Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional

Equações Polinomiais e Números Transcendentes

Cleuber Brasil de Siqueira

Goiânia

2015

sistema de bibliotecas ufg

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR ELETRONICAMENTE OS TRABALHOS DE CONCLUSÃO DE CURSO NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **Trabalho de Conclusão de Curso de Mestrado Profissional**

2. Identificação do Trabalho

Autor (a):	Cleuber Brasil de Siqueira						
E-mail:	cleuber.brasil@hotmail.com						
Seu e-mail pode ser disponibilizado na página? [X]Sim [ ] Não							
Vínculo empregatício do autor	Professor da Rede Estadual de Ensino de Goiás						
Agência de fomento:	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior				Sigla:	CAPES	
País:	Brasil	UF:	DF	CNPJ:	00.889.834/0001-08		
Título:	Equações Polinomiais e Números Transcendentes						
Palavras-chave:	Equações Polinomiais, Números Algébricos, Números Transcendentes						
Título em outra língua:	Polynomial Equations and Transcendent Numbers						
Palavras-chave em outra língua:	Polynomial Equations, Algebraic Numbers, Transcendent Numbers.						
Área de concentração:	Matemática do Ensino Básico						
Data defesa: (dd/mm/aaaa)	27/03/2015						
Programa de Pós-Graduação:	Programa de Mestrado Profissional em Matemática em Rede Nacional						
Orientador (a):	Prof. Dr. Durval José Tonon						
E-mail:	djtonon@gmail.com						
Co-orientador(a):*							
E-mail:							

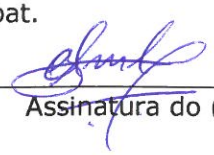
*Necessita do CPF quando não constar no SisPG

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF ou DOC do trabalho de conclusão de curso.

O sistema da Biblioteca Digital de Teses e Dissertações garante aos autores, que os arquivos contendo eletronicamente as teses, dissertações ou trabalhos de conclusão de curso, antes de sua disponibilização, receberão procedimentos de segurança, criptografia (para não permitir cópia e extração de conteúdo, permitindo apenas impressão fraca) usando o padrão do Acrobat.



Assinatura do (a) autor (a)

Data: 08 / 04 / 2015

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

Cleuber Brasil de Siqueira

Equações Polinomiais e Números Transcendentes

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Área de Concentração: Matemática do Ensino Básico

Orientador: Prof. Dr. Durval José Tonon

Goiânia

2015

Ficha catalográfica elaborada automaticamente
com os dados fornecidos pelo(a) autor(a), sob orientação do Sibi/UFG.

Siqueira, Cleuber Brasil de
Equações Polinomiais e Números Transcendentes [manuscrito] /
Cleuber Brasil de Siqueira. - 2015.
91 f.: il.

Orientador: Prof. Dr. Durval José Tonon.
Dissertação (Mestrado) - Universidade Federal de Goiás, Instituto de
Matemática e Estatística (IME) , Programa de Pós-Graduação em
Ensino na Educação Básica (Profissional), Goiânia, 2015.
Bibliografia.
Inclui símbolos, gráfico, lista de figuras.

1. Equações Polinomiais. 2. Números Algébricos. 3. Números
Transcendentes. I. Tonon, Durval José, orient. II. Título.

Cleuber Brasil de Siqueira

Equações Polinomiais e Números Transcendentes

Trabalho de Conclusão de Curso defendido no Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFG, do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como requisito parcial para obtenção do título de Mestre em Matemática, área de concentração Matemática do Ensino Básico, aprovado no dia 27 de março de 2015, pela Banca Examinadora constituída pelos professores:

Prof. Dr. Durval José Tonon
Instituto de Matemática e Estatística-UFG
Presidente da Banca

Prof. Dr. Moiseis dos Santos Cecconello
ICET/UFMT

Prof. Dr. Mário José de Souza
Instituto de Matemática e Estatística-UFG

Cleuber Brasil de Siqueira graduou-se em Matemática pela Universidade Federal de Goiás no ano de 2003 e especializou-se em Matemática do Ensino Básico em 2009, também pela Universidade Federal de Goiás.

Dedico este trabalho à minha esposa Dulce Helena, minha mãe Maria Aparecida, minha irmã Clécia França, ao meu filho João Lucas, que está para nascer e em memória de meu pai João Fernandes e do meu avô Antônio Martins que partiram em meio à minha jornada, mas me deram força enquanto puderam.

Agradecimentos

Agradeço a Deus, que me guia em todos os momentos da minha vida; ao meu pai que, enquanto esteve presente, me apoiou e acreditou neste projeto; à minha mãe por todo o carinho a mim dedicado; à minha esposa, que sempre esteve ao meu lado em todos os momentos. Agradeço ainda à CAPES, pelo apoio financeiro; aos meus colegas do PROFMAT, que lutaram comigo até aqui; e ao meu orientador, Professor Durval José Tonon, pela confiança, paciência e dedicação ao longo do trabalho.

Resumo

O trabalho tem como foco principal o estudo das Equações Polinomiais e uma introdução aos Números Transcendentes, com enfoque especial aos números de Liouville. No entanto, aborda também temas importantes como os conjuntos numéricos, a teoria dos números inteiros, a enumerabilidade de conjuntos e o estudo de polinômios, buscando sempre fazer ligações entre os assuntos através de exemplos pertinentes aos mesmos.

Palavras-chave Equações Polinomiais, Números Algébricos, Números Transcendentes.

Abstract

The work is mainly focused on the study of Polynomial Equations and an introduction to the Transcendent Numbers with a special focus to Liouville numbers. However, it also approaches important issues such as numerical sets, the theory of whole numbers, the enumerability sets and the study of polynomials and always seeking to make connections between issues through relevant examples to them.

Keywords

Polynomial Equations, Algebraic Numbers, Transcendent Numbers.

Lista de Figuras

Sumário

1 Introdução

A construção e formalização dos conjuntos numéricos, tal como os conhecemos hoje, data de séculos atrás e se confunde com a própria história da matemática. Desde os tempos antes de Cristo, as atividades humanas, por mais simples que fossem, dependiam de números e cálculos numéricos. Seja para a simples contagem de um rebanho de ovelhas, para se medir terras férteis para o plantio ou para o escambo de mercadorias, a matemática sempre esteve presente no desenvolvimento da humanidade e seu próprio desenvolvimento se deu através destas relações. As equações polinomiais surgem naturalmente neste contexto. Há registros de que por volta de 1800 a.C, os babilônios já trabalhavam alguns métodos de resolução de equações quadráticas.

Assim, a vários séculos, diversos pensadores, estudiosos e matemáticos (termo que não era utilizado na antiguidade), deram suas contribuições para o estudo das equações polinomiais, trazendo novas técnicas e procedimentos de resoluções ou provando a sua impossibilidade em determinados casos. Daí, em diferentes áreas e ciências, surgiram novas ideias e teorias, como os números complexos e os números transcendentes, como pode ser visto em [6] e [7].

Neste trabalho, os focos principais são o estudo das equações polinomiais e uma introdução aos números transcendentes, com ênfase aos números conhecidos como *Números de Liouville*, em homenagem ao matemático francês que foi o primeiro a trabalhar com esse tipo de número. Porém, procuramos dar um encadeamento lógico ao texto, falando primeiramente sobre os conjuntos numéricos, equações e por último, sobre os transcendentes.

Desta forma, no Capítulo 2, tratamos dos Conjuntos Numéricos. Trazendo em sequência os naturais, inteiros, racionais, irracionais e complexos, buscamos interligar o desenvolvimento dos conjuntos através dos tempos e dos grandes matemáticos que

contribuíram no seu desenvolvimento. Destacam-se uma pequena abordagem sobre aproximações de números irracionais por racionais e o tópico sobre números complexos e suas propriedades geométricas.

O Capítulo 3, que é essencialmente teórico, traz o embasamento necessário aos capítulos seguintes, tratando de parte da teoria de números inteiros e da enumerabilidade de conjuntos numéricos.

No Capítulo 4, fazemos o estudo dos polinômios e das equações polinomiais tais como são abordados no Ensino Médio, que é nosso público alvo. No início do capítulo, procuramos trazer um contexto histórico da evolução das técnicas de resolução de tais equações. Destacam-se aí as demonstrações dos teoremas (exceto pelo *Teorema Fundamental da Álgebra*, cuja prova foge aos objetivos do trabalho) e justificativas de suas utilizações (fato que pouco é trabalhado em sala de aula), além dos exemplos pertinentes à cada tópico.

A seguir, no Capítulo 5, definimos números *inteiros algébricos, algébricos e transcendentes* e provamos a existência dos *transcendentes*, aqueles que não podem ser raízes de equações polinomiais com coeficientes inteiros. Trazendo no final alguns exemplos de famosos números que comprovadamente são transcendentes.

O Capítulo 6 trata dos números de *Liouville*, que foi o primeiro matemático a provar a existência dos transcendentes e definiu um critério para determinar se um número é ou não transcendente. O número determinado por ele em 1844, a saber:

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} = 0,110001000000000000000001...,$$

ficou conhecido como *constante de Liouville* e foi o primeiro número reconhecido pelos matemáticos como transcendente. Por trazer em detalhes o critério mencionado, o capítulo é bastante técnico e exigirá uma atenção maior por parte do leitor. No final, inserimos uma aplicação relativa à esta constante.

Finalmente, no Capítulo 7, apresentamos algumas atividades pertinentes aos assuntos trabalhados, que podem ser desenvolvidas em sala de aula com alunos do Ensino Médio, desde que haja uma boa introdução e fundamentação dos temas e um mínimo de interesse por parte dos estudantes.

O trabalho destina-se a professores do Ensino Básico, como fonte de pesquisa e iniciação ao estudo dos números transcendentes, bem como a alunos do Ensino Médio que buscam aprimorar seus conhecimentos.

2 Conjuntos Numéricos

Neste capítulo, falaremos sobre os conjuntos numéricos, buscando trazer o contexto histórico em que foram sendo inseridos e necessários nas atividades humanas.

2.1 Números Naturais, Inteiros e Racionais

Desde os primórdios, o homem se deparou com a necessidade de fazer contagens. Vestígios de sua importância foram encontrados em cavernas, em desenhos rudimentares de animais ou objetos acompanhados de pequenos traços, dando uma clara idéia de correspondência. Mais tarde, com o início das atividades agrícolas e de pecuária, passou-se a estabelecer correspondências entre conjuntos, usando os dedos das mãos, uma porção de pedras e outros, para contar rebanhos, fazer trocas, etc. Desta forma, "contar" é a atividade matemática mais antiga da humanidade, conforme foi abordado em [8].

Com o passar do tempo, foi percebida a necessidade de se "padronizar" a contagem. Isto é, deu-se início à criação de um processo que fosse universal entre as sociedades da época. Daí originou-se a ideia de números, que inicialmente eram simplesmente relacionados à quantidades, usando um processo de equivalência que atualmente chamamos de correspondência biunívoca. Posteriormente foram simbolizados tais quais os conhecemos hoje e receberam o nome de Números Naturais, como pode ser visto em [8]. Portanto, é importante destacar que, historicamente, a contagem antecede os números.

O Conjunto dos Números Naturais é representado por:

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, ...\}$$

Observe que o número zero (0) não aparece no conjunto acima. Na verdade, apesar

de o dígito zero já ser usado como notação de posição desde cerca de 700 a.C. (como em 100, 1000, etc.), o uso do zero como representação da inexistência, do "nulo" ou "nada", é relativamente recente. Alguns autores trazem o zero como o primeiro dos números naturais, da mesma forma que outros não o fazem, não existindo um consenso em relação ao assunto. No entanto, a exclusão do zero como natural é conveniente do ponto de vista teórico, evitando exceções em diversas propriedades. Assim, em nosso trabalho, ao nos referirmos aos números naturais, excluiremos o número zero.

Com o início do Renascimento surgiu a expansão comercial, que aumentou a circulação de mercadorias, obrigando os comerciantes a expressarem situações envolvendo lucros e prejuízos. A maneira que eles encontraram de resolver tais situações problemas consistia no uso dos símbolos + e -. Utilizando essa nova simbologia, os matemáticos da época desenvolveram técnicas operatórias capazes de expressar qualquer situação envolvendo números positivos e negativos. Surgia um novo conjunto numérico representado pela letra $\mathbb{Z}$ (Zahlen: número em alemão), sendo formado pelos números naturais, seus respectivos opostos e pelo zero (agora uma necessidade). A partir de então, os naturais passaram a ser denominados também de "inteiros positivos". Assim:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

Assim como a necessidade de contar, a necessidade de medir acompanha o homem há séculos. Os comerciantes precisavam medir um produto, os agricultores medir uma cerca, etc. As medições eram feitas fazendo comparações entre o que se queria medir e objetos de tamanho conhecido. Desta forma, observavam e registravam quantas vezes um determinado objeto "cabia" dentro do outro. Como em muitas vezes essa medida não era exata, começaram a representá-las através de frações como: $\frac{1}{2}, \frac{2}{3}, \frac{5}{4}$, etc. Desta forma, deu-se início à ideia de números racionais, que antecede até mesmo a ideia de números negativos.

Mais tarde, os números racionais foram formalizados como todo número que pode ser escrito na forma de uma razão entre dois inteiros ($\frac{a}{b}, b \neq 0$) e representados pela letra $\mathbb{Q}$ (quotiéns - quantas vezes, em latim). Naturalmente, como todo inteiro a pode ser escrito como $\frac{a}{1}$, deduzimos que todo inteiro também é um número racional. Observe que na notação de um número racional $\frac{a}{b}$, é exigido que b seja diferente de zero. A exigência é necessária pois $\frac{a}{b}$ representa também a divisão de a por b e, como se sabe, zero não pode ser um divisor.

Exemplo 1. $\frac{21}{3} = 7$

Exemplo 2. $\frac{3}{2} = 1,5$

Exemplo 3. $\frac{5}{10} = \frac{1}{2} = 0,5$

Exemplo 4. $\frac{2}{25} = 0,08$

Exemplo 5. $\frac{10}{3} = 3,333...$

Exemplo 6. $\frac{5}{11} = 0,454545...$

Observando os exemplos, percebemos que frações distintas podem representar o mesmo número racional, como no exemplo 3. Nesse caso, a fração $\frac{5}{10}$ é dita *redutível*, pois pode ser simplificada e a fração $\frac{1}{2}$ é dita *irredutível*, pois não pode ser simplificada.

A forma decimal do número racional pode ser um número inteiro (quando a divisão do numerador pelo denominador é exata), como no Exemplo 1; uma representação decimal finita, como os Exemplos 2, 3 e 4; ou uma representação decimal infinita, que será chamada de *dízima periódica*. A fração equivalente à dízima periódica é chamada de *fração geratriz*. As dízimas periódicas podem ser simbolizadas colocando-se uma barra acima das casa decimais que se repetem, chamadas de *período* da dízima, como ilustrado abaixo:

$$\frac{5}{11} = 0,454545... = 0,\overline{45}; \quad \frac{1}{3} = 0,333... = 0,\overline{3}; \quad \frac{1}{6} = 0,16666... = 0,1\overline{6}$$

É possível provar que um número racional $\frac{a}{b}$ só tem representação decimal finita se b não tiver outros fatores primos, além de 2 ou 5. Nos Exemplos 2, 3 e 4, os denominadores são: $2; 10 = 2.5$ e $25 = 5.5$.

É interessante observar que, mesmo os números com representação decimal finita, também possuem representações decimais infinitas. Por exemplo, $5,7 = 5,70000... = 5,699999....$ Neste exemplo, a primeira igualdade é obvia, pois podemos colocar quantos zeros quisermos à direita de $5,7$ que a igualdade continua verdadeira. A segunda porém nos traz um certo incômodo. Não parece estranho que $5,7$ seja igual a $5,699999...$? Na verdade a prova de que a igualdade é verdadeira é relativamente simples. Basta proceder como a seguir:
Considere o número $x = 5,699999....$ Logo:

$$10x = 56,99999... \tag{1}$$

$$100x = 569,9999... \tag{2}$$

Subtraindo a equação (1) da equação (2), temos:

$$90x = 513 \Rightarrow x = \frac{513}{90} = 5,7$$

Assim, usando processo semelhante, podemos dizer que $3,45 = 3,45000... = 3,44999999...$; $2,1 = 2,10000... = 2,099999...$, etc.

Pelo que foi colocado, os números decimais finitos e as dízimas periódicas também são números racionais. A formalização dos números racionais é dada por:

$$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}.$$

Uma importante observação que podemos fazer é que os números racionais são fechados em relação às operações de adição, subtração, multiplicação e divisão (exceto

pelo zero, que não pode ser divisor). Ou seja, ao somarmos, subtrairmos, multiplicarmos ou dividirmos dois números racionais, o resultado será sempre um número racional.

2.2 Números Irracionais

Acreditava-se até cerca de 2500 anos atrás, que os números racionais eram suficientes para todas as atividades humanas. No entanto, utilizando o Teorema de Pitágoras, os membros da escola pitagórica observaram que o comprimento da diagonal de um quadrado de lado 1 não poderia ser representado por nenhum número racional. Ou seja, não existe unidade de comprimento, por menor que seja, tal que o lado e a diagonal do quadrado unitário sejam múltiplos inteiros (a esta propriedade entre dois segmentos de reta, chamamos de "incomensurabilidade"). Isso trouxe surpresa e embaraço aos próprios gregos, pois em muitas de suas demonstrações geométricas, supunham que dois segmentos quaisquer sempre admitiam uma unidade de comprimento comum.

Originou-se aí o desenvolvimento de um novo conjunto, o Conjunto dos Números Irracionais, aqueles que não poderiam ser expressos por meio de fração entre dois inteiros. Como a divisão de dois inteiros é sempre exata, decimal finita ou infinita periódica, podemos dizer que a representação decimal de um número irracional é uma dízima não periódica.

Hoje em dia, representamos o comprimento da diagonal do quadrado de lado unitário como a raiz quadrada de 2, como ilustrado na Figura 1. A prova de que $\sqrt{2}$ é irracional é relativamente simples. Porém, será colocada como atividade prática no Capítulo 7, pois precisaríamos de alguns conceitos que ainda não foram abordados.

Outros números irracionais notáveis são: o seno de $60°$ ($sen60° = \frac{\sqrt{3}}{2} = 0,866025403...$), o *pi* ($\pi = 3,141592654...$), que representa a razão entre o perímetro de uma circunferência e seu diâmetro; e o número e ($e = 2,718281828...$), que aparece no estudo das

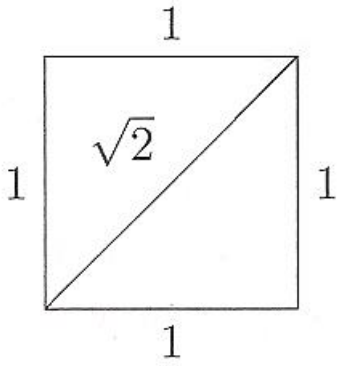


Figura 1: Diagonal do Quadrado de Lado 1

funções logarítmicas e representa a área unitária hachurada abaixo da curva $f(x) = \frac{1}{x}$, conforme a Figura 2. Pode se demonstrar que o valor numérico de e pode ser obtido pela soma:

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + ...$$

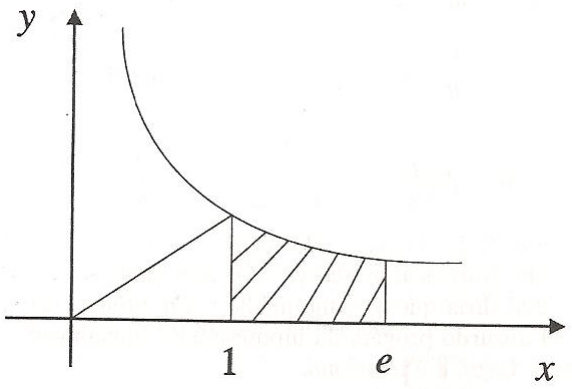


Figura 2: Representação Geométrica de e

Assim, os números irracionais ocorrem naturalmente e de várias maneiras na matemática elementar.

Diferentemente dos números racionais, os irracionais não possuem a propriedade de fechamento. Isto é, ao operarmos dois números irracionais, o resultado nem sempre

é um irracional. Entretanto, é possível provar que ao operarmos um número racional com um irracional, o resultado é outro número irracional.

2.2.1 Aproximação de Irracionais por Racionais

Nesta seção, falaremos brevemente sobre aproximações de números irracionais por racionais. Isso significa que podemos determinar um número racional tão próximo de um irracional quanto for desejado. Apesar de ser um assunto bastante interessante, daremos apenas uma abordagem superficial, pois foge aos objetivos principais do trabalho. Para mais esclarecimentos, sugerimos [6].

Comecemos com um exemplo simples. Vamos considerar o número irracional

$$\sqrt{2} = 1,41421356237....$$

Os números

$$1; 1,4; 1,41; 1,414; 1,4142; 1,41421; ...$$

ou equivalentemente

$$\frac{1}{1}, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \frac{14142}{10000}, \frac{141421}{100000}, ..., \tag{3}$$

formam uma sequência de aproximações cada vez mais próximas de $\sqrt{2}$. Além disso, podemos escrever as desigualdades

$$\begin{aligned}
\frac{1}{1} < \sqrt{2} < \frac{2}{1},\\
\frac{14}{10} < \sqrt{2} < \frac{15}{10},\\
\frac{141}{100} < \sqrt{2} < \frac{142}{100},\\
\frac{1414}{1000} < \sqrt{2} < \frac{1415}{1000},\\
\frac{14142}{10000} < \sqrt{2} < \frac{14143}{10000},
\end{aligned}$$

$$\frac{141421}{100000} < \sqrt{2} < \frac{141422}{100000}, etc.$$

Estas desigualdades mostram que podemos ter números racionais tão próximos de $\sqrt{2}$ quanto desejarmos. Por exemplo, se quisermos um racional com uma aproximação menor que $0,00001$, podemos obtê-los escolhendo os termos da sequência (3), excetuando os 5 primeiros. Para maiores detalhes, sugerimos [6].

Para obtermos aproximações sem necessariamente ter que utilizar potências de 10 como denominadores, vamos utilizar os teoremas a seguir, sem demonstração.

Teorema 1. *Para qualquer número irracional α, existe um único inteiro m, tal que:*

$$-\frac{1}{2} < \alpha - m < \frac{1}{2}.$$

Teorema 2. *Sejam λ um número irracional qualquer e n um número inteiro positivo qualquer. Então existe um número racional de denominador, digamos, $\frac{m}{n}$, tal que:*

$$-\frac{1}{2n} < \lambda - \frac{m}{n} < \frac{1}{2n}.$$

Como exemplo, tomemos $\lambda = \sqrt{2}$ e $n = 23$. Assim, $n\lambda = 23\sqrt{2} = 32,52....$ Logo, o inteiro mais próximo de $23\sqrt{2}$ é 33 e esse será o nosso m do Teorema 1, temos:

$$-\frac{1}{2} < 23\sqrt{2} - 33 < \frac{1}{2} \Rightarrow$$
$$-\frac{1}{2.23} < \sqrt{2} - \frac{33}{23} < \frac{1}{2.23} \Rightarrow$$
$$-\frac{1}{46} < \sqrt{2} - \frac{33}{23} < \frac{1}{46}.$$

Observe que a desigualdade acima corresponde ao que diz o Teorema 2. Prosseguindo, temos:

$$\frac{33}{23} - \frac{1}{46} < \sqrt{2} < \frac{33}{23} + \frac{1}{46} \Rightarrow$$
$$\frac{65}{46} < \sqrt{2} < \frac{67}{46}.$$

Para obter aproximações melhores, basta tomar um valor de n cada vez maior.

2.3 Números Reais

Ao unirmos os números racionais com os números irracionais, obtemos um conjunto mais amplo, denominado de Conjunto dos Números Reais, que será representado pela letra $\mathbb{R}$.

Os números reais formam o sistema de números central da matemática. Em geometria, toda e qualquer discussão sobre comprimentos, áreas ou volumes leva diretamente aos números reais. Ou seja, os números necessários para medir todos os possíveis comprimentos em termos de uma dada unidade de comprimento.

De fato, a geometria oferece um sistema intuitivo e prático para descrever todos os números reais. Se considerarmos a representação dos números como pontos de uma reta, veremos que, apesar de qualquer segmento, por menor que seja, conter uma infinidade de pontos racionais, existem muitos outros pontos (tais como $\sqrt{2}, \pi, e, etc$) medindo comprimentos, que não podem ser expressos por números racionais. Porém, se considerarmos os números reais, todo ponto da reta corresponderá a exatamente um número real e todo número real corresponderá exatamente a um ponto da reta. Logo, existirá uma correspondência biunívoca entre os pontos da reta e os números reais. O fato de qualquer segmento de reta poder ser representado por um número real é conhecido como a propriedade de "completude" dos números reais.

Esta reta será chamada de "reta real" e a correspondência com os números reais é feita de modo que escolhemos um ponto para ser a "origem" da reta, ao qual associamos o número zero. À direita e a partir do ponto de origem, os pontos corresponderão aos números reais positivos e à esquerda, também partindo do ponto de origem, os pontos corresponderão aos números reais negativos. Observe a ilustração da reta real na Figura 3.

Observe que, para determinar o ponto da reta correspondente ao número $\sqrt{5}$ (o

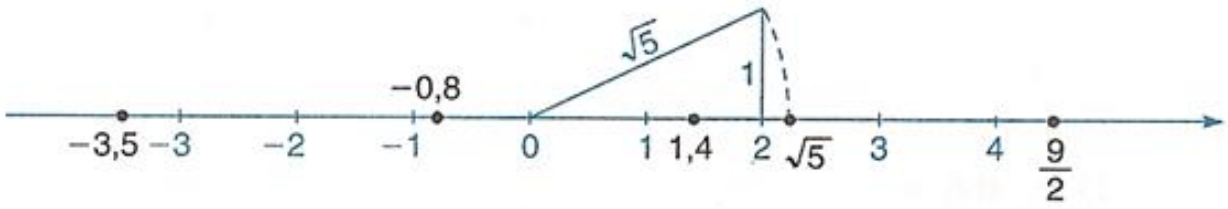


Figura 3: Representação da Reta real.

que equivale a construir um segmento de reta de comprimento $\sqrt{5}$), basta utilizar o Teorema de Pitágoras (triângulo retângulo com catetos medindo uma e duas unidades), régua e compasso.

Na Figura 4, temos um diagrama que representa a relação de inclusão entre os conjuntos que formam os números reais.

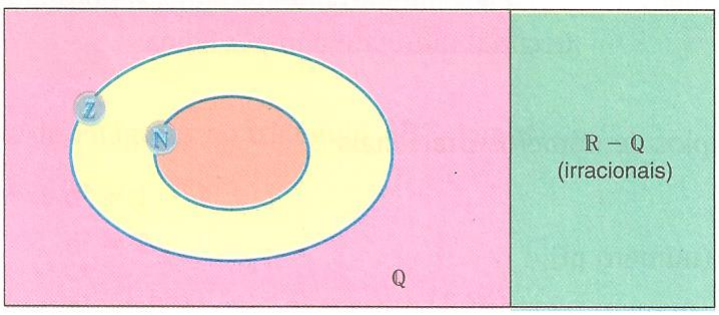


Figura 4: Os Números Reais.

2.4 Números Complexos

As primeiras ideias relativas aos números complexos surgiram no século XVI, em tentativas de se resolver equações que resultavam em raízes de números negativos, que não eram aceitas na época. O primeiro matemático a trabalhar com tais raízes foi o italiano *Girolamo Cardano (1501-1576)* que resolveu o problema de dividir o número 10 em duas partes, tais que o produto entre elas fosse igual a 40. O problema, equivalente

à equação $x^2 - 10x + 40 = 0$, apresenta como solução os números $5 + \sqrt{-15}$ e $5 - \sqrt{-15}$. Porém, o primeiro a estabelecer uma teoria razoavelmente estruturada sobre os novos números foi o também italiano *Rafael Bombelli (1526-1573)*, em sua obra *Álgebra* de 1572.

No entanto, apesar de já aceitos, os matemáticos seguiam mantendo uma certa desconfiança em relação a esses números até o final do século XVIII, quando o suíço *Leonhard Euler (1707-1783)*, em 1777, estabeleceu o símbolo i para representar a $\sqrt{-1}$ e z para representar um número complexo qualquer $a + bi$, mostrando também que o número possuia uma parte real. Foi quando o dinamarquês *Caspar Wessel (1745-1818)*, o alemão *K. F. Gauss (1777-1855)* e o francês *Jean-Robert Argand (1786-1822)* descobriram, independentemente, que esses números possuíam representações e propriedades geométricas, ao se considerar o par (a, b) como as coordenadas de um ponto no plano cartesiano. Assim, qualquer número complexo poderia ser associado a um ponto do plano que ficou conhecido como plano de *Argand-Gauss*. Em 1833, o irlandês *William Rowan Hamilton (1805-1865)* apresentou um artigo à Academia Irlandesa, onde formalizou a álgebra dos números complexos.

A seguir formalizaremos o conjunto dos números complexos e estudaremos algumas dessas propriedades algébricas e geométricas. Porém, vamos relembrar algumas propriedades fundamentais relativas à adição e à multiplicação de números reais.

Considere os números reais a, b, c e d, são válidas as seguintes propriedades:

Propriedade 1. *Comutativa:* $a + b = b + a, \quad ab = ba.$

Propriedade 2. *Associativa:* $(a + b) + c = a + (b + c), \quad (ab)c = a(bc)$

Propriedade 3. *Distributiva da multiplicação em relação à adição:*

$$a(b + c) = ab + ac.$$

Propriedade 4. *Elemento neutro:* $a + 0 = a, \quad a1 = a.$

Propriedade 5. *Elemento simétrico e elemento inverso:*

(i) para todo real a, corresponde um único real $(-a)$ *tal que:*

$$a + (-a) = 0$$

O número $-a$ *é dito simétrico de a.*

(ii) Para todo real a, $a \neq 0$ *, existe um único real* $\frac{1}{a}$*, tal que:*

$$a.(\frac{1}{a}) = 1.$$

O número $\frac{1}{a}$ *é chamado de inverso de a.*

Existem várias maneiras de se definir o conjunto dos Números Complexos, vamos adotar tal qual sugerida em [7].

Definição 1. *Os números complexos constituem um conjunto* $\mathbb{C}$*, onde estão definidas as operações de adição e de multiplicação, com as propriedades 1 a 5. Além disso, os números reais estão incluídos em* $\mathbb{C}$ *e:*

(i) Existe um número complexo i com $i = \sqrt{-1}$.

(ii) Todo número complexo pode ser escrito de uma maneira única na forma $z = a + bi$*, onde a e b são reais (a é chamado parte real e b é chamado parte imaginária do número). Usamos a notação Re(z)=a e Im(z)=b.*

Observação 1. *Se dois números complexos* z_1 *e* z_2 *não são reais (isto é, suas partes imaginárias são diferentes de zero), então não existe a relação de ordem entre eles. Ou seja, o número complexo* z_1 *não é maior, menor ou igual ao número* z_2.

Definição 2. *Dado um número complexo* $z = a + bi$*, definimos:*

(*i*) *O conjugado de z, representado por* $\overline{z}$*, é o número* $\overline{z} = a - bi$*. Ou seja, o conjugado de um número complexo z é o número complexo* $\overline{z}$ *com mesma parte real e parte imaginária simétrica.*

(*ii*) *O módulo de z, representado por* $|z|$*, é o número real* $|z| = \sqrt{a^2 + b^2}$*.*

Com relação a dois números complexos z_1 e z_2 e seus conjugados $\overline{z_1}$ e $\overline{z_2}$, as seguintes propriedades são válidas:

Propriedade 6. $\overline{z_1 + z_2} = \bar{z_1} + \bar{z_2}$

Propriedade 7. $z_1 = \bar{z_1} \Leftrightarrow z_1$ *é um número real*

Propriedade 8. $\overline{z_1.z_2} = \bar{z_1}.\bar{z_2}$

Propriedade 9. $\overline{z_1^n} = (\bar{z_1})^n$

Da definição dada, podemos associar o número complexo $z = a + bi$ ao ponto de coordenadas (a, b), ou ainda ao *vetor* de origem na origem O do plano e extremidade no ponto (a, b), como na Figura 5. No primeiro caso, o ponto (a, b) é chamado de *imagem* do complexo $z = a + bi$ e no último caso, os números a e b são chamados *componentes* do vetor $\overrightarrow{Oz}$.

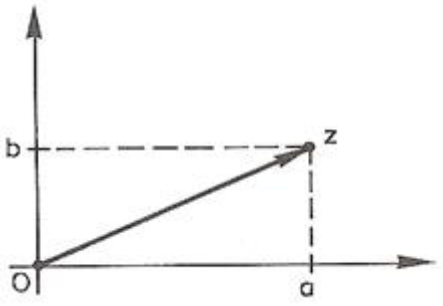


Figura 5: Representação geométrica de $z = a + bi$ no plano cartesiano.

Desta forma, geometricamente, o conjugado $\overline{z}$ de z é representado pelo simétrico de

z relativamente ao eixo Ox e o módulo $|z|$ mede a distância da origem O a z, conforme ilustrado na Figura 6.

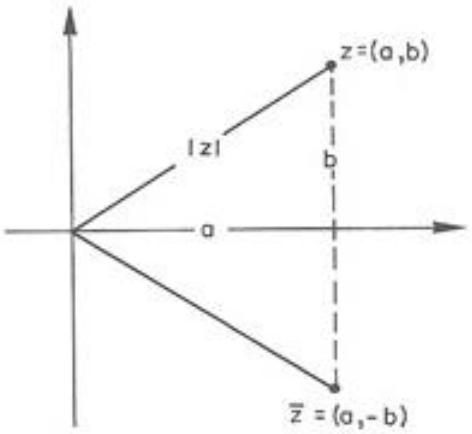


Figura 6: Representação geométrica do Módulo e do Conjugado de z.

Ainda de acordo com a definição, dados dois complexos $z_1 = a + bi$ e $z_2 = c + di$, temos que:

$$z_1 + z_2 = (a + bi) + (c + di) = a + c + bi + di = (a + c) + (b + d)i.$$

Assim, a soma de dois complexos é representada por um vetor, cujas componentes são as somas das componentes dos vetores dados. Como se pode ver na Figura 7, a soma é representada geometricamente pela diagonal do paralelogramo construído sobre os vetores dados.

Para fazer a interpretação geométrica da diferença $z_2 - z_1$, observemos na Figura 8 que:

$$\overrightarrow{Oz_1} + \overrightarrow{z_1z_2} = \overrightarrow{Oz_2}$$

ou

$$\overrightarrow{z_1z_2} = \overrightarrow{Oz_2} - \overrightarrow{Oz_1},$$

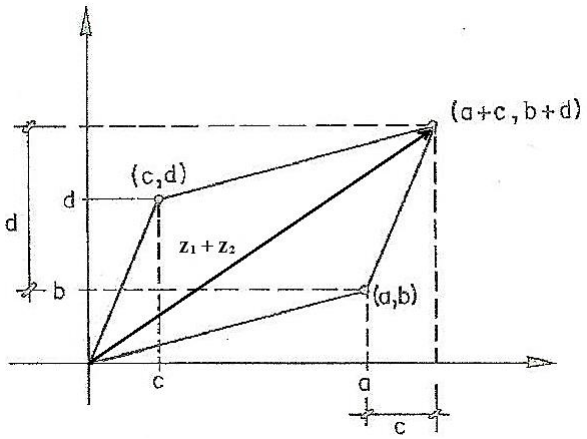


Figura 7: Representação geométrica da soma de dois números complexos.

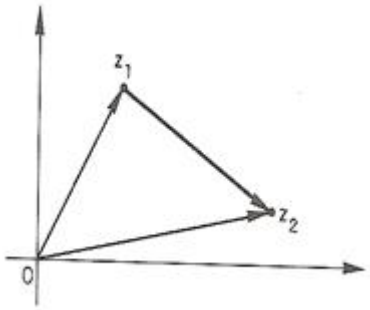


Figura 8: Representação geométrica da diferença de dois números complexos.

ou seja, o vetor que representa a diferença $z_2 - z_1$ é o vetor $\overrightarrow{z_1 z_2}$.

De um modo geral, os Conjuntos Numéricos (bem como outros temas) são apresentados de maneira técnica e desconectada no ensino básico brasileiro. Vários autores de livros-textos não se preocupam em estabelecer o encadeamento histórico social que leva à construção por etapas do conjunto dos números reais, classificando os conjuntos por meio de regras e características. Assim, não levam em consideração o fato de que o aluno, salvo raras exceções, não está preparado para tais abstrações nesse nível, uma vez que o conteúdo é totalmente abordado até o oitavo ano do Ensino Fundamental. Aliando a isto o fato de que a maioria das faculdades de matemática dão pouca ou

nenhuma importância ao tema, muitas vezes os professores também não se interessam em corrigir tais distorções. Isso leva a um ciclo vicioso onde a maioria das crianças e adolescentes têm cada vez mais aversão à matemática.

Em relação aos números complexos, que são apresentados apenas no 3º ano do Ensino Médio, acreditamos que o problema ainda persiste ou chega a ser pior. Uma vez que as omissões dos autores nos livros continuam; os alunos, apesar de já terem uma "certa" idade, na maioria das vezes não apresentam maturidade matemática compatível com o tema e mesmo os professores, em alguns casos, têm dificuldades em relação ao assunto, chegando ao ponto de tratar o tema superficialmente e às vezes até excluí-lo do seu planejamento.

3 Teoria dos Inteiros e Conjuntos Enumeráveis

Neste capítulo, abordaremos algumas definições e propriedades acerca dos números inteiros (conforme podem ser vistos em [1] e [2]) e trataremos da enumerabilidade de conjuntos, tópicos que serão úteis e necessários no decorrer do trabalho.

3.1 Teoria dos Números Inteiros

Propriedade 10. *(Propriedade da Tricotomia) Dados $a, b \in \mathbb{N}$, uma, e apenas uma, das seguintes possibilidades é verificada:*

$(i) a = b$

$(ii) \exists c \in \mathbb{N}$, *tal que* $b = a + c$

$(iii) \exists c \in \mathbb{N}$, *tal que* $a = b + c$.

Diremos que *a é menor do que b*, simbolizado por $a < b$, toda vez que a propriedade (ii) acima é verificada.

Com esta definição, temos que a propriedade (iii) acima equivale a afirmar que $b < a$. Assim a tricotomia nos diz que, dados $a, b \in \mathbb{N}$, uma, e somente uma, das seguintes condições é verificada:

$(i) a = b$

$(ii) a < b$

$(iii) b < a$

Definição 3. *Seja S um subconjunto de $\mathbb{N}$. Dizemos que um número natural a é um menor elemento de S se possui as seguintes propriedades:*

$(i) a \in S$

$(ii) \forall n \in S, a \leq n$

Teorema 3. *(Propriedade da Boa Ordem) Todo subconjunto não vazio de* $\mathbb{N}$ *possui um menor elemento.*

Demonstração. Demonstraremos por redução ao absurdo.

Considere S um subconjunto não vazio de $\mathbb{N}$ e suponha, por absurdo, que S não possua um menor elemento. Mostraremos que, assim, S só pode ser vazio, o que levará a uma contradição.

Considere o conjunto W, complementar de S em $\mathbb{N}$. Devemos mostrar então que $W = \mathbb{N}$. Defina o conjunto

$$I_n = \{k \in \mathbb{N} : k \leq n\},$$

e considere a sentença aberta

$$p(n) : I_n \subset W.$$

Como $0 \leq n$ para todo n, segue-se que $0 \in W$, pois, do contrário, 0 seria um menor elemento de S. Logo, $p(0)$ é verdade. Suponha agora que $p(n)$ seja verdade. Se $n+1 \in S$, como nenhum elemento de I_n está em S, teríamos que $n+1$ é um menor elemento de S, o que não é permitido. Logo, $n+1 \in W$, seguindo então que:

$$I_{n+1} = I_n \cup \{n+1\} \subset W,$$

o que prova que para todo $n \in \mathbb{N}, I_n \subset W$. Portanto, $\mathbb{N} \subset W \subset \mathbb{N}$ e, consequentemente, $W = \mathbb{N}$. □

Definição 4. *Dados* $a, b \in \mathbb{Z}$*, dizemos que* a *divide* b*, e escrevemos* $a|b$*, se existir* $q \in \mathbb{Z}$*, tal que* $b = q.a$*.*

Exemplo 7. $8|24$*, pois* $24 = q.8$ *nos leva a* $q = 3$

Definição 5. *Um número* $p \in \mathbb{Z}$*,* $p \neq 0$ *e* $p \neq \pm 1$*, é primo se os únicos números inteiros que o dividem são* $\pm p$ *e* ± 1*.*

Observação 2. *Dois inteiros a e b são ditos primos entre si, se, dado $p \in \mathbb{Z}$, $p|a$ e $p|b$, então $p = 1$. Isto é, o único divisor comum a a e b for 1.*

Exemplo 8. *Os inteiros $a = 8$ e $b = 9$ são primos entre si. De fato, pois não possuem divisores comuns, exceto o 1.*

Definição 6. *Seja $a \in \mathbb{Z}$. Um número b é chamado de múltiplo de a se $b = aq$, para algum $q \in \mathbb{Z}$.*

Exemplo 9. *24 é múltiplo de $a = 6$, pois se $24 = 6.q$ resulta em $q = 4$.*

Definição 7. *Dados $a, b \in \mathbb{Z}$, um número natural d é chamado de máximo divisor comum de a e b, e representado por $d = mdc(a, b)$, se satisfaz às seguintes condições:*

(i) $d|a$ e $d|b$;

(ii) se $r \in \mathbb{Z}$, é tal que $r|a$ e $r|b$, então $r|d$.

Exemplo 10. *Sejam $a = 60$ e $b = 90$, então $mdc(a, b) = 30$, pois $30|60$, $30|90$ e, dado $r|60$ e $r|90$, temos que $r|30$ (por exemplo, 15|60, 15|90 e 15|30).*

Observação 3. *Se $a = 0$ e $b = 0$, então não existe $mdc(a, b)$; e se $a \neq 0$ e $b = 0$, então $mdc(a, 0) = 0$.*

O teorema a seguir é conhecido como divisão euclideana[1] (ou algoritmo da divisão) e é essencial para o estudo dos números inteiros como um todo, pois torna possível a divisão entre dois números inteiros quaisquer.

[1]Por volta de 300 AC surge em Alexandria um tratado chamado de *Os Elementos* de Euclides. Pouco se sabe sobre os dados biográficos deste grande matemático. Tendo chegado aos dias atuais através de sucessivas edições, o tratado é composto por 13 livros onde se encontra organizado e sistematizado a maior parte do conhecimento matemático da época

Teorema 4. *(Divisão euclideana) Dados a e $b \in \mathbb{Z}$, com $b \neq 0, b < a$. Então existem únicos $q, r \in \mathbb{Z}$ com $0 \leq r < |b|$, tais que:*

$$a = qb + r \tag{4}$$

Demonstração. (i) Existência

Para $(b > 0)$

Consideremos o conjunto dos inteiros múltiplos de b, ordenados da forma:

$$... - 3b \leq -2b \leq -b \leq 0 \leq b \leq 2b \leq 3b...$$

Temos assim uma decomposição da reta em intervalos disjuntos da forma:

$$[qb, (q+1)b) = \{x \in \mathbb{R} : qb \leq x < (q+1)b\},$$

com $q \in \mathbb{Z}$.

Logo, dado $a \in \mathbb{Z}$, a pertence a apenas um destes intervalos. Consequentemente, será da forma $a = qb + r$, com $q \in \mathbb{Z}$ e $r \geq 0$. É claro que, $r < (q+1)b - qb = b$.

Para $(b < 0)$

Apliquemos o teorema para $|b|$, logo existem $q', r \in \mathbb{Z}$, com $0 \leq r < |b|$, tais que:

$$a = q'|b| + r. \tag{5}$$

Fazendo $q = -q'$, como $|b| = -b$, (pois $b < 0$), obtemos de (5), $a = qb + r$, onde $q, r \in \mathbb{Z}$ e $0 \leq r < |b|$.

(ii) Unicidade

Para mostrar que q e r que satisfazem (5) são únicos, suponha que $a = qb + r$ e $a = q_1 b + r_1$, com $0 \leq r < |b|$ e $0 \leq r_1 < |b|$.

Logo:

$$qb + r = q_1 b + r_1 \Rightarrow$$

$$r - r_1 = (q_1 - q)b. \tag{6}$$

Mostremos que $r = r_1$.

De fato, se $r \neq r_1$, então $0 < |r_1 - r|$. Além disso, $|r_1 - r| < b$. Logo, vamos admitir que $r < r_1$, o que implica $r_1 - r > 0$ e $|r_1 - r| = r_1 - r$.

Assim, se $r_1 - r = |b|$, então $r_1 = |b| + r$ e, portanto, $r_1 > |b|$, o que é absurdo.

E, se $r_1 - r > |b|$, então $r_1 > |b| + r > |b|$, gerando o absurdo $r_1 > b$. Logo, pela Propriedade 10:

$$|r_1 - r| = r_1 - r < |b|$$

Segue que:

$$0 < |r_1 - r| < |b| \tag{7}$$

De (6), obtemos:

$$|r_1 - r| = |q_1 - q||b| \tag{8}$$

Substituindo (8) em (7), obtemos:

$$0 < |q_1 - q||b| < |b|.$$

Logo, $0 < |q_1 - q| < 1$, o que é absurdo, pois $|q_1 - q|$ é um número inteiro, uma vez que $q, q_1 \in \mathbb{Z}$. Portanto $r = r_1$. Observe que essa igualdade, combinada com a equação (6), implica em $q_1 = q$, já que $0 = (q_1 - q)b$ e $b \leq 0$ por hipótese. □

Exemplo 11. *Se* $a = 37$ *e* $b = 8$, *então* $q = 4$ *e* $r = 5$, *pois* $37 = 4.8 + 5$

O próximo teorema, conhecido como *Algoritmo de Euclides* [2], traz uma prova construtiva da existência do *mdc* de dois números e é considerada uma obra prima, pois pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios.

[2] Os Elementos de Euclides, Livro VII, Proposição 2.

Teorema 5. *Dados $a, b \in \mathbb{Z}$, pelo menos um deles não nulo, existem $x_0, y_0 \in \mathbb{Z}$, tais que:*

$$ax_0 + by_0 = d,$$

onde $d = mdc(a, b)$.

Demonstração. Considere o conjunto C de todos os inteiros positivos da forma $ax+by$. Ou seja, $C = \{n \in \mathbb{Z} : n > 0 \text{ e } n = ax + by, \text{ para algum } x \text{ e algum } y\ \}$. O conjunto C é não vazio, uma vez que, se tomarmos $x = a$ e $y = b$, teremos $n = aa + bb \in C$. Aplicando o Teorema 3 podemos afirmar que C tem um menor elemento. Dessa forma, existe $d \geq 1$ tal que $d = ax_0 + by_0$, com $x_0, y_0 \in \mathbb{Z}$, e

$$d \leq (ax + by), \tag{9}$$

para todo $ax + by \in C$.

A seguir, afirmamos que:

$$d|(ax + by), \tag{10}$$

para todo $ax + by \in C$.

Para provar a afirmação (10), suponha, por contradição, que $d \nmid (ax + by)$. Assim, existem $q, r \in \mathbb{Z}$, com $0 < r < d$, tais que:

$$ax + by = qd + r = q(ax_0 + by_0) + r,$$

o que implica:

$$r = a(x - qx_0) + b(y - qy_0). \tag{11}$$

Como $r > 0$, a equação (11) nos diz que $r \in C$. Mas isso é um absurdo, pois $r < d$, o que contraria o fato de assumirmos d como o menor elemento do conjunto C. Portanto, $d|(ax + by)$.

A relação $d|(ax+by)$ implica $d||a|$ e $d||b|$ pois, ou um deles é zero e $d|0$, ou ambos são positivos e, nesse caso, ambos estão em C. De fato,

$$|a| = \begin{cases} a + b.0, & se \quad a > 0 \\ -a + b.0, & se \quad a < 0. \end{cases} \tag{12}$$

E, equivalentemente, para $|b|$.

Observe que, se $d||a|$, então $d|a$. De fato, pois $d||a|$ implica que existe $q \in \mathbb{Z}$ tal que $|a| = qd$. Se $a > 0$ a prova está feita. Se $a < 0$, basta tomar $a = (-q)d$. Logo, concluímos que:

$$d|a \quad e \quad d|b \tag{13}$$

Por outro lado, se $k \in \mathbb{N}$ é tal que $k|a$ e $k|b$, então $k|(ax_0 + by_0)$, isto é, $k|d$. Logo, $d|a$ e $d|b$ e também, para algum $k \in \mathbb{N}, k|a$ e $k|b$, então $k|d$. Assim concluímos que d é o máximo divisor comum de a e b. Logo,

$$d = ax_0 + by_0 = mdc(a, b),$$

o que completa a demonstração. □

Lema 1. *Dados $a, x_0, b, y_0, d \in \mathbb{Z}$, se $d|a$ e $d|b$, então $d|(ax_0 + by_0)$.*

Demonstração. Como $d|a$, pela Definição 4, implica que existem $p, q \in \mathbb{Z}$, tais que $a = qd$ e $b = pd$. Logo,

$$ax_0 + by_0 = qdx_0 + pdy_0 = d(qx_0 + py_0).$$

Observe que $k = (qx_0 + py_0) \in \mathbb{Z}$, pois $q, x_0, p, y_0 \in \mathbb{Z}$. Portanto, $ax_0 + by_0 = dk, k \in \mathbb{Z}$. De onde concluímos que

$$d|(ax_0 + by_0)$$

completando a demonstração. □

Exemplo 12. *Temos que* $5|10$ *e* $5|15$*, logo* $5|(10x_0 + 15y_0)$*, para todo* $x_0, y_0 \in \mathbb{Z}$*.*

Lema 2. *Seja* $p \in \mathbb{N}$ *um número primo, e* $a, b \in \mathbb{Z}$*. Se* $p|ab$*, então* $p|a$ *ou* $p|b$*.*

Demonstração. Se $p|a$, não há nada a se provar. Suponha que $p \not| a$, ou seja, p e a são primos entre si. Logo, pelo Teorema 5, existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 + py_0 = 1$. Assim,

$$abx_0 + pby_0 = b \tag{14}$$

Como $p|ab$ (por hipótese) e obviamente $p|pb$, então pelo Lema 1, segue que

$$p|(abx_0 + pby_0).$$

Portanto, da equação (14), obtemos que $p|b$. □

Exemplo 13. *Sejam* $p = 2, a = 8$ *e* $b = 7$*. Temos que* $2|8.7$ *e* $2|8$*.*

Exemplo 14. *Sejam* $p = 5, a = 15$ *e* $b = 10$*. Temos que* $5|15.10$*,* $5|15$ *e* $5|10$*.*

Corolário 1. *Sejam* $p \in \mathbb{Z}$ *um número primo e* $a \in \mathbb{Z}$*. Se* $p|a^n$*, então* $p|a$*.*

Demonstração. Vamos demonstrar usando o Princípio da Indução Finita sobre n. Queremos mostrar que a afirmação: se $p|a^n$ é verdadeira, então $p|a$ é verdadeira para todo $n \in \mathbb{N}$. Para $n = 1$ a afirmação é verdadeira, pois $p|a^1 = p|a$, e por hipótese, $p|a$. Daí temos que para $n = 2$, a afirmação também é verdadeira, pois $p|a^2 = p|a.a$ e pelo lema 2, se $p|a.a$, então $p|a$.

Suponha agora que a afirmação seja verdadeira para $k \in \mathbb{N}$. Ou seja: $p|a^k \Rightarrow p|a$ é verdadeira (hipótese de indução).

Devemos mostrar que a afirmação também é verdadeira para $k + 1, k \in \mathbb{N}$. Isto é: $p|a^{k+1} \Rightarrow p|a$.

Temos que $p|a^{k+1}$ é igual a $p|a^k.a$. Mas, pelo Lema 2, se $p|a^k.a$, então $p|a$ ou $p|a^k$.

Se $p|a$, está provada a afirmação.

Por outro lado, se $p|a^k$, aplicando a hipótese de indução: $p|a^k$ implica que $p|a$. Logo $p|a^{k+1} \Rightarrow p|a$, o que completa a demonstração. □

Proposição 1. *(i) Se $a \in \mathbb{Z}$ é um número par, então a^2 é par. (ii) Se $b \in \mathbb{Z}$ é um número ímpar, então b^2 é ímpar.*

Demonstração. Prova de (i): Se um inteiro a é par, podemos escrevê-lo da forma $a = 2k$, com $k \in \mathbb{Z}$. Assim:

$$a^2 = (2k)^2 \Rightarrow a^2 = 4k^2 \Rightarrow a^2 = 2(2k^2).$$

Como k é inteiro, $2k^2$ também é inteiro. Fazendo $2k^2 = p$, temos que:

$$a^2 = 2p, p \in \mathbb{Z}.$$

Provando que a^2 é par.

Prova de (ii): Se um inteiro b é ímpar, podemos escrevê-lo da forma $a = 2m + 1$, com $m \in \mathbb{Z}$. Assim:

$$b^2 = (2m + 1)^2 \Rightarrow b^2 = 4m^2 + 4m + 1 \Rightarrow b^2 = 2(2m^2 + 2m) + 1.$$

Como m é inteiro, $(2m^2 + 2m)$ também é inteiro. Fazendo $(2m^2 + 2m) = q$, temos que:

$$b^2 = 2q + 1, q \in \mathbb{Z}.$$

Provando que b^2 é ímpar.

Observe que podemos usar a contrapositiva nos dois itens da proposição. Isto é, se a^2 é um inteiro par, então a é um inteiro par. Da mesma forma, se b^2 é um inteiro ímpar, então b é um inteiro ímpar. □

3.2 Conjuntos Enumeráveis

Nesta seção, definiremos conjuntos enumeráveis e estudaremos a enumerabilidade ou não de alguns conjuntos, o que será muito importante no capítulo 4, para mostrar a existência dos números transcendentes. Trataremos deste tópico, conforme foi colocado em [2].

Definição 8. *Dizemos que um conjunto C é enumerável quando seus elementos podem ser colocados em correspondência biunívoca com os números naturais. Isto é, C é enumerável se existir uma função bijetiva $f : \mathbb{N} \longrightarrow C$.*

Exemplo 15. *O conjunto $\mathbb{N}$ dos números naturais obviamente é enumerável, pois basta tomarmos a função identidade $f(n) = n, \quad n \in \mathbb{N}$.*

Exemplo 16. *O conjunto dos números pares positivos, $\{2, 4, 6, ...\}$, é enumerável, bastando, para isso, tomar a função $f(n) = 2n, \quad n \in \mathbb{N}$.*

Exemplo 17. *O conjunto dos múltiplos positivos de 5, $\{5, 10, 15, ...\}$, é enumerável, pois se tomarmos a função $f(n) = 5n, \quad n \in \mathbb{N}$ listaremos todos os elementos do conjunto.*

Exemplo 18. *O conjunto {1,1,2,3,5,8,13,21,34,...}, conhecido como Sequência de Fibonacci, é enumerável. Basta fazer, para todo $n \in \mathbb{N}$, como na Figura 9.*

$$f(n) = \begin{cases} 1, & se \quad n = 1 \\ 1, & se \quad n = 2 \\ a_{n-1} \quad + \quad a_{n-2}, & se \quad n \geq 3 \end{cases}$$

Figura 9: Enumerabilidade da Sequência de Fibonacci.

$$\begin{array}{ccccccccccc}
\cdots, & -3, & & -2, & & -1, & 0, & 1, & 2, & 3, & \cdots \\
 & \updownarrow & & \updownarrow & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
\cdots, & 7, & & 5, & & 3, & 1, & 2, & 4, & 6, & \cdots
\end{array}$$

Figura 10: Enumerabilidade dos Números Inteiros.

Exemplo 19. *O conjunto $\mathbb{Z}$ dos números inteiros é enumerável. Para verificar, basta proceder como na Figura 10.*

Desta forma, podemos enumerar todos os inteiros.

Exemplo 20. *O conjunto dos números racionais positivos é enumerável.*

Da mesma forma que nos inteiros, podemos obter um esquema, através do qual, listaremos todos os números racionais positivos.

$$\begin{array}{ccccccccccc}
\frac{1}{1} & \rightarrow & \frac{1}{2} & & \frac{1}{3} & \rightarrow & \frac{1}{4} & & \frac{1}{5} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
\frac{2}{1} & & \frac{2}{2} & & \frac{2}{3} & & \frac{2}{4} & & \frac{2}{5} & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \nearrow & \\
\frac{3}{1} & & \frac{3}{2} & & \frac{3}{3} & & \frac{3}{4} & & \frac{3}{5} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
\frac{4}{1} & & \frac{4}{2} & & \frac{4}{3} & & \frac{4}{4} & & \frac{4}{5} & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & \nearrow & \\
\frac{5}{1} & & \frac{5}{2} & & \frac{5}{3} & & \frac{5}{4} & & \frac{5}{5} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Figura 11: Enumerabilidade dos Racionais Positivos.

Analisando a Figura 11, percebemos que todos os números da forma $\frac{p}{q}$, $p, q \in \mathbb{N}$,

$q \neq 0$, *aparecem listados, bastando seguir as setas. Assim, mostramos que o conjunto* $\mathbb{Q}^+ = \{x \in \mathbb{Q} : x > 0\}$ *é enumerável. Da mesma forma, podemos mostrar que o conjunto* $\mathbb{Q}^- = \{x \in \mathbb{Q} : x < 0\}$ *é enumerável.*

O próximo teorema trata da enumerabilidade da união de conjuntos. Através dele, mostraremos que o conjunto dos racionais ($\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$) é enumerável e o conjunto $\mathbb{R}$ dos reais não é enumerável.

Teorema 6. (*i*) *A união de um conjunto finito com um conjunto enumerável é enumerável.*

(*ii*) *A união de dois conjuntos enumeráveis é enumerável.*

(*iii*) *A união de um número finito de conjuntos enumeráveis é enumerável.*

(*iv*) *A união enumerável de conjuntos finitos é enumerável.*

(*v*) *A união enumerável de conjuntos enumeráveis é enumerável.*

Demonstração. (*i*) Considere $A = \{a_1, a_2, ..., a_n\}$ o conjunto finito e $B = \{b_1, b_2, b_3, ...\}$ o conjunto enumerável. Para mostrar que $A \cup B$ é enumerável, basta fazer a correspondência biunívoca entre $A \cup B$ e $\mathbb{N}$, conforme o esquema da Figura 12.

$$\begin{array}{cccccccc} a_1, & a_2, & \cdots, & a_n, & b_1, & b_2, & \cdots \\ \updownarrow & \updownarrow & & \updownarrow & \updownarrow & \updownarrow & \\ 1, & 2, & \cdots, & n, & n+1, & n+2, & \cdots \end{array}$$

Figura 12: Enumerabilidade da união de um conjunto finito com um conjunto enumerável.

(*ii*) Se $A = \{a_1, a_2, ...\}$ e $B = \{b_1, b_2, ...\}$ são dois conjuntos enumeráveis, para mostrar que $A \cup B$ é enumerável, basta fazer a correspondência biunívoca como descrita na Figura 13.

$$\begin{array}{ccccccc} a_1, & b_1, & a_2, & b_2, & a_3, & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 1, & 2, & 3, & 4, & 5, & \cdots \end{array}$$

Figura 13: Enumerabilidade da união de dois conjuntos enumeráveis

Assim, os elementos de A serão numerados conforme os números ímpares e os elementos de B conforme os pares, em sequência.

(iii) Considere os k ($k \in \mathbb{N}$) conjuntos enumeráveis $A = \{a_1, a_2, ...\}$, $B = \{b_1, b_2, ...\}$, ..., $K = \{k_1, k_2, ...\}$. Para provar que $A \cup B \cup ... \cup K$ é enumerável, fazemos a correspondência biunívoca definida na Figura 14.

$$\begin{array}{cccccccccc} a_1, & b_1, & ..., & k_1, & a_2, & ..., & k_2, & a_3, ..., & k_3, & \cdots \\ \updownarrow & \updownarrow & & \updownarrow & \updownarrow & & \updownarrow & \updownarrow & \updownarrow & \\ 1, & 2, ..., & & k, & k+1, ..., & & 2k, & 2k+1, ..., & 3k, & \cdots \end{array}$$

Figura 14: Enumerabilidade da união de um conjunto finito de conjuntos enumeráveis.

(iv) Sejam os conjuntos finitos $\beta_1 = \{a_1, a_2, ..., a_n\}$, $\beta_2 = \{b_1, b_2, ..., b_k\}$, $\beta_3 = \{c_1, c_2, ..., c_p\}$,...; onde o conjunto $\Omega = \{\beta_1, \beta_2, \beta_3, ...\}$ é enumerável. Isto é, $\beta_1 \cup \beta_2 \cup \beta_3 ... \cup ...$ é a união de um conjunto enumerável de conjuntos finitos.

Para mostrar que esta união é enumerável, ordenamos os elementos dos conjuntos de forma conveniente e fazemos a correspondência biunívoca como na Figura 15.

$$\begin{array}{ccccccccccc} a_1, & ..., & a_n, & b_1, & ..., & b_k, & c_1, & ..., & c_p, ... \\ \updownarrow & ... & \updownarrow & \updownarrow & ... & \updownarrow & \updownarrow & ... & \updownarrow & ... \\ 1, & ... & n, & n+1, ..., & & n+k, & (n+k)+1, ... & & (n+k)+p, & ... \end{array}$$

Figura 15: Enumerabilidade de um conjunto enumerável de conjuntos finitos.

(v) Sejam os conjuntos enumeráveis $\beta_1 = \{a_{11}, a_{12}, a_{13}...\}$, $\beta_2 = \{a_{21}, a_{22}, a_{23}...\}$, $\beta_3 = \{a_{31}, a_{32}, a_{33}...\}$,..., $\beta_n = \{a_{n1}, a_{n2}, a_{n3}, ...\}$,...; onde o conjunto $\Omega = \{\beta_1, \beta_2, \beta_3, ...\beta_n, ...\}$ é enumerável. Isto é, $\beta_1 \cup \beta_2 \cup ... \cup \beta_n ... \cup ...$ é a união de um conjunto enumerável de conjuntos enumeráveis.

Para mostrar que esta união é enumerável, podemos dispor os elementos como na Figura 16 e listá-los da mesma forma como na ilustração de que o conjunto dos racionais positivos $\mathbb{Q}^+$ é enumerável.

$$\begin{array}{cccc} a_{11}, & a_{12}, & a_{13}, & \cdots \\ a_{21}, & a_{22}, & a_{23}, & \cdots \\ a_{31}, & a_{32}, & a_{33}, & \cdots \\ \vdots & \vdots & \vdots & \ddots \\ a_{n1}, & a_{n2}, & a_{n3}, & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

Figura 16: Enumerabilidade da união de um conjunto enumerável de conjuntos enumeráveis.

□

Corolário 2. *Se A é um conjunto enumerável e B é um conjunto infinito, tal que $B \subset A$, então B é enumerável.*

Demonstração. Como A é um conjunto enumerável, então existe uma correspondência biunívoca entre A e os números naturais. Isto é, dado $a_n \in A$, existe um n natural, tal que a_n esteja relacionado a n. Como $B \subset A$, dado um $b_n \in B$, então $b_n \in A$. Portanto, o conjunto B é enumerável.

□

O próximo teorema tem importância fundamental no trabalho, pois através dele, provaremos a existência de números transcendentes, no Capítulo 5.

Teorema 7. *O conjunto* $\mathbb{R}$ *dos números reais não é enumerável.*

Demonstração. Pelo Corolário 2, para provar que $\mathbb{R}$ não é enumerável, basta provar que um intervalo $I \subset \mathbb{R}$ não é enumerável.Tomemos então o intervalo $I = [0, 1)$, isto é, $I = \{x \in \mathbb{R} : 0 \leq x < 1\}$ e vamos provar que I não é enumerável.

Observe que para todo $x \in I$, x pode ser escrito na forma:

$$0, a_1 a_2 a_3 ...$$

em que $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e algum $a_i \neq 9$.

Como vimos no Capítulo 2, alguns destes números possuem duas representações decimais. Por exemplo: $\frac{1}{4} = 0,25$ ou $\frac{1}{4} = 0,249999....$

Desta forma, consideraremos a representação decimal infinita periódica. Por exemplo, o número $\frac{1}{2}$ será escrito como $0,4999...$ e não como $0,5$.

Suponhamos que I seja enumerável. Poderíamos então ordená-los como a seguir:

$$\begin{aligned} &0, a_{11} a_{12} a_{13} ... \\ &0, a_{21} a_{22} a_{23} ... \\ &0, a_{31} a_{32} a_{33} ... \end{aligned} \tag{15}$$

Formemos agora a seguinte decimal:

$$0, b_1 b_2 b_3 ...$$

de forma que todos os $b_i's$ sejam diferentes de 0 ou 9 e, além disso,

$$b_1 \neq a_{11}, \quad b_2 \neq a_{22}, ...$$

Deste modo, é claro que:

$$0, b_1 b_2 b_3 ... \neq 0, a_{n1} a_{n2} a_{n3} ...$$

para todo n, pois $b_n \neq a_{nn}$. Logo, $0, b_1 b_2 b_3 ...$ não está na representação (15) acima, o que é um absurdo. Portando, I não é enumerável e, consequentemente, $\mathbb{R}$ não é enumerável. $\square$

4 Equações Polinomiais

Neste capítulo, trataremos das equações polinomiais de modo semelhante àquele tratado pelos autores de livros do ensino médio. Porém, daremos um enfoque maior às justificativas de cada método de resolução, provando ou justificando cada proposição sempre que estiver dentro dos objetivos do trabalho.

4.1 Contexto Histórico - Resolução de Equações Polinomiais

Os primeiros registros sobre resoluções de equações do 2º grau foram encontrados aproximadamente em 1700 a.C. e pertencem a civilizações antigas, como os sumérios, os egípcios, os babilônios e os muçulmanos. Esta última se destaca pela obra *Al-jabr W'al-Mugabala*, do matemático e astrônomo *Al-Khowarizmi*, que data do século VIII e inclui uma exposição completa da resolução de equações do 1º e 2º graus. Acredita-se que a palavra *Álgebra* deriva desse nome.

O processo de resolução de equações cúbicas (do terceiro grau) da forma $x^3+mx = n$ se deve ao matemático italiano *Niccolo Fontana Tartaglia (1499-1557)*. No entanto, *Tartaglia* não revelou sua descoberta, confidenciando apenas a seu amigo médico e também matemático italiano *Girolamo Cardano (1501-1576)*. Em 1545, *Cardano* publicou em sua obra *Ars Magna*, o método que lhe fora confiado por *Tartaglia*. O que, embora com referências e agradecimentos a ele, gerou profunda desavença entre eles.

A justificativa de *Cardano* para tal traição, foi a de que tomou conhecimento que *Scipione del Ferro (1465-1526)*, um terceiro compatriota, havia chegado aos mesmos resultados de *Tartaglia* anos antes e que os havia repassado a um discípulo (o que acabou sendo comprovado posteriormente). Temendo a divulgação do trabalho, *Cardano* resolveu publicá-lo.

O fato é que a fórmula para resolução de equações da forma $x^3 + mx = n$, que

atualmente é traduzida por:

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

é conhecida como *fórmula de Cardano*.

Ars Magna também trouxe um método para reduzir equações quárticas (do quarto grau) em equações cúbicas. Isto é, um método de resolução de equações do quarto grau. Esta descoberta foi resultado de um profundo estudo de *Ludovico Ferrari (1522-1565)*, aluno e discípulo de *Cardano*.

A partir de então, inúmeros matemáticos se empenharam em encontrar métodos capazes de determinar as raízes de equações do quinto grau. Em 1799, *Paolo Ruffini (1765-1822)*, publicou um trabalho em que acreditava ter provado a impossibilidade de se resolver tais equações. Porém, seu artigo tinha um pequeno erro e não lhe foi dado crédito pela comunidade científica da época. Apenas em 1824, o norueguês *Niels Henrik Abel (1802-1829)* conseguiu a prova correta para o fato. Além dele, o francês *Évariste Galois (1811-1832)* também provou essa impossibilidade, usando uma teoria diferente, a chamada *Teoria de Galois*, que até os dias atuais é usada para verificar quais equações são ou não passíveis de resolução por fórmulas que envolvem os coeficientes. Para maiores detalhes, veja [3] e [4].

Apesar de toda a discussão e sistematização a respeito da resolução de equações de terceiro e quarto graus por fórmulas "prontas", neste capítulo estaremos interessados em apresentar técnicas que nos forneçam outras alternativas para a resolução destes dois tipos de equação.

4.2 Funções Polinomiais ou Polinômios

Antes de trabalharmos alguns métodos e técnicas de resolução de equações polinomiais, que é o objetivo deste capítulo, necessitaremos de alguns conceitos a respeito

dos polinômios, os quais virão a seguir.

Definição 9. *Seja a sequência de números complexos* $(a_n, a_{n-1}, ..., a_1, a_0)$. *Considere a função* $p : \mathbb{C} \longrightarrow \mathbb{C}$, *dada por*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0. \tag{16}$$

A função p *é denominada função polinomial ou polinômio associado à sequência dada. Em que* $n \in \mathbb{N}$, $a_n, a_{n-1}, ..., a_1, a_0$ *são denominados coeficientes e as parcelas*

$$a_n x^n, a_{n-1} x^{n-1}, ..., a_1 x, a_0$$

são os termos do polinômio $p(x)$.
Definimos ainda o grau de um polinômio como o maior expoente de um termo não nulo (com $a_i \neq 0$*) e representaremos como* $Gr(p)$.

Em determinados casos, para simplificar a notação, usaremos simplesmente p para simbolizar a função polinomial p na variável x, sem perda de generalidade.

Como exemplos, temos:

Exemplo 21. $p(x) = x^4 - 4x^2 - 2$ *é uma função polinomial do quarto grau (ou de grau 4).*

Exemplo 22. $q(x) = 5x^2 + 3$ *é um polinômio do segundo grau (ou de grau 2).*

Exemplo 23. $r(x) = 0x^4 - 2x^3 + 5x - 2$ *é uma função polinomial do terceiro grau (ou de grau 3).*

Definição 10. *Dados um número complexo* k *e um polinômio como na fórmula* (16). *Definimos o valor numérico de* p *em* k, *como a imagem de* k *pela função* p. *Isto é:*

$$p(k) = a_n k^n + a_{n-1} k^{n-1} + ... + a_1 k + a_0.$$

Em particular, se $p(k) = 0$ *dizemos que* k *é uma raiz da função* p.

Exemplo 24. *Dado o polinômio* $p(x) = x^3 + 3x^2 + 2x$, *temos:*

$p(1) = 1^3 + 3.1^2 + 2.1 = 6$

$p(-1) = (-1)^3 + 3.(-1)^2 + 2.(-1) = 0$

Desta forma, o valor numérico de p(x) para $x = 1$ *é 6 e para* $x = -1$ *é 0. Logo, -1 é uma raiz de p.*

Definição 11. *Um polinômio é chamado de "polinômio nulo" ou "identicamente nulo", quando todos os seus coeficientes forem nulos. Isto é* $p(x) = 0x^n + 0x^{n-1} + ... + 0x + 0$. *Logo,* $p(x) = 0$ *para qualquer* $x \in \mathbb{C}$ *e, consequentemente, todo número complexo é raiz de p.*

Para estes polinômios, consideramos $Gr(p) = -\infty$.

Definição 12. *Sejam os polinômios* $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ *e* $g(x) = b_n x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0$. *Dizemos que f e g são "iguais" ou "idênticos", se todos os coeficientes dos termos correspondentes (com mesmo expoente) forem iguais. Ou seja:*

$$f = g \Leftrightarrow a_n = b_n, a_{n-1} = b_{n-1}, ..., a_1 = b_1, a_0 = b_0.$$

A seguir falaremos resumidamente sobre as operações com polinômios, com ênfase na divisão, a qual necessitaremos nas seções seguintes.

Definição 13. *Considere os polinômios não nulos* $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ *e* $g(x) = b_n x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0$, *com* $Gr(f) \geq Gr(g)$. *Definimos:*

(*i*) *Adição:* $f(x) + g(x) = h(x)$, *tal que*

$$h(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + ... + (a_1 + b_1)x + (a_0 + b_0).$$

Ou seja, para somarmos dois polinômios, basta somar os coeficientes dos termos correspondentes.

(ii) Subtração: $f(x) - g(x) = h(x)$, *tal que*

$$h(x) = (a_n - b_n)x^n + (a_{n-1} - b_{n-1})x^{n-1} + ... + (a_1 - b_1)x + (a_0 - b_0).$$

Analogamente à adição, para subtrairmos dois polinômios, devemos subtrair os coeficientes dos termos correspondentes.

(iii) Multiplicação: $f(x).g(x) = (a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0).(b_n x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0) = h(x)$, *onde* $h(x)$ *é obtido aplicando a propriedade distributiva da multiplicação em relação à adição. Observe que, desta forma,* $Gr(h) = Gr(f) + Gr(g)$

(iv) Divisão: A divisão de $f(x)$ *por* $g(x)$ *só é possível se* $Gr(f) \geq Gr(g)$. *Neste caso, "dividir"* f *por* g *consiste em obter dois polinômios* $q(x)$ *e* $r(x)$, *tais que:*

$$f(x) = g(x).q(x) + r(x).$$

Onde $f(x)$ *é o "dividendo",* $g(x)$ *é "divisor",* $q(x)$ *é o "quociente" e* $r(x)$ *o "resto" da divisão. Temos ainda que* $Gr(q) = Gr(f) - Gr(g)$ *e* $Gr(r) < Gr(g)$.

Assim, se g *for um polinômio do primeiro grau, o resto será uma constante. Se* $r(x) = 0$, *dizemos que a divisão é exata.*

São conhecidos alguns métodos para a divisão de polinômios, como o *Método da Chave* (que é semelhante ao processo utilizado no algoritmo de Euclides para a divisão de números naturais), e o *Método de Descartes* [3] (que é baseado no conceito de igualdade de polinômios) ambos utilizados para divisores quaisquer; e ainda o *Algoritmo de Briot-Ruffini*[4] usado para divisões onde o divisor tem grau 1.

Neste trabalho não vamos detalhar nenhuma delas, apenas usar seus resultados,

[3] René Descartes(1596-1650) - notável matemático francês que trouxe várias contribuições para a matemática, dentre elas, o Sistema Cartesiano de Coordenadas.

[4] Paolo Ruffini (1765-1822). Médico e matemático francês; Charles August Briot (1817-1822). Matemático francês

levando-se em conta sua relativa simplicidade e a possível familiaridade do leitor com o tema. Para detalhes mais precisos, veja [3].

Para os Exemplos 25 a 28 a seguir, considere os polinômios $f(x) = 2x^3 + 10x^2 + 11 + 2x$ e $g(x) = 2x^2 + 4x - 1$. Temos:

Exemplo 25. $f(x) + g(x) = 2x^3 + 12x^2 + 15x + 1$

Exemplo 26. $f(x) - g(x) = 2x^3 + 8x^2 + 7x + 3$

Exemplo 27. $f(x).g(x) = 4x^5 + 28x^4 + 60x^3 + 38x^2 - 3x - 2$. *Observe que* $Gr(f) + Gr(g) = 5 = 3 + 2 = Gr(f) + Gr(g)$.

Exemplo 28. $f(x) = g(x).(x+3)+5$. *Isto é, na divisão de* f *por* g, *temos* $q(x) = (x+3)$ *e* $r(x) = 5$. *Obseve que* $Gr(q) = 1 = 3 - 2 = Gr(f) - Gr(g)$ *e* $Gr(r) = 1 = 2 - 1 = Gr(g) - 1$.

A seguir traremos dois teoremas que serão necessários na próxima seção.

Teorema 8. *(Teorema do Resto) O resto da divisão de um polinômio* f *por* $x - a$ *é igual a* $f(a)$.

Demonstração. De acordo com a Definição 13 (iv), temos:

$$f(x) = (x - a).q(x) + r.$$

Como $x - a$ tem grau 1, o resto r é nulo ou tem grau zero. Logo, r é um polinômio constante. Calculando $f(a)$, temos:

$$f(a) = (a - a).q(x) + r \Longrightarrow f(a) = r.$$

O que completa a demonstração. □

Teorema 9. *(Teorema de D'Alembert [5]) Um polinômio f é divisível por $x-a$ se, e somente se, a é raiz de f.*

Demonstração. De acordo com o Teorema 8, temos que $f(a) = r$, sendo r o resto da divisão de f por $(x-a)$. Logo:

($\Rightarrow$) Se f é divisível por $x-a$, então $r = 0$. Então $r = f(a) = 0$, logo, a é raiz de f.

($\Leftarrow$) Por outro lado, se a é raiz de f, então $f(a) = 0$. Então $f(a) = r = 0$, logo, f é divisível por $x-a$.

Completando a demonstração. □

4.3 Equações polinomiais e suas raízes

Trataremos agora de procedimentos e técnicas que irão nos auxiliar na resolução de equações algébricas ou polinomiais com coeficientes complexos. É importante observar que, como será definido a seguir, uma equação polinomial é equivalente à igualdade $p(x) = 0$, com $p(x)$ descrito como na Definição 9.

Definição 14. *Consideremos a função polinomial* $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$. *Definimos como equação polinomial a toda equação da forma* $p(x) = 0$, *isto é:*

$$a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0, \quad a_n \neq 0. \tag{17}$$

Onde $a_n, a_{n-1}, ..., a_1, a_0 \in \mathbb{C}$ *são chamados coeficientes e* $n \in \mathbb{N}$ *é o grau da equação (pois é o maior expoente de um termo não nulo).*

Exemplo 29. $3x^3 - 4x^2 - 2 = 0$ *é uma equação polinomial do terceiro grau (ou de grau 3).*

Exemplo 30. $2x^2 - 5 = 0$ *é uma equação polinomial do segundo grau (ou de grau 2).*

[5] Jean le Rond d'Alembert (1717-1783). Filósofo, físico e matemático francês.

Exemplo 31. $0x^6 - 4x^4 - 3x^2 - 2x = 0$ *é uma equação polinomial do quarto grau (ou de grau 4).*

Definição 15. *Dada uma equação polinomial, chama se raiz da equação todo número que, substituído em lugar de x, torna a igualdade* (17) *verdadeira. O conjunto de todas as soluções de uma equação é chamado de Conjunto Solução ou Conjunto Verdade da equação.*

Exemplo 32. $x = 2$ *e* $x = 3$ *são raízes da equação* $x^2 - 5x + 6 + 0$. *Pois:* $2^2 - 5.2 + 6 = 0$ *e* $3^2 - 5.3 + 6 = 0$.

Exemplo 33. $x = -1$, $x = 1$ *e* $x = 2$ *são raízes da equação* $x^3 - 2x^2 - x + 2 = 0$. *Pois:* $(-1)^3 - 2.(-1)^2 - (-1) + 2 = 0$; $1^3 - 2.1^2 - 1 + 2 = 0$ *e* $2^3 - 2.2^2 - 2 + 2 = 0$.

Teorema 10. *Todo polinômio* $p(x)$ *de grau* $n \geq 1$ *admite pelo menos uma raiz complexa.*

O Teorema 10, conhecido como *Teorema Fundamental da Álgebra* tem uma importância singular no desenvolvimento da álgebra. Várias demonstrações a seu respeito foram apresentadas no final do século XVIII e durante o século XIX, porém nenhuma delas será apresentada devido aos objetivos do trabalho. Algumas delas devido a Gauss [6] e Cauchy [7]. Para o leitor interessado, sugerimos [5].

Como consequência do Teorema 10, obtemos o seguinte resultado que será bastante útil ao longo do capítulo.

Teorema 11. *Teorema da Decomposição - Todo polinômio* $p(x)$ *de grau* $n, n \geq 1$

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a, \quad a_n \neq 0,$$

[6] Johann Carl Friedrich Gauss (1777-1855). Matemático, físico e astrônomo alemão, um dos maiores matemáticos de todos os tempos, com contribuições em diversas áreas.

[7] Augustin-Louis Cauchy (1789-1857). Matemático francês especialista em álgebra e análise.

pode ser decomposto em n fatores do primeiro grau, isto é:

$$p(x) = a_n(x - r_1)(x - r_2)(x - r_3)...(x - r_n), \tag{18}$$

em que $r_1, r_2, r_3, ..., r_n$ *são as raízes de* $p(x)$*. Esta decomposição é única, com exceção da ordem dos fatores.*

Demonstração. (i) Existência:

Seja $p(x)$ um polinômio de grau $n \geq 1$, pelo Teorema 10, $p(x)$ tem pelo menos uma raiz r_1 complexa. Assim, $p(r_1) = 0$ e, de acordo com o Teorema 9, $p(x)$ é divisível por $x - r_1$. Ou seja:

$$p(x) = (x - r_1).q_1, \tag{19}$$

onde q_1 é um polinômio de grau $n - 1$ e coeficiente dominante a_n.

Se $n = 1$, então $n - 1 = 0$ e q_1 é uma constante; portanto, $q_1 = a_n$ e $p(x) = a_n.(x - r_1)$, o que demonstra o teorema.

Se $n \geq 2$, então $n - 1 \geq 1$. Assim o Teorema 10 é aplicável ao polinômio q_1, isto é, q_1 tem pelo menos uma raiz r_2. Logo, $q_1(r_2) = 0$ e q_1 é divisível por $x - r_2$. Ou seja:

$$q_1(x) = (x - r_2).q_2. \tag{20}$$

Substituindo (20) em (19), temos:

$$p(x) = (x - r_1)(x - r_2).q_2,$$

onde q_2 é um polinômio de grau $n - 2$ e coeficiente dominante a_n.

Se $n = 2$, então $n - 2 = 0$ e q_2 é uma constante; portanto, $q_2 = a_n$ e $p(x) = a_n.(x - r_1)(x - r_2)$, o que demonstra o teorema.

Seguindo o mesmo raciocínio e aplicando o Teorema 10 n vezes, chegamos à igualdade:

$$p(x) = (x - r_1)(x - r_2)(x - r_3)...(x - r_n).q_n,$$

onde q_n tem grau $n - n = 0$ e coeficiente dominante a_n. Logo, $q_n = a_n$. Portanto:

$$p(x) = a_n(x - r_1)(x - r_2)(x - r_3)...(x - r_n).$$

O que encerra a demonstração da existência.

(*ii*) Unicidade:

Suponha que $p(x)$ possa ser escrito de duas formas, isto é:

$$p(x) = a_n(x - r_1)(x - r_2)(x - r_3)...(x - r_n)$$

e

$$p(x) = a'_m(x - r'_1)(x - r'_2)(x - r'_3)...(x - r'_m).$$

Reduzindo e ordenando os segundos membros das igualdades, temos:

$$a_n x^n - a_n S_1 . x^{n-1} + ... = a'_m x^m - a'_m S'_1 . x^{m-1} + ...$$

Pela Definição 12, temos que $n = m$ e $a_n = a'_m$; e chegamos à igualdade:

$$(x - r_1)(x - r_2)(x - r_3)...(x - r_n) = (x - r'_1)(x - r'_2)(x - r'_3)...(x - r'_n). \qquad (21)$$

Fazendo $x = r_1$, temos:

$$0 = (r_1 - r'_1)(r_1 - r'_2)(r_1 - r'_3)...(r_1 - r'_n).$$

Se o produto é nulo, um dos fatores $(r_1 - r'_j)$ é nulo. Com uma mudança apropriada na ordem dos fatores, podemos colocar $r_1 = r'_1$. Assim, a igualdade (21) se transforma em:

$$(x - r_1)(x - r_2)(x - r_3)...(x - r_n) = (x - r_1)(x - r'_2)(x - r'_3)...(x - r'_n)$$

ou

$$(x - r_2)(x - r_3)...(x - r_n) = (x - r'_2)(x - r'_3)...(x - r'_n).$$

Fazendo $x = r_2$, temos:

$$0 = (r_2 - r'_2)(r_2 - r'_3)...(r_2 - r'_n).$$

Do mesmo modo, um dos fatores $(r_2 - r'_k)$ é nulo. Novamente com uma mudança apropriada na ordem dos fatores, temos $r_2 = r'_2$. Analogamente, teremos $r_i = r'_i$, para todo $i \in \{1, 2, 3, ..., n\}$. Temos então as igualdades:

$$m = n, a'_m = a_n, r'_1 = r_1, r'_2 = r_2, ..., r'_n = r_n.$$

O que garante a unicidade da decomposição de $p(x)$, completando a demonstração do teorema. □

Como consequência dos Teoremas 10 e 11, obtemos um resultado muito importante para determinarmos o número de raízes de uma equação polinomial.

Corolário 3. *Toda equação polinomial de grau $n, n \geq 1$ admite n, e somente n, raízes complexas.*

Demonstração. Considere uma equação polinomial como em (17).

Na demonstração da existência do Teorema 11, vimos que $p(x)$ admite as raízes (distintas ou não) $r_1, r_2, r_3, ..., r_n$. Ao provarmos a unicidade da decomposição, provamos que essas são as únicas n raízes de $p(x)$ e, consequentemente, da equação polinomial (17). □

4.4 Raízes Múltiplas e Relações de Girard

A seguir falaremos sobre técnicas de resolução de equações polinomiais conhecidas por raízes múltiplas e relações de Girard.

Definição 16. *Dizemos que r é raiz de multiplicidade m $(m \geq 1)$, da equação $p(x) = 0$ se, e somente se:*

$$p(x) = (x - r)^m.q \qquad e \qquad q(r) \neq 0.$$

Isto é, r é raiz de multiplicidade m de $p(x) = 0$ quando o polinômio p é divisível por $(x - r)^m$ e não é divisível por $(x - r)^{m+1}$, ou seja, a decomposição de p apresenta exatamente m fatores iguais a $x - r$. Quando $m = 1$, dizemos que r é raiz simples; quando $m = 2$, dizemos que r é raiz dupla; quando $m = 3$, é raiz tripla; etc.

Exemplo 34. *A equação $x^5(x - 2)^3 = 0$, admite as soluções 0 e 2, de multiplicidades 5 e 3, respectivamente. Observe que a equação é do 8^o grau, mas só possui duas raízes. Isto é: $S = \{0, 2\}$;*

Exemplo 35. *A equação $(x+1)^2.(x-1)^3.(x+2)^4 = 0$ é do 9^o grau e possui as raízes: -1 (dupla), 1 (tripla) e -2 (quádrupla). Assim, $S = \{-2, -1, 1\}$.*

As relações entre coeficientes e raízes de uma equação polinomial que serão desenvolvidas a seguir são conhecidas como *Relações de Girard.* [8]

4.4.1 Equações do 2º Grau

Considere a equação:

$$ax^2 + bx + c = 0 \quad (a \neq 0),$$

de raízes r_1 e r_2. Pelo Teorema 11, sabemos que essa equação pode ser escrita na forma:

$$a(x - r_1)(x - r_2) = 0.$$

Logo, temos a igualdade:

$$ax^2 + bx + c = a(x - r_1)(x - r_2).$$

[8] Albert Girard (1595-1632), matemático francês estudioso das equações polinomiais.

Ou seja:

$$x^2 + \frac{b}{a}x + \frac{c}{a} = x^2 - (r_1 + r_2)x + r_1 r_2$$

Portanto:

$$r_1 + r_2 = -\frac{b}{a} \quad e \quad r_1 r_2 = \frac{c}{a},$$

que são as relações de Girard para equações polinomiais do 2º grau. Observe que na primeira relação temos a soma das duas raízes e na segunda o produto entre elas.

4.4.2 Equações do 3º Grau

Considere a equação:

$$ax^3 + bx^2 + cx + d = 0 \quad (a \neq 0),$$

com raízes r_1, r_2 e r_3. Pelo Teorema 11, essa equação pode ser escrita na forma:

$$a(x - r_1)(x - r_2)(x - r_3) = 0$$

Temos então:

$$ax^3 + bx^2 + cx + d = a(x - r_1)(x - r_2)(x - r_3).$$

Ou seja:

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = x^3 - (r_1 + r_2 + r_3)x^2 + (r_1 r_2 + r_2 r_3 + r_1 r_3)x - r_1 r_2 r_3$$

Assim:

$$r_1 + r_2 + r_3 = -\frac{b}{a}, \quad r_1 r_2 + r_2 r_3 + r_1 r_3 = \frac{c}{a} \ \ e \ \ r_1 r_2 r_3 = -\frac{d}{a},$$

que são as relações de Girard para equações polinomiais do 3º grau. Veja que na primeira relação temos a soma das três raízes, na segunda a soma dos produtos das raízes tomadas duas a duas e na terceira o produto das três raízes.

4.4.3 Equação de grau n

Agora vamos generalizar as relações de Girard para equações polinomiais de grau $n \geq 1$. Seja a equação:

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2 x^2 + a_1 x + a_0 = 0 \quad (a_n \neq 0).$$

Usando n vezes o procedimento anterior, chegaremos a:

$$r_1 + r_2 + r_3 + ... + r_n = -\frac{a_{n-1}}{a_n} \tag{22}$$

$$r_1 r_2 + r_1 r_3 + r_1 r_4 + ... + r_{n-1} r_n = \frac{a_{n-2}}{a_n} \tag{23}$$

$$r_1 r_2 r_3 + r_1 r_2 r_4 + ... + r_{n-2} r_{n-1} r_n = -\frac{a_{n-3}}{a_n} \tag{24}$$

$$\vdots$$

$$r_1 r_2 r_3 ... r_n = (-1)^n \frac{a_0}{a_n}. \tag{25}$$

Onde, na equação (22) temos a soma das n raízes da equação; na equação (23) a soma dos produtos das n raízes tomadas duas a duas; na (24) a soma dos produtos das n raízes tomadas três a três e assim por diante, até chegar na equação (25) que representa o produto de todas as n raízes.

Exemplo 36. *Obtenha as relações de Girard para a equação* $2x^3 - 4x^2 + x + 3 = 0$, *considerando* r, s, *e* t *suas raízes.*

Resolução:

Como a equação é do 3º grau, temos as relações:

$r + s + t = -\frac{b}{a}$; $\quad rs + rt + st = \frac{c}{a} \quad e \quad rst = -\frac{d}{a}$

Logo:

$r + s + t = -\frac{(-4)}{2} = 2$; $\quad rs + rt + st = \frac{1}{2} \quad e \quad rst = -\frac{3}{2}$

Exemplo 37. *Sendo r, s, t e u as raízes da equação $x^4 + 4x^3 + 5x^2 - x + 2 = 0$, obtenha as relações de Girard.*

Resolução:

Agora a equação é do 4º grau, portanto, as relações são:

$r + s + t + u = -\frac{b}{a} = -\frac{4}{1} = -4$

$rs + rt + ru + st + su + tu = \frac{c}{a} = \frac{5}{1} = 5$

$rst + rsu + rtu + stu = -\frac{d}{a} = -\frac{(-1)}{1} = 1$

$rstu = \frac{e}{a} = \frac{2}{1} = 2$

Exemplo 38. *Resolver a equação $x^3 - 8x^2 + 19x - 12 = 0$, sabendo que uma das raízes é igual à soma das outras duas.*

Resolução:

Tomando as raízes como r, s e t, temos as relações de Girard:

$$r + s + t = 8 \tag{26}$$

$$rs + rt + st = 19 \tag{27}$$

$$rst = 12 \tag{28}$$

Do enunciado, temos que:

$$r = s + t. \tag{29}$$

Substituindo (29) em (26): $r + s + t = 8 \Rightarrow r + r = 8 \Rightarrow r = 4$

Logo, o polinômio $p(x) = x^3 - 8x^2 + 19x - 12$, é divisível por $x - 4$. Efetuando a divisão, obtemos $p(x) = (x^2 - 4x + 3)(x - 4)$.

Assim, as raízes s e t, são as raízes da equação $x^2 - 4x + 3 = 0$. Isto é: $s = 1$ e $t = 3$.

Portanto, o conjunto solução da equação é: $S = \{1, 3, 4\}$

4.5 Raízes Complexas

Como vimos no Capítulo 2, um número complexo tem a forma $z = a + bi$, em que $a, b \in \mathbb{R}$ e $i = \sqrt{-1}$. Neste número, a é chamado de parte real, b de parte imaginária e i é chamado de unidade imaginária.

Ao resolvermos a equação polinomial $x^2 - 2x + 5 = 0$, encontramos as raízes $x_1 = 1+2i$ e $x_2 = 1-2i$. Da mesma forma, ao resolvermos $x^2+4 = 0$, encontramos $x_1 = -2i$ e $x_2 = 2i$.

Observe que as raízes das duas equações são *pares de números complexos conjugados*. Mostraremos no teorema a seguir que esta situação ocorre sempre que uma equação polinomial possuir alguma raiz complexa. Ou seja, as raízes complexas aparecem aos pares em uma equação polinomial.

Teorema 12. *Se um número complexo $z = a + bi$, com $b \neq 0$, é raiz de uma equação com coeficientes reais, então seu conjugado $\bar{z} = a - bi$ também é raiz dessa equação.*

Demonstração. Considere a equação polinomial

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0,$$

com $a_n, a_{n-1}, a_{n-2}, ..., a_1, a_0 \in \mathbb{R}$. Considere ainda as Propriedades $6, 7, 8$ e 9 da seção 2.4, a respeito dos números complexos.

Por hipótese, z é raiz da equação. Ou seja, $p(z) = 0$. Logo:

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

Generalizando a propriedade 6, temos:

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

Aplicando as propriedades 7 e 8, vem:

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

Finalmente, aplicando a propriedade 9, temos:

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

Assim, $p(\bar{z}) = 0$, ou seja, $\bar{z}$ também é raiz da equação. □

Exemplo 39. *A equação* $x^2 + mx + n = 0$, $m, n \in \mathbb{R}$, *admite* $5 - 2i$ *como uma raiz. Determine os valores de* m *e* n.

Resolução:

Como $5 - 2i$ *é raiz da equação, pelo Teorema 12,* $5 + 2i$ *é a outra raiz. Usando as relações de Girard, temos que:*

$r_1 + r_2 = -\frac{b}{a} \Rightarrow (5 - 2i) + (5 + 2i) = -\frac{m}{1} \Rightarrow m = -10$

$r_1 r_2 = \frac{c}{a} \Rightarrow (5 - 2i).(5 + 2i) = \frac{n}{1} \Rightarrow n = 29$

Exemplo 40. *Sabendo que* $4 + 3i$ *é raiz da equação* $x^4 - 8x^3 + 15x^2 + 80x - 250 = 0$, *determine as demais raízes.*

Resolução:

Uma vez que $4 + 3i$ *é raiz da equação temos, pelo Teorema 12, que* $4 - 3i$ *também é uma raiz. Assim, nos resta encontrar as outras duas.*

Pelo Teorema 11, temos que o polinômio $p(x)$ *associado à equação pode ser escrito na forma:*

$$p(x) = (x - (4 + 3i)).(x - (4 - 3i))(ax^2 + bx + c).$$

Isto é, $p(x)$ *é divisível por* $(x - 4 - 3i).(x - 4 + 3i) = x^2 - 8x + 25$.

Efetuando a divisão, temos que $p(x) = (x^2 - 8x + 25).(x^2 - 10)$.

Portanto, as demais raízes são obtidas de: $x^2 - 10 = 0$. *Ou seja* $x_3 = -\sqrt{10}$ *e* $x_4 = \sqrt{10}$

4.6 Raízes Racionais

Nesta seção, desenvolveremos um método que permitirá identificar se uma equação polinomial de coeficientes inteiros admite raízes racionais e, caso admita, obteremos suas raízes.

Teorema 13. *Considere a equação polinomial:*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2 x^2 + a_1 x + a_0 = 0, \quad a_n \neq 0.$$

Com $a_n, a_{n-1}, ..., a_1, a_0 \in \mathbb{Z}$. *Se a equação admite uma raiz racional* $\frac{p}{q}$, *em que* $p, q \in \mathbb{Z}, q \neq 0$ *e* p *e* q *são primos entre si, então* p *é divisor de* a_0 *e* q *é divisor de* a_n.

Demonstração. Se $\frac{p}{q}$ é uma raiz de $f(x) = 0$, temos:

$$a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + a_{n-2}\frac{p^{n-2}}{q^{n-2}} + ... + a_1 \frac{p}{q} + a_0 = 0$$

Multiplicando a equação por q^n, temos:

$$a_n p^n + a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + ... + a_1 pq^{n-1} + a_0 q^n = 0$$

Isolando $a_n p^n$ e, depois, $a_0 q^n$, temos as equações:

$$a_n p^n = -q[a_{n-1}p^{n-1} + a_{n-2}p^{n-2}q + ... + a_1 pq^{n-2} + a_0 q^{n-1}] \tag{30}$$

$$a_0 q^n = -p[a_n p^{n-1} + a_{n-1}p^{n-2}q + ... + a_1 q^{n-1}]. \tag{31}$$

Como $a_0, a_1, a_2, ..., a_n, p$ e q são todos números inteiros, obtemos que α e β descritos abaixo são inteiros.

$$\alpha = [a_{n-1}p^{n-1} + a_{n-2}p^{n-2}q + ... + a_1 pq^{n-2} + a_0 q^{n-1}]$$

$$\beta = [a_n p^{n-1} + a_{n-1}p^{n-2}q + ... + a_1 q^{n-1}].$$

Assim, a equação (30) equivale a:

$$\frac{a_n p^n}{q} = -\alpha \in \mathbb{Z}$$

e equação (31) equivale a:

$$\frac{a_0 q^n}{p} = -\beta \in \mathbb{Z}$$

Desta forma, concluímos que:

(i) $a_n p^n$ é divisível por q e, como p^n e q são primos entre si, a_n é divisível por q.

(ii) $a_0 q^n$ é divisível por p e, como q^n e p são primos entre si, a_0 é divisível por p. □

Exemplo 41. *Determinar as três raízes da equação* $3x^3 - 7x^2 + 8x - 2 = 0$.

Resolução:

Observe que não dispomos de nenhuma informação sobre as raízes e que todos os coeficientes da equação são inteiros. Logo, aplicando o Teorema 13, se a equação possuir alguma raiz racional $\frac{p}{q}$, *com* $p \in \mathbb{Z}$, $q \in \mathbb{Z}^*$, p *e* q *primos entre si, então* p *será divisor de* -2 *e* q *será divisor de* 3. *Isto é:* $p \in \{-2, -1, 1, 2\}$ *e* $q \in \{-3, -1, 1, 3\}$. *Assim, os candidatos a raízes racionais são:* $\pm 1, \pm 2, \pm\frac{1}{3}, \pm\frac{2}{3}$. *Considerando o polinômio* $f(x) = 3x^3 - 7x^2 + 8x - 2$, *associado à equação, temos:*

$$f(1) = 2, \quad f(-1) = -20, \quad f(2) = 10, \quad f(-2) = -70,$$
$$f(\tfrac{1}{3}) = 0, \quad f(-\tfrac{1}{3}) = -\tfrac{50}{9}, \quad f(\tfrac{2}{3}) = \tfrac{10}{9}, \quad f(-\tfrac{2}{3}) = -\tfrac{34}{3}.$$

Logo, a única raiz racional é $x = \dfrac{1}{3}$ *e o polinômio* $f(x)$ *é divisível por* $(x - \frac{1}{3})$. *Efetuando a divisão, chegamos a* $f(x) = (x - \frac{1}{3})(3x^2 - 6x + 6)$, *o que nos fornece as raízes* $x = 1 - i$ *e* $x = 1 + i$. *Então o conjunto solução da equação é:* $S = \{1 - i, 1 + i, \frac{1}{3}\}$.

Exemplo 42. *Pesquisar as raízes racionais da equação* $2x^3 + x^2 - 25x + 12 = 0$.

Resolução:

De acordo com o Teorema 13, se a equação possuir alguma raiz racional $\frac{p}{q}$, *com* $p, q \in \mathbb{Z}$, $q \neq 0$, p *e* q *primos entre si, então* p *será divisor de* 12 *e* q *será divisor de*

2. *Assim,* $p \in \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$ *e* $q \in \{-2, -1, 1, 2\}$. *Logo, as possíveis raízes racionais são:* $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm\frac{1}{2}, \pm\frac{3}{2}$. *Fazendo os cálculos, obtemos as raízes* $x = \frac{1}{2}$, $x = -4$ *e* $x = 3$. *Portanto, a equação possui apenas raízes racionais.*

5 Números Transcendentes

No capítulo anterior, trabalhamos métodos e técnicas de resolução de equações polinomiais ou algébricas quaisquer. Neste capítulo, trataremos exclusivamente de equações polinomiais que possuam coeficientes inteiros. Isto é, equações da forma:

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2 x^2 + a_1 x + a_0 = 0$$

em que $a_n, a_{n-1}, ..., a_1, a_0$ são números inteiros.

Assim, chegaremos a um novo conjunto numérico, o conjunto dos números chamados de *Transcendentes*. Estes números, apesar de serem difíceis de se verificar, existem em profusão, sendo que podemos estabelecer uma bijeção entre o conjunto dos números *transcendentes* e um subconjunto próprio não enumerável.

Definição 17. *Definimos como Inteiro Algébrico a todo número que é solução de uma equação polinomial da forma:*

$$x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0 \tag{32}$$

em que $a_{n-1}, a_n, ..., a_1, a_0$ são números inteiros.

Exemplo 43. *Qualquer inteiro k é inteiro algébrico, pois é solução da equação $x - k = 0$.*

Exemplo 44. *$\sqrt{2}$ e $-\sqrt{2}$ são inteiros algébricos, pois são raízes da equação $x^2 - 2 = 0$.*

Exemplo 45. *$i = \sqrt{-1}$ e $-i = -\sqrt{-1}$ são inteiros algébricos complexos, pois são raízes da equação $x^2 + 1 = 0$.*

Teorema 14. *Um número inteiro algébrico real é um número inteiro ou um número irracional.*

Demonstração. Como qualquer inteiro a é inteiro algébrico, devemos mostrar apenas que um número racional não inteiro não pode ser inteiro algébrico.

Para tanto, considere k um inteiro algébrico. Suponha, por contradição, que $k = \frac{p}{q}$ seja um número racional. Onde $p, q \in \mathbb{Z}, q > 1$, p, q primos entre si. Ou seja, k é um racional não inteiro. Como k é raiz de uma equação do tipo (32), substituindo $\frac{p}{q}$ na equação, temos:

$$(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + ... + a_1(\frac{p}{q}) + a_0 = 0 \rightarrow \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + ... + a_1\frac{p}{q} + a_0 = 0$$

Multiplicando por (q^n), temos:

$$p^n + a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + ... + a_1pq^{n-1} + a_0q^n = 0 \Rightarrow$$

$$p^n = -a_{n-1}p^{n-1}q - a_{n-2}p^{n-2}q^2 - ... - a_0q^n \Rightarrow$$

$$p^n = q(-a_{n-1}p^{n-1} - a_{n-2}p^{n-2}q - ... - a_0q^{n-1}).$$

Logo, $q|p^n$. Considere um fator k de q, com $k \neq 1$ ($k = q$, se q for primo). Pelo Lema 2, $k|p$. Mas isso é um absurdo, pois tomamos, inicialmente, p e q primos entre si. Assim, um inteiro algébrico não pode ser racional não inteiro. □

5.1 Números Algébricos e Transcendentes

Nesta secão, definiremos os números algébricos e provaremos a existência dos números transcendentes.

Definição 18. *Definimos como Número Algébrico a todo número que é solução de uma equação polinomial da forma:*

$$a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0, \quad a_n \neq 0. \tag{33}$$

Em que $a_n, a_{n-1}, a_n, ..., a_1, a_0$ *são números inteiros. Um número* ***não algébrico*** *é chamado de* ***Número Transcendente****.*

Observe a diferença entre as definições de *Inteiro Algébrico* e *Número Algébrico*. Enquanto o primeiro é solução de uma equação do tipo (32), em que $a_n = 1$, o segundo é solução de uma equação do tipo (33) em que a_n é um inteiro qualquer diferente de zero. Logo, todo *Inteiro Algébrico* é também um *Número Algébrico*.

Concluímos então que todo racional $\frac{p}{q}, q \neq 0$, p, q primos entre si, é um número algébrico, pois é solução da equação $qx - p = 0$.

Dados dois números algébricos α e β, as seguintes propriedades de fechamento são válidas:

(i) A soma $\alpha + \beta$ é um número algébrico.

(ii) O produto $\alpha.\beta$ é um número algébrico.

(iii) O simétrico $-\alpha$ é um número algébrico.

(iv) Se $\alpha \neq 0$, o inverso α^{-1} é um número algébrico.

Para provar que nem todo número real é algébrico, isto é, que existem números *transcendentes*, recorremos à demonstração feita por por G. Cantor.[9], como pode ser vista em [2] e [6].

Teorema 15. *O conjunto de todos os números algébricos é enumerável.*

Demonstração. Consideremos um polinômio com coeficientes inteiros

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0, \quad a_n \neq 0, n \in \mathbb{N}. \tag{34}$$

E definimos sua *altura* como sendo o número natural

$$|p| = |a_n| + |a_{n-1}| + ... + |a_1| + |a_0| + n. \tag{35}$$

[9]George Cantor (1845-1918), matemático russo-alemão, estudioso da teoria dos conjuntos.

Ou seja, sua *altura*, $|p|$ é igual à soma dos valores absolutos dos seus coeficientes inteiros, mais o grau do polinômio. Por exemplo, no polinômio $p(x) = 2x^3 - 3x^2 + 2x - 5$ a altura é dada por $|p| = 2 + 3 + 2 + 5 + 3 = 15$.

Pelo Corolário 3, se $p(x) = 0$, com $p(x)$ dado em (34), então $p(x)$ tem exatamente n *raízes* complexas, sendo que todas, algumas ou nenhuma delas podem ser reais.

Observe que o número de polinômios do tipo (34) com uma determinada altura é um número finito, devido à definição dada em (35). Portanto, as raízes de todos os polinômios de uma dada altura formam um conjunto finito.

Assim, o conjunto de todas as raízes de todos os polinômios de todas as alturas formam um conjunto enumerável, pois pelo item (iv) do Teorema 6, a união de enumerável de conjuntos finitos é enumerável. Logo, o conjunto dos números *algébricos* é enumerável. □

Teorema 16. *Existem Números Transcendentes.*

Demonstração. Pelo Teorema 15, o conjunto dos números algébricos é enumerável. Logo, existem números reais que não são algébricos, pois do contrário, o conjunto dos números reais $\mathbb{R}$ seria enumerável, o que contraria o Teorema 7. Portanto, existem números *transcendentes*. □

Uma vez que todo número racional é algébrico, fica claro que todo número transcendente é irracional. Podemos ilustrar isso como na Figura 17 a seguir.

Na figura, $\sqrt{2}$ e $\sqrt[3]{7}$ aparecem como exemplos de números algébricos, pois satisfazem as equações $x^2 - 2 = 0$ e $x^3 - 7 = 0$, respectivamente. Por outro lado, os números $\log 2$ e π aparecem como exemplos de números transcendentes. Sabe-se desde o final do século XIX que π e e são transcendentes. Ao passo que a transcendência de números como $2^{\sqrt{2}}$ e $\log 2$ foi provada somente em 1934.

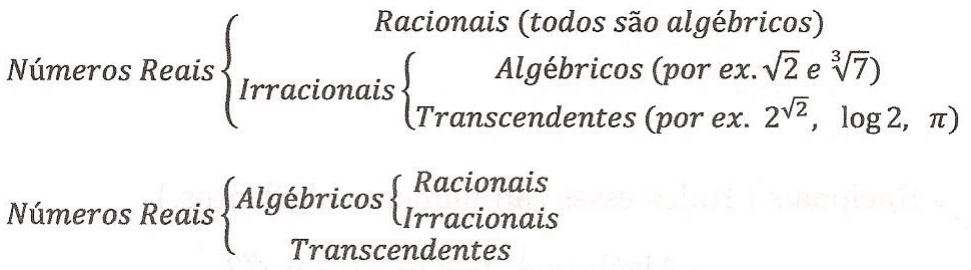


Figura 17: Números Algébricos e Transcendentes

O número $2^{\sqrt{2}}$ foi usado por *Hilbert* [10] para ilustrar seu famoso 7° problema, o qual consistia em determinar se um número da forma α^{β} é algébrico ou transcendente, sendo α, β números algébricos com $\alpha \neq 0$, $\alpha \neq 1$ e β não racional (que tornariam o problema simples, pois o resultado seria um número algébrico).

O problema foi resolvido em 1934 por *Gelfond* e *Schneider* [11], de modo independente, provando que todo número α^{β} nas condições dadas é transcendente. A resolução do problema ficou conhecida como *Teorema de Gelfond-Schneider* e provou que números como $2^{\sqrt{2}}$ e $\log 2$, entre outros, são transcendentes.

A justificativa para $\log 2$ é relativamente simples, pois tomando $\alpha = 10$ e $\beta = \log 2$; e aplicando a definição de logaritmo decimal, temos que:

$$\alpha^{\beta} = 10^{\log 2} = 2.$$

Nesse caso, se $\beta = \log 2$ fosse irracional algébrico, pelo *Teorema de Gelfond-Schneider*, 2 seria transcendente, o que é absurdo. Logo, $\log 2$ só pode ser transcendente.

Generalizando o teorema, é possível provar que qualquer número da forma $\log_n m$

[10] David Hilbert (1862-1943). Matemático alemão que em 1900, no Congresso Internacional de Matemáticos em Paris, listou 23 problemas nas mais diversas áreas que nortearam o desenvolvimento da Matemática no século XX

[11] Alexander Gelfond (1906-1968). Matemático soviético; Theodor Schneider (1911-1988). Matemático alemão.

(com n, m racionais positivos, $n \neq 1$ e $\log_n m$ irracional), é transcendente.

Como exemplo, ao aplicarmos o mesmo raciocínio para o número $\log_3 5$, se este for um irracional algébrico, então 5 seria transcendente, pois:

$$\alpha^\beta = 3^{\log_3 5} = 5.$$

O que também é absurdo. Logo o número $\log_3 5$ é transcendente.

No caso de $n = 10$, basta que m não pertença à sequência:

$$...10^{-4}, 10^{-3}, 10^{-2}, 10^{-1}, 10^0, 10^1, 10^2, 10^3, 10^4, ...,$$

para que o número $\log m$ seja transcendente.

Outra curiosidade a respeito do estudo de números algébricos e transcendentes diz respeito à construção de segmentos de retas utilizando os métodos da Geometria Euclideana. Ou seja, usando apenas régua e compasso. É possível provar que podemos construir um segmento de comprimento igual a qualquer número racional e, ainda, igual a qualquer número da forma $\sqrt{a}$, sendo a um inteiro positivo. Prova-se ainda, que apenas os segmentos de comprimento igual a $p + q\sqrt{a}$, com p, q racionais e a um inteiro positivo, ou suas combinações (estes números são chamados de *surdos*), podem ser construídos usando tais instrumentos. Observando que os números *surdos* assim definidos são todos algébricos, concluímos que *um segmento com comprimento igual a um número transcendente não pode ser construído com o uso de régua e compasso.* Note que nem todos os números algébricos são *surdos*, assim nem todo segmento do tamanho de um algébrico qualquer pode ser construído com régua e compasso. Por exemplo, $\sqrt[3]{2}$ é algébrico, pois é solução de $x^3 - 2 = 0$, porém não é um número *surdo*, pois não é da forma $p + q\sqrt{a}$.

O fato de que $\sqrt[3]{2}$ não pode ser construído com régua e compasso resolveu um antigo problema geométrico conhecido como *A duplicação do cubo*, que consistia em obter um

cubo, cujo volume seria o dobro do volume de um cubo dado. Observe que, se um cubo tem aresta a u.m., seu volume será igual a a^3 u.v. e um cubo com o volume dobrado, ($2a^3$ u.v.), deveria ter aresta medindo $a\sqrt[3]{2}$, o que é impossível de se construir pelos métodos da Geometria Euclideana, como foi colocado anteriormente. Logo, o problema não tem solução.

Outro problema geométrico famoso que foi resolvido com a teoria dos números algébricos e transcendentes foi o problema da *Quadratura do Círculo*, que consistia em construir um círculo com área igual à de um quadrado dado ou construir um quadrado de área igual à de um círculo dado. Ora, um círculo de raio r tem área igual a πr^2. Logo, para construir um quadrado de mesma área, seu lado deveria ter comprimento igual a $r\sqrt{\pi}$. Desta forma, $\sqrt{\pi}$ deveria ser algébrico e, consequentemente, π também deveria ser, o que já vimos que não é verdade. Assim, o problema da *Quadratura do Círculo* também não tem solução.

6 Os Números de Liouville

Os números *transcendentes*, apesar de existirem em abundância como foi mostrado no Teorema 16, são difíceis de serem encontrados. Assim, é bastante trabalhoso e complicado provar que um determinado número real é transcendente. Alguns números que comprovadamente são transcendentes são o π e o e, cujas provas são devidas a alguns matemáticos, entre eles, I. Niven [12] e C. Hermite [13], respectivamente.

O matemático J. Liouville [14], em 1844, foi o primeiro a demonstrar a existência dos números *transcendentes* e a estabelecer um critério para mostrar a transcendência de um número real. Trataremos a seguir deste critério, conforme pode ser visto em [2].

Definição 19. *Um número algébrico α é de grau n se ele for raiz de uma equação polinomial de grau n e se não existir uma equação polinomial de menor grau, da qual α seja raiz.*

Exemplo 46. *Todo número racional $\frac{p}{q}$, $(p, q \in \mathbb{Z},\ q \neq 0)$, é algébrico de grau 1 pois é raiz da equação do 1^o grau $qx - p = 0$.*

Definição 20. *Um número real α é dito aproximável na ordem n por racionais, se existirem uma constante $c > 0$ e uma sucessão $\left\{\frac{p_j}{q_j}\right\}$ de racionais diferentes, com $q_j > 0$ e $mdc(p_j, q_j) = 1$, tais que:*

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{c}{q_j^n}. \tag{36}$$

Obviamente, se um número α é aproximável na ordem n, então ele é aproximável em qualquer ordem k, com $k < n$. De (36), temos:

$$\left|\alpha - \frac{p_j}{q_j}\right| < c \tag{37}$$

[12] Ivan Niven(1915-1999), matemático estadunidense que aperfeiçoou a demonstração equivocada de R. Moritz para a transcendência de π.

[13] Charles Hermite (1822-1901), matemático francês.

[14] Joseph Liouville(1809-1882), matemático francês.

Isso mostra que a sucessão q_j não se mantém limitada. Assim, concluímos que $q_j \to +\infty$. Logo, de (36) temos:

$$\lim_{j\to\infty}\left(\frac{p_j}{q_j}\right) = \alpha \tag{38}$$

É interessante observar que o importante da Definição 20 não é a existência de uma sucessão de racionais convergindo para α, pois estas sucessões sempre existem qualquer que seja o número real α (essa é a chamada densidade dos racionais no conjunto dos reais). O mais importante que a definição nos traz é que uma sucessão particular de racionais converge para α de certo modo, ou seja, de acordo com (36). Ainda na Definição 20, é importante que se tome os racionais todos diferentes, o que implica que podemos tomá-los diferentes de α, mesmo no caso de α ser racional.

Teorema 17. *Todo número racional (ou algébrico de grau 1) é aproximável na ordem 1 e não é aproximável na ordem $k, k > 1$.*

Demonstração. Provaremos primeiramente que um número racional é aproximável na ordem 1. Seja $\frac{p}{q}, q > 0$ e $mdc(p, q) = 1$. Então, pelo Teorema 5, existem $x_0, y_0 \in \mathbb{Z}$, tais que:

$$px_0 - qy_0 = 1. \tag{39}$$

Considerando a equação:

$$px - qy = 1, \tag{40}$$

sabemos que ela possui infinitas soluções, pois todos os pares de números da forma:

$$x_t = x_0 + qt \quad e \quad y_t = y_0 + pt, \tag{41}$$

para todo $t \in \mathbb{Z}$, são soluções para (40). Ou seja:

$$px_t - qy_t = 1 \tag{42}$$

Fixando um k natural, tal que $k > -\frac{x_0}{q}$, e considerando as sucessões $\{x_j\}$ e $\{y_j\}$ definidas a partir de (41), por:

$$x_j = x_0 + q(k+j), \quad y_j = y_0 + p(k+j), j \in \mathbb{N}. \tag{43}$$

Pela condição imposta a k, temos $x_j > q_j$ e, assim, $x_j > 0$, pois $q > 0$. Afirmamos agora que:

$$\frac{y_j}{x_j} \neq \frac{y_{j'}}{x_{j'}}, \quad se \;\; j \neq j^{'}. \tag{44}$$

Pois, se existir a igualdade dos racionais em (44), por (41) e (39), podemos concluir que $j = j^{'}$. Por (42), deduzimos que os $x_j^{'}s$ e $y_j^{'}s$ definidos em (43) satisfazem a:

$$\left|\frac{p}{q} - \frac{y_j}{x_j}\right| = \frac{1}{qx_j} < \frac{2}{x_j}.$$

O que mostra que $\frac{p}{q}$ é aproximável na ordem 1.

Provemos agora que um número racional não é aproximável na ordem $k, k > 1$. Para todo $\frac{m}{n} \neq \frac{p}{q}$, com $n > 0$, temos:

$$\left|\frac{p}{q} - \frac{m}{n}\right| = \frac{|pn - qm|}{qn} \geq \frac{1}{qn}. \tag{45}$$

Observe que, se $\frac{p}{q}$ fosse aproximável na ordem 2, existiria um $c > 0$ e uma sucessão de racionais $\frac{m_j}{n_j}$ diferentes, tais que:

$$\left|\frac{p}{q} - \frac{m_j}{n_j}\right| < \frac{c}{n_j^2}. \tag{46}$$

De (45) e (46), temos que $\frac{1}{qn_j} < \frac{c}{n_j^2}$, isto é, $n_j < qc$. Mas isso não é possível, uma vez que $n_j \to \infty$. Portanto, $\frac{p}{q}$ não aproximável na ordem 2 e, consequentemente, também não é aproximável em nenhuma ordem superior. □

Teorema 18. *Todo número irracional é aproximável na ordem 2. Isto é, existe $c > 0$, tal que a desigualdade abaixo é verdadeira para infinitos racionais $\frac{p}{q}$ distintos:*

$$\left|\lambda - \frac{p}{q}\right| < \frac{c}{q^2}.$$

Demonstração. Considere α um número irracional e $n \in \mathbb{N}$. Representemos por $[x]$ a parte inteira de um número real x. Isto é, o maior inteiro menor ou igual a x. Por exemplo, se $x = 2,343867$, $[x] = 2$. Considere ainda os $n+1$ números reais dados:

$$0; \alpha - [\alpha]; 2\alpha - [2\alpha]; 3\alpha - [3\alpha]; ...; n\alpha - [n\alpha], \tag{47}$$

todos pertencentes ao intervalo $[0,1) = \{x : 0 \leq x < 1\}$. Tomemos a partição do intervalo $[0,1)$ em n intervalos, disjuntos dois a dois, da forma:

$$\left[\frac{j}{n}, \frac{j+1}{n}\right), \quad j = 0, 1, ..., n-1. \tag{48}$$

Evidentemente, pelo menos dois dos reais em (47) estão em um mesmo intervalo descrito em (48). Digamos que eles sejam $n_1\alpha - [n_1\alpha]$ e $n_2\alpha - [n_2\alpha]$, com $0 \leq n_1 < n_2 \leq n$, para os quais temos:

$$|n_2\alpha - [n_2\alpha] - n_1\alpha + [n_1\alpha]| < \frac{1}{n}. \tag{49}$$

Sejam agora os inteiros $k = n_2 - n_1$ e $h = [n_2\alpha] - [n_1\alpha]$, com $k > 0$ e $h \geq 0$. Assim, (49) pode ser escrito como:

$$|k\alpha - h| < \tfrac{1}{n} \quad \text{ou} \quad \left|\alpha - \tfrac{h}{k}\right| < \tfrac{1}{nk}$$

o que implica que:

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{k^2}, \tag{50}$$

onde utilizamos $k < n$ para a última desigualdade. Resumindo, mostramos que para cada n, existe um racional da forma $\frac{h}{k}$, com $k < n$, para o qual (50) se verifica. Provemos agora que (50) se verifica para um número infinito de racionais $\frac{h}{k}$ distintos.

Suponha, por contradição, que esse número não seja infinito. Isto é, existem apenas n racionais $\frac{h_1}{k_1}, \frac{h_2}{k_2}, ..., \frac{h_r}{k_r}$ que satisfazem (50). Considere:

$$\epsilon = min\left\{\left|\alpha - \frac{h_1}{k_1}\right|, ..., \left|\alpha - \frac{h_r}{k_r}\right|\right\}$$

e tome $n \in \mathbb{N}$, tal que $\frac{1}{n} < \epsilon$. Pelo que foi feito acima, existe um racional $\frac{h}{k}$, tal que:

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{nk}.$$

Como $\frac{1}{nk} < \frac{1}{n} < \epsilon$, temos que $\frac{h}{k} \neq \frac{h_i}{k_i}$, para $i = 1, 2, ..., r$. O que é absurdo, pois $\frac{h}{k}$ satisfaz (50). O que completa a demonstração. □

Teorema 19. *Seja α um número algébrico real de grau n. Então existe uma constante $A > 0$, tal que:*

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{Aq^n} \tag{51}$$

para todo racional $\frac{p}{q}$. (Se $n = 1$, tomemos $\frac{p}{q} \neq \alpha$)

Demonstração. Considere α a solução de uma equação polinomial da forma:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0. \tag{52}$$

Seja $d > 0$ tal que, no intervalo $[\alpha - d, \alpha + d]$ a única raiz de $f(x) = 0$ é α. Sabemos que d existe, pois a equação tem no máximo n raízes reais e d pode ser qualquer número menor que a menor das distâncias de α às demais raízes reais. Em seguida, observemos que a derivada $f'(x)$ de $f(x)$ é um polinômio de grau $n - 1$ e, portanto, ela é limitada em qualquer intervalo finito. Seja então $M > 0$ tal que:

$$|f'(x)| < M, \quad para \quad x \in [\alpha - d, \alpha + d]. \tag{53}$$

Para todo racional $\frac{p}{q}$, com $q > 0$, em $[\alpha - d, \alpha + d]$, aplicando o teorema do valor médio, temos:

$$f(\alpha) - f(\frac{p}{q}) = (\alpha - \frac{p}{q}).f'(\psi),$$

onde $\psi \in (\alpha - d, \alpha + d)$. Como $f(\alpha) = 0$, obtemos:

$$\left|f(\frac{p}{q})\right| = \left|\alpha - \frac{p}{q}\right| .|f'(\psi)| \leq M. \left|\alpha - \frac{p}{q}\right|, \tag{54}$$

usando (53) no último passo.

Para chegarmos à desigualdade (51), precisamos de uma estimativa inferior para $f(\frac{p}{q})$, que pode ser:

$$\left|f(\frac{p}{q})\right| = \left|\frac{a_n p^n + a_{n-1} q p^{n-1} + ... + a_0 q^n}{q^n}\right| \geq \frac{1}{q^n}. \tag{55}$$

Logo, de (54) e (55), temos a desigualdade:

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{Mq^n},$$

para $\frac{p}{q} \in [\alpha - d, \alpha + d]$. Se $\frac{p}{q}$ não estiver nesse intervalo, teremos:

$$\left|\alpha - \frac{p}{q}\right| > d$$

e como $q \geq 1$, temos

$$\left|\alpha - \frac{p}{q}\right| > \frac{d}{q^n}.$$

Finalmente, se tomarmos $\frac{1}{A}$ como o menor dos números $\frac{1}{M}$ e d, chegamos à desigualdade (51) para todo racional $\frac{p}{q}$. □

Corolário 4. *Se α é um número algébrico real de grau n, então α não é aproximável na ordem $n+1$.*

Demonstração. Suponha, por contradição, que existe $c > 0$ e uma sucessão $\{\frac{p_j}{q_j}\}$ de racionais distintos, tais que:

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{c}{q_j^{n+1}}. \tag{56}$$

Para estes racionais, segue de (51) e (56) que:

$$\frac{1}{Aq_j^n} < \frac{c}{q_j^{n+1}} \quad ou \quad q_j < A_c.$$

Mas isso é absurdo, pois $q_j \to +\infty$. Logo, α não é aproximável na ordem $n+1$. □

Definição 21. *Dizemos que um número real α é um número de Liouville, se existir uma sucessão $\{\frac{p_j}{q_j}\}$, $q_j > 0$, $mdc(p_j, q_j) = 1$, com todos os elementos diferentes, e tal que:*

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j}. \tag{57}$$

Teorema 20. *Todo número de Liouville é transcendente.*

Demonstração. Por contradição, vamos supor que exista um certo número α de *Liouville* que seja algébrico de grau n. Logo, pelo Teorema 19, a relação (51) seria válida para todo racional e, em particular, para os $\frac{p_j}{q_j}$ da Definição 21. Teríamos então:

$$\frac{1}{Aq_j^n} < \left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j}$$

o que implicaria:

$$q_j^{j-n} < A. \tag{58}$$

Como $q_j \to +\infty$, temos que a desigualdade (58) não pode ser verdadeira para j suficientemente grande. Portanto, α não pode ser algébrico. □

Lema 3. *Seja α um número real, tal que:*

$$\left|\alpha - \frac{m_j}{n_j}\right| < \frac{1}{n_j^j},$$

onde $\{\frac{m_j}{n_j}\}$ é uma sucessão de racionais distintos e $n_j > 0$. Então α é um número de Liouville.

Observe que não foi exigido que $mdc(m_j, n_j)$ seja igual a 1.

Demonstração. Considere a sucessão $\{\frac{p_j}{q_j}\}$, com $q_j > 0$ e $mdc(p_j, q_j) = 1$ definida por:

$$\frac{p_j}{q_j} = \frac{m_j}{n_j}.$$

Temos então:

$$\left|\alpha - \frac{p_j}{q_j}\right| = \left|\alpha - \frac{m_j}{n_j}\right| < \frac{1}{n_j^j} \leq \frac{1}{q_j^j}.$$

O que implica em:

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j}.$$

Portanto α é um número de *Liouville*. □

Exemplo 47. *Seja o número:*

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}. \tag{59}$$

Considere a sucessão de racionais definida por

$$\frac{m_j}{n_j} = \sum_{k=1}^{j} \frac{1}{10^{k!}}.$$

Temos assim:

$$\left|\alpha - \frac{m_j}{n_j}\right| = \sum_{k=j+1}^{\infty} \frac{1}{10^{k!}} = \frac{1}{10^{(j+1)!}} \underbrace{\left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + ...\right)}_{(I)}. \tag{60}$$

Observe que a expressão entre parênteses (I) pode ser majorada por:

$$1 + \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + ... = \frac{10}{9}$$

Assim, o último membro de da equação (60) pode ser majorado por:

$$\frac{1}{(10^{j!})^j 10^{j!}} . \frac{10}{9} < \frac{1}{(10^{j!})^j},$$

logo:

$$\left|\alpha - \frac{m_j}{n_j}\right| < \frac{1}{(10^{j!})^j}$$

e como $n_j = 10^{j!}$, temos:

$$\left|\alpha - \frac{m_j}{n_j}\right| < \frac{1}{n_j^j}$$

Portanto $\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}}$ é um número de Liouville.

Observação 4. *O número:*

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} = 0,110001000000000000000001...$$

é chamado de constante de Liouville e foi o primeiro número historicamente reconhecido como transcendente. Observe que o algarismo 1 ocupa a casa decimal correspondente a $k!$ *(casas decimais 1, 2, 6, 24, 120,...) e as demais casas são ocupadas pelo algarismo 0. Como acabou de ser mostrado, a constante de Liouville é um número de Liouville.*

Exemplo 48. *Qualquer número da forma:*

$$\alpha = \sum_{k=1}^{\infty} \frac{a_k}{10^{k!}}$$

onde $a_k \in \{1, 2, 3, ..., 9\}$*, é um número de Liouville.*

Entre as aplicações da *constante de Liouville* podemos destacar o seu uso para provar que entre dois números reais sempre existe um irracional. Observe na Proposição 2.

Proposição 2. *Dados dois números reais* a *e* b*, com* $a \neq b$*, sempre existe um número irracional entre eles.* [15]

Demonstração. Suponha, sem perda de generalidade, que a e b são positivos e que $a < b$. Vamos dividir a demonstração em dois casos.

Caso 1: a e b são racionais.

Consideremos o número $\alpha = 0,110001000000000000000000100...$ (*constante de Liouville*) que é irracional e está entre 0 e 1.

Então o número $t = a + \alpha(b - a)$ é irracional e está entre a e b.

De fato, t irracional pois, do contrário, $\alpha = \dfrac{t - a}{b - a}$ seria racional (pelas operações de

[15] Extraído da Revista do Professor de Matemática, nº 9, 1986 , página 64.

fechamento dos racionais). Mas, como já foi provado, α é irracional.

Para provar que t está entre a e b, provemos que $a < t$ e $t < b$:

(i) Temos que $\alpha > 0$ e $b - a > 0$, pois $a < b$. Logo $\alpha(b-a) > 0$ e $a + \alpha(b-a) > a$, ou seja, $t > a$,

(ii) Temos que $\alpha < 1$ e $b > a$, logo $\alpha(b-a) < b-a$. Daí, $a+\alpha(b-a) < b$. Como $a < t$ e $t < b$, concluímos que t está entre a e b.

Caso 2: a ou b ou ambos são irracionais.

Consideremos, agora, o número $t = a' + \alpha(b' - a')$. Onde a' e b' são os truncamentos dos desenvolvimentos decimais de a e b respectivamente, tomando-se um número suficiente de casas decimais e alterando-se alguma casa em a' e b' entre a e b e fazendo $a' \neq b'$.

Por exemplo se $a = \sqrt{2}$ e $b = \sqrt{2} + 10^{-7}$, temos $a = 1,41421356...$ e $b = 1,41421366....$ Fazendo $a' = 1,4142135$ e $b' = 1,4142136$, teremos que somar um ao algarismo da última casa decimal de a' para ter $a < a'$. Assim, $a' = 1,4142136$ que é igual a b'. Então devemos ter mais uma casa decimal em b' para ter $a' < b'$. Teremos então $a' = 1,4142136$ e $b' = 1,41421366$.

Desta forma, teremos a' e b' racionais e retornamos ao caso 1, obtendo t entre a e b. Como a' e b' estão entre a e b, temos que t está entre a e b.

□

7 Atividades Propostas

Neste último capítulo, traremos atividades que podem ser desenvolvidas com alunos do Ensino Médio a respeito de alguns temas tratados no trabalho.

Apesar do cunho estritamente matemático da maioria (apenas a última é dada como aplicação de equações polinomiais), consideramos como atividades interessantes e curiosas, como o processo de determinação da geratriz de uma dízima periódica, a localização de números irracionais na reta real, a prova da irracionalidade de alguns números reais, entre outras.

Desta forma, as atividades propostas buscam aguçar a curiosidade e desenvolver o raciocínio lógico das demonstrações aos alunos deste nível.

Atividade 1. *Determine a fração geratriz da dízima periódica* $1,133333....$

Resolução. Considere $x = 1,133333....$ Temos:

$$10x = 11,33333... \tag{61}$$

$$100x = 113,33333... \tag{62}$$

Subtraindo (61) de (62), temos:

$$90x = 102 \Rightarrow x = \frac{102}{90} = \frac{51}{45} = 1,133333...$$

Atividade 2. *Determine uma aproximação racional para o número* $\sqrt{3}$.

Resolução. Aplicando o Teorema 2, seção 2.2.1, vamos tomar $\lambda = \sqrt{3}$ e, aleatoriamente, $n = 32$ em:

$$-\frac{1}{2n} < \lambda - \frac{m}{n} < \frac{1}{2n}$$

Como $32\sqrt{3} = 55,4256...$, fazemos $m = 55$. Temos então:

$$-\frac{1}{2.32} < \sqrt{3} - \frac{55}{32} < \frac{1}{2.32} \Rightarrow$$

$$-\frac{1}{64} < \sqrt{3} - \frac{55}{32} < \frac{1}{64} \Rightarrow$$
$$\frac{55}{32} - \frac{1}{64} < \sqrt{3} < \frac{55}{32} + \frac{1}{64} \Rightarrow$$
$$\frac{109}{64} < \sqrt{3} < \frac{111}{64}.$$

Atividade 3. *Prove que $\sqrt{2}$ é um número irracional.*

Demonstração. Suponha, por absurdo, que $\sqrt{2}$ seja racional, ou seja, $\sqrt{2} = \frac{p}{q}$, $p, q \in \mathbb{Z}, q \neq 0$ e $mdc(p, q) = 1$. Logo:

$$p^2 = 2q^2.$$

Então p^2 é um número par. Pela Proposição 1, seção 3.1, p também é um número par. Suponha $p = 2k, k \in \mathbb{Z}$. Daí

$$p^2 = 4k^2 \Rightarrow 2q^2 = 4k^2 \Rightarrow q^2 = 2r^2.$$

Então q^2 é par, o que implica que q também é par. Mas isto não é possível, pois $mdc(p, q) = 1$. Portanto $\sqrt{2}$ é irracional. □

Atividade 4. *Prove que $\sqrt{3}$ é um número irracional.*

Demonstração. Da mesma forma que na atividade anterior, vamos supor que $\sqrt{3}$ seja racional, isto é $\sqrt{3} = \frac{p}{q}$, $p, q \in \mathbb{Z}, q \neq 0$ e $mdc(p, q) = 1$. Então:

$$p^2 = 3q^2.$$

Então p^2 é divisível por 3. Portanto, pelo Corolário 1, seção 3.1, p é divisível por 3. Suponha $p = 3k, k \in \mathbb{Z}$. Daí

$$p^2 = 9k^2 \Rightarrow 3q^2 = 9k^2 \Rightarrow q^2 = 3k^2.$$

Então q^2 também é divisível por 3, o que é absurdo, pois p e q são primos entre si. Portanto $\sqrt{3}$ é irracional. □

Atividade 5. *Verifique que o número $\sqrt{2}+\sqrt{3}$ é um número algébrico.*

Demonstração. Suponha que $x = \sqrt{2}+\sqrt{3}$. Então $x - \sqrt{2} = \sqrt{3}$.
Elevando ao quadrado ambos os membros, temos:

$$x^2 - 2x\sqrt{2} + 2 = 3 \Rightarrow x^2 - 1 = 2x\sqrt{2}.$$

Novamente elevando ao quadrado, temos:

$$x^4 - 2x^2 + 1 = 8x^2 \Rightarrow x^4 - 10x^2 + 1 = 0.$$

Logo, $\sqrt{2}+\sqrt{3}$ é raíz da equação $x^4 - 10x^2 + 1 = 0$ e, portanto, um número algébrico. □

Atividade 6. *Com o auxílio de régua e compasso, localize na reta real os pontos correspondentes aos números irracionais $\sqrt{2}$ e $\sqrt{3}$.*

Resolução. Para representar $\sqrt{2}$ marcamos a partir da origem, com o auxílio da régua, o triângulo retângulo isósceles com cateto de medida 1. Logo, a hipotenusa do triângulo terá medida $\sqrt{2}$. Assim, com o auxílio do compasso, marcamos na reta real o ponto que corresponde ao número $\sqrt{2}$
Para marcar o ponto correspondente a $\sqrt{3}$, usamos o ponto já marcado equivalente a $\sqrt{2}$ e desenhamos o triângulo retângulo de catetos com medidas 1 e $\sqrt{2}$. Assim, teremos a hipotenusa do novo triângulo medindo $\sqrt{3}$. Com o compasso, marcamos o ponto desejado.
Os procedimentos estão ilustrados na Figura 18 a seguir.

Observe que podemos utilizar os mesmos procedimentos para localizar os pontos correspondentes a $-\sqrt{2}$ e $-\sqrt{3}$.

Atividade 7. *Mostre que o número complexo $z = 2 - i$ é um número algébrico.*

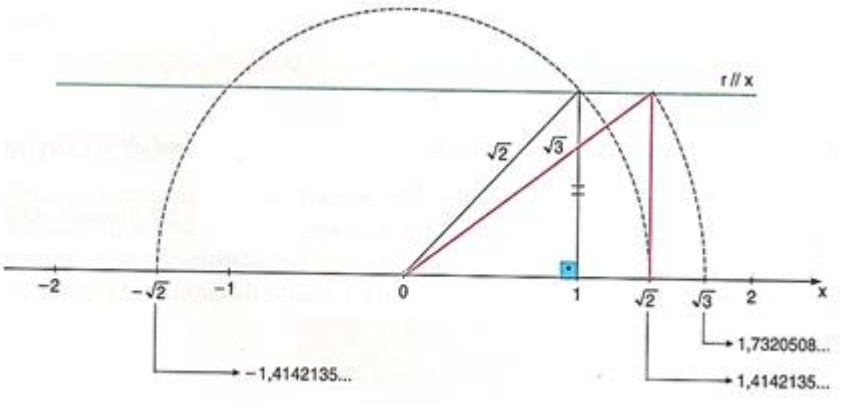


Figura 18: Representação de $\sqrt{2}$ e $\sqrt{3}$ na reta real.

Demonstração. Devemos encontrar uma equação polinomial com coeficientes inteiros tal que $2-i$ seja uma de suas raízes. Usando o Teorema 12, seção 4.5, temos que, se $2-i$ é raiz da suposta equação, então seu conjugado $2+i$ também será. Aplicando agora o Teorema 11, seção 4.3, podemos obter uma equação do 2º grau tal que da forma

$$(x-(2-i)).(x+(2+i))=0,$$

em que $2-i$ e $2+i$ sejam raízes. Assim, desenvolvendo o primeiro membro da equação, temos a equação do 2º grau $x^2-4x+5=0$ com raízes $2-i$ e $2+i$. Logo, $2-i$ é um número algébrico □

Atividade 8. *Determinar as raízes da equação* $3x^3+2x^2-7x+2=0$.

Resolução. De acordo com o Teorema 13, seção 4.6, se $\frac{p}{q}$, $(p,q\in\mathbb{Z},\ q\neq 0)$, é raiz da equação, então p é divisor de 2 e q é divisor de 3. Logo, as possíveis raízes racionais pertencem ao conjunto $\{-1,1,-2,2,-\frac{1}{3},\frac{1}{3},-\frac{2}{3},\frac{2}{3}\}$.

Considerando o polinômio $f(x)=3x^3+2x^2-7x+2$, verificamos que $f(1)=0$. Portanto, $x=1$ é raiz da equação.

Aplicando o Teorema 9, seção 4.2, temos que $f(x)=(x-1)q(x)$. Para determinar

$q(x)$ efetuamos a divisão de $f(x)$ por $(x-1)$ e obtemos $f(x) = (x-1)(3x^2+5x-2)$. Finalmente, resolvendo a equação $3x^2+5x-2=0$, encontramos as outras duas raízes, a saber: $x=-2$ e $x=\dfrac{1}{3}$. Logo: $S=\{-2, \frac{1}{3}, 1\}$.

Atividade 9. *Determine as raízes da equação $x^3-5x^2+7x-3=0$, sabendo que uma raiz é dupla.*

Resolução. Como uma das raízes é dupla, vamos representá-las por r_1, r_1, r_2. As relações de Girard para equações do 3º grau nos fornece:

$$r_1+r_2+r_3 = -\frac{b}{a},$$
$$r_1r_2+r_1r_3+r_2r_3 = \frac{c}{a},$$

$$r_1r_2r_3 = -\frac{d}{a}.$$

Logo:

$$r_1+r_1+r_2 = 5 \Rightarrow 2r_1+r_2 = 5 \Rightarrow r_2 = 5-2r_1 \tag{63}$$

$$r_1r_1+r_1r_3+r_1r_3 = 7 \Rightarrow r_1^2+2r_1r_3 = 7 \tag{64}$$

$$r_1r_1r_2 = 3 \Rightarrow r_1^2r^2 = 3 \tag{65}$$

Substituindo (63) em (64), obtemos $3r_1^2-10r_1+7=0$. Resolvendo esta equação para r_1, temos que $r_1=\frac{7}{3}$ ou $r_1=1$. Testando para o polinômio $f(x)=x^3-5x^2+7x-3$, encontramos $f(\frac{7}{3})=-\frac{32}{27}$ e $f(1)=0$. Logo, $r_1=1$. Substituindo $r_1=1$ em (63), temos $r_2=3$. Portanto, $S=\{1,3\}$.

Atividade 10. *Um engenheiro projetou duas caixas d'água de mesma altura. Uma em formato de cubo e a outra em formato de paralelepípedo reto retângulo com $6m^2$ de área da base. O volume da caixa cúbica deve ser $4m^3$ menor que o da outra caixa. Nessas condições, qual deve ser a medida da aresta da caixa cúbica?*

Resolução. Podemos ilustrar o exercício como na Figura 19 a seguir. Assim, cha-

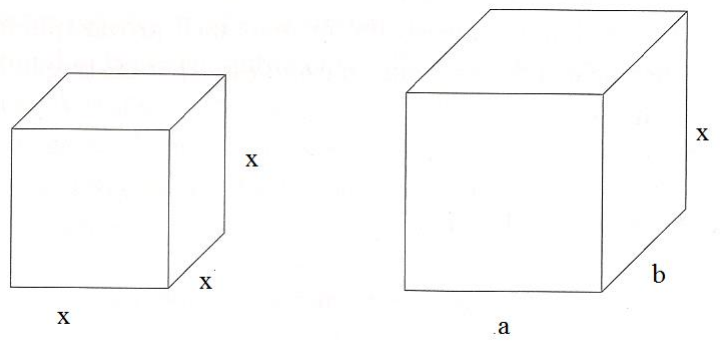


Figura 19: Representação geométrica da Atividade 10.

mamos a aresta da caixa cúbica de x, as arestas da base da outra caixa de a, b e x, já que as alturas são iguais. Pelas condições do problema, temos:

$$x^3 = abx - 4 \Rightarrow$$

$$x^3 = 6x - 4 \Rightarrow$$

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

Para resolver a equação acima, aplicamos o Teorema 13, seção 4.6, e pesquisamos suas possíveis raízes racionais, encontrando a raiz $x_1 = 2$.
Aplicamos agora o Teorema 11, seção 4.3, seção e chegamos a:

$$x^3 - 6x + 4 = (x - 2)(x^2 + 2x - 2) = 0.$$

Assim, resolvendo a equação $(x^2 + 2x - 2) = 0$, encontramos as raízes:

$$x_2 = -1 - \sqrt{3} \;\; e \;\; x_3 = -1 + \sqrt{3}.$$

Como a aresta não pode ser negativa, concluímos que as possíveis medidas que satisfazem o problema são 2 m ou $-1 + \sqrt{3}$ m, que vale aproximadamente $0,73m$.

8 Considerações finais

No decorrer da elaboração deste trabalho, buscamos aliar os temas abordados às suas justificativas, tentando interligá-los e exemplificar sempre que possível.

Vimos que os números *transcendentes* (cujo próprio nome já causa calafrios em leigos), apesar de apresentarem uma teoria complexa por trás de suas comprovações, decorrem naturalmente do estudo das equações polinomiais, portanto pode ser abordado, mesmo que de modo superficial, em sala de aula.

Percebemos assim que apesar dos assuntos tratados, em sua maioria, não serem triviais, é possível com esforço e embasamento teórico adequados, trabalhá-los de modo gradativo com estudantes do Ensino Médio. Isto foi mostrado através das atividades propostas no último capítulo, que estão dentro do que pode ser exigido de um aluno secundarista.

Aliás, os alunos do ensino básico, nosso público alvo e razão do programa PROFMAT, carecem de desafios e novas metodologias, as quais os professores deste nível nem sempre estão dispostos a buscar. Não se pode exigir que o aluno tenha um bom aprendizado se o próprio professor não tem segurança ou competência naquilo que está ministrando.

Daí a importância do aprimoramento profissional dos professores do ensino básico brasileiro, principalmente da rede pública, onde a defasagem matemática é gritante. Porém, para que haja uma reversão nesse quadro, mesmo que a médio ou longo prazo, é preciso que os profissionais envolvidos se conscientizem desta necessidade, e busquem meios de atingir tal objetivo.

Referências

[1] Hefez, Abramo. *Elementos de Aritmética - 2ª Edição*, Sociedade Brasileira de Matemática (SBM) - Rio de Janeiro, 2006.

[2] Figueiredo, Djairo Guedes. *Números Irracionais e Transcendentes - 3ª Edição*, Sociedade Brasileira de Matemática (SBM) - Rio de Janeiro, 2002.

[3] Iezzi, Gelson. *Fundamentos de Matemática Elementar - Vol. 6 - 6ª Edição*, Atual Editora - São Paulo, 1998.

[4] Dante, Luiz Roberto. *Matemática - Contexto e Aplicações, Vol. 3 - 1ª Edição*, Editora Ática - São Paulo, 2011.

[5] Oliveira, Oswaldo Rio Branco de. *Teorema Fundamental da Álgebra*. São Paulo, 2011. Disponível em: $<$ *http* : *//www.ime.usp.br/ oliveira/TFACOLEGIAL5.pdf* $>$. Acesso em: 17 de Fevereiro de 2015.

[6] Niven, Ivan. *Números: Racionais e Irracionais - 1ª Edição*, Sociedade Brasileira de Matemática (SBM) - Rio de Janeiro, 2012.

[7] Carmo, Manfredo Perdigão do; Morgado, Augusto César; Wagner, Eduardo. *Trigonometria e Números Complexos - 3ª Edição*, Sociedade Brasileira de Matemática (SBM) - Rio de Janeiro, 2005.

[8] Duarte, Carlos Eduardo de Lima. *Conjuntos Numéricos*. Natal, 2013. Disponível em: $< bit.profmat - sbm.org.br >$. Acesso em: 25 de Agosto de 2014.