrm{Ker}F = \{v \in V : F(v) = 0\}.$$

Uma transformação linear $F : V \longrightarrow U$ é *singular* se existir um $v \in V$, com $v \neq 0$, tal que $F(v) = 0$. Assim, $F : V \longrightarrow U$ é *não-singular* se, e somente se, $\mathrm{Ker}F = \{0\}$ se, e somente se, F é injetora. Uma transformação linear bijetiva é denominada *isomorfismo.*

Seja V um espaço vetorial sobre um corpo $\mathbb{K}$. Consideremos o caso especial de transformações lineares $T : V \longrightarrow V$, isto é, de V nele mesmo. Elas são também denominadas *operadores lineares.*

Consideremos um polinômio f sobre um corpo $\mathbb{K}$:

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

Se A é uma matriz quadrada sobre $\mathbb{K}$, então definimos a matriz polinomial sobre $\mathbb{K}$ como

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

Em particular, diremos que A é uma *raiz* ou *zero* do polinômio f se $f(A) = 0$.

Agora, suponhamos que $T : V \longrightarrow V$ é um operador linear sobre V. Se

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

então definimos $f(T)$ do mesmo modo como fizemos para matrizes:

$$f(T) = a_n T^n + \cdots + a_1 T + a_0 I.$$

Também diremos que T é um *zero* ou *raiz* de f se $f(T) = 0$.

Se A é uma representação matricial de T, então $f(A)$ é a representação matricial de $f(T)$. Em particular, $f(T) = 0$ se, e somente se, $f(A) = 0$.

Seja $T : V \longrightarrow V$ um operador linear num espaço vetorial V sobre um corpo $\mathbb{K}$. Um escalar $\lambda \in \mathbb{K}$ é chamado *autovalor* de T, se existe um vetor não-nulo $v \in V$, para o qual

$$T(v) = \lambda v.$$

Todo vetor não nulo que satisfaça esta relação é chamado um **autovetor** de T associado ao autovalor λ.

Note que cada múltiplo escalar kv de um autovetor v é também um autovetor de T, pois

$$T(kv) = kT(v) = k(\lambda v) = \lambda(kv).$$

O conjunto de todos os autovetores associados a λ é um subespaço de V, chamado *auto-espaço* associado ao autovalor λ.

O próximo teorema dá uma caracterização importante de autovalores, que é frequentemente usada como sua definição.

Teorema 1.2. *Seja $T : V \longrightarrow V$ um operador linear. Então $\lambda \in \mathbb{K}$ é um autovalor de T se, e somente se, o operador $\lambda I - T$ é singular. O autoespaço associado ao autovalor λ é o núcleo de $\lambda I - T$.*

Prova. λ é um autovalor de T se, e somente se, existe um vetor não nulo v tal que

$$T(v) = \lambda v \Leftrightarrow (\lambda I - T)(v) = 0,$$

isto é, $\lambda I - T$ é singular. Além disso, v está no autoespaço de λ se, e somente se, as relações acima acontecem. Portanto, v está no núcleo de $\lambda I - T$. ■

Se $\mathcal{B}$ é uma base ordenada arbitrária de V e $A = [T]_{\mathcal{B}}$, então $(\lambda I - T)$ é inversível se, e somente se, a matriz $(\lambda I - A)$ é inversível.

Seja A é uma matriz quadrada de ordem n sobre o corpo $\mathbb{K}$, um *autovalor* de A em $\mathbb{K}$ é um escalar λ em $\mathbb{K}$ tal que a matriz $(\lambda I - A)$ seja singular, ou seja, não-invertível.

A matriz

$$xI_n - A$$

é denominada *matriz característica* de A. Seu determinante,

$$\det(xI - A),$$

que é um polinômio em x, $p_A(x)$, denomina-se o *polinômio característico* de A.

Da mesma forma que para matrizes de ordem n, os autovalores de T serão as raízes do polinômio característico de T. Em particular, isto nos mostra que T não pode ter mais que n autovalores distintos. É importante ressaltar que T pode não ter nenhum autovalor.

Teorema 1.3. *Seja A uma matriz quadrada de ordem n sobre um corpo $\mathbb{K}$. Um escalar $\lambda \in \mathbb{K}$ é um autovalor de A se, e somente se, λ é uma raiz do polinômio característico $p(x) = det(xI_n - A)$ de A.*

Prova. Pelo Teorema (1.3), λ é um autovalor de A se, e somente se, $\lambda I - A$ é singular, ou seja, $\det(\lambda I - A) = 0$, isto é, λ é uma raiz de p. ■

Exemplo 1.2. *Seja T o operador linear sobre $\mathbb{R}^2$ que é representado em relação à base ordenada canônica pela matriz*

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Então o polinômio característico de T (ou de A) é

$$p_A(x) = det(xI - A) = \begin{vmatrix} x & 1 \\ -1 & x \end{vmatrix} = x^2 + 1.$$

Note que o polinômio do Exemplo não possui raízes reais. Portanto, T não possuem autovalores. Se U é um operador linear sobre $\mathbb{C}^2$ que é representado por A em relação à base ordenada canônica, então U possui dois autovalores, i e $-i$. Vemos aqui um ponto sutil. Ao discutirmos os autovalores de uma matriz A, precisamos tomar o cuidado de estipular o corpo envolvido. A matriz A não possui nenhum valor característico em $\mathbb{R}$, mas possui dois valores característicos em $\mathbb{C}$.

Exemplo 1.3. *Seja A uma matriz quadrada de ordem 3,*

$$A = \begin{pmatrix} 3 & 1 & -1 \\ 2 & 2 & -1 \\ 2 & 2 & 0 \end{pmatrix}$$

O polinômio característico de A é

$$p_A(x) = det(xI_3 - A) = \begin{vmatrix} x-3 & -1 & 1 \\ -2 & x-2 & 1 \\ -2 & -2 & x \end{vmatrix} = x^3 - 5x^2 + 8x - 4 = (x-1)(x-2)^2.$$

Portanto, os autovalores de A são 1 e 2.

Lema 1.1. *Suponhamos que $T(v) = \lambda v$ e que f é qualquer polinômio em $\mathbb{K}[x]$. Então $f(T)(v) = f(\lambda)v$, ou seja, $f(\lambda)$ é o autovalor de $f(T)$ associado ao autovetor v.*

Prova. Como $T(v) = \lambda v$ temos que

$$T^2(v) = T(T(v)) = T(\lambda v) = \lambda T(v) = \lambda^2 v.$$

Assim, indutivamente, obtemos

$$T^m(v) = \lambda^m v, \ \forall \ m \in \mathbb{N}.$$

Agora, seja

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

um polinômio qualquer. Então

$$f(T)(v) = f(\lambda)v.$$

Portanto, $f(\lambda)$ é o autovalor de $f(T)$ associado ao autovetor v. ■

Capítulo 2

Matriz Circulante

Matrizes circulantes são predominantes em muitos ramos da matemática. Essas matrizes aparecem naturalmente em áreas da matemática, onde as raízes da unidade desempenham um importante papel, e aqui apresentaremos algumas das razões dessa importância. No entanto, elas são onipresentes, muitos fatos sobre essas matrizes podem ser provadas usando apenas álgebra linear básica. Isso torna a área bastante acessível para alunos de graduação à procura de problemas em pesquisa e/ou professores de matemática em busca de temas com interesse exclusivo para apresentar aos seus alunos.

2.1 Conceitos e Propriedades

Em tudo que segue $n \in \mathbb{N}$, com $n \geq 2$. Nossos objetos de estudo neste capítulo são: o espaço vetorial complexo $\mathbb{C}^n$ e o anel das matrizes complexas $M_n(\mathbb{C})$. Estudaremos a multiplicação de matrizes $M \in M_n(\mathbb{C})$ por vetores $v \in \mathbb{C}^n$. A este respeito, podemos identificar o vetor v como um vetor coluna (matriz coluna). No entanto, por vezes, é útil matematicamente e mais conveniente tipograficamente, considerar

$$v = (v_0, v_1, v_2, \ldots, v_{n-1}) \in \mathbb{C}^n \longleftrightarrow V = v^T \in M_{n\times 1}(\mathbb{C}).$$

como um vetor coluna.

Seja

$$\mathcal{E} = \{e_0, e_1, \ldots, e_{n-1}\}$$

a *base ortonormal canônica* para $\mathbb{C}^n$, em que

$$e_i = (\delta_{i,0}, \ldots, \delta_{i,n-1}), \;\; i = 0, \ldots n-1,$$

e $\delta_{i,j}$ é o **delta de Kronecker**[1]

$$\delta_{i,j} = \begin{cases} 1, & \text{se} \quad i = j \\ 0, & \text{se} \quad i \neq j. \end{cases}$$

Então cada vetor v pode ser escrito de modo único sob a forma

$$v = (v_0, v_1, v_2, \ldots, v_{n-1}) = \sum_{i=0}^{n-1} v_i e_i,$$

sendo os escalares v_i as componentes de v com respeito à base $\mathcal{E}$.

Sejam $S = \{0, 1, \ldots, n-1\}$ e $\sigma : S \to S$ a permutação definida por

$$\sigma(i) = \begin{cases} i-1, & \text{se} \quad 1 \leq i \leq n-1 \\ n-1, & \text{se} \quad i = 0. \end{cases}$$

Vamos definir o operador *deslocamento cíclico* $T_\sigma : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ associado a σ por

$$T_\sigma(v_0, v_1, v_2, \ldots, v_{n-1}) = (v_{\sigma(0)}, v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n-1)}).$$

Note que

$$T_\sigma^2(v_0, v_1, v_2, \ldots, v_{n-1}) = (v_{\sigma^2(0)}, v_{\sigma^2(1)}, v_{\sigma^2(2)}, \ldots, v_{\sigma^2(n-1)}).$$

Em geral,

$$T_\sigma^k = T_{\sigma^k} \text{ e } T_\sigma^n = T_{\sigma^n} = I.$$

Se $v \in \mathbb{C}^n$, com $v \neq 0$, então é fácil verificar que

$$\mathcal{B} = \{v, T(v), \ldots, T^{n-1}(v)\}$$

é uma base ordenada para $\mathbb{C}^n$.

[1] Leopold Kronecker estudou em Berlim e obteve o grau de doutor em 1845 com uma tese sobre Teoria dos Números. As suas principais contribuições para a matemática foram no campo da álgebra e continuidade de funções.

Sejam

$$q(x) = 1 + 2x + x^2 + 3x^3 \in \mathbb{R}[x] \text{ e } W = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

em que W é a transposta da representação matricial de T_σ em relação a base ordenada canônica para $\mathbb{R}^4$, pois

$$T_\sigma(e_0) = e_1, \;\; T_\sigma(e_1) = e_2, \;\; T_\sigma(e_2) = e_3 \text{ e } T_\sigma(e_3) = e_0.$$

Então é fácil verificar que

$$C = q(W) = \begin{pmatrix} 1 & 2 & 1 & 3 \\ 3 & 1 & 2 & 1 \\ 1 & 3 & 1 & 2 \\ 2 & 1 & 3 & 1 \end{pmatrix}$$

é uma matriz obtida deslocando ciclicamente os elementos da primeira linha uma unidade para à direita. Isto motiva a seguinte definição:

Uma *matriz circulante* $C = \mathrm{circ}\{v\}$ associada a um vetor $v \in \mathbb{C}^n$ é a matriz $n \times n$ cujas linhas são dadas por iterações do operador deslocamento cíclico agindo em sua k-ésima linha, $T_\sigma^{k-1}(v), \;\; k = 1, \ldots, n$:

$$C = \begin{pmatrix} v_0 & v_1 & v_3 & \cdots & v_{n-1} \\ v_{n-1} & v_0 & v_1 & \cdots & v_{n-2} \\ v_{n-2} & v_{n-1} & v_0 & \cdots & v_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_1 & v_2 & v_3 & \cdots & v_0 \end{pmatrix}.$$

A ordenação escolhida

$$C = \mathrm{circ}\,(v_0, v_1, v_2, \ldots, v_{n-1})$$

é apenas uma convenção adequada para impor uma notação cíclica em que os números v_k devem realmente obedecer. Observe que C é a matriz mudança de base da base $\mathcal{B}$ para a base $\mathcal{E}$.

Exemplo 2.1. *A partir do vetor* $v = (a, b, c) \in \mathbb{R}^3$*, podemos gerar a matriz circulante*

$$C_3 = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}.$$

Veremos que as matrizes circulantes desempenham um papel importante em várias aplicações, dentre as quais a que mais nos chama a atenção é a forma simples como se calcula seus autovalores e autovetores utilizando raízes n-ésimas da unidade.

2.2 Matrizes de Permutações

Um caso particular de matriz circulante é a matriz de permutação

$$W = \text{circ}\{e_i\},$$

a qual é a matriz identidade com sua linha superior mudada para a parte inferior.

Exemplo 2.2. *Quem é* $W = circ\{e_1\}$*, quando* $n = 3$*? Como* $e_1 = (0, 1, 0)$ *temos que*

$$W = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Note que se $W_i = \text{circ}\{e_i\}$ e $W_j = \text{circ}\{e_j\}$, então

$$W_i \cdot W_j = W_{i+j} \ \text{ e } \ W_i = W^i$$

em que os índices são lidos módulo n. É claro que $W_0 = I$ e

$$W^t = W^{-1},$$

pois

$$WW^t = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I.$$

Neste caso, W é *matriz ortogonal*, ou seja, $WW^T = I$. Observe que

$$C = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} = aI + bW + cW^2.$$

Como $W^3 = I$ temos que W é uma raiz da equação $x^3 - 1 = 0$. Assim, a equação

$$x^n - 1 = 0$$

desempenha um papel importante neste trabalho. As raízes dessa equação são denominadas *raízes n-ésimas da unidade*. É comum definir essas raízes por

$$\omega = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right) = e^{\frac{2\pi i}{n}}$$

conhecida como Fórmula de Euler[2]. Neste caso, as raízes da equação $x^n - 1 = 0$ são dadas pelas potências n-ésimas de ω e, para cada $k \in \mathbb{N}$, com $k = 0, 1, \ldots, n-1$, tem-se

$$\omega^k = e^{\frac{2\pi i k}{n}}.$$

Portanto,

$$1, \omega, \omega^2, \ldots, \omega^{n-1}$$

são as raízes n-ésimas (distintas) de $x^n - 1 = 0$.

Para explorar uma outra base para $\mathbb{C}^n$, consideremos os vetores (autovetores normalizados de W)

$$x_k = \frac{1}{\sqrt{n}}(1, \omega^k, \omega^{2k}, \ldots, \omega^{(n-1)k}) \in \mathbb{C}^n, \;\; k = 0, 1, \ldots, n-1,$$

de modo que os vetores x_k formam uma base para $\mathbb{C}^n$. Assim, para cada k, podemos construir uma matriz especial a partir da *Matriz de Vandermonde*, colocando os vetores

[2]A Fórmula de Euler, cujo nome é uma homenagem a Leonhard Euler, é uma fórmula matemática da área específica da análise complexa, que mostra uma relação entre as funções trigonométricas e a função exponencial.

x_k como colunas

$$Q = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)^2} \end{pmatrix}.$$

Dada $A \in M_n(\mathbb{C})$, a transposta conjugada de A é denominada *Hermitiana* e aqui denotada por A^*.

Uma matriz $A \in M_n(\mathbb{C})$ é:

- Hermitiana, se $A = A^*$.
- Unitária, se $A^{-1} = A^*$.
- Normal, se $AA^* = A^*A$.

Claramente, matrizes unitárias e Hermitianas são sempre normais. Em particular, como W é uma matriz real e $W^* = W^T$ temos que W é unitária e, portanto, normal.

Um resultado importante que caracteriza matrizes normais é que elas são unitariamente diagonalizáveis, ou seja, A é normal se, e somente se, existir uma matriz unitária U tal que U^*AU seja diagonal.

Passamos a construir uma diagonalização para W. Como W é uma matriz de permutação, o *polinômio característico* de W é:

$$\begin{aligned} P(x) &= \det \begin{pmatrix} x & -1 & 0 & \cdots & 0 \\ 0 & x & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \\ -1 & 0 & 0 & \cdots & x \end{pmatrix} \\ &= (-1)^{n+1}(-1)(-1)^{n-1} + (-1)^{n+n} x \cdot x^{n-1} \\ &= x^n - 1. \end{aligned}$$

Portanto, os autovalores de W são as raízes n-ésimas da unidade. É fácil verificar que

$$v(\omega) = (1, \omega, \omega^2, \ldots, \omega^{n-1})$$

é o autovetor de W associado ao autovalor ω. Mais geralmente, como

$$\omega^k = e^{\frac{2k\pi i}{n}}, \;\; k = 0, 1, 2, \ldots, n-1$$

temos que os autovetores de W são:

$$v(\omega^0), v(\omega^1), \ldots, v(\omega^{n-1})$$

associados aos autovalores

$$\omega^0 = 1, \omega^1, \ldots, \omega^{n-1}.$$

Sejam Q a matriz cujas as colunas são esses autovetores e D a matriz diagonal cujos elementos diagonais sejam os autovalores associados. Então

$$WQ = QD. \tag{2.1}$$

É fácil verificar que

$$Q^{-1} = \frac{Q^*}{n}$$

e, por conseguinte,

$$\left(\frac{1}{\sqrt{n}}\right) Q$$

é uma matriz unitária. Consequentemente, a equação (2.1) pode ser escrito sob a forma

$$W = \left(\frac{1}{\sqrt{n}} Q\right) D \left(\frac{1}{\sqrt{n}} Q\right)^* \tag{2.2}$$

que é uma diagonalização unitária de W.

Exemplo 2.3. *Seja*

$$Q = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix},$$

com ω a raiz cúbica da unidade. Devemos mostrar que W é diagonalizável, ou seja,

$$W = \left(\frac{Q}{\sqrt{3}}\right) D \left(\frac{Q}{\sqrt{3}}\right)^*.$$

Solução. Como

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

temos que $\det(Q) = -3i\sqrt{3} \neq 0$. Assim, Q^{-1} existe. Note que

$$\begin{aligned} Q^*Q &= \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \\ &= \begin{pmatrix} 3 & 1+\omega+\omega^2 & 1+\omega+\omega^2 \\ 1+\omega+\omega^2 & 3 & 1+\omega+\omega^2 \\ 1+\omega+\omega^2 & 1+\omega+\omega^2 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \end{aligned}$$

pois $1 + \omega + \omega^2 = 0$, de modo que

$$Q^*Q = 3I \text{ e } Q^{-1} = \frac{1}{3}Q^*.$$

Portanto,

$$W = \left(\frac{Q}{\sqrt{3}}\right) D \left(\frac{Q}{\sqrt{3}}\right)^*,$$

que é o resultado desejado. ■

Vamos estender estes resultados, via autovalores e autovetores, para matrizes circulantes gerais. Como vimos uma matriz circulante pode ser representada como

$$C = \mathrm{circ}\{v\} = \sum_{i=0}^{n-1} v_i W^i.$$

O polinômio

$$q(x) = q_C(x) = \sum_{i=0}^{n-1} v_i x^i \in \mathbb{R}[x] \tag{2.3}$$

associado a matriz circulante $C = \mathrm{circ}\{v\}$ é denominado o *representante* de $C = \mathrm{circ}\{v\}$.

Neste caso,

$$C = q(W).$$

Assim, pelo Lema 1.1, existe uma relacionamento entre os autovalores de W e os de $C = q(W)$. Mais precisamente, como as raízes n-ésima da unidade ω^k são os autovalores de W temos que $q(\omega^k)$ são os autovalores de C. Portanto,

$$q(W)Q = Qq(D)$$

e

$$C = q(W) = \left(\frac{1}{\sqrt{n}}Q\right) q(D) \left(\frac{1}{\sqrt{n}}Q\right)^*.$$

Com o objetivo de tornar claro estas ideais vamos finalizar esta seção com exemplos particulares e alguns comentários sobre equações polinomiais gerais vinculadas a matrizes circulantes.

Exemplo 2.4. *Dado*

$$C = \begin{bmatrix} -2 & b & \bar{b} \\ \bar{b} & -2 & b \\ b & \bar{b} & -2 \end{bmatrix},$$

com $b = e^{\frac{2\pi i}{9}}$. *Calcule os polinômios representante e característico de* C.

Solução. Note que

$$q(x) = -2 + bx + \bar{b}x^2 \in \mathbb{C}[x]$$

é o polinômio representante de C. Como

$$W = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

temos que $x^3 - 1 = 0$ é a equação característica de W. Assim,

$$1, \ \omega \ \text{e} \ \omega^2 = \bar{\omega},$$

com

$$\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i,$$

são os autovalores de W. Logo,

$$q(1) = -2 + 2\cos\left(\frac{2\pi}{9}\right), \quad q(\omega) = -2 + 2\cos\left(\frac{8\pi}{9}\right) \text{ e } q(\omega^2) = -2 + 2\cos\left(\frac{14\pi}{9}\right)$$

são os autovalores de C e

$$v(1) = (1, 1, 1), \quad v(\omega) = (1, \omega, \omega^2) \text{ e } v(\omega^2) = (1, \omega^2, \omega)$$

são os autovetores de C associados a estes autovalores. Pondo

$$Q = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \text{ e } D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$$

obtemos

$$W = \left(\frac{1}{\sqrt{3}}Q\right) D \left(\frac{1}{\sqrt{3}}Q\right)^* \text{ e } C = q(W) = \left(\frac{1}{\sqrt{3}}Q\right) q(D) \left(\frac{1}{\sqrt{3}}Q\right)^*.$$

Observe que o polinômio característico de C é

$$p_C(x) = det(xI - C) = x^3 + 6x^2 + 9x + 3$$

e

$$q(1) = -2 + 2\cos\left(\frac{2\pi}{9}\right), \quad q(\omega) = -2 + 2\cos\left(\frac{8\pi}{9}\right) \text{ e } q(\omega^2) = -2 + 2\cos\left(\frac{14\pi}{9}\right)$$

são suas raízes. ∎

Exemplo 2.5. *Dado*

$$C = \begin{pmatrix} 1 & 2 & 1 & 3 \\ 3 & 1 & 2 & 1 \\ 1 & 3 & 1 & 2 \\ 2 & 1 & 3 & 1 \end{pmatrix}.$$

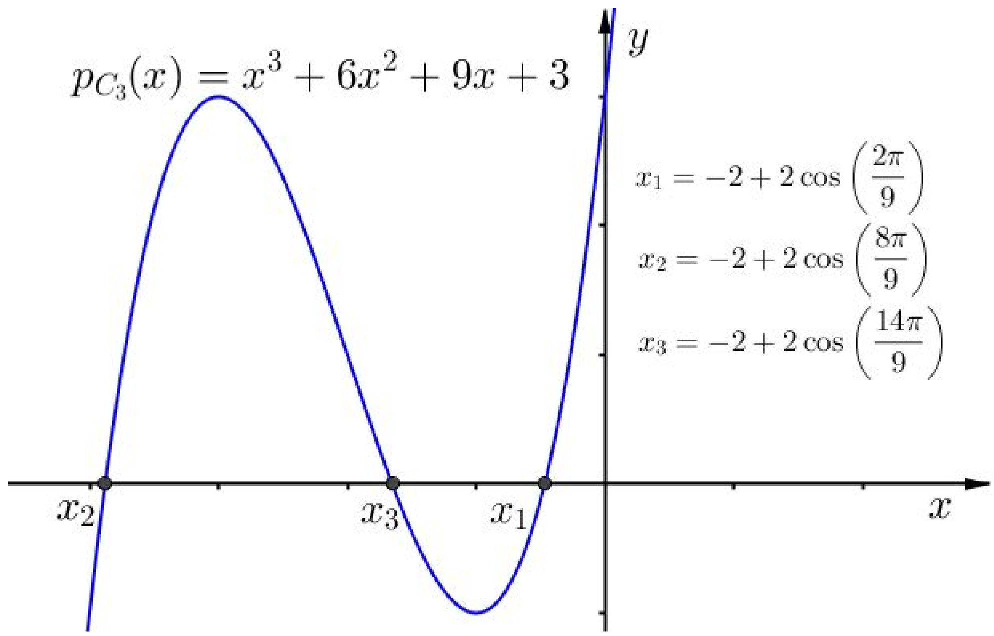


Figura 2.1: Representação gráfica de p_C.

Escreva C sob a forma

$$C = q(W) = \left(\frac{1}{\sqrt{4}}Q\right) q(D) \left(\frac{1}{\sqrt{4}}Q\right)^*.$$

Solução. Note que

$$q(x) = 1 + 2x + x^2 + 3x^3 \in \mathbb{R}[x]$$

é o polinômio representante de C. Como

$$W = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

temos que $x^4 - 1 = 0$ é a equação característica de W. Assim,

$$1, \ -1, \ i \text{ e } -i$$

são os autovalores de W. Logo,

$$q(1) = 7, \ \ q(-1) = -3, \ \ q(i) = -i \ \text{e} \ q(-i) = i$$

são os autovalores de C e

$$v(1) = (1,1,1,1), v(-1) = (1,-1,1,-1), v(i) = (1,i,-1,-i) \ \text{e} \ v(-i) = (1,-i,-1,i)$$

são os autovetores de C associados a estes autovalores. Pondo

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{pmatrix} \ \text{e} \ D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}$$

obtemos

$$C = q(W) = \left(\frac{1}{2}Q\right) q(D) \left(\frac{1}{2}Q\right)^{*}.$$

Observe que o polinômio característico de C é

$$p_C(x) = det(xI - C) = x^4 - 4x^3 - 20x^2 - 4x - 21$$

e

$$q(1) = 7, \ \ q(-1) = -3, \ \ q(i) = -i \ \text{e} \ q(-i) = i$$

são suas raízes. Portanto,

$$p_C(x) = (x+3)(x-7)(x^2+1),$$

que é o resultado desejado. ■

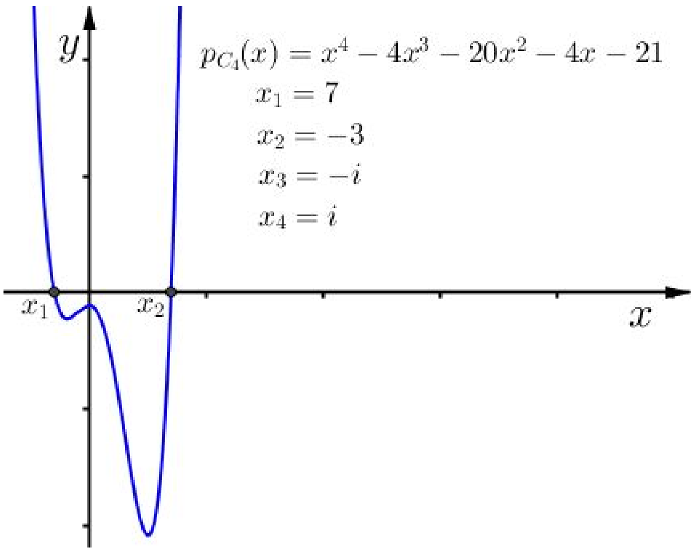


Figura 2.2: Representação gráfica de p_C.

Como esses exemplos sugerem, as matrizes circulantes proporcionam uma nova forma de construir polinômios com raízes conhecidas. É claro que os elementos do conjunto

$$\{\alpha_1, \ldots, \alpha_n\},$$

são as raízes do polinômio

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

Assim, desenvolvendo, determinamos os coeficientes deste polinômio. Normalmente, resolver uma equação polinomial envolve o processo inverso: começamos com os coeficientes e extraímos as raízes. Matrizes circulantes oferecem uma terceira via: começamos com uma matriz circulante $C = q(W)$ e geramos as duas coisas simultaneamente: os coeficientes e as raízes de um polinômio f. Neste caso,

- f é o polinômio característico de C, ou seja,

$$f(x) = p_C(x).$$

- Os coeficientes podem ser obtidos a partir da identidade

$$p_C(x) = det(xI - C).$$

- As raízes (os autovalores de C) podem ser encontradas aplicando o polinômio representante q nas raízes n-ésimas de unidade.

Veremos no próximo Capítulo que esta abordagem nos leva a um método unificado para resolver de forma geral as equações quadráticas, cúbicas e quárticas.

Capítulo 3

Equações

3.1 História

As equações constituem, pelo menos do ponto de vista prático, a parte mais importante da Matemática. "Modelar um problema", mesmo entre os leigos, é generalizadamente entendido como colocá-lo dentro de um mecanismo do qual ele sairá resolvido.

Equações algébricas são aquelas em que a incógnita aparece apenas submetida às chamadas operações algébricas. A equação algébrica na forma

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0, \;\; \forall \;\; n \in \mathbb{N},$$

é denominada *equação polinomial*.

Dentre os antigos documentos matemáticos que conhecemos, os mais famosos são o Papiro de Ahmes (1650 a.C.), também conhecido como de Rhind e o Papiro de Moscou (1850 a.C.). É importante ressaltar que os documentos matemáticos naquela época não empregavam alta dosagem de simbologia à qual estamos atualmente acostumados. Um dos problemas de Ahmes dizia: "*Uma quantidade, somada a seus* $\frac{2}{3}$*, mais sua metade e mais sua sétima parte perfaz* 33*. Qual é esta quantidade?*". No simbolismo atual escrevemos:

$$x + \frac{2}{3}x + \frac{1}{2}x + \frac{1}{7}x = 33 \Leftrightarrow \frac{97}{42}x = 33,$$

o que é uma equação do 1.^{o} grau.

Os Babilônios, na mesma época, já conseguiam trabalhar com equações do 2.^{o} grau e as resolviam por um método baseado no mesmo raciocínio empregado pelos hindus quase três milênios mais tarde, o chamado "completamento de quadrado". Embora os resultados fossem corretos, os tabletes que contém soluções de equações do 2.^{o} grau apresentam, como todos os demais, apenas sequências do tipo "*faça isto*", "*faça aquilo*", "*este é o resultado*", sem qualquer justificativa lógica sobre o caminho seguido.

A fórmula geral para a solução das equações do 2.^{o} grau é amplamente conhecida mas merece aqui alguns comentários. Em primeiro lugar, seu encontro fundamentou-se na ideia de buscar uma forma de reduzir o grau da equação do 2.^{o} para o 1.^{o}, através da extração de raízes quadradas. Este foi o engenhoso instrumento que os hindus utilizaram com sucesso para chegar à *fórmula de Bhaskara*. Seja a equação do 2.^{o} grau

$$ax^2 + bx + c = 0, \text{ com } a \neq 0.$$

Então

$$x^2 + \frac{b}{a}x = -\frac{c}{a}.$$

Como

$$x^2 + \left(\frac{b}{a}\right)x$$

não é um quadrado perfeito, a ideia foi somar aos dois membros algo que torna o lado esquerdo um quadrado perfeito. Claramente, a quantidade a ser somada era

$$\left(\frac{b}{2a}\right)^2,$$

ou seja,

$$x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} = -\frac{c}{a} + \frac{b^2}{4a^2}. \tag{3.1}$$

Assim, como o primeiro membro da igualdade (3.1) é um quadrado perfeito, podemos reescrevê-la sob forma:

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2} \Rightarrow x + \frac{b}{2a} = \pm\sqrt{\frac{b^2 - 4ac}{4a^2}}.$$

Logo, as soluções são dadas pelas fórmulas

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

a qual é a célebre *fórmula de Bhaskara*, embora não tenha sido deduzida por ele, imortalizou seu nome. As equações do 2.^{o} grau são a chave para a solução de um problema clássico: *encontrar dois números, x e y, conhecendo-se sua soma S e seu produto P.* Este enunciado corresponde ao sistema:

$$\begin{cases} x+y &= S \\ xy &= P \end{cases}$$

cujas soluções são

$$x = \frac{S+\sqrt{S^2-4P}}{2} \ \text{ e } \ y = \frac{S-\sqrt{S^2-4P}}{2}.$$

Vencidas as equações do 2.^{o} grau, a inesgotável curiosidade dos matemáticos levou-se a conjecturar sobre as formas de resolver as equações do 3.^{o} grau. Os árabes também tiveram papel importante, embora não tenham encontrado a solução.

Consta que, por volta de 1510, um professor de Matemática da Universidade de Bolonha, chamado Scipione del Ferro, encontrou uma forma geral de resolver as equações do tipo

$$x^3 + \beta x + \gamma = 0.$$

Embora tenha morrido sem publicar sua descoberta, ele revelou para seu aluno, Antônio Maria Fior que, mais tarde, tentou adquirir notoriedade valendo-se da descoberta do mestre. Naquela época era bastante frequente o lançamento de desafios entre os sábios e Fior elegeu Tartaglia, já bastante conhecido por seu talento, como alvo. Tartaglia aceitou o desafio, até porque não levava Fior em grande consideração mas, pouco antes da data marcada, veio a saber que seu oponente estava armado de um método descoberto pelo falecido professor Scipione del Ferro. Sentindo-se ameaçado, conforme mais tarde relatou o próprio Tartaglia, "*mobilizei todo o entusiasmo, a aplicação e a arte de que fui capaz, objetivando encontrar uma regra para a solução daquelas equações, o que consegui a 10 de fevereiro de* 1535". Mas foi mais longe: além de resolver as equações do tipo

$$x^3 + \beta x + \gamma = 0,$$

também, achou a fórmula geral para as equações do tipo

$$x^3 + \beta x^2 + \gamma = 0,$$

que Fior não conhecia. Desse modo Fior saiu humilhado do episódio e hoje só é lembrado como alguém que recebeu o merecido castigo ao pretender fama às custas de outrem.

Cardano ficou sabendo que Tartaglia achara a solução e resolveu pedir-lhe que a revelasse para que fosse publicada em seu livro PRATICA ARITHMETICAE GENERALIS, Tartaglia não aceitou de imediato, porém cedeu mais tarde após inúmeros juramentos de segredo do Cardano. Conforme qualquer um poderia prever, Cardano quebrou todas as promessas e juramentos e, em 1545, fez publicar na ARS MAGNA, a fórmula revelada por Tartaglia. Embora tenha feito diversos elogios a ele, acrescentou que, independentemente e trinta anos antes, Scipione del Ferro chegara aos mesmos resultados. A reação de Tartaglia foi pronta e explosiva: publicou sua versão dos fatos e denunciou Cardano por haver traído um sagrado juramento sobre a Bíblia. Em defesa de Cardano veio seu discípulo Ferrari, o descobridor da solução das equações do 4.^{o} grau. Após debates e longas trocas de insultos, a posteridade foi injusta com o sofrido Tartaglia: a fórmula que ele deduzira e que ensinara ao desleal inimigo, ao invés de receber seu nome, é hoje generalizadamente conhecida como fórmula de Cardano. O que ocorreu com a fórmula de Bhaskara repetiu-se nas equações do 3.^{o} grau.

Lembremos que Tartaglia solucionara os tipos especiais

$$x^3 + \beta x + \gamma = 0 \text{ e } x^3 + \beta x^2 + \gamma = 0$$

e não a equação geral

$$ax^3 + bx^2 + cx + d = 0. \tag{3.2}$$

Comecemos esclarecendo que qualquer equação geral pode ser transformada facilmente em um daqueles tipos especiais, digamos

$$x^3 + \beta x + \gamma = 0,$$

fazendo a substituição $x = y + m$ na equação (3.2) e calculando m de modo a anular o termo do 2.^{o} grau.

Seja a equação

$$ax^3 + bx^2 + cx + d = 0.$$

Então, fazendo a substituição $x = y + m$, teremos

$$a(y+m)^3 + b(y+m)^2 + c(y+m) + d = 0$$

e desenvolvendo, obtemos

$$ay^3 + y^2(b + 3am) + y(3am^2 + 2bm + c) + (m^3a + bm^2 + cm + d) = 0.$$

Assim, impondo a condição $b + 3am = 0$, tem-se

$$m = -\frac{b}{3a}$$

e a nova equação do 3.^{o} grau em y será do tipo

$$y^3 + \beta y + \gamma = 0.$$

Logo, se soubermos resolvê-la, acharemos x que é $y + m$. Portanto, quando encontrou a solução das equações do tipo

$$x^3 + \beta x + \gamma = 0$$

Tartaglia deu uma resposta geral e não apenas particular ao problema, o que aumentou seu mérito.

Agora vamos ao "segredo". Todas as grandes descobertas, invariavelmente, partem de uma ideia fundamental. Neste caso, a ideia de Tartaglia foi supor que a solução procurada era composta de parcelas. Assim, escreveu:

$$x = A + B \Rightarrow x^3 = (A+B)^3 = A^3 + B^3 + 3ABx,$$

ou seja,

$$x^3 - 3ABx - (A^3 + B^3) = 0.$$

Mas, ao mesmo tempo

$$x^3 + \beta x + \gamma = 0.$$

Portanto,

$$\left\{\begin{array}{rcl} -3AB & = & \beta \\ -(A^3+B^3) & = & \gamma, \end{array}\right.$$

ou ainda,

$$A^3B^3 = -\frac{\beta^3}{27} \text{ e } A^3+B^3 = -\gamma.$$

Logo, A^3 e B^3 são dois números dos quais conhecemos a soma e o produto que é um problema clássico que se resolve com equações do segundo grau. Portanto,

$$A^3 = -\frac{\gamma}{2} + \sqrt{\left(\frac{\gamma}{2}\right)^2 + \left(\frac{\beta}{3}\right)^3} \text{ e } B^3 = -\frac{\gamma}{2} - \sqrt{\left(\frac{\gamma}{2}\right)^2 + \left(\frac{\beta}{3}\right)^3}.$$

Como $x = A + B$, temos que

$$x = \sqrt[3]{-\frac{\gamma}{2} + \sqrt{\left(\frac{\gamma}{2}\right)^2 + \left(\frac{\beta}{3}\right)^3}} + \sqrt[3]{-\frac{\gamma}{2} - \sqrt{\left(\frac{\gamma}{2}\right)^2 + \left(\frac{\beta}{3}\right)^3}}. \tag{3.3}$$

Esta é a fórmula de Cardano, que não foi descoberta por ele, mas sim por Tartaglia.

Vejamos como funciona o método de Tartaglia, em um exemplo concreto. Considere a equação

$$x^3 - 6x - 9 = 0,$$

com $\beta = -6$ e $\gamma = -9$. Logo,

$$\begin{aligned} x &= \sqrt[3]{-\frac{9}{2} + \sqrt{\left(\frac{9}{2}\right)^2 + \left(-\frac{6}{3}\right)^3}} + \sqrt[3]{-\frac{9}{2} - \sqrt{\left(\frac{9}{2}\right)^2 + \left(-\frac{6}{3}\right)^3}} \\ &= \sqrt[3]{\frac{9}{2} + \sqrt{\frac{49}{4}}} + \sqrt[3]{\frac{9}{2} - \sqrt{\frac{49}{4}}} \\ &= \sqrt[3]{\frac{9+7}{2}} + \sqrt[3]{\frac{9-7}{2}} \\ &= \sqrt[3]{8} + \sqrt[3]{1} \\ &= 2 + 1 \\ &= 3. \end{aligned}$$

Por simples verificação, constata-se que 3, realmente, é a solução da equação e a fórmula, como esperado, funcionou.

Na fórmula (3.3), destaquemos o radicando

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

Neste ponto ocorre um fato curioso chegando a ter um aspecto paradoxal. Se $D \leq 0$, então as três raízes da equação

$$x^3 + \beta x + \gamma = 0$$

são reais. A fórmula exprime $x = A + B$ como soma de duas raízes cúbicas de números complexos. Este é chamado tradicionalmente o "caso irredutível", pois ao tentar eliminar os radicais, recai-se noutra equação do terceiro grau. Um impontante exemplo é dado pela equação

$$x^3 - 3x + 1 = 0$$

em que

$$D = -\frac{3}{4}.$$

podendo ter três raízes reais e distintas, com uma delas sendo

$$x = \sqrt[3]{-\frac{1}{2} + \frac{\sqrt{3}}{2}i} + \sqrt[3]{-\frac{1}{2} - \frac{\sqrt{3}}{2}i}.$$

Isto parece um número complexo mas, é um número real, como veremos mais adiante.

À primeira vista, achou-se que as equações do 3.^{o} grau estavam vencidas pela fórmula de Cardano (de Tartaglia!), analogamente ao que a fórmula de Bhaskara fizera com as equações do 2.^{o} grau. A mais elementar dúvida que surge naturalmente em quem observa a fórmula (3.3) é a seguinte: se a fórmula de Bhaskara exibe, de maneira tão simples, as duas raízes das equações do 2.^{o} grau, por que a Cardano só apresenta uma?

Podemos ver num exemplo em Garbi [6] que a equação

$$x^3 - 15x - 4 = 0$$

possui $x = 4$ como uma de suas raízes, entretanto, se tentarmos resolvê-la pela fórmula

(3.3), teremos

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$$

e caímos não apenas na extração de raízes quadradas de números negativos, mas também na extração de raízes cúbicas de números de natureza desconhecida. O homem que conseguiu atravessar a ponte que levava aos novos números foi Rafael Bombelli, nascido em Bolonha, Itália, em 1530 e engenheiro hidráulico por profissão. Ele era aquele tipo de pessoa, nascido para fazer História: corajoso, pertinaz e sempre disposto a pensar em coisas novas.

Os estudos de Bombelli começaram com a tentativa de conciliar o resultado fornecido pela fórmula de Cardano para a equação

$$x^3 - 15x - 4 = 0,$$

com a raiz constatada por simples observação.

Conforme ele mesmo revelou em 1572 no livro **L'Algebra parte Maggiore dell'Arithmetica**, seu método baseou-se no "pensamento rude" segundo o qual

$$\sqrt[3]{2 + \sqrt{-121}} \text{ e } \sqrt[3]{2 - \sqrt{-121}}$$

deveriam ser números da forma

$$a + \sqrt{-b} \text{ e } a - \sqrt{-b},$$

respectivamente. Assim, ele escreveu

$$\sqrt[3]{2 + \sqrt{-121}} = a + \sqrt{-b} \text{ e } \sqrt[3]{2 - \sqrt{-121}} = a - \sqrt{-b}.$$

Com alguns cálculos, obtemos $a = 2$ e $b = 1$, pois

$$(2 + \sqrt{-1})^3 = 2 + \sqrt{-121} \text{ e } (2 - \sqrt{-1})^3 = 2 - \sqrt{-121}.$$

Assim,

$$x = (2 + \sqrt{-1}) + (2 - \sqrt{-1}) = 4$$

resultado que se esperava obter.

L. Ferrari, nascido em Bolonha 1522 e falecido por volta de 1560, foi o mais famoso dos discípulos de Cardano. Oriundo da mais humilde das condições, foi trabalhar como servo na residência de Cardano quando tinha 15 anos, mas sua brilhante inteligência logo foi reconhecida pelo mestre e disto decorreu uma promoção a secretário. A partir dos 18 anos, Ferrari passou a ensinar por conta própria em Milão e, através da proteção do Cardeal de Mantova, alcançou posições que lhe proporcionaram uma boa renda. Logo após tornar-se professor de Matemática na Universidade de Bolonha, veio a falecer aos 38 anos de idade, provavelmente envenenado por sua irmã.

Dentro do costume então vigente entre os matemáticos, de proporem problemas uns aos outros como forma de desafio, um certo Zuanne de Tonini da Coi submeteu a Cardano uma questão que envolvia a equação

$$x^4 + 6x^2 - 60x + 36 = 0.$$

Após inúmeras tentativas sem êxito, Cardano passou a questão ao jovem Ferrari que, num lampejo de gênio, encontrou o método geral para a solução das equações do 4.^{o} grau.

Antes de mostrar o raciocínio seguido por Ferrari, vamos relembrar que a equação geral do 4.^{o} grau

$$ax^4 + bx^3 + cx^2 + dx + e = 0$$

sempre pode ser transformada em outra do tipo

$$y^4 + \beta y^2 + \gamma y + \delta = 0 \tag{3.4}$$

fazendo a substituição $x = y + m$ e calculando m de modo a anular o termo de 3.^{o} grau.

Ferrari olhou a equação (3.4) e procurou reagrupar os termos de modo que, nos dois membros da igualdade houvesse polinômios quadrados perfeitos. Se tal reagrupamento fosse possível, seriam extraídas as raízes quadradas, cair-se-ia em equações do 2.^{o} grau e o problema estaria resolvido.

A equação foi, então, escrita assim:

$$x^4 + (\beta + \alpha)x^2 + (\delta + \phi) = \alpha x^2 - \gamma x + \phi$$

em que α e ϕ são números a serem determinados de forma que os dois lados da igualdade sejam quadrados perfeitos. Para que isso ocorra, é necessário e suficiente que os discriminantes daqueles dois trinômios, ao mesmo tempo, sejam iguais a *zero*, ou seja,

$$(\beta+\alpha)^2 - 4(\delta+\phi) = 0 \text{ e } \gamma^2 - 4\alpha\phi = 0$$

resolvendo o sistema, temos

$$\alpha^3 + 2\beta\alpha^2 + (\beta^2 - 4\delta)\alpha - \gamma^2 = 0$$

que é uma equação do 3.^{o} grau em α. Como tais equações pode ser resolvidas, acha-se α, em seguida ϕ e extraem-se as raízes quadradas

$$\sqrt{x^4 + (\beta+\alpha)x^2 + (\delta+\beta)} = \pm\sqrt{\alpha x^2 - \gamma x + \phi}.$$

Para cada alternativa de sinal $+$ ou $-$ tem-se uma equação do 2^o grau, ambas com duas soluções. Portanto, para a equação do 4.^{o} grau, o método fornece quatro raízes, de uma forma semelhante ao que acontece na fórmula de Bhaskara. Os passos para a solução da equação geral do 4.^{o} grau são:

1. Toma-se a equação geral e faz-se uma transformação do tipo $x = y + m$ de modo a cair-se em uma equação do 4.^{o} grau em y sem o termo do 3.^{o} grau;

2. Reagrupam-se seus termos de modo a fazer com que ambos os lados da igualdade sejam quadrados perfeitos. Cai-se em uma equação do 3.^{o} grau em α. Se ela for completa, faz-se a transformação $\alpha = \alpha' + t$ de modo a obter-se uma equação do 3.^{o} grau em α', sem o termo do 2.^{o} grau;

3. Resolve-se a equação em α' pelo método de Tartaglia;

4. Soma-se t a α' e obtém-se α. Obtido α calcula-se ϕ;

5. Com α e ϕ, extraem-se as raízes quadradas dos dois lados da igualdade e obtém-se os quatro valores possíveis de y. Soma-se m a y e obtém-se as quatro raízes da equação geral.

Um método perfeito do ponto de vista teórico, mas bastante trabalhoso. O grande mérito de Ferrari foi haver demonstrado que a solução das equações do 4.^{o} grau era possível apenas com operações algébricas.

Exemplo 3.1. *Vamos aplicar o método de Ferrari na equação*

$$x^4 - 15x^2 - 10x + 24 = 0.$$

Solução. Vamos procurar encontrar α e ϕ tais que

$$x^4 - (15 - \alpha)x^2 + (24 + \phi) = \alpha x^2 + 10x + \phi$$

com ambos os lados da igualdade quadrados perfeitos. Para isto

$$(15 - \alpha)^2 - 4(24 + \phi) = 0 \text{ e } 100 - 4\alpha\phi = 0$$

dessa segunda equação isolamos

$$\phi = \frac{25}{\alpha}$$

nos levando a equação

$$\alpha^3 - 30\alpha^2 + 129\alpha - 100 = 0.$$

Esta equação, sendo do 3.^{o} grau, é solúvel algebricamente e suas raízes são

$$\alpha_1 = 1, \ \ \alpha_2 = 4 \text{ e } \alpha_3 = 25.$$

Para $\alpha_1 = 1$ e $\phi_1 = 25$, chegamos as raízes $x_1 = 4$, $x_2 = -3$, $x_3 = -2$ e $x_4 = 1$. E, de modo análogo, para $\alpha_2 = 4$, e $\phi_2 = 25/4$, obtemos $\alpha_3 = 25$ e $\phi_3 = 1$ produzem as mesmas raízes a menos da ordem. ■

A tentativa de resolver as equações de grau $n \geq 5$ fracassou. Entre 1824 e 1826, Abel conseguiu mostrar que a equação geral de grau 5 não é solúvel por radicais. Finalmente, Galois $(1811 - 1832)$ indicou critérios para uma equação qualquer ser solúvel, usando a teoria que leva seu nome, criada exatamente para esta finalidade, podendo ser encontrada em Endler [5, §9].

3.2 Método Circulante

Para ilustrar a ideia principal desta seção, consideramos o problema de encontrar expressões exatas para as raízes do polinômio

$$f(x) = x^3 + 6x^2 + 9x + 3.$$

É bastante natural tentarmos a fatoração do polinômio por algum caminho adequado, ou olhar para o teste das raízes racionais, este último sem sucesso pois os divisores de 3 são

$$\{1, -1, 3, -3\}$$

que não são raízes de f. No entanto, f é o polinômio característico de uma matriz circulante correspondente a

$$C = \begin{bmatrix} -2 & b & \bar{b} \\ \bar{b} & -2 & b \\ b & \bar{b} & -2 \end{bmatrix},$$

com $b = e^{\frac{2\pi i}{9}}$, tais que as raízes de f são os autovalores de C. E, estas, são obtidas pelas inspeções

$$q(1), \;\; q(\omega) \;\text{ e }\; q(\bar{\omega}),$$

no polinômio representante

$$q(x) = -2 + bx + \bar{b}x^2.$$

De modo mais geral, dado um polinômio f, tentaremos encontrar uma matriz circulante C, tendo f como seu polinômio característico. Em seguida, a primeira linha de C define o polinômio representante q diferente de f, e as raízes de f são obtidas através da aplicação de q nas raízes n-ésimas de unidade.

Passemos agora a exibir o processo unificado de resolução das equações polinomiais, de no máximo grau 4, via matrizes circulantes, começando pelo caso mais simples, que é o quadrático.

3.2.1 Quadráticas

Consideremos o polinômio

$$f = x^2 + \alpha x + \beta \in \mathbb{R}[x]$$

e a matriz circulante

$$C = \begin{pmatrix} a & b \\ b & a \end{pmatrix} = aI + bW.$$

O polinômio característico de C é

$$p_C(x) = \det(xI - C) = x^2 - 2ax + a^2 - b^2.$$

Desejamos encontrar a e b, para que este polinômio característico seja igual a f ou, equivalentemente, resolver o sistema não homogêneo

$$\begin{cases} -2a &= \alpha \\ a^2 - b^2 &= \beta. \end{cases}$$

Neste caso,

$$a = -\frac{\alpha}{2} \text{ e } b = \pm\sqrt{\frac{\alpha^2}{4} - \beta}.$$

Como veremos, não há perda de generalidade, em considerarmos b com o sinal positivo. Assim,

$$C = \begin{pmatrix} -\frac{\alpha}{2} & \sqrt{\frac{\alpha^2}{4} - \beta} \\ \sqrt{\frac{\alpha^2}{4} - \beta} & -\frac{\alpha}{2} \end{pmatrix} \text{ e } q(x) = -\frac{\alpha}{2} + x\sqrt{\frac{\alpha^2}{4} - \beta}.$$

Sendo

$$W = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

temos que $x^2 - 1 = 0$ é a equação característica de W. Logo,

$$1 \text{ e } -1$$

são as raízes da unidade (autovalores de W). Portanto,

$$q(1) = -\frac{\alpha}{2} + \sqrt{\frac{\alpha^2}{4} - \beta} \text{ e } q(-1) = -\frac{\alpha}{2} - \sqrt{\frac{\alpha^2}{4} - \beta}$$

são as raízes de f (autovalores de C). Observe que se definirmos b com o sinal negativo, então obtemos as mesmos raízes de f, embora os valores de $q(1)$ e $q(-1)$ são permutados.

Exemplo 3.2. *Considere o polinômio* $f(x) = x^2 - 5x + 6 \in \mathbb{R}[x]$.

Solução. É claro que 2 e 3, são as raízes de f. Mas, vamos utilizar o método das circulantes para obtê-las. Consideremos a matriz circulante

$$C = \begin{pmatrix} a & b \\ b & a \end{pmatrix} = aI + bW.$$

tal que $p_C = f$. Assim, as raízes de f serão os autovalores da matriz C. Neste caso,

$$p_C(x) = \det(xI - C) = (x-a)^2 - b^2 = x^2 - 2ax + a^2 - b^2.$$

Logo,

$$x^2 - 2ax + a^2 - b^2 = x^2 - 5x + 6 \Leftrightarrow a = \frac{5}{2} \text{ e } b = \frac{1}{2}.$$

Portanto,

$$C = \begin{pmatrix} \frac{5}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{5}{2} \end{pmatrix} \text{ e } q(x) = \frac{5}{2} + \frac{1}{2}x.$$

Consequentemente,

$$q(1) = \frac{5}{2} + \frac{1}{2} = 3 \text{ e } q(-1) = \frac{5}{2} - \frac{1}{2} = 2$$

são as raízes de f. ■

3.2.2 Cúbicas

Consideremos o polinômio

$$f = x^3 + \alpha x^2 + \beta x + \gamma \in \mathbb{R}[x]$$

e a matriz circulante

$$C = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} = aI + bW + cW^2.$$

O polinômio característico de C é

$$p_C(x) = \det(xI - C) = (x-a)^3 - 3bc(x-a) - (b^3 + c^3).$$

Esta expressão sugere a mudança de variável

$$y = x - a,$$

a qual transforma p_C em um polinômio sem o termo de grau 2 em y. Veremos que o desenvolvimento via matriz circulante inspira, de uma forma muito natural, um passo preliminar na solução tradicional da cúbica através de uma mudança linear de variáveis na eliminação do termo quadrático. Mais geralmente, seja

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

Então a mudança linear

$$y = x - \frac{a_{n-1}}{n}$$

elimina o termo de grau $(n-1)$, apenas usando operações algébricas elementares.

No contexto de matrizes circulantes ganhamos uma nova maneira de pensar sobre este resultado. Para ver isto, seja f o polinômio característico da matriz C. Então a soma das raízes é a soma dos autovalores, isto é, o *traço* de C. Assim, eliminar o termo de grau $(n-1)$ é equivalente ao traço de C ser igual zero, em símbolos, $\mathrm{tr}(C) = 0$.

Note que como uma matriz circulante C possui a diagonal principal constante, digamos

a. Então

$$\mathrm{tr}(C) = na \Rightarrow a = -\frac{a_{n-1}}{n}.$$

Isto nos dá duas conclusões: primeiro, a, determina um dos parâmetros da matriz circulante (e o termo constante do polinômio representante q). Segundo tal, como no caso da cúbica,

$$y = x - a = x - \frac{a_{n-1}}{n}$$

é a mudança linear que elimina o termo de grau $(n-1)$. Estas observações indicam que, uma mudança linear de variáveis pode ser sempre realizada para eliminar o termo de grau $(n-1)$ de um polinômio geral de grau n. Daqui em diante, suponhamos que tal mudança linear já foi feita.

Retornaremos ao caso cúbico. Sejam

$$f(x) = x^3 + \beta x + \gamma$$

e a matriz circulante

$$C = \begin{pmatrix} 0 & b & c \\ c & 0 & b \\ b & c & 0 \end{pmatrix} = bW + cW^2.$$

O polinômio característico de C é

$$p_C(x) = \det(xI - C) = x^3 - 3bcx - b^3 - c^3.$$

Desejamos encontrar b e c, para que este polinômio característico seja igual a f ou, equivalentemente, resolver o sistema não homogêneo

$$\begin{cases} 3bc & = & -\beta \\ b^3 + c^3 & = & -\gamma. \end{cases} \tag{3.5}$$

Elevando ao cubo a primeira equação em (3.5), obtemos

$$\begin{cases} b^3c^3 & = & -\frac{\beta^3}{27} \\ b^3 + c^3 & = & -\gamma \end{cases}.$$

Observe, desse modo, que b^3 e c^3 são as raízes da equação

$$z^2 + \gamma z - \frac{\beta^3}{27} = 0,$$

a qual denomina-se *resolvente quadrática* da cúbica. Tais raízes são dadas por

$$-\frac{\gamma}{2} \pm \sqrt{\frac{\gamma^2}{4} + \frac{\beta^3}{27}}. \tag{3.6}$$

Neste ponto é tentador escrever

$$b = \sqrt[3]{-\frac{\gamma}{2} + \sqrt{\frac{\gamma^2}{4} + \frac{\beta^3}{27}}} \quad \text{e} \quad c = \sqrt[3]{-\frac{\gamma}{2} - \sqrt{\frac{\gamma^2}{4} + \frac{\beta^3}{27}}}. \tag{3.7}$$

Assim,

$$C = \begin{pmatrix} 0 & b & c \\ c & 0 & b \\ b & c & 0 \end{pmatrix} \text{ e } q(x) = bx + cx^2.$$

Como

$$W = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

temos que $x^3 - 1 = 0$ é a equação característica de W. Logo,

$$1, \;\; \omega \text{ e } \bar{\omega}$$

são as raízes da unidade (autovalores de W). Portanto,

$$q(1), \;\; q(\omega) \text{ e } q(\bar{\omega})$$

são raízes de f (autovalores de C).

Na verdade, as igualdades em (3.7), são perfeitamente válidas quando todas as operações envolvem apenas os números reais. Num domínio maior, dos números complexos, existe alguma ambiguidade associada com a extração de raízes quadradas e cúbicas. Neste caso, definimos b por (3.7), usando qualquer um dos valores da raiz quadrada e cúbica, e, em seguida, tomar

$$c = -\frac{\beta}{3b}.$$

Isso produz uma solução de (3.5), nos levando para as raízes de f como já foi explicado. Todas as opções para b resultam nas mesmas raízes.

3.2.3 Quárticas

Para completar esta parte do trabalho, destacaremos a equação quártica. O ponto de partida é o polinômio do 4.^{o} grau

$$f = x^4 + \beta x^2 + \gamma x + \delta \in \mathbb{R}[x],$$

e para evitar um caso trivial, vamos assumir que nem todos os coeficientes sejam nulos. Consideremos a matriz circulante

$$C = \begin{pmatrix} 0 & b & c & d \\ d & 0 & b & c \\ c & d & 0 & b \\ b & c & d & 0 \end{pmatrix} = bW + cW^2 + dW^3.$$

O polinômio característico de C é

$$p_C(x) = x^4 - (4bd + 2c^2)x^2 - 4c(b^2 + d^2)x + c^4 - b^4 - d^4 - 4bdc^2 + 2b^2d^2.$$

Igualando este a f produz o sistema não homogêneo

$$\begin{cases} 4bd + 2c^2 &= -\beta \\ 4c(b^2 + d^2) &= -\gamma \\ c^4 - b^4 - d^4 - 4bdc^2 + 2b^2d^2 &= \delta \end{cases} \tag{3.8}$$

A partir das duas primeiras equações desse sistema vamos determinar bd e $b^2 + d^2$ em função de c. Nos inspirando reescrever a terceira equação da forma

$$c^4 - (b^2 + d^2)^2 + 4(bd)^2 - 4bdc^2 = \delta$$

e, consequentemente, obter uma equação em c:

$$c^4 - \frac{\gamma^2}{16c^2} + \frac{(\beta + 2c^2)^2}{4} + (2c^2 + \beta)c^2 = \delta.$$

Simplificando-se, teremos

$$c^6 + \frac{\beta}{2}c^4 + \left(\frac{\beta^2}{16} - \frac{\delta}{4}\right)c^2 - \frac{\gamma^2}{64} = 0, \tag{3.9}$$

que é uma equação polinomial cúbica em c^2 (conhecida como *resolvente cúbica*), e, em princípio, é solúvel através dos métodos já vistos. Isto leva a um valor diferente de zero para c (uma vez que os coeficientes β, γ e δ não são todos nulos), em seguida, encontramos valores correspondentes para b e d, de modo que (3.8) seja satisfeito. Desta forma, construímos a matriz circulante

$$C = bW + cW^2 + dW^3 = q(W).$$

Assim,

$$C = \begin{pmatrix} 0 & b & c & d \\ d & 0 & b & c \\ c & d & 0 & b \\ b & c & d & 0 \end{pmatrix} \text{ e } q(x) = bx + cx^2 + dx^3.$$

Como

$$W = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

temos que $x^4 - 1 = 0$ é a equação característico de W. Logo,

$$1, -1, \ i \ \text{ e } \ -i$$

são as raízes da unidade (autovalores de W). Portanto,

$$q(1) = b + c + d, q(-1) = -b + c - d, q(i) = -c + i(b - d) \ \text{ e } \ q(-i) = -c - i(b - d)$$

são as raízes de f (autovalores de C). Isso completa a solução da quártica, e a abordagem "circulante" para resolver equações polinomiais de grau pequeno.

3.3 Raízes Reais

Concluiremos este trabalho com uma discussão de quais critérios para equações cúbicas ou quárticas com coeficientes reais devam possuir para que todas as raízes sejam reais. Sabemos que estes polinômios são caracterizados pela condição de que a circulante correspondente seja Hermitiana, e que por sua vez leva a condições sobre os coeficientes do polinômio.

Uma questão conexa diz respeito à polinômios com coeficientes racionais e raízes racionais. O caso especial em que todas as entradas na circulante correspondente também são racionais foi discutido em Bridges [3]. Para que não haja um desvio dos nossos objetivos neste trabalho, podemos afirmar o resultado para o caso cúbico: os coeficientes, as raízes e a matriz circulante são todos racionais:

$$x^3 + \beta x + \gamma = 0 \Leftrightarrow 27\gamma^2 + 4\beta^3 = 0.$$

Vamos prosseguir com a discussão sobre raízes reais. Um polinômio com coeficientes reais possui raízes reais se, e somente se, existir uma matriz circulante Hermitiana. Para a cúbica

$$f(x) = x^3 + \beta x + \gamma,$$

a circulante associada

$$\begin{bmatrix} 0 & b & c \\ c & 0 & b \\ b & c & 0 \end{bmatrix}$$

é Hermitiana precisamente quando b e c são complexos conjugados e, consequentemente, quando b^3 e c^3 são complexos conjugados.

Agora, a equação (3.6) garante que

$$27\gamma^2 + 4\beta^3 \leq 0$$

é uma condição necessária e suficiente para que b e c sejam conjugados. Neste caso,

$$f \text{ possui três raízes reais} \Leftrightarrow 27\gamma^2 + 4\beta^3 \leq 0.$$

Existe uma interpretação geométrica interessante de localizar as raízes quando todas são reais. Como $c = \bar{b}$ temos que as raízes

$$q(1) = b + \bar{b}, \;\; q(\omega) = \omega b + \bar{\omega}\bar{b} \text{ e } q(\bar{\omega}) = \bar{\omega} b + \omega\bar{b},$$

são as *partes reais* de três pontos igualmente espaçados em torno de um círculo no plano complexo. Na verdade, fazendo $h = 2b$, as raízes da cúbica são as partes reais de

$$h, \;\; \omega h \text{ e } \bar{\omega} h,$$

respectivamente, e estes são igualmente distribuídos em torno do círculo $|z| = |h|$. Então, geometricamente, podemos encontrar as raízes da seguinte forma: dobramos b e o localizamos no plano complexo. A partir daí construímos um triângulo equilátero tendo $2b$ como um de seus vértices e centro na origem. Em seguida projetamos os vértice no eixo real. Esta construção está ilustrada na Figura (3.1). Embora esta construção é aplicável

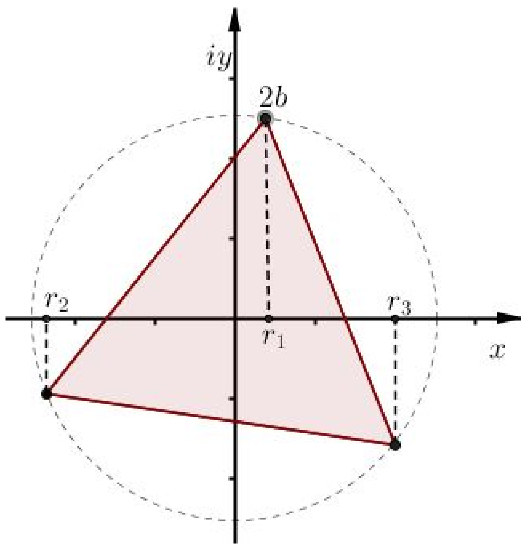


Figura 3.1: Representação gráfica das raízes de f.

no caso especial de um cúbico (sem termo quadrático), o caso geral é essencialmente o mesmo, pois os polinômios do tipo

$$f(x) = x^3 + \alpha x^2 + \beta x + \gamma$$

podem ser transformados em

$$\tilde{f}(x) = x^3 + \tilde{\beta} x + \tilde{\gamma}$$

como já vimos na Seção 3.1 deste capítulo, onde as raízes ficam transladadas de $\frac{\alpha}{3}$. As raízes de f, são ainda projeções dos vértices do referido triângulo, mas com centro é $-\frac{\alpha}{3}$, em vez da origem.

Para a quártica

$$f(x) = x^4 + \beta x^2 + \gamma x + \delta,$$

vamos supor, como antes que nem todos os coeficientes sejam iguais a zero. A circulante é

$$\begin{bmatrix} 0 & b & c & d \\ d & 0 & b & c \\ c & d & 0 & b \\ b & c & d & 0 \end{bmatrix}$$

que é Hermitiana apenas quando $d = \bar{b}$ e c é real. Agora, qualquer solução para (3.8) produz uma circulante com polinômio característico f. Após a análise anterior, uma tal solução pode ser construída usando qualquer valor para c satisfazendo (3.9). Por conseguinte, a fim de que todas as raízes de f sejam reais e, consequentemente, para todos as circulantes correspondentes serem Hermitianas, é necessário que todas as raízes da equação (3.9) sejam reais. A equação (3.9) é cúbica em c^2, a condição necessária para esta redução é que a cúbica.

$$x^3 + \frac{\beta}{2} x^2 + \left(\frac{\beta^2}{16} - \frac{\delta}{4} \right) x - \frac{\gamma^2}{64} = 0, \tag{3.10}$$

deve ter todas as raízes reais não negativas. Por outro lado, se (3.10) tem todas as raízes reais não negativas, então f tem todas as raízes reais. Isso pode ser comprovado utilizando matrizes circulantes através da construção de uma solução do sistema (3.8) para o qual a circulante correspondente é Hermitiana. A conclusão final, em qualquer caso, é a seguinte caracterização: as raízes de f são todas reais se, e somente se, (3.10) tem todas as raízes reais não negativas.

Mostramos como a abordagem via circulantes compara com abordagens familiares para equações cúbicas e quárticas. A nova perspectiva fornecida por circulantes não só fornece soluções unificadas das equações, mas também oportuniza uma nova maneira de olhar para questões conexas, incluindo a eliminação do termo de grau $(n-1)$ e caracterizam equações com raízes reais. Desse modo a abordagem circulante se coloca num cenário geral.

Para ilustrar a "interpretação geométrica agradável dos locais das raízes quando todas são reais", faremos um exemplo completo.

Exemplo 3.3. *Vamos considerar o polinômio* $f = x^3 + 6x^2 + 9x + 3 \in \mathbb{R}[x]$ *e analisá-lo via circulantes.*

Solução. Já vimos que a mudança de variáveis

$$x = y - 2$$

elimina o termo do segundo grau, nos levando ao polinômio reduzido

$$f(y-2) = y^3 - 3y + 1,$$

que reescrevê-lo na indeterminada x, ficando com

$$g(x) = \tilde{f}(x) = x^3 - 3x + 1,$$

cujo gráfico fica transladado duas unidades para direita. Veja a Figura (3.2).

O gráfico $\tilde{f}$ (construído com o sofware GEOGEBRA) nos mostra de imediato que ele possui três raízes reais. Porém, vamos usar o método circulante para encontrar uma expressão que nos dê as raízes de $\tilde{f}$ como os autovalores da circulante $C = \mathrm{circ}\{(0, b, c)\}$. O polinômio característico de C é

$$p_C(x) = x^3 - 3abx - (b^3 + c^3).$$

Logo, devemos resolver o sistema de equações em b e c gerado pela igualdade $\tilde{f}(x) = p_C(x)$

ou $g(x) = p_C(x)$, ou seja,

$$\left\{\begin{array}{rcr} 3bc & = & 3 \\ b^3 + c^3 & = & -1 \end{array}\right. \Rightarrow \left\{\begin{array}{rcr} b^3c^3 & = & 1 \\ b^3 + c^3 & = & -1 \end{array}\right.$$

fazendo $b^3 = z$, temos que b^3 e c^3 são as raízes da resolvente

$$z^2 + z + 1 = 0,$$

com

$$z_1 = e^{\frac{2\pi i}{3}} \text{ e } z_2 = \bar{z}_1.$$

Como $b = \sqrt[3]{z}$ temos que

$$b_k = e^{\left(\frac{2\pi}{9} + \frac{2k\pi}{3}\right)i}, \;\; k = 0, 1, 2.$$

Tomemos

$$b = e^{\frac{2\pi i}{9}},$$

pois para qualquer k escolhido, as raízes de $\tilde{f}$ são as mesmas. O fato de $b = \bar{c}$, ou seja,

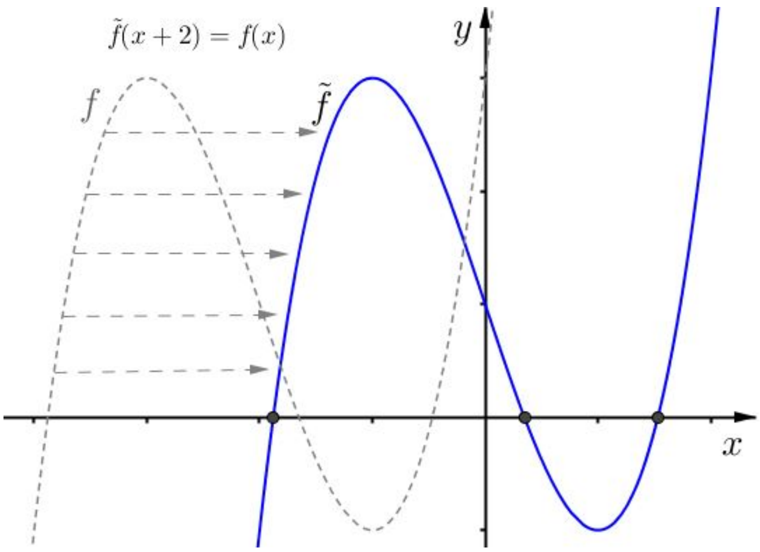


Figura 3.2: Representação gráfico de $\tilde{f}$.

b e c são complexas conjugadas, nos leva a concluir que a circulante $C = \text{circ}\{(0, b, \bar{b})\}$ é Hermitiana. Além disso,

$$27 \cdot 1^2 + 4 \cdot (-3)^3 = -81 < 0$$

é condição necessária e suficiente para que $\tilde{f}$ possua todas as suas raízes reais.

A interpretação geométrica que se refere às raízes reais, nos diz que: quando $c = \bar{b}$, as raízes

$$\tilde{q}(1), \ \ \tilde{q}(\omega) \ \text{e} \ \ tildeq(\bar{\omega})$$

são partes reais de três pontos igualmente espaçados em torno de um círculo de raio 2 centrado na origem do plano complexo como mostra a Figura (3.3). De fato, o representante de C é

$$\tilde{q}(x) = bx + \bar{b}x^2 \ \text{e} \ \omega_k = e^{\frac{2k\pi}{3}i}, \ \text{com} \ k = 0, 1, 2$$

nos fornece

$$\tilde{q}(\omega_k) = 2\mathrm{Re}(b\omega_k),$$

pois $\omega^2 = \bar{\omega}$. Logo, basta fazer $h = 2b$ e observar que as raízes de $\tilde{f}$ são as partes reais dos complexos h, ωh e $\bar{\omega}h$. Escrevemos

$$\tilde{q}(x) = e^{\frac{2\pi i}{9}}x + e^{-\frac{2\pi i}{9}}x^2$$

obtemos as raízes

$$\begin{aligned} \tilde{q}(1) &= 2\cos\left(\frac{2\pi}{9}\right) \approx 1,5321; \\ \tilde{q}(\omega) &= 2\cos\left(\frac{8\pi}{9}\right) \approx -1,8793 \ \text{e} \\ \tilde{q}(\bar{\omega}) &= 2\cos\left(\frac{14\pi}{9}\right) \approx 0,3472. \end{aligned}$$

Portanto, as raízes de f são dadas por

$$q(x) = -2 + e^{\frac{2\pi i}{9}}x + e^{-\frac{2\pi i}{9}}x^2,$$

ou seja,

$$
\begin{aligned}
q(1) &= -2+2\cos\left(\frac{2\pi}{9}\right) \approx -0,4679;\\
q(\omega) &= -2+2\cos\left(\frac{8\pi}{9}\right) \approx -3,8793 \text{ e}\\
q(\bar{\omega}) &= -2+2\cos\left(\frac{14\pi}{9}\right) \approx -1,6528,
\end{aligned}
$$

que é o resultado desejado. ■

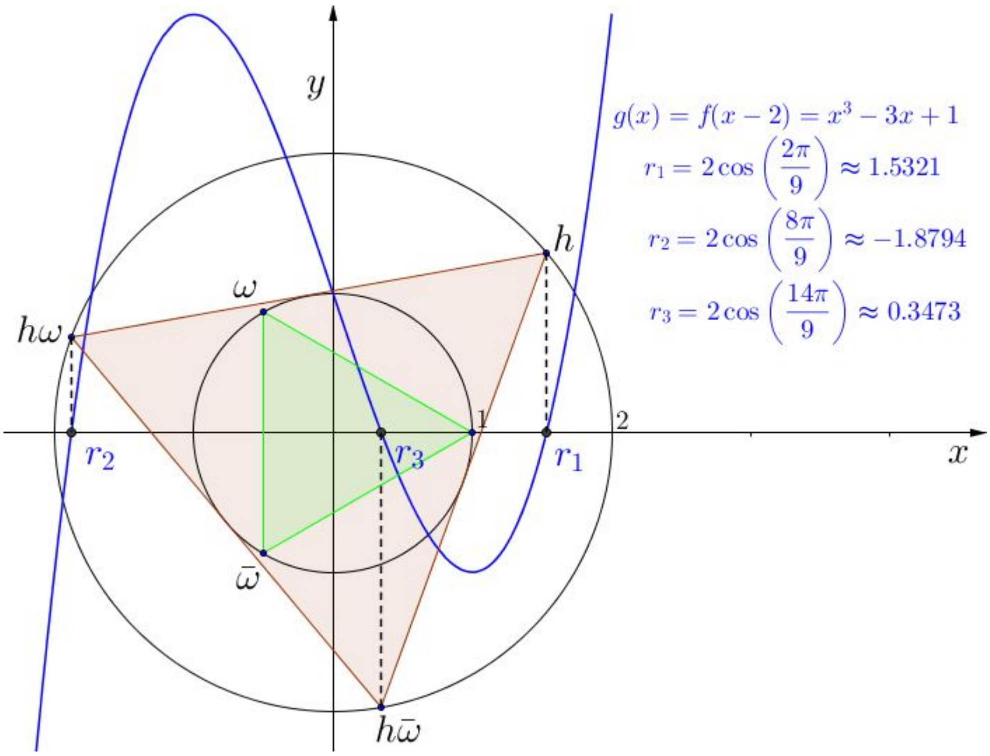


Figura 3.3: Interpretação geométrica das raízes de g.

Apêndice A

Biografias

A.1 Girolamo Cardano

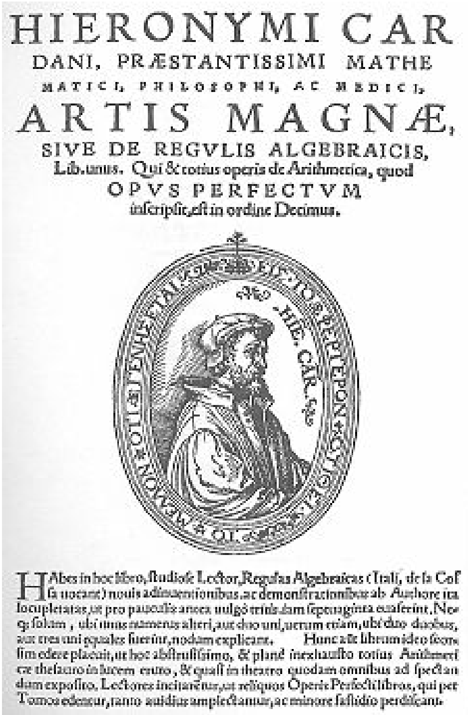
Figura A.1: Girolamo Cardano

Girolamo Cardano, nascido em Paiva em 1501 e falecido em Roma em 1576, o mínimo a ser dito é que levou uma vida marcada por contrastes e extremos. Excepcional cientista, dedicou-se também à Astrologia. Protegido do Papa Gregório XIII, acabou acusado de heresia por haver divulgado o horóscopo de Jesus Cristo. Astrólogo do Vaticano, escreveu um livro louvando a Nero, o grande perseguidor de cristãos do Império Romano. Autor do LIBER DE LUDO ALEAE, onde brilhantemente introduziu a ideia de probabilidade que se usa modernamente, ali também ensinou maneiras de se trapacear nos jogos.

Filho ilegítimo de um advogado de Milão, professor em Bolonha, Pavia e Milão, constituiu uma família absolutamente desagregada. Seu filho mais velho foi condenado à morte por haver assassinado a esposa. De seu mais novo, Cardano, num acesso de fúria, arrancou as duas orelhas. Em um documento por ele mesmo redigido, definiu-se como desbocado, espião, melancólico, traidor, invejoso, solitário, obsceno, desonesto, incomparavelmente vicioso e portador de total desprezo pela religião.

Apesar destes traços pessoais nada significantes, Cardano legou à posteridade um livro que, à época, era sem dúvida o maior compêndio algébrico existente: a ARTIS MAGNAE

SIVE DE REGULIS ALGEBRAICIS, mais conhecida por ***Ars Magna***, publicada em Nurenberg, na Alemanha, em 1545.



HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui & totius operis de Arithmetica, quod
OPVS PERFECTVM
inscripsit, est in ordine Decimus.

HAbes in hoc libro, studiose Lector, Regulas Algebraicas (Itali, de la Cossa vocant) nouis adinuentionibus, ac demonstrationibus ab Authore ita locupletatas, ut pro pauculis antea uulgò tritis, iam septuaginta euaserint. Neq; solum, ubi unus numerus alteri, aut duo uni, uerum etiam, ubi duo duobus, aut tres uni æquales fuerint, nodum explicant. Hunc aũt librum ideo seorsim edere placuit, ut hoc abstrusissimo, & planè inexhausto totius Arithmeticæ thesauro in lucem eruto, & quasi in theatro quodam omnibus ad spectandum exposito, Lectores incitarentur, ut reliquos Operis Perfecti libros, qui per Tomos edentur, tanto auidius amplectantur, ac minore fastidio perdiscant.

Figura A.2: Frontispício da célebre Ars Magna (1545), de Cardano

A.2 Nicolò Fontana

Figura A.3: Tartaglia

Nicolò Fontana, apelidado Tartaglia, em comum com Cardano só tinha o talento matemático e a nacionalidade italiana. Nascido em Bréscia, em 1501, desde a infância teve a vida marcada pelo infortúnio, pelas lutas, pelas asperezas e por toda a sorte de dificuldades. Aos onze anos, em 1512, Bréscia foi tomada pelas tropas francesas comandadas por Gaston de Foix. Parte da população, inclusive mulheres e crianças, refugiou-se na igreja. Impiedosamente, cavalarianos invadiram o local sagrado, chacinando indiscriminadamente quem encontraram pela frente. Diante da própria mãe, o menino Nicolò foi gravemente ferido por golpes de sabre e abandonado moribundo entre cadáveres. Contam os relatos que a aflita mãe, mulher humilde e paupérrima, salvou-o lambendo-lhes as feridas, à falta de qualquer medicamento. Do triste incidente, Nicolò levou para o resto da vida uma profunda cicatriz na boca, o que lhe provocou permanentemente defeito na fala, daí o apelido Tartaglia, que quer dizer gago. "Se minha barba não escondesse minhas cicatrizes, eu parecia um mostro", escreveu ele, anos depois, em um dos seus livros.

A despeito de infância tão amarga, Tartaglia desde cedo demonstrou grande amor pelos estudos e infinita vontade de aprender. Entretanto, mal começou a ser alfabetizado, sua mãe retirou-o da escola por absoluta impossibilidade de pagá-la. Tartaglia passou então a estudar por si mesmo, nos raros livros que conseguia obter aqui e ali. Sem dinheiro para comprar papel, pena e tinta, dirigia-se à noite ao cemitério, onde escrevia com carvão sobre as lápides dos túmulos. Através deste caminho espinhoso, Tartaglia construiu sua cultura e, em 1535, encontramo-lo a ganhar o sustento como professor de ciência em Verona, Vicenza, Bréscia e Veneza. Ao longo da vida publicou diversas obras, utilizando o cognome Tartaglia, e foi o primeiro, cerca de 100 anos antes de Galileu, a realizar cálculos na técnica da artilharia. Mas o que o colocou definitivamente nos anais da Matemática foram suas disputas com Cardano sobre as equações do 3º grau.

Apêndice B

Álgebra

B.1 Elementos de Álgebra

Definição B.1. *$(A, +, \cdot)$ é um anel se são verificadas as seguintes propriedades, quaisquer que sejam $a, b, c \in A$.*

A_1) $(a + b) + c = a + (b + c)$, $\forall a, b, c \in A$.

A_2) $\exists 0 \in A$; $a + 0 = 0 + a = a$.

A_3) $\forall x \in A$, *existe um único* $y \in A$, *denotado por* $y = -x$, *tal que* $x + y = y + x = 0$.

A_4) $a + b = b + a$.

A_5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

A_6) $a \cdot (b + c) = a \cdot b + a \cdot c$

Definição B.2. *Se um anel $(A, +, \cdot)$ satisfaz a propriedade:*

A_7) $\exists 1 \in A$, $0 \neq 1$ *tal que* $x \cdot 1 = 1 \cdot x = x$, $\forall x \in A$ *dizemos que* $(A, +, \cdot)$ *é um anel com unidade 1.*

Definição B.3. *Se um anel $(A, +, \cdot)$ satisfaz a propriedade:*

A_8) $\forall x, y \in A$, $x \cdot y = y \cdot x$, *dizemos que* $(A, +, \cdot)$ *é um anel comutativo.*

Definição B.4. *Se um anel $(A, +, \cdot)$ satisfaz a propriedade:*

$A_9)$ $\forall x, y \in A$, $x \cdot y = 0 \Rightarrow x = 0$ *ou* $y = 0$, *dizemos que* $(A, +, \cdot)$ *é um anel sem divisores de zero.*

Definição B.5. *Se* $(A, +, \cdot)$ *é um anel comutativo, com unidade e sem divisores de zero, dizemos que* $(A, +, \cdot)$ *é um Domínio de Integridade.*

Definição B.6. *Se o Domínio de Integridade* $(A, +, \cdot)$ *satisfaz a propriedade:*

$A_{10})$ $\forall x \in A$, $x \neq 0, \exists y \in A$ *tal que* $x \cdot y = y \cdot x = 1$, *dizemos que* $(A, +, \cdot)$ *é um corpo e comumente denotamos por* $\mathbb{K}$

Definição B.7. *Dado um corpo* $\mathbb{K}$, *dizemos que* $\mathbb{E}$ *é uma extensão de* $\mathbb{K}$ *e denotamos por* $(\mathbb{E}/\mathbb{K})$, *se* $\mathbb{K}$ *é um subcorpo de* $\mathbb{E}$, *isto é, se* $\mathbb{K}$ *é subconjunto de* $\mathbb{E}$ *e é fechado em relação aos inversos e às operações de corpo.*

Definição B.8. *Sejam* G *e* G' *grupos munidos da operação* $*$ *e* $\varphi : G \longrightarrow G'$ *uma função de* G *em* G'. *Dizemos que* φ *é um homomorfismo se*

$$\varphi(x * y) = \varphi(x) * \varphi(y), \forall x, y \in G.$$

Definição B.9. *Se o homomorfismo* $\varphi : G \longrightarrow G'$ *for bijetivo dizemos que* φ *é um isomorfismo e neste caso dizemos que* G *é isomorfo a* G' *e denotamos por* $G \simeq G'$.

Referências Bibliográficas

[1] Boyer, C. B., *História da Matemática* (Ed. Blücher Ltda., Editora da USP, São Paulo, 1974).

[2] Boldrini, J. L. [et al], *Álgebra Linear*, (Editora HARBRA Ltda, UNICAMP, São Paulo, 1980).

[3] Bridges, W. G. and Mena, R. A., "Rational Circulants with rational spectra and cyclic strongly regular graphs," (*Ars Combin.*, 1979 [143-161]).

[4] Catalan, E. "Recherches sur les Déterminants." *Bulletin de l'Académie Royale de Belgique* (2e série) 13 (1846), 534-555.

[5] Endler, O., *Teoria dos Corpos*, (Monog. de Matemática Nº 44, IMPA, 1987).

[6] Garbi, G. G., *O Romance das Equações Algébricas* (Ed. Livraria da Física, São Paulo, 2007).

[7] Geller, D., Kra, I., Popescu, S., Simanca, S.: "On circulant matrices." (Preprint, *Stony Brook University*, 2012)

[8] Hoffman, K. e Kunze, R., *Álgebra Linear*, (Editora Polígono, São Paulo, 1971).

[9] Kalman, D., White, J. E.: "Polynomial Equation and Curculant Matrices." (*The American Mathematical Monthly*, Vol. 108, No. 9 (Nov., 2001), pp. 821 - 840).

[10] Lima, E. L., *Meu Professor de Matemática e Outras Histórias*, (Editora da SBM, Rio de Janeiro, 1991).

[11] Lipschutz, S., *Álgebra Linear*, (Editora McGraw-Hill do Brasil Ltda, Rio de Janeiro, 1971).

[12] Silva, A. de A. e, *Álgebra Linear*, (Editora Universitária/UFPB, 2007).

[13] Ungar, A. A., "A unified approach for solving quadratic, cubic and quartic equations by radicals," (*Int. J. Comp. Math. Appl.*, 19 (1990), pp. 33–39)