UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

CHRISTIANO DE ALMEIDA SALES

POLINÔMIOS COM RAÍZES NO CÍRCULO UNITÁRIO

FORTALEZA
2017

CHRISTIANO DE ALMEIDA SALES

POLINÔMIOS COM RAÍZES NO CÍRCULO UNITÁRIO

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de Concentração: Ensino de Matemática.

Orientador: Prof. Dr. José Alberto D. Maia.

FORTALEZA

2017

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

S155p Sales, Christiano de Almeida.
Polinômios com raízes no círculo unitário / Christiano de Almeida Sales. – 2017.
45 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2017.
Orientação: Prof. Dr. José Alberto Duarte Maia.

1. Polinômios. 2. Equações Algébricas. 3. Raízes no Círculo Unitário. I. Título.

CDD 510

CHRISTIANO ALMEIDA SALES

POLINÔMIOS COM RAÍZES NO CÍRCULO UNITÁRIO

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática. Área de Concentração: Ensino de Matemática.

Trabalho aprovado em 30 de agosto de 2017.

BANCA EXAMINADORA

Prof. Dr. José Alberto Duarte Maia (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. José Valter Lopes Nunes
Universidade Federal do Ceará (UFC)

Prof. Dr. Francisco Régis Vieira Alves
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

Dedico este trabalho aos meus queridíssimos pais, Jaime e Regina, e às minhas preciosíssimas avós, Diva e Lourdes.

AGRADECIMENTOS

Agradeço aos meus estimados pais pela valiosa educação, reconfortante amparo e entusiasmado incentivo ao longo de minha caminhada.

Agradeço à minha amada esposa Laís e aos meus queridos filhos Gabriel e Miguel que restauraram meu ânimo em momentos cruciais e me fizeram seguir em frente.

Agradeço a todos os professores e colegas de turma que contribuíram na minha formação,

Agradeço de modo muito especial ao dileto Prof Dr Alberto Maia que de forma paciente mitigou alguns entraves na elaboração desse trabalho e demonstrou notável atenção quando solicitado, se empenhando em colaborar para o meu amadurecimento como matemático. Ao senhor, reservo sincera admiração e respeito, pois encontrou o equilíbrio de exigir de mim para que desenvolvesse e me proporcionou a orientação adequada para que lograsse êxito.

Agradeço a Deus e à Nossa Senhora por todas as bençãos a mim concedidas.

Para que serve a Matemática?

"Existe um fluxo de ideias que acontecem e criam descobertas que vão ajudar alguém em algum determinado campo. Muitas vezes há algo que vem à tona e acaba sendo o que faltava para alguém resolver um problema concreto. Às vezes, a pessoa que usa uma máquina vê um problema matemático que vai acabar sendo a diversão de um matemático abstrato que nem liga para máquinas. A Matemática permeia a descoberta em Física e em outras áreas."

(ARTUR ÁVILA).

RESUMO

O objetivo deste trabalho é caracterizar os polinômios em Q[x] que possuem raízes no círculo untário. A partir dessa caracterização vamos estimar quantas são essas raízes. Para tanto, vamos estabelecer uma correspondência entre a família de polinômios palindrômicos $P(x)$ de grau $2m$ e suas respectivas transformadas de Chebyshev. Isso permitirá relacionar a quantidade de raízes de $P(x)$ no círculo unitário com a quantidade de raízes reais da transformada de Chebyshev de $P(x)$ no intervalo [-2,2]. Por fim, com o auxílio da Regra dos Sinais de Descartes, estimaremos a quantidade de raízes da transformada de Chebyshev no referido intervalo. Este trabalho foi norteado pelo artigo de título: "Roots in unity circle" do autor Keith Conrad.

Palavras-chave: Polinômios. Equações Algébricas. Raízes no Círculo Unitário.

ABSTRACT

The objective of this work is to characterize the polynomials in mathbb Q [x] that have roots in the unary circle. From this characterization we will estimate how many are these roots. For this, we will establish a correspondence between the family of palindromic polynomials $P(x)$ of degree $2m$ and their respective Chebyshev transformations. This will allow to relate the number of roots of $P(x)$ in the unit circle with the quantity of real roots of the Chebyshev transform of $P(x)$ in the interval [-2,2]. Finally, with the aid of the Descartes Rule of Signals, we will estimate the amount of roots of the Chebyshev transform in the said range. This work was guided by the title article: "Roots in unity circle" by author Keith Conrad.

Key words:: Polynomials. Algebraic Equations. Roots in the Unit Circle.

SUMÁRIO

1 INTRODUÇÃO

No século XVI na Itália, surgiram as primeiras ideias de números complexos, isso possibilitou o estudo de equações cujas soluções, em época anterior, eram ditas inexistentes.

A partir de então, alguns matemáticos se ocuparam em desbravar essa nova seara e ampliaram as contribuições algébricas e geométricas desses novos números. Graças a esses avanços, hoje nos são completamente entendidas as soluções de equações do tipo $x^n - 1 = 0$, cujas raízes são vértices de um polígono regular de n lados, inscrito no círculo unitário, e são chamadas de raízes n-ésimas da unidade.

Nesse amadurecimento algébrico e geométrico dos números complexos, destaca-se uma importante contribuição dada pelo matemático alemão Johann Carl Friedrich Gauss expressa em sua tese de doutorado. Referimo-nos ao famoso Teorema Fundamental da Álgebra. Esse Teorema permitiu um estudo mais rigoroso e amplo das equações polinomiais.

Embora o referido teorema tenha resolvido o problema da existência de soluções, não há uma indicação de como tais soluções podem ser encontradas. De fato, o problema da inexistência de fórmulas de resoluções para equações gerais de grau maior ou igual a 5, só foi resolvido graças aos trabalhos dos matemáticos Niels Abel e Évariste Galois.

Nesse trabalho, vamos considerar o problema de localizar as raízes de uma equação polinômial no plano complexo. Mais específicamente, nosso objetivo é estudar os polinômios em $\mathbb{Q}[x]$ que possuem raízes no círculo unitário. Para isso, mostrar que um polinômio irredutível em $\mathbb{Q}[x]$ que possui raiz de módulo unitário é necessariamente palindrômico. Daí, vamos explorar a relação entre um polinômio palindrômico e sua transfomada de Chebyshev. Nesse contexto utilizaremos a regra de sinais de Descartes, que permite estimar a quantidade de raízes de um polinômio em um determinado intervalo da reta real.

Esse trabalho está organizado conforme a seguinte descrição. Inicialmente, fazemos uma abordagem sobre números complexos no capítulo 2, apresentando as principais propriedades e representações.

Em seguida falamos sobre o Teorema Fundamental da Álgebra e sobre a Regra dos Sinais de Descartes. Isso nos servirá de suporte para desenvolver o estudo dos polinômios que norteiam esse trabalho.

Por fim, no último capítulo, caracterizaremos a família dos polinômios em $\mathbb{Q}[x]$ que admitem raízes no círculo unitário e mostraremos uma forma de como elucidar a quantidade dessas raízes.

Esse trabalho foi norteado pelo artigo de título: "Roots in unity circle" do autor Keith Conrad.

2 NÚMEROS COMPLEXOS

Conforme Gilbert G. Garbi, em sua obra intitulada Romance das Equações Algébricas GARBI (2010), foi na Itália no século XVI onde matemáticos buscavam resolver equações do 3º grau que se percebeu que os números reais não eram suficientes e as primeiras ideias da criação do conjunto dos números complexos surgiram.

Por volta de 1.510, o italiano Scipione del Ferro encontrou a forma geral para resolver equações do tipo $x^3 + px + q = 0$. Posteriormente, seu compatriota Tartaglia sem conhecer a solução dada por Scipione, achara também a solução geral dessas equações e foi além, pois conseguiu resolver as do tipo $x^3 + px^2 + q = 0$.

Tal proeza chegou ao conhecimento de outro italiano chamado Cardano que até aquele momento estava convencido da impossibilidade de se obter uma solução geral para equações do terceiro grau. Cardano solicitou a Tartaglia a revelação desse trabalho mediante muitas promessas e jurou segredo. Este astuto matemático foi atendido, no entanto, ao contrário do que havia acordado, em 1.545 publicou na Ars Magna a fórmula de Tartaglia. E a história injustamente a nomeou como a Fórmula de Cardano, que em linguagem matemática de hoje pode ser descrita conforme abaixo:

$$x = \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

A fórmula de Cardano estimulou os matemáticos da época a refletirem sobre algo novo, pois pode-se chegar a uma solução real pela extração da raiz quadrada de um número negativo, bem como pela extração de raízes cúbicas de números de natureza desconhecida. A partir de então, houve um enfrentamento por parte dos matemáticos da época a fim de compreender melhor esses números.

Portanto, segundo Garbi, os números complexos despertaram interesse sobre sua compreensão e aplicação a partir de esforços para a resolução de equações de grau 3 e não de grau 2. Segundo o citado autor, isso se deve ao fato de que os matemáticos até o século XV não se inquietavam quando o discriminante de uma equação do 2º grau era menor do que zero. Neste caso, conformavam-se em dizer que o problema não tinha solução.

Entretanto, nota-se que há equações de grau 3 com soluções reais conhecidas, mas cuja determinação passava pela extração de raízes quadradas de números negativos. A partir desta constatação, concluiu-se que os números reais já não eram suficientes para se tratar com equações algébricas. Portanto, o conceito de número precisava ser estendido.

Nesse contexto, discutiremos a seguir as principais definições básicas sobre números complexos e polinômios. Para tanto, usamos como inspiração e fonte a obra MUNIZ NETO (2012).

2.1 Representação Algébrica dos Números Complexos

Um contemporâneo de Cardano, também italiano, o engenheiro hidráulico Rafael Bombelli, foi quem alcançou primeiro o entendimento desses novos números. Bombelli, ao tentar resolver a equação $x^3 = 15x+4$, para a qual já conhecia a solução, $x = 4$, chegou ao seguinte resultado:

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

Bombelli admitiu que as raízes cúbicas acima poderiam ser escritas como $2 + m\sqrt{-1}$ e $2 - m\sqrt{-1}$ e, portanto, $x = 4$.

Mais adiante, em seu trabalho L'Algebra, adotou a notação $a + b\sqrt{-1}$ para descrever um número complexo e estabeleceu que $\sqrt{-1}.\sqrt{-1} = -1$. Registrou ainda as fórmulas para a adição e multiplicação conforme a seguir:

$$(a + b\sqrt{-1}) + (c + d\sqrt{-1}) = (a + c) + (b + d)\sqrt{-1}$$

$$(a + b\sqrt{-1}).(c + d\sqrt{-1}) = (ac - bd) + (bc + ad)\sqrt{-1}$$

Mesmo diante do esforço de Bombelli de entender números da forma $a+b\sqrt{-1}$, à época houve muita resistência em aceitar esses números, em virtude dos matemáticos não terem ainda um entendimento geométrico que os representassem.

Porém, nas décadas seguintes, houve colaborações de outros matemáticos, dentre os quais destaco três. Os franceses Fermat e Descartes que consolidaram o estudo da Geometria Analítica associando a Algebra à Geometria, sendo este último quem primeiro intitulou esses números de imaginários e o suiço Euler que propôs a denominação i para $\sqrt{-1}$. Com isso, segundo Bombelli, temos $i^2 = -1$.

Agora, denotaremos o conjunto dos números complexos por $\mathbb{C}$ e usaremos a notação sugerida por Euler. Todo número $z \in \mathbb{C}$, poderá ser escrito na forma $z = a + bi$, em que a é chamada parte real de z e b o coeficiente da parte imaginária de z. Dessa forma, se $z = a + bi$, escreveremos $a = Re(z)$ e $b = Im(z)$.

Com essas notações, as operações de adição e de multiplicação definidas por

Bombelli se reescrevem na forma:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

$$(a + bi).(c + di) = (ac - bd) + (ad + bc)i.$$

Além disso, temos $a + bi = a' + b'i \Leftrightarrow a = a'$ e $b = b'$.

Por outro lado, quaisquer números $z, z', z'' \in \mathbb{C}$ valem as propriedades a seguir:

1. Comutativas: $z + z' = z' + z$ e $z.z' = z'.z$
2. Associativas: $z + (z' + z'') = (z + z') + z''$ e $z.(z'.z'') = (z.z').z''$
3. Distributivas: $z.(z' + z'') = z.z' + z.z''$
4. Existência de elemento neutro: $0 + z = z$ e $z \cdot 1 = z$
5. Existência de inverso aditivo(oposto): $z + (-z) = 0$
6. Existência de inverso multiplicativo: Se $z \neq 0$, então existe $z^{-1} \in \mathbb{C}$

Por conta dessas propriedades, dizemos que o conjunto dos números complexos munido com as operações de soma e produto é um corpo. De forma mais geral, um corpo é um conjunto equipado com duas operações de tal modo que as propriedades descritas acima são satisfeitas. Podemos observar que o conjunto dos números racionais, e também o conjunto dos números reais, munidos com as operações usuais são exemplos de corpos.

2.2 Representação Geométrica dos Números Complexos

Em meio a diversas contribuições de matemáticos no esforço de desbravar os desafios impostos por esses novos números, coube ao suíço Leonhard Euler dar uma robusta e sólida contribuição nesse tema, esse legado proporcionou que a história o reconhecesse como o notável matemático que dominou os números complexos.

Adiante segue a representação geométrica de um número complexo $z = a + bi$, ou seja, a representação de z pelo par ordenado (a, b) no plano, como ponto de $\mathbb{R}^2$.

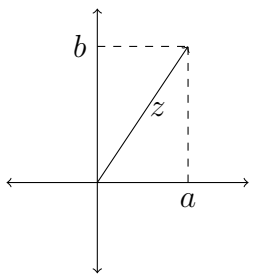

Figura 1 : Número complexo $z = a + bi$

Pela definição de números complexos, temos:

$$a + bi = a' + b'i \Leftrightarrow (a, b) = (a', b')$$

Então, as descrições algébricas da soma e multiplicação, ficam assim definidas:

$$(a, b) + (a', b') = (a + a') + (b + b')$$

$$(a, b).(a', b') = (aa' - bb', ab' + ba')$$

Abaixo mostra a representação geométrica dos números complexos $z, z', z + z'$.

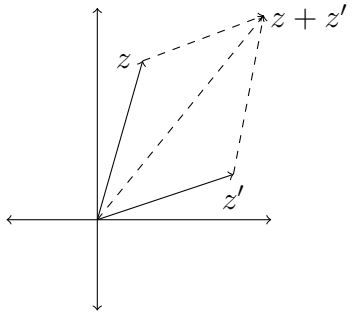

Figura 2 : Número complexo $z + z'$

Dado um número complexo $z = a + bi$, o conjugado de z é definido como o número complexo $\overline{z} = a - bi$ que corresponde geometricamente ao simétrico de z com respeito ao eixo horinzontal, conforme representado abaixo.

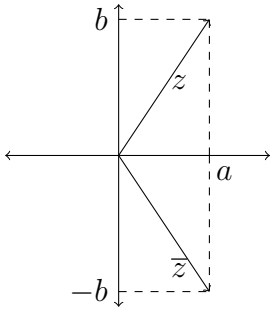

Figura 3 : Número complexo conjugado $\overline{z} = a - bi$

A conjugação tem as seguintes propriedades:

1. $\overline{z} = 0 \Leftrightarrow z = 0$
2. $\overline{\overline{z}} = z, \forall z \in \mathbb{C}$
3. $\overline{z} = z \Leftrightarrow z \in \mathbb{R}$
4. $\overline{z \pm w} = \overline{z} \pm \overline{w}$
5. $\overline{z.w} = \overline{z}.\overline{w}$
6. se $z \neq 0$, então $\overline{z^{-1}} = \overline{z}^{-1}$
7. $Re(z) = \frac{z+\overline{z}}{2}$ e $Im(z) = \frac{z-\overline{z}}{2i}$

O módulo do número complexo $z = a + bi$ é o número real não negativo

$|z| = \sqrt{a^2 + b^2}$. A interpretação geométrica do módulo de z é o módulo do vetor de origem em $(0, 0)$ e de extremidade (a, b).

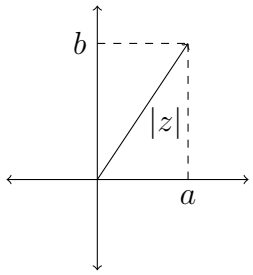

Figura 4 : Módulo do número complexo $|z| = \sqrt{a^2 + b^2}$

2.3 Forma Polar e as Fórmulas de De Moivre

No estudo dos números complexos, considerando as relevantes contribuições nesse conteúdo, é justo também destacar o matemático françês Abraham de Moivre, que foi responsável por relacionar números complexos com trigonometria. O que denominamos hoje de fórmula polar.

Esta representação permite que o cálculo do produto e da divisão de números complexos, bem como o de calcular potências e extrair raízes sejam realizados de forma menos trabalhosa e também permite a interpretação geométrica dessas operações.

Seja $z = a + bi$ um número complexo não nulo. O ponto $P = (a, b)$ do plano, que corresponde ao número $z \neq 0$, é diferente da origem $O = (0, 0)$. Portanto, o segmento de reta OP, de comprimento $r = |z| = \sqrt{a^2 + b^2} \neq 0$, determina com a semirreta positiva do eixo real um ângulo θ, cuja medida em radianos está no intervalo $[0, 2\pi]$.

O número real θ é chamado de argumento principal de z e é denotado por $arg(z) = \theta$. Abaixo temos a representação gráfica. Geometricamente, o argumento de z é a medida em radianos do ângulo o qual devemos girar o semi eixo positivo da reta real, no sentido anti-horário, até coincidir com o segmento OP.

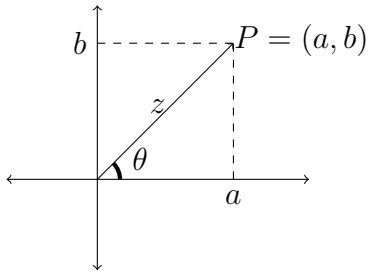

Figura 5 : Número complexo $z = a + bi$ e o $arg(z) = \theta$

A forma polar ou forma trigonométrica do número complexo não nulo $z = a + bi$, com módulo $r = \sqrt{a^2 + b^2}$ e argumento $arg(z) = \theta$, é obtida por observar que $a = r\cos\theta$ e $b = rsen\theta$. Assim, escrevemos:

$$z = r(\cos\theta + isen\theta).$$

Essa representação, nos permite deduzir que se $z_1 = r_1(\cos\theta_1 + isen\theta_1)$ e $z_2 = r_2(\cos\theta_2 + isen\theta_2)$, então

$$z_1 \cdot z_2 = r_1 r_2(\cos(\theta_1 + \theta_2) + isen(\theta_1 + \theta_2)).$$

Daí, um argumento indutivo, permite estabelecer que se $z_1, z_2, \ldots z_n$ são números complexos tais que $z_k = r_k(\cos\theta_k + isen\theta_k)$, para $k = 1, 2, \ldots, n$, então

$$z_1 \cdot z_2 \cdots z_n = r_1 r_2 \cdot r_n(\cos(\theta_1 + \theta_2 + \cdots + \theta_n) + isen(\theta_1 + \theta_2 + \cdots + \theta_n)).$$

Em particular, no caso em que temos todos os $z_1, z_2, \ldots z_n$ iguais a um certo número complexo $z = r(\cos\theta + isen\theta)$, a fórmula acima se reduz a:

$$z^n = r^n(\cos(n\theta) + isen(n\theta)).$$

Essa é chamada de "primeira fórmula de De Moivre"

A chamada "segunda fórmula de De Moivre" é estabelecida quando fixamos um número complexo $w = r_0(cos\alpha + isen\alpha)$ e consideramos as soluções complexas da equação $x^n = w$. Assim, estamos interessados nas raízes complexas n-ésimas de w. Para determiná-las, observamos que se um número complexo $z = r(\cos\theta + isen\theta)$ satisfizer essa equação, então pela primeira fórmula de De Moivre segue que

$$r^n(\cos(n\theta) + isen(n\theta)) = r_0(cos\alpha + isen\alpha).$$

Daí, tomando o módulo de ambos os membros, concluímos que $r^n = r_0$, de

onde segue que $r = \sqrt[n]{r_0}$, pois tanto r quanto r_0 são números reais positivos.

Diante dessa conclusão, a equação acima se reduz ao seguinte sistema de equações trigonométricas:

$$\begin{cases} \cos(n\theta) &= cos\alpha \\ sen(n\theta) &= sen\alpha \end{cases}$$

Isso nos diz que $n\theta$ e α são arcos côngruos. Portanto, existe $k \in \mathbb{Z}$ tal que $n\theta = \alpha + 2k\pi$. Logo,

$$\theta = \frac{\alpha + 2k\pi}{n}.$$

Por outro lado, lembrando que α e θ pertencem ao intevalo $[0, 2\pi)$, segue que $0 \leq \alpha + 2k\pi < 2n\pi$ e daí $0 \leq k < n$. Além disso, é fácil ver que para cada $k \in \{0, 1, 2, \ldots, n-1\}$ temos que

$$z_k = \sqrt[n]{r_0}(cos(\frac{\alpha + 2k\pi}{n}) + sen(\frac{\alpha + 2k\pi}{n}))$$

é raiz n-ésima de w. Também devemos observar que um polinômio não nulo com coeficientes em um corpo tem o seu grau como limitante para o número de raízes, veja o 2.6. Assim, vemos que z_k, com $k = 0, 1, 2, \ldots, n-1$ são todas as raízes n-ésimas de w.

2.4 Raízes da Unidade

Chamamos de raízes n-ésimas da unidade, as raízes complexas n-ésimas de 1. Em outras palavras, as raízes n-ésimas da unidade são as soluções complexas da equação $x^n - 1 = 0$. Note que 1 é a única raiz 1-ésima da unidade. No caso geral, as raízes n-ésimas de 1 são dadas pela segunda fórmula de De Moivre. Vejamos o que ocorre com $n \geq 2$.

Se o número complexo $z = r(\cos\theta + isen\theta)$ for uma raiz n-ésima da unidade, então como $\theta = arg(1) = 0$, segue pela fórmula de De Moivre que:

$$z = z_k = \cos\frac{2k\pi}{n} + \sin\frac{2k\pi}{n}, \text{ para algum } k \in \{0, 1, 2, 3 \ldots, n-1\}.$$

Vale observar que se tomarmos $\xi = z_1$, isto é, $\xi = \cos\frac{2k\pi}{n} + \sin\frac{2k\pi}{n}$, então $z_k = \xi \cdot z_{k-1}$. Em particular, como $|\xi| = 1$ segue que z_k é obtido de z_{k-1} por meio de uma rotação no sentido anti-horário de amplitude $\frac{2\pi}{n}$. Isso nos diz que as raízes da unidade estão regularmente distribuídas ao longo do círculo unitário, dividindo-o em n partes iguais, sendo $z_0 = 1$. Em outros termos, as raízes n-ésimas da unidade correspondem aos vértices de um polígono regular de n lados, inscrito no círculo de centro na origem e raio 1, de forma que um dos vértices seja o ponto 1.

Dessa forma se n for ímpar, devido a simetria do polígono, temos que o número 1 é a única raíz real. Por outro lado, se n for par, temos que -1 e 1 são as únicas raízes reais.

A seguir vemos a representação geométrica das raízes complexas cúbicas e quartas da unidade.

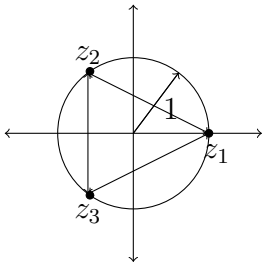

Figura 6 : Raízes cúbicas da unidade $x^3 = 1$

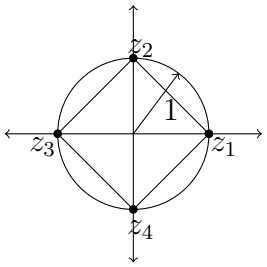

Figura 7 : Raízes quárticas da unidades $x^4 = 1$

Para cada $n \in \mathbb{N}$ fixado, o conjunto das raízes complexas n-ésimas da unidade, denotado por $U_n(\mathbb{C})$ é um conjunto finito com n elementos e possui as seguintes propriedades:

1. $z_1, z_2 \in U_n(\mathbb{C}) \Rightarrow z_1 \cdot z_2 \in U_n(\mathbb{C})$.
2. $z \in U_n(\mathbb{C}) \Rightarrow z^{-1} \in U_n(\mathbb{C})$.
3. $1 \in U_n(\mathbb{C})$.

Por conta disso, normalmente dizemos que $U_n(\mathbb{C})$ é o grupo das raízes n-ésima da unidade em $\mathbb{C}$.

2.5 Polinômios e Suas Raízes

Lembramos que ao falarmos de um polinômio com coeficientes em um corpo $\mathbb{K}$ referimo-nos a uma expressão do tipo

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

em que os coeficientes $a_0, a_1, \ldots, a_n$ são elementos de $\mathbb{K}$. Além disso, quando escrevemos uma tal espressão, convencionamos que $a_n \neq 0$ e nesse caso dizemos se tratar de um polinômio de grau n, e escrevemos $\partial P(x) = n$. Por outo lado, o polinômio nulo é aquele em que todos os coeficientes são iguais a zero e nesse caso o grau não é definido. O conjunto de todos os polinômios com coeficientes em $\mathbb{K}$ será denotado por $\mathbb{K}[x]$. Observamos ainda que $\mathbb{K}$ é considerado um subconjunto $\mathbb{K}[x]$.

Nesse contexto, os elementos de $\mathbb{K}$ são ditos polinômios constantes. Para indicar que um elemento $P(x) \in \mathbb{K}[x]$ é um polinômio constante, correspondendo a um elemento $z \in \mathbb{K}$, escrevemos $R(x) \equiv z$. Em particular, para indicar que $P(x) \in \mathbb{K}[x]$ é o polinômio nulo, escrevemos $P(x) \equiv 0$ e a negativa desse fato é indicada por $P(x) \not\equiv 0$.

Neste tópico, admitiremos que o leitor tem familiaridade com as operações básicas envolvendo polinômios. Nesse caso, não definiremos tais operações e em particular não demonstraremos o algoritmo da divisão. Todavia, apresentamos a seguir o enunciado desse importante teorema:

Teorema 2.1. (Algoritmo de Divisão) *Dados dois polinômios $A(x), B(x) \in \mathbb{K}[x]$, com $B(x)$ não nulo , existem polinômios $Q(x)$ e $R(x)$ em $\mathbb{K}[x]$, univocamente determinado, satisfazendo as condições:*

$$A(x) = B(x) \cdot Q(x) + R(x) \text{ e } \partial R(x) < \partial B(x) \text{ ou } R(x) \equiv 0.$$

Observaçao 2.2. *Se ocorrer $R(x) \equiv 0$ dizemos que o polinômio $B(x) \in \mathbb{K}[x]$ divide o polinômio $A(x) \in \mathbb{K}[x]$, ou ainda, que a divisão de $A(x)$ por $B(x)$ é exata. Nesse caso, usamos a notação $B(x)|A(x)$.*

Lema 2.3. *Se $B(x)|A(x)$, então $\partial B(x) \leq \partial A(x)$.*

Demonstração: Bem, por hipótese, segue que existe $Q(x) \in \mathbb{K}[x]$ tal que $A(x) = Q(x) \cdot B(x)$. Daí, se tivemos $\partial Q(x) = m$ e $\partial B(x) = n$ segue que $\partial A(x) = m + n$. De fato, escrevendo

$$Q(x) = q_m x^m + \cdots + q_1 x + q_0 \text{ com } q_m \neq 0 \text{ e } B(x) = b_n x^n + \cdots + b_1 x + b_0 \text{ com } b_n \neq 0$$

segue que

$$A(x) = (q_m \cdot b_n)x^{m+n} + \cdots + (q_1 b_0 + b_1 q_0)x + q_0 b_0.$$

Assim, como $q_m \neq 0$ e $b_n \neq 0$, vemos que $q_m \cdot b_n \neq 0$, pois em um corpo não há divisores de zero. Dessa forma,

$$\partial A(x) = m + n \geq n.$$

□

Um elemento $z \in \mathbb{K}$ é dito uma raiz de uma polinômio $P(x)$, se ocorrer

$$a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 = 0.$$

Com o auxílio do algoritmo da divisão podemos mostrar que se $z \in \mathbb{K}$ for raiz de $P(x)$, então existe $Q(x) \in \mathbb{K}[x]$ tal que $P(x) = (x - z) \cdot Q(x)$.

De fato, suponhamos que $P(z) = 0$. Pela divisão euclidiana de $P(x)$ por $x - z$, existem $Q(x), R(x) \in \mathbb{K}[x]$ tais que

$$P(x) = Q(x)(x - z) + R(x)$$

onde $R(x) \equiv 0$ ou $gr(r(x)) < gr(x - z) = 1$. Em qualquer caso, $R(x) \equiv r \in \mathbb{K}$. Daí e $P(x) = q(x)(x - \beta) + r$. Avaliando $P(x)$ em $x = z$, temos:

$$0 = P(z) = q(z)(z - z) + r = r,$$

mostrando que $x - z$ divide $P(x)$.

Reciprocamente, suponhamos que $x - z$ divida $P(x)$. Então, existe $Q(x) \in \mathbb{K}[x]$ tal que $P(x) = Q(x)(x - z)$. Portanto:

$$P(z) = Q(z)(z - z) = Q(z).0 = 0.$$

Lema 2.4. *Dados um polinômio não nulo $P(x) \in \mathbb{K}[x]$ e um elemento $z \in \mathbb{K}$ temos que o conjunto $\mathcal{X}_z := \{n \in \mathbb{N}; (x - z)^n$ divide $P(x)\}$ é um subconjunto finito de $\mathbb{N}$.*
Demonstração: Se $n \in \mathcal{X}_z$, então $(x - z)^n$ divide $P(x)$. Daí, pelo lema 2.3, segue que $n = \partial(x-z)^n \leq \partial P(x)$. Isso nos diz que $\mathcal{X}_z$ é um subconjunto de $\mathbb{N}$ limitado superiormente, o que garante que $\mathcal{X}_z$ é finito.

□

Observaçao 2.5. *Convencionamos que $(x - z)^0 \equiv 1$. Em particular, temos que $0 \in \mathcal{X}_z$. Definimos a multiplicidade de z como raiz de $P(x)$ como sendo o elemento máximo de $\mathcal{X}_z$. Note que a multiplicidade será igual a "zero" se z não for raiz de $P(x)$. Em todo caso, a multiplicidade não supera o grau do polinômio.*
Teorema 2.6. *Se $P(x) \in \mathbb{K}[x]$ é um polinômio de grau n, então $P(x)$ tem no máximo n raízes em $\mathbb{K}$, contadas com multiplicidade.*
Demonstração: Vamos raciocinar por indução em $n = gr(P(x))$, na forma do segundo princípio de indução. Vejamos:
Seja $P(x)$ um polinômio de grau n. Se $P(x)$ não tem raízes em $\mathbb{K}$, nada há para demonstrar

e temos que o resultado é válido. Suponhamos o resultado verdadeiro para polinômios de grau menor que n e que $P(x)$ possui uma raiz $z \in \mathbb{K}$, digamos de multiplicidade m. Nesse caso, $(x-z)^m$ divide $P(x)$ em $\mathbb{K}[x]$. Logo existe $Q(x) \in \mathbb{K}[x]$, com $Q(z) \neq 0$, tal que $P(x) = Q(x)(x-z)^m$. Essa igualdade garante que $\partial Q(x) = n-m$ e além disso, toda raiz de $P(x)$ distinta de z deve ser raiz de $Q(x)$. Com efeito, se que $\alpha \in \mathbb{K}$ é raiz de $P(x)$, então $0 = P(\alpha) = Q(\alpha).(\alpha - z) \Leftrightarrow Q(\alpha) = 0$, pois $\alpha \neq z$. Daí, α é raiz de $Q(x)$. Por fim, a hipótese de indução nos diz que $Q(x)$ tem no máximo $n-m$ raízes em $\mathbb{K}$. Logo, $P(x)$ tem no máximo n raízes em $\mathbb{K}$, contada com multiplicidade.

□

Exemplo 2.7. O teorema acima indica que o grau é o limite para o número de raízes. Por outro lado, o número efetivo de raízes depende do corpo que considerarmos. Vejamos o caso do polinômio $x^2 - 7 \in \mathbb{Q}[x]$: Não possui raízes em $\mathbb{Q}$. No entanto, em $\mathbb{R}$ tem duas raízes $\sqrt{7}$ e $-\sqrt{7}$. Já o polinômio $x^2 + 7 \in \mathbb{Q}[x] \subset \mathbb{R}[x]$ não possui raízes reais, mas possui duas raízes em $\mathbb{C}$, a saber: $\pm i.\sqrt{7}$.

2.6 Fatoração de Polinômios

Se $\mathbb{K}$ é um corpo, o conjunto $\mathbb{K}[x]$ munido com as operações usuais de soma e multiplicação de polinômios possui propriedades semelhantes ao conjunto dos números inteiros. Por exemplo, em $\mathbb{K}[x]$ vale um resultado análogo ao teorema fundamental da aritmética. Para estabelecer esse resultado, precisamos primeiro introduzir o conceito de polinômio irredutível, que por sua vez no nosso cantexto fará o papel desempenhado pelos números primos.

Sejam $f(x) \in \mathbb{K}[x]$ um polinômio não constante. Dizemos que $f(x)$ é um polinômio irredutível em $\mathbb{K}[x]$ se satisfizer a propriedade abaixo.

"Se $f(x) = g(x) \cdot h(x)$, com $g(x), h(x) \in \mathbb{K}[x]$, então $h(x)$ ou $g(x)$ é um polinômio constante não nulo."

Nesse caso, também costumamos dizer que o polinômio $f(x)$ é irredutível sobre $\mathbb{K}$. Caso o polinômio $f(x)$ não satizfaça a condição acima, diremos tratar-se de um polinômio redutível.

Por exemplo, o polinômio x^2-7 é redutível sobre $\mathbb{R}$, pois $x^2-7 = (x-\sqrt{7})(x+\sqrt{7})$. Por outro lado, $x^2 - 7$ é irredutível em $\mathbb{Q}[x]$, pois tem grau 2 e não tem raiz em $\mathbb{Q}$.

Lembrando que o grau de um produto de polinômios é a soma dos graus dos fatores, nos convencemos que um polinômio de grau 1, chamado de polinômio linear, é necessariamente irredutível sobre qualquer corpo que contenha seus coeficientes. Em se tratando de $\mathbb{C}$, a exceção dos polinômios de grau 1, todos os demais polinômios são

redutíveis. Isso é uma consequência do Teorema Fundamental da Álgebra, o qual apresentaremos na próxima seção.

É claro que um polinômio $P(x) \in \mathbb{K}[x]$ de grau maior que 1, que possui uma raiz z no corpo $\mathbb{K}$ certamente é redutível sobre esse corpo, pois o algoritmo da divisão nos ensina que existirá um polinômio $Q(x) \in \mathbb{K}[x]$ tal que $(Px) = (x - z) \cdot Q(x)$. No entanto, o exemplo de $P(x) = x^4 + 4 \in \mathbb{Q}[x]$, conforme segue

$$P(x) = x^4 + 4 = x^4 + 4x^2 + 4 - 4x^2 = (x^2 + 2)^2 - (2x)^2 = (x^2 - 2x + 2) \cdot (x^2 + 2x + 2)$$

mostra que um polinômio pode ser redutível sobre um corpo (no caso,$\mathbb{Q}$) sem necessariamente possuir raiz nesse corpo.

Por outro lado, é claro que um polinômio de grau 2 ou grau 3 que é redutível sobre um corpo $\mathbb{K}$, é divisível por um polinômio linear com coeficientes em $\mathbb{K}$. Consequentemente, tais polinômios possuem raiz em $\mathbb{K}$. Dessa forma, para polinômios de grau 2 ou 3 a redutibilidade é equivalente ao fato de possuir raiz no corpo. Equivalentemente, a irredutibilidade é equivalente ao fato de não possuir raiz no corpo (Não esqueça, isso só vale para polinômios de grau 2 ou 3).

A seguir destacamos algumas características importantes dos polinômios irredutíveis.

Lema 2.8. *Se $P(x), A(x) \in \mathbb{K}[x]$ são tais que $P(x)$ é irredutível e não divide $A(x)$, então existem polinomios $S(x), T(x) \in \mathbb{K}[x]$ tais que*

$$P(x) \cdot S(x) + A(x) \cdot T(x) = 1$$

Demonstração: Como $P(x)$ não divide $A(x)$, o algoritmo da divisão nos diz que existem $Q_1(x), R_1(x) \in \mathbb{K}[x]$, com $R_1(x) \not\equiv 0$ e $\partial R_1(x) < \partial P(x)$, tais que

$$A(x) = P(x) \cdot Q_1(x) + R_1(x).$$

Do mesmo modo, existem $Q_2(x), R_2(x) \in \mathbb{K}[x]$, tais que

$$P(x) = R_1(x) \cdot Q_2(x) + R_2(x), \text{ com } R_2(x) \equiv 0 \text{ ou } \partial R_2(x) < \partial R_1(x).$$

Se ocorrer $R_2(x) \not\equiv 0$, continuamos o processo e obtemos $Q_3(x), R_3(x) \in \mathbb{K}[x]$, tais que

$$R_1(x) = R_2(x) \cdot Q_3(x) + R_3(x), \text{ com } R_3(x) \equiv 0 \text{ ou } \partial R_3(x) < \partial R_2(x).$$

Como uma sequência decrescente de números naturais "$\partial P(x) > \partial R_1(x) > \partial R_2(x) > \partial R_3(x) > \ldots$" não pode ser infinita, concluímos que o procedimento de divisões sucessivas necessariamente termina, e o faz exatamente quando ocorrer o primeiro resto

nulo, isto é, paramos no ponto em que $R_k(x)$ divide $R_{k-1}(x)$, implicando que $R_{k+1}(x) \equiv 0$.

Dessa forma, a identidade $R_{k-2}(x) = R_{k-1}(x)\cdot Q_k(x)+R_k(x)$ garante que $R_k(x)$ divide $R_{k-2}(x)$. E, por sua vez, a identidade $R_{k-3}(x) = R_{k-2}(x) \cdot Q_{k-1}(x) + R_{k-1}(x)$ implica que $R_k(x)$ divide $R_{k-2}(x)$. Portanto, repetindo esse argumento, vemos que $R_k(x)$ divide $R_k(x)$ divide cada $R_j(x)$, com $j = 1, 2, 3, \ldots, k-1$ e consequentemente, $R_k(x)$ divide $P(x)$ e também divide $A(x)$. Mas, como $P(x)$ é irredutível que não divide $A(x)$ só nos resta a possibilidade de $R_k(x)$ ser um polinômio constante não nulo.

Por outro lado, as identidades descritas acima podem ser reescritas na forma

$$R_k(x) = R_{k-2}(x) - R_{k-1}(x) \cdot Q_k(x) = R_{k-2}(x) - (R_{k-3}(x) - R_{k-2}(x) \cdot Q_{k-1}(x)) \cdot Q_k(x)$$

$$= R_{k-2}(x)(1 + Q_{k-1}(x) \cdot Q_k(x)) - R_{k-3}(x) \cdot Q_k(x)$$

$$= (R_{k-4}(x) - R_{k-3}(x) \cdot Q_{k-2}(x))(1 + Q_{k-1}(x) \cdot Q_k(x)) - R_{k-3}(x) \cdot Q_k(x)$$

$$= R_{k-4}(x) \cdot (1 + Q_{k-1}(x) \cdot Q_k(x)) - R_{k-3}(x) \cdot (Q_{k-2}(x)(1 + Q_{k-1}(x) \cdot Q_k(x)) + Q_k(x)).$$

A continuação dessas substituições nos convence de que para cada $j = 1, 2, \ldots, k$ existem polinômios $A_j(x), B_j(x) \in \mathbb{K}[x]$ tais que

$$R_k(x) = R_{k-(j+1)}(x) \cdot A_j(x) + R_{k-j}(x) \cdot B_j(x).$$

Convencionamos que $R_0(x) = P(x)$ e $R_{-1}(x) = A(x)$. Portanto, temos em particular que

$$R_k(x) = A(x) \cdot A_k(x) + P(x) \cdot B_k(x).$$

Por fim, como $R_k(x)$ é constante não nulo, podemos dividir ambos os membros por essa constante, obtendo assim:

$$P(x) \cdot S(x) + A(x) \cdot T(x) = 1, \text{ com } S(x), T(x) \in \mathbb{K}[x].$$

□

Proposição 2.9. *Se um polinômio irredutível divide o produto de dois outros polinômios, então ele divide um dos fatores desse produto.*

Demonstração: Sejam $A(x), B(x), P(x) \in \mathbb{K}[x]$ são polinômios tais que $P(x)$ é irredutível e $P(x)|A(x)B(x)$. Suponhamos que $P(x)$ não divide $A(x)$. Assim, pelo lema anterior existem $S(x), T(x) \in \mathbb{K}[x]$ tais que

$$P(x) \cdot S(x) + A(x) \cdot T(x) = 1.$$

Daí, multiplicando tudo por $B(x)$ obtemos:

$$B(x) = B(x) \cdot P(x) \cdot S(x) + B(x) \cdot A(x) \cdot T(x).$$

Portanto, vemos que $P(x)|B(x)$ e isso termina a demonstração.

□

Teorema 2.10. *Se $\mathbb{K}$ é corpo, então todo polinômio não constante em $\mathbb{K}[x]$ ou é irredutível em $\mathbb{K}[x]$ ou pode ser escrito como um produto de polinômios irredutíveis em $\mathbb{K}[x]$.*
Demonstração: Seja $P(x) \in \mathbb{K}[x]$ um polinômio não constante. Se $P(x)$ for irredutível nada temos para provar. Suponhamos então que $P(x)$ é um polinômio redutível de grau $n \in \mathbb{N}$ e suponhamos que o resultado vale para todo polinômio de grau menor que n. Bem, sendo $P(x)$ um polinômio redutível, segue que existem polinômios $P_1(x), P-2(x) \in \mathbb{K}[x]$ não constantes tais que $P(x) = P_1(x) \cdot P_2(x)$. Daí, como $\partial P(x) = \partial P_1(x) + \partial P_2(x)$, segue que os dois fatores são polinômios da grau menor que n e assim, a hipótese garante que ambos podem ser escritos como produto de polinômios irredutíveis ou são eles próprios irredutíveis. Em todo caso, obtemos uma decomposição de $P(x)$ como produto de irredutíveis.

A unicidade da decomposição, a menos de fatores constantes e da ordem do fatores irredutíveis, segue como uma aplicação da proposição 2.9.

□

3 TEOREMA FUNDAMENTAL DA ÁLGEBRA

Como vimos na seção anterior, os polinômios lineares sempre são irredutíveis sobre seu corpo de coeficientes. Por outro lado, também vimos exemplos de polinômios irredutíveis de grau maior que 1. Nesse sentido, um corpo para o qual os únicos polinômios irredutíveis são os lineares é em larga medida especial. Por exemplo, o corpo dos números reais não possui tal propriedade, uma vez que o polinômio $x^2 + 1 \in \mathbb{R}[x]$ é irredutível de grau 2. Esse mesmo polinômio, pensado como elemento de $\mathbb{Q}[x]$, nos convence de que o corpo dos números racionais também não possui tal propriedade. Naturalmente, a esta altura, o leitor deve perguntar-se sobre a existência de corpos com tal característica. O objetivo dessa seção é mostrar que o corpo dos números complexos é um exemplo do que chamamos de corpo *algebricamente fechado.*

Depois que Leonard Euler mostrou que as equações do tipo $z^n = w$ tinham n soluções em $\mathbb{C}$, os matemáticos passaram a acreditar que toda equação de grau n deveria ter n raízes complexas. Este fato só foi constatado por outro notável matemático, o alemão Carl Friedrich Gauss que aos 21 anos de idade, em sua tese de doutorado, provou sob o título de Teorema Fundamental da Álgebra que:

Teorema 3.1. *Todo polinômio não constante com coeficientes complexos possui pelo menos uma raiz complexa.*

Não vamos apresentar uma demonstração para o teorema, pois isso nos desviaria do foco do nosso objetivo principal. Além disso, a literatura apresenta um vasto número de referências para o tema, nas quais podemos encontrar inúmeras demonstrações.

Por outro lado, por ser menos ambundante na literatura, vamos apresentar uma demonstração para uma redução que normalmente se faz durante algumas dessas demonstrações. Explícitamente, temos do seguinte resultado:

Proposição 3.2. *: É sufiente provar o Teorema Fundamental da Álgebra (TFA) para polinômios com coeficientes reais.*

Demonstração: Dado um polinômio $A(x) \in \mathbb{C}[x]$, escrevemos

$$A(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

Definimos um novo polinômio, tomando os conjugados dos coeficientes de $A(x)$.

$$\overline{A}(x) := \overline{a}_n x^n + \overline{a}_{n-1} x^{n-1} + \ldots + \overline{a}_1 x + \overline{a}_0.$$

Agora observamos que o produto $P(x) := A(x)\overline{A}(x)$ possui coeficientes reais.

Com efeito, começamos convencionado que $a_i = 0$ para $i > n$ e escrevendo

$$P(x) = c_m x^m + c_{m-1}x^{m-1} + \ldots + c_1 x + c_0, \text{ com } m = 2n.$$

Daí, pela definição de multiplicação de polinômios, segue que para cada $j = 0, 1, 2 \ldots, m$ temos:

$$c_j = \sum_{i=0}^{j} a_i \cdot \overline{a}_{j-i} = \sum_{i=0}^{j} \overline{a}_i \cdot a_{j-i}.$$

A segunda das igualdades acima é uma manifestação da comutatividade do produto "$A(x)\overline{A}(x) = \overline{A}(x)A(x)$."

Dessa forma, segue que

$$2c_j = c_j + c_j = \sum_{i=0}^{j}(a_i \cdot \overline{a}_{j-i} + \overline{a}_i \cdot a_{j-i}).$$

Com isso, observando que

$$a_i \cdot \overline{a}_{j-i} + \overline{a}_i \cdot a_{j-i} = a_i \cdot \overline{a}_{j-i} + \overline{a_i \cdot \overline{a}_{j-i}} \in \mathbb{R},$$

concluímos que $c_j \in \mathbb{R}$.

Por fim, assumindo que o Teorema Fundamental da Álgebra seja verdadeiro para polinômios com coeficientes reais, segue que existe $z \in \mathbb{C}$ tal que $P(z) = 0$.

Portanto, temos $A(z) \cdot \overline{A}(z) = 0$. O que implica $A(z) = 0$ ou $\overline{A}(z) = 0$. No primeiro caso, vemos que z é raiz de $A(x)$. Já o segundo caso nos diz que z é raiz de $\overline{A}(x)$, ou seja,

$$\overline{A}(z) = \overline{a}_n z^n + \overline{a}_{n-1}z^{n-1} + \ldots + \overline{a}_1 z + \overline{a}_0 = 0.$$

Nesse caso, tomando conjugado de ambos os membros, obtemos:

$$a_n \overline{z}^n + a_{n-1}\overline{z}^{n-1} + \ldots + a_1 \overline{z} + a_0 = 0.$$

Logo, $\overline{z}$ é raiz de $A(x)$.

Isso mostra que se o TFA for verdadeiro para polinômios em $\mathbb{R}[x]$, então também vale para polinômios em $\mathbb{C}[x]$.

□

Observaçao 3.3. *Mantidas as notações acima, vele observar que se $z \in \mathbb{C}$ for raiz de $A(x)$, então $\overline{z}$ é raiz de $\overline{A}(x)$. Se $A(x) \in \mathbb{R}[x]$, como nesse caso $A(x) = \overline{A}(x)$, podemos concluir que se $z \in \mathbb{C}$ for raiz de $A(x)$, então $\overline{z}$ também é raiz de $\overline{A}(x)$. Em outras*

palavras, as raízes complexas (não reais) de um polinômio com coeficientes reais aparecem aos pares conjugados. Como consequência, um polinômio de grau impar com coeficientes reais possui pelo menos uma raiz real.

Um imediata consequência do TFA é a seguinte:

Proposição 3.4. *Em $\mathbb{C}[x]$ os únicos polinômios irredutíveis são os lineares.*

Demonstração: De fato, se $P(x) \in \mathbb{C}[x]$ é um polinômio irredutível, então $P(x)$ não é constante. Daí, o TFA garante que existe $z \in \mathbb{C}$ talque $P(z) = 0$. Dessa forma, segue que $X - z$ divide $P(x)$. Agora, pela irredutibilidade de $P(x)$ temos que a única possibilidade é que exista uma constante $a \in \mathbb{C}$, tal que $P(x) = a(x - z)$. Isso Mostra que $P(x)$ é linear.

□

Corolário 3.5. *Em $\mathbb{C}[x]$ todo polinômio se decompõe como produto de polinômios lineares.*

Demonstração: Basta lembrar que todo polinômio com coeficientes em um corpo se decompõe como produto de polinômios iredutíveis, os quais no caso do corpo dos números complexo são necessariamente lineares, conforme a proposição anterior.

□

Lembre que um polinômio linear em $\mathbb{C}[x]$ tem a forma $ax + b$, com $a, b \in \mathbb{C}$ e $a \neq 0$. Podemos ainda reescrever na forma $a(x - z)$, onde $z = -\frac{b}{a}$. Com isso, O resultado acima nos permite escrever um polinômio $P(x) \in \mathbb{C}[x]$ na forma:

$$P(x) = c(x - z_1) \cdot (x - z_2) \cdot (x - z_3) \cdots (x - z_n), \text{ onde } n = \partial P(x).$$

Proposição 3.6. *Em $\mathbb{R}[x]$ os únicos polinômios irredutíveis são os lineares e os quadráticos com discriminante negativo..*

Demonstração: Seja $P(x) \in \mathbb{R}[x]$ um polinômio irredutível. Assim $P(x)$ não é constante e vamos considerar dois casos: Se o grau de $P(x)$ for impar, então pela observação 3.3 $P(x)$ possui raiz real, digamos $a \in \mathbb{R}$. Nesse caso $X - a$ divide $P(x)$, o que pela irredutibilidade permite concluir que $P(x)$ é linear. No caso em que o grau de $P(x)$ seja par, digamos $\partial P(x) = m$ (par), escrevemos a decomposição

$$P(x) = c(x - z_1) \cdot (x - z_2) \cdot (x - z_3) \cdots (x - z_m),$$

onde $z_1, z_2, \ldots z_m \in \mathbb{C}$, são as raizes de $P(x)$.

Note que $z_i \notin \mathbb{R}$, pois do contrário recairíamos no caso anterior, contradizendo o fato do grau ser par. Assim, novamente pela observação 3.3, temos que $\overline{z}_i$ também é raiz $P(x)$. Dessa forma, $\{z_1, z_2, \ldots, z_m\} = \{\overline{z}_1, \overline{z}_2, \ldots, \overline{z}_m\}$. Logo, também podemos escrever

$$P(x) = c(x - \overline{z}_1) \cdot (x - \overline{z}_2) \cdot (x - \overline{z}_3) \cdots (x - \overline{z}_m).$$

Multiplicando essas expressões para $P(x)$, obtemos

$$P(x)^2 = c^2(x^2 - (z_1 + \overline{z}_1)x + z_1\overline{z}_1)(x^2 - (z_2 + \overline{z}_2)x + z_2\overline{z}_2)\dots(x^2 - (z_m + \overline{z}_m)x + z_m\overline{z}_m).$$

Por fim, note que para todo $j = 1, 2, \dots, m$, o polinômio $Q_j(x) = x^2 - (z_j + \overline{z}_j)x + z_j\overline{z}_j$ tem coeficientes reais e é irredutível sobre $\mathbb{R}$, pois tem grau 2 e não possui raiz real. Assim, pela proposição 2.9, segue que por exemplo $Q_1(x)$ divide $P(x)$ em $\mathbb{R}[x]$. Então a irredutibilidade de $P(x)$ sobre $\mathbb{R}$ garante que existe uma constante $a \in \mathbb{R}$ tal que $P(x) = aQ_1(x)$. Isso prova que $P(x)$ é um polinômio quadrático que não possui raiz real. □

4 A REGRA DE SINAIS DE DESCARTES

Embora o TFA garanta que um polinômio com coeficientes em $\mathbb{C}$ possui todas as raízes em $\mathbb{C}$, o referido teorema não indica como podemos encontrar todas essas raízes. De fato, graças aos esforços de matemáticos como Evarist Galois e Abel sabemos que para grau maior que 4 não existe uma fórmula que expresse as raízes de um polinômio em termos de operações elementares envolvendo seus coeficientes.

Por outro lado, em muitos casos nos interessa apenas estimar a quantidade de raízes satisfazendo determinadas condições. Com efeito, um de nossos principais objetivos nesse trabalho é estimar a quantidade de raízes que um polinômio com coeficientes racionais possui em cima do círculo unitário.

No caso de polinômios com coeficientes reais é de interesse estimar a quantidade de raízes em um determinado intervalo. Nesse contexto, diversos resultado podem ajudar. Dentre os quais, citamos o teorema do valor intermediário, que em sua versão para polinômios é conhecido como "Teorema de Bolsano". No entanto, o objetivo dessa seção é apresentar uma outra ferramente, a chamada " Regra de Sinais de Descartes", abreviadamente (RSD). Com esse instrumento, podemos estimar o número de raizes positivas olhando apenas para os coeficientes do polinômio.

Para enunciar o referido resultado, lembramos que dois números reais não nulos a, b têm o mesmo sinal corresponde ao fato que $a \cdot b > 0$. Daí, dado um polinômio $P(x) \in \mathbb{R}[x]$, descartando os eventuais coeficientes nulos, podemos escrevê-lo na forma:

$$P(x) = a_1 x^{n_1} + a_2 x^{n_2} + \ldots + a_k x^{n_k},$$

onde nenhum coeficiente é nulo e convencionamos que $n_1 > n_2 > \ldots > n_k \geq o$.

Com essa notação, definimos a *variação* de $P(x)$, representada por $v(P(x))$, como sendo o número de mudanças de sinais entre os termos de sequência $a_1, a_2, \ldots, a_k$, considerados nessa ordem.

Por exemplo, a variação do polinômio $P(x) = 2X^6 - 3x^3 - x^2 + 2x - 5$ é $v(P(x)) = 3$, pois considerando a sequência $2, -3, -1, 2, -5$ temos três mudanças de sinais.

Por comodidade, introduzimos a notação $R_+(P(x))$ para representar o número de raízes positivas do polinômio. Com essas definições podemos enunciar a regra de sinais de Descartes

Teorema 4.1. *Dado um polinômio $P(x) \in \mathbb{R}[x]$, temos que $R_+(P(x)) \leq v(P(x))$ e além disso $R_+(P(x))$ e $v(P(x))$ têm a mesma paridade.*

Demonstração: Recomendamos cosultar WANG (2004).

A imediata aplicação dessa regra ao polinômio

$$P(x) = 2x^6 - 3x^3 - x^2 + 2x - 5,$$

já nos diz que tal polinômio possui no máximo três raízes positivas, pois $v(P(x)) = 3$. Além disso, como $v(P(x)) = 3$ é impar, segue que $R_+(P(x))$ também é impar. Portanto, o número de raízes positivas desse polinômio é 1 ou 3.

O exemplo acima não foi conclusivo, mas em alguns casos a regras nos fornece uma informação exata. Por exemplo, se um polinômio com coeficientes reais apresentar apenas uma mudança de sinal, isto é, variação $v(P(x)) = 1$. Então tal polinômio possuirá exatamente uma raiz positiva. De fato, nesse caso $R_+(P(x))$ seria impar e $R_+(P(x)) \leq 1$, donde $R_+(P(x)) = 1$.

Para nosso objetivo, precisaremos estimar o número de raízes de um polinômio com coeficientes racionais no intervalo $[-2, 2]$, veja o teorema 5.6. Para isso precisamos adaptar a regra de sinais de Descartes. Nesse sentido, as seguintes notações serão úteis

1. $R_-(P(x))$ é o número de raízes negativas de $P(x)$.
2. $R_a(P(x))$ é o número de raízes de $P(x)$ que são maiores que $a \in \mathbb{R}$.

Observaçao 4.2. *Sejam $a, b \in \mathbb{R}$, com $a < b$. Com as notações acima, é claro que $R_a(P(x)) \geq R_b(P(x))$ e o número de raízes de $P(x)$ no intervalo $(a, b]$ é dado por*

$$R_a(P(x)) - R_b(P(x)).$$

Para estimar os números do tipo $R_a(P(x))$, nos será útil o seguinte resultado.

Lema 4.3. *Dados $P(x) \in \mathbb{R}[x]$ e $a \in \mathbb{R}$, então vale que $R_-(P(x)) = R_+(P(-x))$ e $R_a(P(x)) = R_+(P(x + a))$*

Demonstração: Para fixar ideias, sejam $Q(x) := P(-x)$ e $P_a(x) = P(x + a)$. Agora consideremos os conjuntos

$$X = \{\alpha \in \mathbb{R} | \alpha < 0 \text{ e } P(\alpha) = 0\},$$

$$X_1 = \{\beta \in \mathbb{R} | \beta > 0 \text{ e } Q(\beta) = 0\},$$

$$X_2 = \{\gamma \in \mathbb{R} | \gamma > a \text{ e } P(\gamma) = 0\},$$

$$X_3 = \{\theta \in \mathbb{R} | \theta > 0 \text{ e } P_a(\theta) = 0\}.$$

Daí, basta observar que $\alpha \in X \Leftrightarrow -\alpha \in X_1$. Claramente, $\alpha > 0 \Leftrightarrow -\alpha < 0$ e além disso, como $Q(-) = P(-(-\alpha)) = P(\alpha)$, nos mostra que $P(\alpha) = 0 \Leftrightarrow Q(-\alpha) = 0$. Em outras palavra, a função $\varphi : X \to X_1$, dada por $\varphi(\alpha) = -\alpha$ estabelece uma bijeção entre esses conjuntos.

Do mesmo modo, temos que $\gamma \in X_2 \Leftrightarrow \gamma - a \in X_3$. De fato, temos que

$\gamma > a \Leftrightarrow \gamma - a >$. Por outo lado, temos $P_a(\gamma - a) = P((\gamma - a) + a) = P(\gamma)$ o que mostra que $P(\gamma) = 0 \Leftrightarrow P_a(\gamma - a) = 0$. De outra forma, a função $\psi : X_2 \to X_3$, definida por $\psi(\gamma) = \gamma - a$ determina uma bijação entre os conjuntos X_2 e X_3.

□

Para a próxima proposição, lembramos que dado um polinômio $P(x)$ a notação $P^{(k)}(x)$ indica a sua derivada de ordem "k". Ademais, a derivada de ordem "zero" é o próprio polinômio.

Proposição 4.4. *Dados $P(x) \in \mathbb{R}[x]$ e $a \in \mathbb{R}$, temos que*

$$P(x+a) = \frac{P^{(n)}(a)}{n!}x^n + \frac{P^{(n-1)}(a)}{(n-1)!}x^{n-1} + \ldots + \frac{P^{(2)}(a)}{2!}x^2 + \frac{P^{(1)}(a)}{1!}x^1 + P(a).$$

Demonstração: Segue diretamente da expansão de Taylor para o polinômio $P(x)$, na vizinhança de $x_0 = a$. Veja NASCIMENTO (2015).

Corolário 4.5. *Sejam $P(x) \in \mathbb{R}[x]$, polinômio de grau n, e $a \in \mathbb{R}$. Temos que o número de raízes de $P(x)$ maiores que a não supera número de mudança de sinais na sequência (descartados os termos eventualmente nulos)*

$$P(a), P^{(1)}(a), P^{(2)}(a), \ldots, P^{(n)}(a).$$

Além disso, os dois números referidos têm a mesma paridade.

Demonstração: Basta lembrar que $R_a(P(x))$ (número de raízes de $P(x)$ maiores que a) coincide com $R_+(P_a(x))$(número de raízes positivas de $P(x+a)$. Esse último número, pela regra de Descartes não supera, e tem a mesma paridade que, o número de mudanças de sinais na sequência

$$\frac{P^{(n)}(a)}{n!}, \frac{P^{(n-1)}(a)}{(n-1)!}, \ldots + \frac{P^{(2)}(a)}{2!}, \frac{P^{(1)}(a)}{1!}, P(a).$$

Por fim, é claro que a variação do sinal nesse sequência é a mesma que na sequência

$$P(a), P^{(1)}(a), P^{(2)}(a), \ldots, P^{(n)}(a),$$

pois a ordem relativa dos termos foi mantida e para eliminar os denominadores, multiplicamos por números positivos, o que mostra que os sinais dos respectivos termos também não foram alterados.

□

5 POLINÔMIOS COM RAÍZES NO CÍRCULO UNITÁRIO

Neste capítulo vamos apresentar resultados que caracterizam os polinômios com coeficientes racionais que possuem raiz no círculo unitário. Para tanto, utilizamos como principal fonte a obra CONRAD (2017).

Sabemos que todo polinômio $P(x) \in \mathbb{Q}[x]$ se fatora como produto de polinômios irredutíveis. Consequentemente, temos que $P(x)$ possui raiz no círculo unitário se e somente se algum de seus fatores irredutíveis possui tal raiz.

Ou seja, é suficiente caracterizar os polinômios irredutíveis em $\mathbb{Q}[x]$ que possuem raiz no círculo unitário. Nesse sentido, começamos destacando o seguinte resultado.

Lema 5.1. *Dados $\alpha \in \mathbb{C}$ e $P(X) \in Q[x]$ um polinômio não nulo tal que $P(\alpha) = 0$, temos que as seguintes afirmações são equivalentes.*

1. *O grau de $P(x)$ é mínimo com respeito a todos os polinômios não nulos em $\mathbb{Q}[x]$ que se anulam em α.*
2. *$P(x)$ divide qualquer outro polinômio $Q(x) \in \mathbb{Q}[x]$ que se anula em α.*
3. *$P(x)$ é irredutível em $\mathbb{Q}[x]$.*

Demonstração:

($1 \Rightarrow 2$)

Usando o algoritmo da divisão escrevemos $Q(x) = P(x)G(x) + R(x)$, com $G(x), R(x) \in \mathbb{Q}[x]$ e Grau$(R(x))$ <Grau$(P(x))$, caso $R(x)$ não seja nulo. Note que $R(\alpha) = Q(\alpha) - P(\alpha)G(\alpha) = 0$. Portanto, a minimalidade do grau de $P(x)$ garante que $R(x)$ é identicamente nulo e como consequência temos que $P(x)$ divide $Q(x)$.

($2 \Rightarrow 3$)

Se $P(x) = F(x).G(x)$, então Grau$(F(x))$ $\leq$Grau$(P(x))$; Grau$(G(x))$ $\leq$Grau$(P(x))$ e $F(\alpha).G(\alpha) = P(\alpha) = 0$. Assim, $F(\alpha) = 0$ ou $G(\alpha) = 0$ e portanto, $P(x)$ divide $F(x)$ ou $P(x)$ divide $G(x)$. No primeiro caso, concluímos que $G(x)$ é constante e no segundo $F(x)$ é constante. Isso mostra que $P(x)$ é irredutível.

($3 \Rightarrow 1$)

Seja $P_1(x)$ um polinômio cujo grau seja mínimo com respeito a todos os polinômios não nulos que se anulam em α. Pelo que já provamos, segue que $P_1(x)$ divide $P(x)$. Mas como $P(x)$ é irredutível, concluímos que existe uma constante não nula $c \in \mathbb{Q}$, tal que $P(x) = cP_1(x)$. Em particular, $P(x)$ e $P_1(x)$ têm o mesmo grau e por

conseguinte concluímos que o grau de $P(x)$ é mínimo com respeito a todos os polinômios não nulos em $\mathbb{Q}[x]$ que se anulam em α.

O resultado seguinte caracteriza os polinômios irredutíveis em $\mathbb{Q}[x]$ que possuem raiz no círculo unitário.

Teorema 5.2. *Seja $P(x)$ um polinômio com coeficientes racionais e irredutível em $\mathbb{Q}[x]$, com grau $n > 1$. Se $P(x)$ tem uma raiz no círculo unitário, então n é par e*

$$x^n P(\frac{1}{x}) = P(x).$$

Demonstração: Seja $\alpha \in \mathbb{C}$ uma raiz de $P(x)$, com $|\alpha| = 1$. Sendo $|\alpha|^2 = \alpha.\overline{\alpha}$, segue que $\overline{\alpha} = \frac{1}{\alpha}$. Como $P(x)$ tem coeficientes reais, sabemos que $P(\overline{\alpha}) = 0$, ou seja, $P(\frac{1}{\alpha}) = 0$. Portanto, α anula o polinômio $Q(x) := x^n P(\frac{1}{x})$.
Por outro lado, Se

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

então

$$P(\frac{1}{x}) = \frac{a_n}{x^n} + \frac{a_{n-1}}{x^{n-1}} + \cdots + \frac{a_1}{x} + a_0.$$

Portanto,

$$Q(x) = x^n P(\frac{1}{x}) = a_n + a_{n-1}x + \ldots + a_1 x^{n-1} + a_0 x^n.$$

Além disso, como $P(x)$ é irredutível e tem grau $n > 1$, segue que $a_0 \neq 0$. Assim, $Q(x)$ é um polinômio em $\mathbb{Q}[x]$ de grau n e α é uma de suas raizes. Dessa forma, devido a irredutibilidade de $P(x)$ o lema 5.1 nos permite concluir que existe $c \in \mathbb{Q}$ tal que $Q(x) = cP(x)$.

Fazendo $x = 1$, temos $Q(1) = c.P(1) \Rightarrow c = 1$, pois que $Q(1) = P(1) \neq 0$ haja vista que $P(x)$ é um polinômio irredutível em $\mathbb{Q}[x]$ de grau $n > 1$. Portanto, $P(x) = Q(x) = x^n P(\frac{1}{x})$. Para o que falta, note que para $x = -1$, temos $P(-1) = (-1)^n P(-1) \Rightarrow (-1)^n = 1 \Rightarrow n$ par, desde que $P(-1) \neq 0$. □

5.1 Polinômios Palindrômicos

Na demonstração do **teorema 5.2** vimos que se o polinômio irredutível $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Q}[x]$ possuir raiz no círculo unitário, então $P(x) = x^n P(\frac{1}{x})$. Mais geralmente, um polinômio $P(x) \in \mathbb{C}[x]$ que satisfaz $P(x) = x^n P(\frac{1}{x})$ é chamado de polinômio *palindrômico*. Note que $P(x)$ ser palindrômico é equivalente a $a_k = a_{n-k}$, para todo $k = 0, 1, 2, \ldots, n$. O resultado a seguir nos diz que se o grau de $P(x)$ for par temos uma outra condição que também é equivalente ao fato de ser palindrômico.

Teorema 5.3. *Para um polinômio $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ com grau*

par, $n = 2m$, as seguintes afirmações são equivalentes:

1. *$a_k = a_{n-k}$ para todo $k \leq n$.*
2. *$x^n P(\frac{1}{x}) = P(x)$.*
3. *$P(x) = x^m g(x + \frac{1}{x})$ para um polinômio $g(X) \in \mathbb{C}[X]$, de grau m.*

Demonstração:

(**1** $\Leftrightarrow$ **2**)

Basta notar que $x^n P(\frac{1}{x}) = a_n + a_{n-1}x + \ldots + a_1 x^{n-1} + a_0 x^n$. Daí, teremos $P(x) = x^n P(\frac{1}{x})$ se e somente se $a_k = a_{n-k}$ para todo $k \leq n$.

(**3** $\Rightarrow$ **2**)

Por hipótese, $P(x) = x^m g(x + \frac{1}{x})$. Daí substituindo x por $\frac{1}{x}$, ficamos com:

$$P(\frac{1}{x}) = \frac{1}{x^m} g(x + \frac{1}{x}).$$

Dessa forma,

$$x^n P(\frac{1}{x}) = x^{2m} \frac{1}{x^m} g(x + \frac{1}{x}) = x^m g(x + \frac{1}{x}) = P(x).$$

(**2** $\Rightarrow$ **3**)

Vamos raciocinar por indução em m.

Se $m = 1$, então $P(x) = a_2 x^2 + a_1 x + a_0 = x(a_2 x + \frac{a_0}{x} + a_1)$, como $a_2 = a_0$, vemos que

$$P(x) = x(a_0(x + \frac{1}{x}) + a_1).$$

Isso mostra que o resultado vale para $m = 1$ com $g(X) = a_0 X + a_1$.

Suponhamos que o resultado vale para todo polinômio palindrômico de grau $2m'$ com $m' < m$ e provemos usando essa hipótese que ele também vale para nosso polinômio $P(x)$, palindrômico de grau $n = 2m$.

Com efeito, começamos considerando o polinômio

$$P_1(x) := P(x) - a_n(x^2 + 1)^m = \sum_{j=0}^{n} a_j x^j - a_n \sum_{l=0}^{m} \binom{m}{l} x^{2l} = \sum_{j=0}^{n} b_j x^j,$$

onde $b_{2k} = a_{2k} - a_n \binom{m}{k}$ e $b_{2k+1} = a_{2k+1}$, para $k = 0, 1, 2, \ldots$

Dessa forma, temos

$$b_{n-(2k+1)} = b_{2(m-k-1)+1} = a_{2(m-k-1)+1} = a_{n-(2k+1)} = a_{2k+1} = b_{2k+1}$$

e

$$b_{n-2k} = b_{2(m-k)} = a_{2(m-k)} - a_n\binom{m}{m-k} = a_{(n-2k)} - a_n\binom{m}{k} = a_{2k} - a_n\binom{m}{k} = b_{2k}.$$

Essas igualdades nos dizem que $P_1(x)$ é palindrômico. Agora, note que se $P_1(x)$ for identicamente nulo, então

$$P(x) = a_n(x^2+1)^m = a_n x^m (x + \frac{1}{x})^m$$

e basta tomarmos $g(X) = a_n X^m$. Por outro lado, se $P_1(x)$ não for identicamente nulo, seja $j_0 \in \{0, 1, 2, \ldots, n\}$ o menor índice tal que $b_{j_0} \neq 0$. Com isso, temos que $b_j = 0$ para todo $j < j_0$ e consequentemente $b_{n-j} = 0$ para todo $j < j_0$, mas $b_{n-j_0} \neq 0$.

Portanto, vemos que

$$P_1(x) = b_{j_0}x^{j_0} + b_{j_0+1}x^{j_0+1} + \ldots + b_{n-j_0}x^{n-j_0} = x^{j_0}P_2(x),$$

onde $P_2(x) = b_{j_0} + b_{j_0+1}x + \ldots + b_{n-j_0}x^{n-2j_0}$ é um polinômio palindrômico de grau $n-2j_0 = 2(m-j_0)$. Note $m - j_0 < m$, pois $b_0 = a_0 - a_n = 0$, de onde vemos que $j_0 \geq 1$. Assim, a hipótese de indução garante que existe um polinômio $g_2(X) \in \mathbb{C}[X]$, de grau $m - j_0$, tal que $P_2(x) = x^{m-j_0}g_2(x + \frac{1}{x})$. Como consequência, segue que

$$P(x) = P_1(x) + a_n x^m (x + \frac{1}{x})^m = x^{j_0}P_2(x) + a_n x^m (x + \frac{1}{x})^m = x^m(a_n(x + \frac{1}{x})^m + g_2(x + \frac{1}{x})).$$

Isso prova o resultado para $P(x)$, bastando tomarmos $g(X) = a_n X^m + g_2(X) \in \mathbb{C}[X]$.

Observaçao 5.4. O polinômio $g(X)$ tal que $P(x) = x^m g(x + \frac{1}{x})$ ´ chamado de transformada de Chebyshev de $P(x)$. A existência de $g(X)$ também pode ser provada observando que

$$P(x) = \sum_{j=0}^{m} a_j(x^j + x^{n-j}) = x^m \sum_{j=0}^{m} a_j(x^{j-m} + x^{m-j}) = x^m \sum_{j=0}^{m} a_{m-j}(x^j + \frac{1}{x^j}).$$

Por outro lado, um argumento indutivo baseado na identidade

$$X^{j+1} + Y^{j+1} = (X+Y)(X^j + Y^j) - XY(X^{j-1} + Y^{j-1})$$

garante que para cada $j \in \mathbb{N}$ existe $g_j(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ tal que

$$X^j + Y^j = g_j(X + Y, XY).$$

Portanto, substituindo X por x e Y por $\frac{1}{x}$ vemos que $x^j + \frac{1}{x^j} = g_j(x + \frac{1}{x}, 1)$. Dessa forma, tomando $g(X) = \sum_{j=0}^{m} a_{m-j} g_j(X, 1)$, segue que $P(x) = x^m g(x + \frac{1}{x})$.

Exemplo 5.5. Para reescrever o polinômio $P(x) = x^8 - x^5 - x^4 - x^3 + 1$ na forma $P(x) = x^m g(x + \frac{1}{x})$, observe que $P(x)$ é palindrômico e tem grau par. Então, pelo Teorema 5.3, é possível reescrevê–lo na forma desejada.

$$P(x) - (x^2 + 1)^4 = x^2(-4x^4 - x^3 - 7x^2 - x - 4) = x^2 P_1(x),$$

onde $P_1(x) = -4x^4 - x^3 - 7x^2 - x - 4$ é um polinômio palindrômico de grau 4 e portanto, podemos repetir o argumento, como segue:

$$P_1(x) + 4(x^2 + 1)^2 = -x^3 + x^2 - x = -x(x^2 - x + 1) = -x^2(x + \frac{1}{x} - 1)$$

Por fim, voltanto ao polinômio $P(x)$, temos:

$$P(x) = (x^2 + 1)^4 + x^2 P_1(x) = x^4[(x + \frac{1}{x})^4 - 4(x + \frac{1}{x})^2 - (x + \frac{1}{x}) + 1]$$

O teorema 5.3 estabelece uma correspondência entre a família de polinômios palindrômicos $P(x)$ de grau $2m$ e as respectivas transformadas de Chebyshev. A seguir, veremos que por meio dessa correspondência as raízes de $P(x)$ no círculo unitário se relacionam com as raízes reais de sua transformada.

Teorema 5.6. *Seja um polinômio $P(x) \in \mathbb{Q}[x]$ um polinômio palindrômico de grau par e seja $g(x) \in \mathbb{Q}[x]$ sua transformada de Chebyshev, isto é, $P(x) = x^m g(x + \frac{1}{x})$. Nessas condições, as raízes de $P(x)$ no círculo unitário, considerando os pares recíprocos, correspondem às raízes de g no intervalo $[-2, 2]$. Explicitamente, a referida correspondência é dada por*

$$(\alpha, \frac{1}{\alpha}) \Leftrightarrow \alpha + \frac{1}{\alpha}.$$

Demonstração: Pela definição, temos $P(x) = 0 \Leftrightarrow g(x + \frac{1}{x}) = 0$ (note que $P(0) = a_0 = a_n \neq 0$). Se $|x| = 1$, então $x = \cos\theta + isen\theta$. Portanto, $x + \frac{1}{x} = 2\cos\theta \in [-2, 2]$. Reciprocamente, para cada $t \in [-2, 2]$ a equação $t = x + \frac{1}{x}$, possui duas raízes x e x', tais que $x + x' = t$ e $x \cdot x' = 1$. Assim, $|x| = 1$ e se $g(t) = 0$, então $f(x) = 0$. Além disso, como $t^2 - 4 \leq 0$, temos que x e x' só são reais quando $t = \pm 2$, caso em que $x = x' = \pm 1$. Para $t \neq \pm 2$ temos que x e x' são complexos conjugados de módulo unitário.

□

O teorema acima reduz o trabalho de contagem das raízes de $P(x)$ no círculo unitário ao trabalho de contagem das raízes de $g(X)$ no intervalo $[-2, 2]$. Dessa forma,

o problema é simplificado, pois trata-se de investigar um novo polinômio cujo grau é metade do grau do polinômio inicial. Porém, permanece o desafio de contar as raízes da transformada de Chebyshev. Para tanto, será fundamental o uso da Regra de Sinais de Descartes como ferramenta facilitadora.

Observaçao 5.7. Destacamos que a relação $t = 2\cos\theta$, observada na demonstração acima, nos diz que as raízes negativas de $g(X)$ no intervalo $(-2, 2)$, correspondem a pares conjugados de raízes de $P(x)$ localizadas no semiplano complexo onde a parte real é negativa. Do mesmo modo, as raízes positivas de $g(X)$ em $(-2, 2)$, correspondem a pares conjugados de raízes de $P(x)$ localizadas no semiplano complexo onde a parte real é positiva. Por outro lado cada raiz real positiva de $g(X)$ fora do intervalo $[-2, 2]$ corresponde a um par de raízes reais positivas de $P(x)$, cujo produto é 1. Da mesma forma, cada raiz real negativa de $g(X)$ fora do intervalo $[-2, 2]$ corresponde a um par de raízes reais nagativas de $P(x)$, de produto 1.

5.2 Aplicações

Vamos apresentar algumas aplicações do Teorema 5.6. Naturalmente, todos os exemplos apresentados aqui tratam-se de polinômios palindrômicos, pois como vimos no teorema 5.2, essa é uma condição necessária para que um polinômio irredutível possua raiz no círculo unitário.

No caso geral, para sabermos se um polinômio com coeficientes racionais possui raiz no círculo unitário, precisamos decompô-lo como produto de fatores irredutíveis e verificar se algum desse fatores é palindrômico. Acompanhando cada um dos exemplos, segue a respectiva representação geométrica das raízes no plano complexo.

Obsevamos que a notação $g^{(k)}(X)$ indica a derivada de ordem "k" do polinômio $g(X)$.

Exemplo 5.8. O polinômio $P(x) = x^4 - 2x^3 - 2x + 1$ é palindrômico de grau 4 (par) e, conforme o teorema 5.3, pode ser escrito da seguinte forma:

$$P(x) = x^2[(x + \frac{1}{x})^2 - 2(x + \frac{1}{x}) - 2]$$

Para saber quantas raízes no círculo unitário possui $P(x)$ é suficiente determinar quantas raízes em $[-2, 2]$ possui a transformada de Chebyshev $g(X) = X^2 - 2X - 2$ de $P(x)$. Para isso, utilizaremos o lema 4.5.

Pelo referido lema, temos que a quantidade de raízes maiores que 2 não supera

(e tem a mesma paridade) a variação no sinal dos termos da sequência:

$$g(2) = -2, g^{(1)}(2) = 2, g^{(2)}(2) = 2.$$

Notamos que ocorre uma variação de sinal, então concluímos que $g(X)$ possui uma raiz real maior que 2.

Por outro lado, o mesmo lema garante que a quantidade de raízes maiores que -2 não supera (e tem a mesma paridade) a variação no sinal dos termos da sequência

$$g(-2) = 6, g^{(1)}(-2) = -6, g^{(2)}(-2) = 2.$$

Percebemos duas mudanças de sinal. Logo, $g(X)$ possui duas ou nenhuma raiz real maior que -2. Como já sabemos que G(X) possui uma raiz maior que 2, então necessariamente existe duas raízes maiores que -2, uma das quais é negativa e pertence ao intervalo $(-2, 2) \subset [-2, 2]$.

Portanto, $g(X)$ admite apenas uma raiz em $[-2, 2]$, que é negativa, veja que -2 e 2 não são raízes de $g(X)$. Como se pode ver em CONRAD (2017) , as raízes de $g(x)$ são aproximadamente -0.732 e 2.732.

Pelo teorema 5.6, significa dizer que $P(x) = x^4 - 2x^3 - 2x + 1$ possui duas raízes conjugadas no círculo unitário. Conforme a observação 5.7, essas raízes localizam-se no semiplano onde a parte real é negativa.

Por fim, a regra de sinais de Descartes aplicada diretamente ao polinômio $P(x)$, nos diz que tal polinômio possui 2 ou nenhuma raiz real positiva, pois a sequência de coeficientes de $P(x) : 1, -2 - 2, 1$ apresenta variação igual a 2.

Por outro lado, de acordo com o lema 4.5, o número de raízes de $P(x)$ que são maiores do que 1 não supera, e tem a mesma paridade que, a variação de sinal nos termos da sequência:

$$P(1) = -2, P^{(1)}(1) = -4, P^{(2)}(1) = 0, P^{(3)}(1) = 12, P^{(4)}(1) = 24.$$

Como temos apenas uma mudança de sinal, segue que nosso polinômio $P(x)$ possui uma raiz maior que 1. Daí, dado que já sabemos que existem duas ou nenhuma raiz positiva, segue que de fato, existem duas tais raízes.

Em outras palavras, das quatro raízes de $P(x)$, duas são complexas conjugadas e estão no círculo unitário e as outras duas são números reais positivos, uma das quais é maior que 1. Também poderíamos chegar a essa conclusão, usando o fato que $g(X)$ possui uma raiz real maior que 2, veja a observação 5.7.

A seguir reproduzimos a representação geométrica das quatro raízes de $P(x)$:

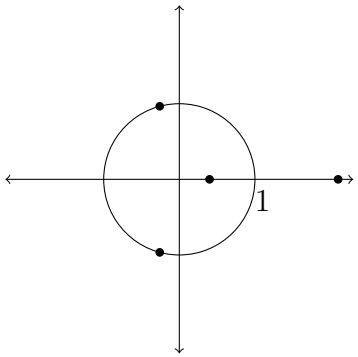

Figura 8 : Raízes de $x^4 - 2x^3 - 2x + 1$

Exemplo 5.9. O polinômio palindrômico de grau par $P(x) = x^6 - x^4 + 2x^3 - x^2 + 1$ pode ser reescrito como:

$$x^3[(x + \frac{1}{x})^3 - 4(x + \frac{1}{x}) + 2]$$

Iniciaremos investigando quantas raízes em $[-2, 2]$ possui a transformada de Chebyshev $g(X) = X^3 - 4X + 2$ de $P(x)$.

Ora, o número procurado é dado por $R_{(-2)}(g(X)) - R_{(2)}(g(X))$. Novamente, o lema 4.5 nos diz como estimar cada uma dessas parcelas.

Como a sequência $g(2) = 2, g^{(1)}(2) = 8, g^{(2)}(2) = 12, g^{(3)}(2) = 6$, não apresenta variação de sinal, concluímos que $g(X)$ não possui raiz real maior que 2, isto é, $R_2(g(X)) = 0$.

Observando agora $g(-2) = 2, g^{(1)}(-2) = 8, g^{(2)}(-2) = -12, g^{(3)}(-2) = 6$, percebemos duas mudanças de sinal. Logo $g(X)$ possui duas ou nenhuma raiz real maior que -2.

Para dirimir a ambiguidade na determinação de $R_{-2}(G(X))$, consideremos a sequência

$$g(1) = -1, g^{(1)}(1) = -1, g^{(2)}(1) = 6, g^{(3)}(1) = 6.$$

Como temos apenas uma variação de sinal, segue que $g(X)$ possui uma raiz real maior que 1. Consequentemente, pelo que já vimos, $g(X)$ admite duas raizes em $[-2, 2]$. Observe que como $g(X)$ tem grau 3, a outra raiz também será real negativa fora do intervalo $-2, 2]$(pode-se verificar que $g(x)$ possui as seguintes raízes, $-2.214, 0.539$ e 1.675, em valores aproximados). Isso significa dizer que $P(x)$ possui dois pares de raízes conjugadas no círculo unitário.

As duas outras raízes de $P(x)$, de acordo com a observação 5.7 são reais e negativas com produto igual a 1, pois como vimos $g(X)$ possui uma raiz negativa fora do intervalo $[-2, 2]$.

Dessa forma, das seis raízes de $P(x)$, temos dois pares de raízes complexas con-

jugadas de módulo unitário localizadas no semiplano complexo cuja parte real é positiva e as outras duas são números reais negativos com produto igual a 1.

Temos a seguinte representação geométrica para as raízes de $P(x)$:

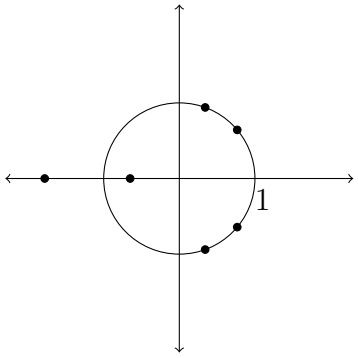

Figura 9 : Raízes de $x^6 - x^4 - 2x^3 - x^2 + 1$

Exemplo 5.10. O polinômio $P(x) = x^8 + 4x^6 - x^5 + 5x^4 - x^3 + 4x^2 + 1$ é palindrômico de grau par e pode ser escrito da seguinte forma:

$$P(x) = x^4[(x + \frac{1}{x})^4 - (x + \frac{1}{x}) - 1]$$

Logo sua transformada de Chebyshev é $g(X) = X^4 - X - 1$. Vamos estimar $R_{(-2)}(g(X))$ e $R_{(2)}(g(X))$.

Observe inicialmente que a regra de sinais de Descartes garante que $g(X)$ possui exatamente uma raiz positiva, pois a sequência de coeficientes $1, -1, -1$ apresenta variação igual a 1.

Por outro lado, como $g(-X) = X^4 + X - 1$, vemos que $g(-X)$ possui exatamente uma raiz positiva e por isso, $g(X)$ possui exatamente uma raiz negativa (veja 4.3). Assim, $g(X)$ possui exatamente duas raízes reais (uma positiva e uma negativa).

Observando $g(2) = 13, g^{(1)}(2) = 31, g^{(2)}(2) = 48, g^{(3)}(2) = 48, g^{(4)}(2) = 24$, notamos que não houve variação de sinal, então concluímos que $g(X)$ não possui raiz real maior que 2. Daí, a única raiz positiva de $g(X)$ é menor que 2. Em particular, está em $[-2, 2]$. De fato, pode-se verificar que as raízes de $g(X) = X^4 - X - 1$ são aproximamadamente -0.724 e $1, 22$.

Por sua vez, a sequência

$$g(-2) = 17, g^{(1)}(-2) = -33, g^{(2)}(-2) = 48, g^{(3)}(-2) = -48, g^{(4)}(-2) = 24,$$

apresenta quatro mudanças de sinal. Logo $g(X)$ possui quatro, duas ou nenhuma raiz real maior que -2. Como já sabemos que $G(x)$ possui exatamente duas raizes reais (uma das quais é positiva), só nos resta uma possibilidade, a saber, $g(X)$ possui duas raizes reais maiores que -2, as quais necessariamente estão em $[-2, 2]$. Consequentemente, $g(X)$ não possui raiz real fora do intervalo $[-2, 2]$, e então $P(x)$ não possui raiz real.

Assim, podemos concluir que $P(x) = x^8 + 4x^6 - x^5 + 5x^4 - x^3 + 4x^2 + 1$ não

possui rais real e possui dois pares de raízes conjugadas no círculo unitário, conforme representação geométrica abaixo.

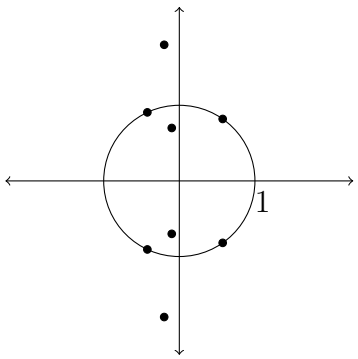

Figura 10 : Raízes de $x^8 + 4x^6 - x^5 + 5x^4 - x^3 + 4x^2 + 1$

Exemplo 5.11. Para o polinômio $P(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$, que é palindrômico de grau 10, podemos reescrever:

$$P(x) = x^5[(x + \frac{1}{x})^5 + (x + \frac{1}{x})^4 - 5(x + \frac{1}{x})^3 - 5(x + \frac{1}{x})^2 + 4(x + \frac{1}{x}) + 3].$$

Assim, sua transformada de Chebyshev é $g(X) = X^5+X^4-5X^3-5X^2+4X+3$. Observando a sequência

$$g(2) = -1, g^{(1)}(2) = 32, g^{(2)}(2) = 138, g^{(3)}(2) = 258, g^{(4)}(2) = 264, g^{(5)}(2) = 120,$$

notamos que houve apenas uma variação de sinal, então concluímos que $g(X)$ possui exatamente uma raiz real maior que 2.

Com isso, a regra de sinais de Descartes garante que $g(X)$ possui exatamente duas raizes positivas, pois a sequência de coeficientes $1, 1, -5, -5, 4, 3$ apresenta variação igual a 2 e já sabemos que existe uma raiz maior que 2. Em outras palavras, $g(X)$ possui duas raízes positivas: uma maior e outra menor que 2.

Por sua vez, temos que

$$g(-2)=-1, g^{(1)}(-2)=12, g^{(2)}(-2)=-62, g^{(3)}(-2)=162, g^{(4)}(-2)=-216, g^{(5)}(-2)=120$$

apresenta cinco mudanças de sinal. Logo $g(X)$ possui uma, três ou cinco raízes reais maiores que -2. Como já sabemos que $g(x)$ possui exatamente duas raízes reais positivas, segue que $g(X)$ possui três ou cinco raízes maiores que -2.

Como a análise acima não foi conclusiva, vamos estimar o números de raízes

de $g(X)$ maiores que -1. Para isso, consideremos a sequência

$$g(-1)=-1, g^{(1)}(-1)=0, g^{(2)}(-1)=12, g^{(3)}(-1)=6, g^{(4)}(-1)=-96, g^{(5)}(-1)=120$$

que apresenta três mudanças de sinal. Logo $g(X)$ possui uma ou três raízes reais maiores que -1. Como já sabemos que $g(x)$ possui exatamente duas raízes reais positivas, segue que $g(X)$ possui exatamente três raízes maiores que -1.

Além disso, a sequência

$$g(-\frac{3}{2})=\frac{3}{32}, g^{(1)}(-\frac{3}{2})=-\frac{47}{16}, g^{(2)}(-\frac{3}{2})=-\frac{11}{2}, g^{(3)}(-\frac{3}{2})=69, g^{(4)}(-\frac{3}{2})=-156, g^{(5)}(-\frac{3}{2})=120$$

apresenta quatro mudanças no sinal. Logo,$g(X)$ possui quatro, duas ou nenhuma raiz maior que $-\frac{3}{2}$. Mas, como já sabemos que $g(x)$ possui três raízes maiores que -1 podemos concluir que $g(X)$ admite quatro raízes maiores que $-\frac{3}{2}$.

Ora, descobrimos anteriormente que $g(X)$ possui três ou cinco raizes maiores que -2, então podemos concluir que $g(X)$ admite cinco raízes maiores que -2, sendo uma delas maior que 2. Em outras palavras, todas as raízes de $g(X)$ são reais, quatro delas estão no intervalo $[-2, 2]$ e a outra é maior que 2.

De fato, pode-se verificar com a ajuda de uma máquina que $g(X)$ possui, em valores aproximados, as seguintes raízes, $-1.886, -1.468, -0.584, 0.913, 2.026$.

Dessa forma, das dez raízes de $P(x)$, temos quatro pares de raízes complexas conjugadas de módulo unitário e as outras duas são números reais positivos cujo produto é 1.

A seguir a representação geométrica das raízes de $P(x)$

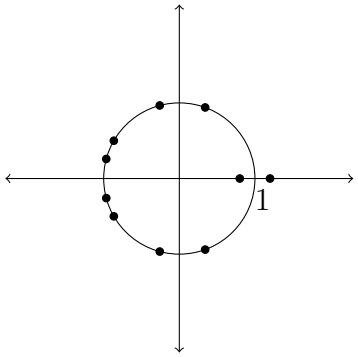

Figura 11 : Raízes de $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$

6 CONCLUSÃO

O presente trabalho foi um estudo sobre os polinômios $P(x)$ em $\mathbb{Q}[x]$ que possuem raízes no círculo unitário. Isso me proporcionou aprender sobre como caracterizar essa família de polinômios $P(x)$ e saber mais sobre os polinômios palindrômicos. Além disso, estudei sobre o algoritmo que obtém as transformadas de Chebyshev de $P(x)$ e sobre as correspondências das raízes de P(x) com as raízes de suas tranformadas de Chebyshev no intervalo [-2,2]. Elenquei, ainda, a Regra dos Sinais de Descartes como ferramenta para elucidar a quantidade de raízes reais das transformadas de Chebyshev no intervalo $[-2, 2]$.

O estudo desse tema limitou-se a investigar polinômios de coeficientes racionais que possuem raízes no círculo untário. No entanto, essa pesquisa pode ser extendida para polinômios de coeficientes reais, e mais geralmente, coeficientes complexos. Para tanto, é importante estudar transformação de Möbius, em especial a correspondência entre o eixo real e o disco unitário, a fim de ampliar a compreensão desses polinômios.

Por fim, esse estudo me permitiu conhecer mais a fundo problemas relacionados a famílias de polinômios palindrômicos e, principalmente sobre os polinômios $P(x)$ em $\mathbb{Q}[x]$ que possuem raízes no círculo unitário. Em contato com outros trabalhos sobre o assunto, obtive uma visão mais ampla dos principais problemas ligados a esse tópico.

Além disso, minha dedicação a esse trabalho contribuiu para sedimentar novos conhecimentos em temas correlatos e ajudou-me a aperfeiçoar um modo mais rigoroso de escrever em linguagem Matemática.

REFERÊNCIAS

GARBI, Gilberto Geraldo. **Romance das Equações Algébricas.** São Paulo: Livraria da Física, 2010.

NASCIMENTO, Carlos Kleber Alves. **Polinômios, equações algébricas e o estudo de suas raízes reais**. 2015. 81f. Dissertação (Mestrado em Matemática em Rede Nacional) – Centro de Ciências,Universidade Federal do Ceará, Fortaleza, 2015.

WANG, Xiaoshen. **A Simple Proof of Descartes's Rule of Signs.** *Virginia: American Mathematical Monthly*, v. 111, p. 525–526, 2004.

CONRAD, Keith. **Roots on a Circle.** Keith Conrad's Home Page. Disponível em: <https://kconrad.math.uconn.edu/blurbs/galoistheory/numbersoncircle.pdf>. Acesso em: 11 de maio, 2017.

MUNIZ NETO, Antonio Caminha. **Polinômios**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.