UNIVERSIDADE FEDERAL DO PARÁ

INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

LEONARDO CARLOS RODRIGUES PANTOJA

NÚMEROS ALGÉBRICOS E NÚMEROS TRANSCENDENTES

Belém-Pará

2018

LEONARDO CARLOS RODRIGUES PANTOJA

NÚMEROS ALGÉBRICOS E NÚMEROS TRANSCENDENTES

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Pará - UFPA, como requisito parcial, para obtenção do grau de Mestre em Matemática.

Orientadora: Profª. Drª. Irene Castro Pereira.

Belém-Pará

2018

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

P198n Pantoja, Leonardo Carlos Rodrigues
Números Algébricos e Números Transcendentes / Leonardo Carlos Rodrigues Pantoja. — 2018
67 f. : il. color

Dissertação (Mestrado) - Programa de Pós-graduação em Matemática em Rede Nacional (PROFMAT) , Instituto de Ciências Exatas e Naturais, Universidade Federal do Pará, Belém, 2018.
Orientação: Profa. Dra. Irene Castro Pereira

1. Números racionais. 2. Números reais. 3. Irracionalidade. 4. Números algébricos. 5. Números transcendentes. I. Pereira, Irene Castro , *orient.* II. Título

---

CDD 510

LEONARDO CARLOS RODRIGUES PANTOJA

NÚMEROS ALGÉBRICOS E NÚMEROS TRANSCENDENTES

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal do Pará - UFPA, para obtenção do grau de Mestre em Matemática. Orientadora: Profª. Drª. Irene Castro Pereira

APROVADO EM: 12 / 06 / 2018

BANCA EXAMINADORA:

Profª. Drª. Irene Castro Pereira - PROFMAT/ICEN/UFPA
Orientadora

Profª. Drª. Joelma Morbach - PROFMAT/ICEN/UFPA
Membro da Banca

Prof. Dr. Juaci Picanço da Silva - FACMAT/ICEN/UFPA
Membro da Banca

Prof. Dr. Marcel Vinhas Bertolini - FACMAT/ICEN/UFPA
Membro da Banca

Dedicatória

Ao amor da minha vida, meu filho, Renzo Gabriel, por ser o maior incentivador dessa conquista.

Agradecimentos

A Deus, a causa primária de todas as coisas, pela minha vida abençoada.

Aos meus pais, José Luiz Carlos da Silva e a Alita Rocha da Silva, pela incansável dedicação em prol da minha educação.

Aos meus demais familiares, pelas diversas colaborações e contribuições em minha vida.

A minha orientadora, professora Irene Castro, pelas sábias orientações e pelo vasto conhecimento matemático ensinado.

Ao meu coordenador de mestrado, professor Valcir, pela paciência e apoio técnico.

A todos os professores do meu curso de mestrado, pelo vasto conhecimento transmitido.

A secretária do curso do PROFMAT Carmem, por toda ajuda técnica.

A todos os meus companheiros de mestrado, por todos os momentos vividos, apoio e incentivos durante o curso.

Ao amigo de turma Leandro Farias, pelo gigantesco conhecimento compartilhado com nossa turma e pela imensa disponibilidade em ajudar os demais mestrandos.

Aos meus grandes amigos Gílson Meireles e Ronaldo Lima, que além da colaboração matemática, foram importantíssimos num momento delicado de minha vida.

A todos os meus amigos de trabalho, pelas diversas ajudas durante o curso.

A professora Elisângela Rodrigues, pela revisão ortográfica.

A Gabriela Patricia, pelo grande apoio durante o mestrado.

A Priscila Rodrigues e a Rosa Costa, pela colaboração e dedicação na criação do meu amado filho.

Ao meu grande amigo, Michel Caldas Ramos, por sempre acreditar em mim.

Ao meu compadre André leite, pela amizade e consideração.

Ao professor Fernando Pimentel, por acreditar e me incentivar na busca dessa conquista.

Aos meus grandes amigos, que de alguma forma contribuíram para meu sucesso.

A todas as pessoas que de forma direta ou indireta, contribuíram para a realização desse sonho.

Ao William Melo pelo apoio técnico.

Epígrafe

"Nunca será um verdadeiro matemático aquele que não for um pouco de poeta."

(Karl Weierstrass)

Resumo

Ao nos depararmos com os números reais no ensino básico, observamos que certos números são de mais difíceis manipulação operacional do que outros. Se levarmos em consideração as operações algébricas básicas (adição e multiplicação com inteiros não nulos e potenciação com expoente inteiro positivo, aplicadas em números reais), a quantidade de números que as "respeitam", torna-se ainda menor. Esse detalhe operacional está intimamente ligado à diferença em grau de complexidade nas demonstrações da irracionalidade de certos números. Por exemplo, provar a irracionalidade de $\sqrt{2}$ é bem menos trabalhoso do que provar a irracionalidade de π. Por trás dessa diferença em complexidade existe uma magnifica propriedade que a maioria dos números reais possui, a ***transcendência***. Isso nos permite classificar, desde o ensino básico, os números reais em algébricos e transcendentes. Ou seja, números bem comportados em relação as operações algébricas e outros que não "respeitam"as leis operacionais algébricas básicas para o qual o nosso mundo foi concebido.

Palavras-chave: Corpos ordenados; Números racionais; Números reais; Irracionalidade; Números algébricos; Números transcendentes; Construções geométricas.

Abstract

When we come across the actual numbers in elementary education, we note that certain numbers are of more difficult operational manipulation than others. If we take into account the basic algebraic operations (addition and multiplication with nonzero integers and positive integer exponentiation, applied in real numbers), the number of numbers that "respect"them becomes even smaller. This operational detail is closely linked to the difference in degree of complexity in the demonstrations of the irrationality of certain numbers. For example, proving the irrationality of $\sqrt{2}$ is much less laborious than proving the irrationality of π. Behind this difference in complexity is a magnificent property that most real numbers have, ***transcendence***. This allows us to classify, from basic education, the real numbers into algebraic and transcendent ones. That is, well-behaved numbers in relation to algebraic operations and others that do not "respect"the basic algebraic operating laws for which our world was conceived.

Keywords: Ordained bodies; Rational numbers; Real numbers; Irrationality; Algebraic numbers; Transcendent numbers; Geometric constructions.

Conteúdo

Introdução

A história da matemática nos relata diversas situações onde várias teorias só puderam evoluir após uma rigorosa fundamentação teórica de assuntos considerados base. Dentre tais assuntos, podemos citar o conjunto dos números reais, assunto esse , que é de suma importância para estudo da análise matemática.

Diversos matemáticos colaboraram para estruturação e fundamentação rigorosa dos números reais, como por exemplo George Cantor e Richard Dedekind. É válido ressaltar que esses dois matemáticos buscaram promover tal estruturação de maneiras distintas. Dedekind desenvolveu o método chamado de "cortes de Dedekind", influenciado pela teoria das proporções do matemático grego Eudoxo. Enquanto que Cantor buscou definir cada número real como uma classe de equivalência de sequências de Cauchy de números racionais.

No ensino fundamental, a abordagem feita sobre o conjunto dos números reais começa no 8º ano, apenas como mais um conjunto numérico, que é obtido pela união do conjunto números dos racionais com o conjunto dos números irracionais. No ano seguinte, no 9º ano, os números reais servem como base para os métodos resolutivos das equações do segundo grau, tornam-se também, peça fundamental para os estudos das funções afins e funções quadráticas.

É importante ressaltar que tais números são primordiais para os estudos geométricos, marcando presença em cálculos que envolvem medidas de segmentos, perímetros e áreas de figuras planas tanto no 8º quanto no 9º ano. Não podemos deixar de frisar outra aplicação no 9º ano, em que tais números são utilizados nos estudos de razões e proporções, e nos cálculos que envolvem as razões trigonométricas, nesse caso sendo crucial no processo de racionalização.

No ensino médio, os números reais em relação ao 9º ano do fundamental, além de servir de base para os estudos de equações e funções, só que agora além auxiliar na revisão dos assuntos do ensino fundamental, passam a estudar outros tipos de equações, como por exemplo exponenciais e as logarítmicas. Outro assunto que necessita do conhecimento dos

números reais são as sequencias numéricas.

Nas séries seguintes, o 2º ano e o 3º ano, os números reais continuam tendo grande presença e importância, como na trigonometria e na geometria, só que com questões mais complexas. Além de serem muito utilizados nos cálculos estatísticos, principalmente os que envolvem médias, variâncias e consequentemente, desvios padrões.

É notável a presença dos números reais no ensino básico e no ensino superior tão quanto sua relevância no processo de ensino-aprendizagem da matemática, porém, não vemos um estudo mais aprofundado sobre certas propriedades, como por exemplo, a irracionalidade, cuja a abordagem limita-se a exemplificações de números irracionais e a defini-los como algo contrário a racionalidade. Diversos livros didáticos introduzem os números irracionais através de uma visão geométrica vinculada ao teorema de Pitágoras. Esse é o caso da raiz quadrada de dois, que deu origem à crise dos incomensuráveis no mundo grego (podendo ser aprofundada em [1]). Tais livros didáticos também citam o número π como resultado da comparação entre a circunferência e seu diâmetro, enquanto outros poucos explicam a origem do número e, a constante de Euler.

Como podemos observar, o ensino dos números reais no ensino básico resume-se a uma abordagem calculista e quando se trata de irracionalidade, a abordagem limitando-se a alguns meros exemplos. A classificação dos números em racionais e irracionais é limitada, desde que, analisada por uma ótica mais profunda.

Diversos alunos do ensino básico, e sem exagero nenhum, muitos alunos também do ensino superior, após adquirirem conhecimento sobre os números reais, concluem que racionais e irracionais são completamente diferentes, que não possuem nenhuma ligação ou semelhança. Tal pensamento estimulou a questão que norteia nossa proposta de trabalho: existe elo entre números racionais e números irracionais? Nossa resposta é sim!

Se observarmos outro detalhe, certos números irracionais que sujeitos as operações algébricas básicas, resultam em números racionais, como por exemplo: elevando a raiz quadrada de dois a segunda potência obtemos como resultado o número racional 2. Sabemos que tal resultado é de suma importância para prova da irracionalidade de raiz quadrada de dois. Seguindo a mesma linha de raciocínio, por que que tal procedimento não é eficaz para a demonstração da irracionalidade do número π?

A resposta de tal questão está ligada a algo mais profundo, a uma característica mais peculiar de certos números reais, a **"transcendência"**. Tal fato, incentivou certos matemáticos a classificarem os números reais de outra forma: em números algébricos e trans-

cendentes.

A teoria transcendente dos números teve contribuição de diversos matemáticos mas, foi graças o matemático francês **Joseph Liouvillle** (1809-1882) que tal teoria realmente nasceu. Liouville criou uma propriedade na qual os números transcendentes se adequavam e consequentemente, apresentou ao mundo o primeiro número transcendente, a constante de Liouville.

O termo números transcendentes, foi utilizado por **Leonhard Paul Euler** (1707-1783), pois em sua concepção, esses números transcendem as operações algébricas, justamente as leis onde esse mundo foi concebido. Porém, o termo transcendente já tinha sido utilizado por **Gottfried W. Leibniz** (1646-1716) em seus estudos sobre funções transcendentes.

Dentre os vários colaboradores, destacamos ainda, o matemático francês **Charles Hermite** (1822-1901) que em 1873, provou que e (Número de Euler) é transcendente. Aproximadamente uma década após esta célebre constatação, o alemão **Ferdinand von Lindemann** (1852-1939), influenciado pelos "métodos de Hermite", publicou uma bela e "simples"demonstração que π era transcendente, e consequentemente, que o antigo problema da quadratura do círculo não poderia ser resolvido.

Outro importantíssimo resultado é atribuído ao grande matemático russo-germânico **Georg Cantor** (1845-1918), que em 1874, provou que quase todo numero é transcendente. Esta teoria vive um grande paradoxo, apesar de quase todos os números serem transcendentes, demonstrar a transcendência de um número é, em geral, uma tarefa tão complicada (MARQUES 2013), justamente por causa da não "obediência"às operações algébricas por partes desses números.

Dando continuidade, o matemático soviético **Alexander O. Gelfond** (1906 -1968), em 1934, e o matemático alemão **Theodor Schneider** (1911-1988), em 1935, resolveram independentemente o famoso 7º problema de Hilbert proposto em 1900 sobre a transcendência de números com o **"O teorema de Gelfond-Schneider"** (como ficou conhecido), definiu a natureza algébrica da potenciação de números, estabelecendo uma larga classe de números transcendentes.

Não podemos esquecer do grande matemático inglês falecido recentemente, **Alan Baker** (1939 -2018) que recebeu a Medalha Fields em 1970, devido a suas pesquisas sobre formas logarítmicas. Sendo um dos resultados mais relevantes do últimos anos, na teoria transcendente.

O capítulo inicial, revisará certos conceitos e definições matemáticas "básicas", como

por exemplo: corpos, corpos ordenados, corpo dos racionais, números irracionais, chegando ao corpo ordenado completo dos reais.

No capítulo seguinte, o capítulo 2, serão citados alguns números irracionais e suas respectivas demonstrações de irracionalidade. Demonstrações essas, que possuem uma roupagem mais "acessível"a todos os interessados em tal leitura.

Já o capítulo 3, apresentará as principais definições e propriedades dos números algébricos e dos números transcendentes, permitindo-nos expor outra classificação dos números reais.

Dando continuidade, o capítulo 4 está destinado ao início da teoria transcendente, a teoria de Liouville e a apresentação do primeiro número comprovadamente transcendente, a constante de Liouville.

O penúltimo capítulo, o capítulo 5, retratará de resultados importantíssimos na teoria transcendente, como por exemplos: o teorema de Hermite-Lindemann, teorema de Gelfond-Schneider, o teorema de Baker e a fantástica conjectura de Schanuel.

A última parte deste trabalho, o capítulo 6, fará a conexão entre geometria e os números transcendentes, especificamente, a impossibilidade da quadradura do círculo com apenas régua (sem marcações) e compasso.

O objetivo geral deste trabalho é apresentar os principais conceitos e propriedades dos números algébricos e dos números transcendentes. Mas para alcançarmos tal objetivo devemos gradativamente seguir os seguintes objetivos específicos: apresentar a estrutura do corpo dos números racionais e do corpo dos números reais, ampliar o conceito de irracionalidade, definir o corpo dos números algébricos e suas propriedades, definir e exemplificar os números transcendentes, presentar alguns dos principais resultados sobre números transcendentes e utilizar a teoria dos números algébricos e transcendentes nas construções geométricas com régua e compasso.

Por fim, a proposta deste trabalho é enriquecer o conhecimento do professor do ensino básico a respeito de um dos assuntos mais relevantes da matemática: os números reais, aprimorando o conceito de irracionalidade, trabalhando com as operações algébricas básicas e consequentemente, apresentando outra classificação para os números reais.

Capítulo 1

Corpos

Neste capítulo, tendo como referências [10] e [12], recordaremos a definição de uma das estruturas algébricas mais importantes da matemática: os corpos. Citaremos suas propriedades e apresentaremos alguns dos principais exemplos desse tipo de estrutura.

1.1 Corpos

Um corpo é um conjunto $K \neq \emptyset$, munido de duas operações, chamadas *adição* e *multiplicação*, que satisfazem certas condições, chamadas *axiomas de corpo*, abaixo especificadas.

A adição faz corresponder a cada par de elementos $x, y \in K$ sua *soma* $x + y \in K$. enquanto a multiplicação associa a esses elementos o seu produto $x \cdot y \in K$. Os axiomas de corpo são os seguintes:

Axiomas da adição

A1. *Associatividade* - quaisquer que sejam $x, y, z \in K$, tem-se $(x + y) + z = x + (y + z)$.

A2. *Comutatividade* - quaisquer que sejam $x, y, z \in K$, tem-se $x + y = y + x$.

A3. *Elemento neutro* - existe $0 \in K$ tal que $x + 0 = x$, seja qual for $x \in K$. O elemento 0 chama-se *zero*.

A4. *Simétrico* - todo elemento $x \in K$ possui um simétrico $x \in K$ tal que $x + (-x) = 0$.

Axiomas da multiplicação

M1. *Associatividade* - dados quaisquer x, y, z em K, tem-se $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

M2. *Comutatividade* - sejam quais forem $x, y \in K$, vale $x \cdot y = y \cdot x$.

M3. *Elemento neutro* - existe $1 \in K$ tal que $1 \neq 0$ e $x \cdot 1 = x$, qualquer que seja $x \in K$. O elemento 1 chama-se *um*.

M4. *Inverso Multiplicativo* - todo $x \neq 0$ em K possui um inverso x^{-1}, tal que $x \cdot x^{-1} = 1$.

Por fim, as operações de adição e multiplicação num corpo K acham-se relacionadas por um axioma, com o qual fica completa a definição de corpo.

Axioma da distributividade.

D1.*D*ados x, y, z quaisquer, em K, tem-se $x \cdot (y + z) = x \cdot y + x \cdot z$.

Da comutatividade, segue-se que

$$0 + x = x \text{ e } -x + x = 0$$

A soma $x + (-y)$ será indicada com a notação $x - y$ é chamada a *diferença* entre x e y. A operação $(x, y) \mapsto x - y$ chama-se *subtração*.

O elemento neutro da adição será chamado de zero e denotaremos por 0. Ou seja, se $x + \theta = x$ (para algum $x \in K$ e algum $\theta \in K$) então $\theta = x - x$, ou seja, $\theta = 0$. Resulta também que todo $x \in K$ tem somente um simétrico: se $x + y = 0$, então, $y = 0 - x$, ou seja, $y = -x$. Também temos $-(-x) = x$, já que $(-x) + x = 0$.

Finalmente, vale a lei do corte: $x + z = y + z \Rightarrow x = y$. Concluímos assim que as regras usuais relativas à adição e subtração decorrem dos quatro axiomas acima e são, portanto, válidas em qualquer corpo.

Por comutatividade, segue-se que $x \cdot 1 = 1 \cdot x = x$ para todo $x \in K$, e que $x \cdot x^{-1} = x^{-1} \cdot x = 1$ para todo $x \neq 0$ em K.

Consequentemente, valem propriedades análogas às que foram acima demonstradas para adição.

Dados x e y em K, com $y \neq 0$, escreve-se também $\dfrac{x}{y}$ em vez de $x \cdot y^{-1}$. A operação $(x, y) \mapsto \dfrac{x}{y}$, definida para x qualquer e $y \neq 0$ em K, chama-se *divisão* e o resultado $\dfrac{x}{y}$ é o *quociente* de x por y.

Se $y \neq 0$, tem-se $\dfrac{x}{y} = z \Leftrightarrow x = y \cdot z$. Daí se deduz a utilíssima *lei do corte:* Se $x \cdot z = y \cdot z$ e $z \neq 0$, então $x = y$. (É importante ter em mente que $x \cdot z = y \cdot z$ só implica $x = y$ quando

se sabe, *a priori* que $z \neq 0$.) Se $x \cdot y = x$ para todo $x \in K$ então, tomando $x = 1$ obtemos $y = 1$. Isto prova a unicidade do 1. Sabendo-se apenas que $x \cdot y = x$ para um certo x, há duas possibilidades: se $x \neq 0$ então $y = 1$, pela lei do corte. Se, porém, $x = 0$ então y pode ser qualquer pois, $0 \cdot y = 0$ para todo $y \in K$. Finalmente, se $x \cdot y = 1$ então, como veremos abaixo, $x \neq 0$ e $y \neq 0$ e (multiplicando por x^{-1}) concluímos $y = x^{-1}$. Isto prova a unicidade do elemento inverso.

Por comutatividade, tem-se também $(x + y) \cdot z = x \cdot z + y \cdot z$.

De D1 temos que $x \cdot 0 = 0$ para todo $x \in K$. Com efeito,

$$x \cdot 0 + x = x \cdot 0 + x \cdot 1 = x(0 + 1) = x \cdot 1 = x, \text{ donde } x \cdot 0 = 0.$$

Por outro lado, dados $x, y \in K$ com $x \cdot y = 0$, segue-se que $x = 0$ ou $y = 0$. Com efeito, se for $x \cdot y = 0$ e $x \neq 0$, então obtemos $x \cdot y = x \cdot 0$ e, por corte, $y = 0$. Assim, num corpo K, tem-se $x \cdot y \neq 0$ sempre que os dois fatores x e y forem ambos diferentes de zero.

No axioma da distributividade está a explicação da "regras dos sinais"da Álgebra Elementar: $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$ e $(-x) \cdot (-y) = x \cdot y$. De fato, em primeiro lugar temos $(-x) \cdot y + x \cdot y = (-x + x) \cdot y = 0 \cdot y = 0$, donde $(-x) \cdot y = -(x \cdot y)$. Analogamente, $x \cdot (-y) = -(x \cdot y)$. Logo $(-x) \cdot (-y) = -[x \cdot (-y)] = -[-(x \cdot y)] = x \cdot y$. Em particular, $(-1) \cdot (-1) = 1$.

Exemplos de corpos.

Exemplo 1. O conjunto $\mathbb{Q}$ dos números racionais, com as operações

$$\frac{p}{q} + \frac{p'}{q'} = \frac{pq' + p'q}{qq'} \text{ e } \frac{p}{q} \cdot \frac{p'}{q'} = \frac{pp'}{qq'}.$$

(Lembremos a igualdade: $\dfrac{p}{q} = \dfrac{p'}{q'} \Leftrightarrow pq' = p'q$.) O simétrico de $\dfrac{p}{q}$ é $-\dfrac{p}{q}$. O zero é $\dfrac{0}{q}$. seja qual for $q \neq 0$. O inverso do número racional $\dfrac{p}{q} \neq 0$ é $\dfrac{q}{p}$.

Exemplo 2. O corpo $\mathbb{Z}_2 = \{0, 1\}$, formado apenas por dois elementos distintos 0 e 1, com as operações $0 + 1 = 1 + 0 = 1$, $0 + 0 = 1 + 1 = 0$, $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$ e $1 \cdot 1 = 1$. Aqui, o simétrico da cada elemento é ele próprio (e o inverso também).

Exemplo 3. O corpo $\mathbb{Q}(i)$, cujos elementos são os pares ordenados $z = (x, y)$ de números racionais. (Ou seja, como conjunto, $\mathbb{Q}(i) = \mathbb{Q} \times \mathbb{Q}$.) As operações são definidas assim: $(x, y) + (x', y') = (x + x', y + y')$ e $(x, y) \cdot (x', y') = (xx' - yy', x'y + xy')$. O zero é o elemento $(0, 0)$ e a unidade é o elemento $(1, 0)$. Escrevendo x para representar o par $(x, 0)$ e usando a notação $i = (0, 1)$, observamos que cada elemento $z = (x, y) = (x, 0) + (0, y)$ pode escrever-se como $z = x + iy$ e que as operações acima foram definidas de modo que

os "números complexos"da forma $z = x + iy$ se somem e multipliquem da maneira usual, com cuidado de notar que $i^2 = -1$. $\mathbb{Q}(i)$ chama-se *corpo dos números complexos racionais*. A verificação dos axiomas fica a cargo do leitor. Por exemplo, dado $z = (x, y) \neq 0$, tem-se $z^{-1} = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)$.

Exemplo 4. O conjunto $\mathbb{Q}(t)$, das funções racionais $r(t) = \frac{p(t)}{q(t)}$, onde p e q são polinômios com coeficientes racionais, sendo q não identicamente nulo. Se $u(t)$ é também não identicamente nulo, tem-se $\frac{p(t)}{q(t)} = \frac{p(t) \cdot u(t)}{q(t) \cdot u(t)}$.

Para encerrar estas considerações gerais sobre corpos, observemos um fato útil. Num corpo K, $x^2 = y^2 \Rightarrow x = \pm y$. Com efeito $x^2 = y^2 \Rightarrow x^2 - y^2 = 0 \Rightarrow (x + y)(x - y) = 0 \Rightarrow x + y = 0$ ou $x - y = 0$. No primeiro caso, $x = -y$ e, no segundo, $x = y$.

1.2 Corpos ordenados

Um *corpo ordenado* é um corpo K, tal que existe um subconjunto P no qual as seguintes condições são satisfeitas:

P1. A soma e o produto de elementos positivos[1]são positivos. Ou seja, $x, y \in P \Rightarrow x + y \in P$ e $x \cdot y \in P$.

P2. Dado $x \in K$, exatamente uma das três alternativas seguintes ocorre: ou $x = 0$, ou $x \in P$ ou $-x \in P$.

O conjunto P satisfazendo $P1$ e $P2$ é chamado de conjunto dos elementos *positivos* de K.

Assim, se indicarmos com $-P$ o conjunto dos elementos $-x$, onde $x \in P$ e $\{0\}$ dois a dois disjuntos. Os elementos de $-P$ chamam-se *negativos*.

Num corpo ordenado, se $a \neq 0$ então $a^2 \in P$. Com efeito, sendo $a \neq 0$, ou $a \in P$ ou $-a \in P$. No primeiro caso, $a^2 = a \cdot a \in P$. No segundo caso $a^2 = (-a) \cdot (-a) \in P$. Em particular, num corpo ordenado $1 = 1 \cdot 1$ é sempre positivo. Segue-se que $-1 \in -P$. Em particular, num corpo ordenado, -1 não é quadrado de elemento algum.

Exemplo 5. $(\mathbb{Q},+,\cdot)$ é um corpo ordenado, no qual o conjunto P é formado pelos números racionais $\frac{p}{q}$ tais que $p \cdot q \in \mathbb{N}$. (intuitivamente, isto significa que os inteiros p e q têm "o mesmo sinal").

Exemplo 6. O corpo $\mathbb{Q}(t)$ pode ser ordenado chamando-se uma fração $r(t) = \frac{p(t)}{q(t)}$ positiva quando, no polinômio pq, o coeficiente do termo de mais alto grau for positivo. O

[1]Intuitivamente, um elemento ou número é dito positivo quando é maior do que zero.

conjunto P das frações positivas segundo esta definição cumpre as condições P1 e P2. Com efeito, dadas as frações positivas $r = \frac{p}{q}$ e $r' = \frac{p'}{q'}$, os coeficientes dos termos de graus mais elevados em pq e em $p'q'$ são > 0. Em $r + r'$, o produto do numerador pelo denominador é o polinômio $pq(q')^2 + p'q' \cdot q^2$, cujo termo de mais alto grau deve ter coeficiente positivo. Logo, a soma de duas frações "positivas"é positiva. As demais afirmações se verificam sem dificuldade.

Exemplo 7. O corpo $\mathbb{Z}_2$ não pode ser ordenado pois $1 + 1 = 0$ enquanto num corpo ordenado 1 deve ser positivo e a soma $1 + 1$, de dois elementos positivos deveria ainda ser positiva. Também o corpo $\mathbb{Q}(i)$, dos números complexos racionais, não comporta uma ordenação compatível com suas operações pois o quadrado do elemento $i = (0, 1)$ é igual a -1.

Num corpo ordenado K, escreveremos $x < y$, e diremos que x é *o menor do que* y, para significar que $y - x \in P$, ou seja, que $y = x + z$, onde $z \in P$. Nas mesmas circunstâncias, escreve-se também $y > x$ e diz-se que y *é maior do que* x.

Em particular $x > 0$ significa que $x \in P$, isto é, que x é positivo, enquanto $x < 0$ quer dizer que x é negativo, isto é, que $(-x) \in P$. Se $x \in P$ e $y \in (-P)$ tem-se sempre $x > y$.

A relação de ordem $x < y$ num corpo ordenado K goza das propriedades seguintes:

O1. *Transitividade*: se $x < y$ e $y < z$ então $x < z$.

O2. *Tricotomia*: dados, $x, y \in K$, ocorre exatamente uma das alternativas seguintes: ou $x = y$, ou $x < y$, ou $x > y$.

O3. *Monotonicidade da adição*: se $x < y$ então, para todo $z \in K$, tem-se $x + z < y + z$.

O4. *Monotonicidade da multiplicação*: se $x < y$ então, para todo $z > 0$, tem-se $xz < yz$. Se, porém, tivermos $z < 0$, então $x < y$ implica $xz > yz$.

Demonstremos estas propriedades:

O1. Dizer $x < y$ e $y < z$ significa afirmar que $y - x \in P$ e $z - y \in P$. Por P1 concluímos que $(z - y)(y - x) \in P$, ou seja, $z - x \in P$, o que significa $x < z$.

O2. Dados $x, y \in K$, ou $y - x \in P$, ou $y - x = 0$, ou $y - x \in -P$ (isto é, $x - y \in P$). No primeiro caso tem-se $x < y$, no segundo $x = y$ e no terceiro $x > y$. Estas possibilidades se excluem mutuamente, por P2.

O3. Se $x < y$ e $z > 0$ então $y - x \in P$, donde $(y + z) - (x + z) = y - x \in P$. Isso significa que $x + z < y + z$.

O4. Se $x < y$ e $z > 0$ então $y - x \in P$ e $z \in P$. Logo $(y - x) \cdot z \in P$, isto é, $y \cdot z - x \cdot z \in P$, o que significa $x \cdot z < y \cdot z$.Se, porém, $x < y$ e $z < 0$, então $y - x \in P$ e $-z \in P$, donde

$(y-x)\cdot(-z)\in P$, isto é, $x\cdot z - y\cdot z \in P$, o que significa $y\cdot z < x\cdot z$.

Em particular, num corpo ordenado K, $x<y$ é equivalentemente $a-y<-x$. Basta multiplicar ambos os membros de qualquer uma adição destas desigualdades por -1.

Segue-se de O1 e O3 que $x<y$ e $x'<y'$ implica $x+x'<y+y'$, ou seja, podem-se somar duas desigualdades, membro a membro. Com efeito, por O3, $x<y \Rightarrow x+x'<y+y'$ e $x'<y' \Rightarrow y+x'<y+y'$. Por O1, concluímos $x+x'<y+y'$.

Analogamente, de O1 e O4 segue-se que $0<x<y$ e $0<x'<y'$ implicam $xx'<yy'$, isto é, podem-se multiplicar membro a membro duas desigualdades formadas por elementos positivos.

Num corpo ordenado K, o produto de um elemento $x>0$ por um elemento $y<0$ dá um elemento $xy<0$. (Basta observar que $x(-y)=-(x\cdot y)$ ou então ambos os membros de $y<0$ por x.) Como $1>0$, concluímos de $x\cdot x^{-1}=1$ que se $x>0$ deve ser $x^{-1}>0$ também. Assim, o inverso de um elemento positivo é positivo. Segue-se que $x>0$ e $y>0$ implica $\dfrac{x}{y}>0$.

Se $x<y$ e ambos são positivos, então $y^{-1}<x^{-1}$. Basta observar que $\dfrac{1}{y}-\dfrac{1}{x}=\dfrac{x-y}{xy}$.

Num corpo ordenado K, escreve-se $x\leq y$ para significar que $x<y$ ou $x=y$. Lê-se: "x é menor do que ou igual a y". Nas mesmas circunstâncias, escreve-se $y\geq x$. Isto quer dizer, evidentemente, que $y-x\in P\cup\{0\}$. Os elementos do conjunto $P\cup\{0\}$ chamam-se *não-negativos* e são caracterizados pela relação $x\geq 0$.

Tem-se, evidentemente, $x\leq x$ para todo $x\in K$.

Dados $x,y\in K$, tem-se $x=y$ se, e somente se, $x\leq y$ e $y\leq x$. É muito frequente, em Análise, provar-se que dois números x e y são iguais mostrando-se primeiro que $x\leq y$ e, depois, que $y\leq x$.

Com exceção de O2 (tricotomia), que é substituída pelas propriedades $x\leq x$ (reflexidade) e $x\leq y$, $y\leq x \Leftrightarrow x=y$ (anti-simetria), todas as propriedades acima demonstradas para a relação $x<y$ transferem-se para $x\leq y$.

Num corpo ordenado K, como $1>0$, temos $1<1+1<1+1+1<...$ e o subconjunto de K formado por estes elementos é, portanto, infinito. Mais precisamente, vamos mostrar como se pode considerar o conjunto $\mathbb{N}$, dos números naturais, naturalmente imerso em K.

Temporariamente, indiquemos com o símbolo $1'$ o elemento unidade do corpo ordenado K. Definamos uma função $f:\mathbb{N}\to K$ pondo $f(1)=1'$, $f(2)=1'+1'$, etc. A maneira correta de definir f é por indução: $f(1)=1'$ e $f(m+1)=f(m)+1'$. Por indução, verifica-se que $f(m+n)=f(m)+f(n)$ e que (como todos os valores $f(n)$ são positivos)

$m < p \Rightarrow f(m) < f(p)$. Assim, a função $f : \mathbb{N} \to K$ define uma bijeção do conjunto $\mathbb{N}$ dos números naturais sobre um subconjunto $\mathbb{N}' = f(\mathbb{N})$, formado pelos elementos $1'$, $1'+1'$, $1'+1'+1'$, etc. Costuma-se identificar $\mathbb{N}'$ com $\mathbb{N}$ e considerar os números naturais contidos em K. Isto é o que faremos. Temos $\mathbb{N} \subset K$ e voltamos a escrever 1, em vez de $1'$.

Em particular, todo corpo ordenado é infinito e tem "característica zero", isto é $1+1+...+1 \neq 0$ sempre.

Dado um corpo ordenado K e considerando $\mathbb{N} \subset K$, como estamos fazendo, os simétricos $(-n)$ dos elementos $n \in \mathbb{N}$ e mais o zero $(0 \in K)$ constituem um grupo abeliano, que se identifica com o grupo $\mathbb{Z}$ dos inteiros. Assim, temos $\mathbb{N} \subset \mathbb{Z} \subset K$.

Mais ainda, dados $m, n \in \mathbb{Z}$, com $n \neq 0$, existe o inverso $n^{-1} \in K$. Podemos, portanto, nos referir ao conjunto formado por todos os elementos $m \cdot n^{-1} = \dfrac{m}{n} \in K$, onde $m, n \in$ e $n \neq 0$. Este conjunto é um subcorpo de K (isto é, as operações de K, quando aplicadas a elementos deste conjunto dão resultados ainda no conjunto). Trata-se do menor subcorpo de K. Com sucessivas de 1, todo subcorpo de k deve conter em $\mathbb{Z}$, deve conter o conjunto das frações $\dfrac{m}{n}$, $m, n \in \mathbb{Z}$, $n \neq 0$. Evidentemente, este menor subcorpo de k identifica-se ao corpo $\mathbb{Q}$ dos números racionais.

Concluímos assim que, dado um corpo ordenado k, podemos considerar, de modo natural, as inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset K$. Por exemplo, o corpo $\mathbb{Q}(t)$ contém as frações do tipo $\dfrac{p}{q}$, onde p e q são polinômios constantes, inteiros, com $q \neq 0$. estas frações formam o corpo $\mathbb{Q}$ e tem-se $\mathbb{Q} \subset \mathbb{Q}(t)$.

Exemplo 8. *Desigualdade Bernoulli.* Em todo corpo ordenado K, se $n \in \mathbb{N}$ e $x \geq -1$, vale:

$$(1+x)^n \geq 1 + n \cdot x$$

deduz-se

$$(1+x)^{n+1} = (1+x)^n \cdot (1+x) \geq (1+nx)(1+x) = 1+nx+x+nx^2 = 1+(n+1)x+n \cdot x^2 \geq 1+(n+1)x$$

.

A desigualdade anterior pode ser demonstrada pelo princípio da indução finita. Tal demonstração pode ser vista na referência [2].

Teorema 1. *Num corpo K, as seguintes afirmações são equivalentes:*

(i) $N \subset K$ é ilimitado superiormente;

(ii) dados $a, b \in K$, com $a > 0$, existe $n \in \mathbb{N}$ tal que $n \cdot a > b$;

(iii) dado qualquer $a > 0$ em K, existe $n \in \mathbb{N}$ tal que $0 < \frac{1}{n} < a$.

Demonstração: (i) $\Rightarrow$ (ii). Como $\mathbb{N}$ é ilimitado, dados $a > 0$ e b em K, existe $n \in \mathbb{N}$ tal que $\frac{b}{a} < n$ e, portanto, $b < a \cdot n$. Para provar que (ii) $\Rightarrow$ (iii), dado $a > 0$, existe, em virtude de (ii), um $n \in \mathbb{N}$ tal que $n \cdot a > 1$. Então $0 < \frac{1}{n} < a$. Finalmente, mostremos que (iii) $\Rightarrow$ (i). Dado qualquer $b > 0$ existe, por (iii) um $n \in \mathbb{N}$ tal que $\frac{1}{n} < \frac{1}{b}$, ou seja, $n > b$. Assim, nenhum elemento > 0 em k pode ser cota superior de $\mathbb{N}$. Evidentemente, um elemento ≤ 0 também não pode. Logo $\mathbb{N}$ é ilimitado superiormente.

Definição 1. Um corpo ordenado K chama-se *arquimediano* quando nele é válida qualquer das três condições equivalentes citadas no Teorema anterior.

Assim, o corpo $\mathbb{Q}$ dos números racionais é arquimediano, enquanto o corpo $\mathbb{Q}(t)$ das funções racionais, com a ordem introduzida no Exemplo 6, é não-arquimediano.

1.3 $\mathbb{R}$ é um corpo ordenado completo

Nada do que foi dito até pode distinguir $\mathbb{R}$ de $\mathbb{Q}$ pois os números racionais também constituem um corpo ordenado. Acabaremos agora nossa caracterização de $\mathbb{R}$, descrevendo-o como um corpo ordenado completo, propriedade que $\mathbb{Q}$ não tem.

Um conjunto $X \subset \mathbb{R}$ diz-se *limitado superiormente* quando existe algum $b \in \mathbb{R}$ tal que $x \leq b$ para todo $x \in X$. Neste caso, diz-se que b é uma *cota superior* de X. Analogamente, diz-se que o conjunto $X \subset \mathbb{R}$ é *limitado inferiormente* quando existe $a \in \mathbb{R}$ tal que $a \leq x$ para todo $x \in X$. Neste caso diz-se que a é então uma *cota inferior* de X. Se X é limitado superior e inferiormente, diz-se que X é um conjunto *limitado*. Isto significa que X está contido em algum intervalo.

Seja $X \subset \mathbb{R}$ limitado superiormente e não-vazio. Um número $b \in \mathbb{R}$ chama-se *supremo* do conjunto X se é a menor das cotas superiores de X. Mais explicitamente, b é o supremo de X quando cumpre as duas condições:

S1. Para todo $x \in X$, tem-se $x \leq b$;

S2. Se $c \in \mathbb{R}$ é tal que $x \leq c$ para todo $x \in X$ então $b \leq c$.

A condição S2 admite a seguinte reformulação:

S2'. Se $c < b$ então existe $x \in X$ com $c < x$.

Com efeito, S2' diz que nenhum número real menor do que b pode ser cota superior de X. Às vezes se exprime S2' assim: para todo $\epsilon > 0$ existe $x \in X$ tal que $b - \epsilon < x$.

Escrevemos $b = \sup X$ para indicar que b é o supremo do conjunto X.

Analogamente, se $X \subset \mathbb{R}$ é um conjunto não-vazio, ilimitado inferiormente, um número real a chama-se o *ínfimo* do conjunto X, e escreve-se $a = \inf X$, se é a maior das cotas inferiores de X. Isto equivale às duas afirmações:

I1. Para todo $x \in X$ tem-se $a \leq x$;

I2. Se $c \leq x$ para todo $x \in X$ então $c \leq a$.

A condição I2 pode também ser formulada assim:

I2'. Se $a < c$ então existe $x \in X$ tal que $x < c$.

De fato, I2' diz que nenhum número maior do que a é cota inferior de X. Equivalentemente: para todo $\epsilon > 0$ existe $x \in X$ tal que $x < a + \epsilon$.

Diz-se que um número $b \in X$ é o *maior elemento* (ou *elemento máximo*) do conjunto X quando $b \geq x$ para todo $x \in X$. Isto quer dizer que b é uma cota superior de X, *pertencente* a X. Por exemplo, b é o elemento máximo do intervalo fechado $[a, b]$ mas o intervalo $[a, b)$ não possui maior elemento. Evidentemente, se um conjunto X possui elemento máximo este será supremo. A noção de supremo serve precisamente para substituir a ideia de maior elemento de um conjunto quando esse maior elemento não existe. O supremo do conjunto $[a, b)$ é b. Considerações inteiramente análogas podem ser feitas em relação ao ínfimo.

A afirmação de que o corpo ordenado $\mathbb{R}$ é *completo* significa que todo conjunto não-vazio, limitado superiormente, $X \in \mathbb{R}$ possui supremo $b = \sup X \in \mathbb{R}$.

Exemplo 9. Vejamos agora outro exemplo de um conjunto limitado superiormente num corpo ordenado K, o qual não possui supremo em K. Para isso, tomemos um corpo não-arquimediano K. O conjunto $\mathbb{N} \subset K$ é limitado superiormente. Se $b \in K$ é uma cota superior de $\mathbb{N}$ então $n + 1 \leq b$ para todo $n \in \mathbb{N}$. Segue-se que $n \leq b - 1$ qualquer qualquer que seja $n \in \mathbb{N}$. Em outras palavras, se $b \in K$ for uma cota superior de $\mathbb{N}$, $b - 1$ também o será. Como $b - 1 < b$, segue-se que, num corpo não-arquimediano K, o conjunto $\mathbb{N}$ dos números naturais é limitado superiormente mas não existe $\sup \mathbb{N}$ em K.

Um corpo ordenado K chama-se *completo* quando todo subconjunto não-vazio, limitado superiormente, $X \subset K$, possui supremo em K.

Resulta da definição que, num corpo ordenado completo, todo conjunto não-vazio, limitado inferiormente, $Y \subset K$, possui um ínfimo. Com efeito, dado Y, seja $X = -Y$, isto é, $X = \{-y; y \in Y\}$. Então X é não-vazio e limitado superiormente; logo existe $a = \sup X$. Como se vê facilmente, tem-se $-a = \inf Y$.

Segue-se do exemplo anterior que *todo corpo ordenado completo é arquimediano.*

Adotaremos, a partir de agora, o axioma fundamental da Análise Matemática.

Axioma. *Existe um corpo ordenado completo,* $\mathbb{R}$*, chamado corpo dos números reais.*

Passaremos a examinar agora algumas propriedades dos números reais que resultam imediatamente da definição de $\mathbb{R}$ como um corpo ordenado completo.

Voltamos a enfatizar que, em todo o restante deste livro, as únicas propriedades dos números reais que usaremos são aquelas que decorrem de ser $\mathbb{R}$ um corpo ordenado completo. Isto inclui, evidentemente, as proposições demonstradas no início deste capítulo sobre corpos e corpos ordenados em geral.

Existe em $\mathbb{R}$ um número positivo a tal que $a^2 = 2$ (a existência pode ser comprovada pelo teorema dos intervalos encaixantes, disponível em [6], pp. 19-21). Este número é representado pelo símbolo $\sqrt{2}$. É claro que só existe um número positivo cujo quadrado é 2, pois $a^2 = b^2 = 2 \Rightarrow 0 = a^2 - b^2 = (a-b)(a+b) \Rightarrow a + b = 0$ ou $a - b = 0$. No primeiro caso, $a = -b$ (logo não podem ser a e b ambos positivos) e no segundo $a = b$. Pelo Lema de Pitágoras, $\sqrt{2}$ não é um número racional.

Aos elementos do conjunto $\mathbb{R} - \mathbb{Q}$, isto é, aos números reais que não são racionais, chamaremos *números irracionais*. Assim, $\sqrt{2}$ é um número irracional.

Capítulo 2

Um Pouco Sobre Irracionalidade

Apresentaremos neste próximo capítulo, o princípio da boa ordenação (P.B.O) e o Princípio fundamental da teoria dos números, resultados esses que exercerão papel fundamental nas provas sobre a irracionalidade de certos números.

Dentre tais provas, comprovaremos a irracionalidade de $\sqrt{2}$ e caso mais geral , $\sqrt{p}$,onde p é um número primo qualquer, e as "confrontaremos"(no sentido de complexidade), com as provas da irracionalidade do número e (numero de Euler) e do número π.

2.1 Um Resultado Fundamental

Um dos principais fatos nos fundamentos de matemática é o conhecido Princípio da Boa Ordenação (ou da boa ordem). Apesar de parecer óbvio em certo sentido, é extremamente poderoso. Recordemos seu enunciado **Princípio da Boa Ordenação.** *Todo subconjunto não vazio $\mathbb{A}$ de números naturais possui um elemento mínimo, isto é, existe $n_0 \in \mathbb{A}$, tal que $n_0 \leq n$ para todo $n \in \mathbb{A}$.*

O PBO, como é conhecido, não é válido para os inteiros e muito menos para os racionais. Assim, de algum modo, o PBO captura algo especial sobre os números naturais.

Princípio Fundamental da Teoria dos Números. *Dado $m \in \mathbb{Z}$, não existe $n \in \mathbb{Z}$ tal que $m < n < m + 1$.*

Demonstração. Como $m < n < m + 1$ se e somente se $0 < n - m < 1$, então basta-nos mostrar que não existe número natural entre 0 e 1 (observe que $n - m$ é inteiro positivo). Para mostrar este último fato, supondo o contrário, temos que o conjunto $\mathbb{A} = \{n \in \mathbb{N} :$

$0 < n < 1\}$ é não vazio. Portanto, pelo Princípio da Boa Ordenação, existe $n_0 \in \mathbb{A}$ mínimo. Assim $0 < n_0 < 1$, e, multiplicando essa desigualdade por n_0, obtemos $0 < n_0^2 < n_0 < 1$, logo $n_0^2 \in \mathbb{A}$, contrariando a minimalidade de n_0.

2.2 Irracionalidade de $\sqrt{2}$

O número $\sqrt{2}$ tem uma história muito rica. Sua definição vem da geometria (a medida da hipotenusa de um triângulo retângulo com catetos de comprimento 1) e da álgebra (um número real positivo x, tal que $x \cdot x = 2$). A demonstração de sua irracionalidade é frequentemente atribuída a Hippasus de Metapontum (500 a.C.), que pertencia à escola pitagórica. Reza a lenda, que tal demonstração teria lhe custado a vida, pois na época os gregos não acreditavam na existência de números incomensuráveis. Abaixo, o número $\sqrt{2}$ com 30 casas decimais e sua escrita como uma série e um produto infinito

- $\sqrt{2} = 1,41421356237309504880168872421...$
- $\sqrt{2} = \sum_{n=0}^{\infty} (-1)^{n+1} \frac{(2n-3)!!}{(2n)!!}$
- $\sqrt{2} = \left(\frac{2 \cdot 2}{1 \cdot 3}\right)\left(\frac{6 \cdot 6}{5 \cdot 7}\right)\left(\frac{10 \cdot 10}{9 \cdot 11}\right)...$

onde $m!!$ é o fatorial duplo de m.

Nesta seção aprestaremos duas demonstrações de que $\sqrt{2}$ é irracional. São baseadas na ótima referência [13] e podem, em geral, ser aplicadas na demonstração da irracionalidade de $\sqrt{n}$, quando n não é quadrado perfeito.

2.2.1 Frações irredutíveis

Suponha que $\sqrt{2} = \frac{p}{q}$. Se d=mdc(p, q), então $\frac{p}{d}$ e $\frac{q}{d}$ são primos entre si. Portanto podemos supor, sem perda de generalidade, que $\frac{p}{q}$ é Irredutível, isto é, mdc$(p, q) = 1$. Por um simples cálculo Algébrico, temos $2q^2 = p^2$. A partir desse ponto faremos as duas demonstrações:

1. Logo p^2 é par implicando $p = 2k$, para algum $k \in \mathbb{Z}$. Assim, $q^2 = 2k^2$ e consequentemente q também é par. Daí, mdc$(p, q) \geq 2$, contrariando a coprimalidade de p e q.

2. Logo $q^2 \mid p^2$ e como $\text{mdc}(p, q) = 1$, então $q^2 = \text{mdc}(p^2, q^2) = 1$. Nesse caso, $2 = p^2 \in \{1, 4, 9, ...\}$, o que é impossível.

2.3 Irracionalidade de $\sqrt{p}$

Vamos supor que a raiz quadrada de um primo p é um número racional e pode ser escrita como uma fração com numerador a e denominador b, ambos primos entre si; ou seja, a fração é irredutível. Como segue:

$$\sqrt{p} = \frac{a}{b}$$

Elevamos os dois membros ao quadrado.

$$p = \frac{a^2}{b^2}$$

Multiplicamos os dois membros da equação por b^2 e obtemos:

$$pb^2 = a^2$$

Analisando esta última equação, observamos a direita da igualdade, temos um número inteiro com quantidade par de fatores primo p. Enquanto que o lado esquerdo da igualdade nos mostra que o mesmo número inteiro possui quantidade ímpar de fatores primos p. Esse fato contradiz o Teorema Fundamental da Aritmética.

Portanto, a raiz quadrada de um primo p, é irracional.

2.4 Irracionalidade de e

Apresentaremos a seguir as demonstrações tanto da existência quanto a da irracionalidade do número e. Número esse, presente em diversas situações do nosso cotidiano, como por exemplo: no calculo dos juros contínuos, no fenômeno de desintegração radioativa, no crescimento bacteriano e na datação feita pelo teste do carbono 14.

O primeiro a demonstrar a irracionalidade de e foi o grande matemático suíço L. Euler, utilizando frações contínuas. A demonstração que apresentaremos está presente na referência [17], e é de autoria de outro brilhante matemático, o francês Joseph Fourier, que utilizou o método de truncamento de séries.

2.4.1 Existência do Número e

Teorema 1. *O* $\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$ *existe e está compreendida entre* 2 *e* 3.

Demonstração. Vamos provar que o $\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$ existe.

Seja $u=\left(1+\frac{1}{n}\right)^n$

Qualquer que seja n inteiro positivo, $(\mathbf{u_n})$ é uma potência de base positiva, portanto, também positiva. Vamos mostrar que $(\mathbf{u_n})$ é crescente, desenvolvendo o termo geral segundo a fórmula do binômio de Newton:

$$\mathbf{u_n}=1+n\frac{1}{n}+\frac{n(n-1)}{2!}\frac{1}{n^2}+...+\frac{n(n-1)(n-2)...2.1}{n!}\frac{1}{n^n}$$

$$\mathbf{u_n}=1+\frac{1}{1!}+\frac{1}{2!}\frac{n(n-1)}{n^2}+\frac{1}{3!}\frac{n(n-1)(n-2)}{n^3}+...+\frac{1}{n!}\frac{n(n-1)(n-2)...2.1}{n^n}$$

ou ainda

$$\mathbf{u_n}=1+\frac{1}{1!}+\frac{1}{2!}\left(1-\frac{1}{n}\right)+\frac{1}{3!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)+...+\frac{1}{n!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)...\left(1-\frac{n-1}{n}\right)$$

temos então:

$$u_n>1+\frac{1}{1!}+\frac{1}{2!}\left(1-\frac{1}{n-1}\right)+\frac{1}{3!}\left(1-\frac{1}{n-1}\right)\left(1-\frac{2}{n-1}\right)+...$$

$$...+\frac{1}{(n-1)!}\left(1-\frac{1}{n-1}\right)\left(1-\frac{2}{n-1}\right)...\left(1-\frac{n-2}{n-1}\right)=u_{n-1}$$

Conclui-se que $u_n>u_{n-1}$ para n inteiro e positivo qualquer. Logo a sucessão $\mathbf{u_n}$ é crescente.

Demonstraremos agora que a sucessão de termo geral $\mathbf{u_n}$ é limitada superiormente.

$$\mathbf{u_n}=\left(1+\frac{1}{n}\right)^n<1+\frac{1}{1!}+\frac{1}{2!}+...+\frac{1}{n!}$$

e como $n!>2^{n-1}$ para $n\geq 3$ inteiro, temos:

$$\mathbf{u_n}\leq 1+1+\frac{1}{2}+\frac{1}{2^2}+...+\frac{1}{2^{n-1}}=1+2-\frac{1}{2^{n-1}}\leq 3$$

que prova ser 3 maior que qualquer sucessão e, portanto, esta é limitadamente superiormente. Então a sucessão de termo geral $\mathbf{u_n}=\left(1+\frac{1}{n}\right)^n<3$

Sabemos que $\mathbf{u_n}<3$ para todo $\mathbf{n}$ inteiro e positivo, portanto

$$\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n\leq 3$$

e

$$\mathbf{u_n} = \left(1 + \frac{1}{n}\right)^n \geq 1 + \frac{1}{1!} = 2$$

Definição 1. Definimos o número e como sendo o $\lim_{n\to\infty}\left(1 + \frac{1}{n}\right)^n$.

2.4.2 O Número e é Irracional

Para mostrar a irracionalidade de e fazemos uso de uma interessante caracterização deste, objeto do próximo Lema.

LEMA 1.

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + ... + \frac{1}{n!} + ... \tag{2.1}$$

Demonstração. Toda função de classe C^∞[1]pode ser escrita como um polinômio de Taylor:

$$f(x) = f(x_0) + \frac{f'(x_0)}{1!}(x - x_0) + \frac{f''(x_0)}{2!}(x - x_0)^2 + ... + \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n + ...$$

ou

$$f(x) = f(x_0) + \sum_{n=1}^{\infty} \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n.$$

No caso particular de $f(x) = e^x$, em torno da origem (ou seja $x_0 = 0$), temos:

$$f(x) = f(0) + \frac{f'(0)}{1!}(x) + \frac{f''(0)}{2!}(x^2) + ... + \frac{f^{(n)}(0)}{n!}(x^n) + ... \tag{2.2}$$

Sabe-se que $f^{(n)}(x) = e^x$, $\forall n \in 1, 2, ...$, ou seja, $f'(x) = e^x$, $f''(x) = e^x$, $f'''(x) = e^x$ e assim por diante.

Em particular para $x_0 = 0$ tem-se $f^{(n)}(0) = e^0 = 1 \; \forall \in 1, 2, 3, ...$

Note ainda que $f(0) = e^0 = 1$.

Da observação acima e de (2.2), segue que $e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + ... + \frac{x^n}{n!} + ...$

Teorema 1. *O número e é irracional*

Demonstração. É demonstrado no Lema anterior que:

$$e^1 = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + ... + \frac{1}{n!} + ... \tag{2.3}$$

Suponha que e seja um número racional, isto é, e pode ser escrito da forma $\frac{p}{q}$ com $p, q \in \mathbb{Z}$. Suponha ainda que $\frac{p}{q}$ seja a forma irredutível, isto é, $(p, q) = 1$. Da relação

[1]Uma função f é chamada de classe C^∞, quando se pode derivar f tantas vezes quantas se deseje, em todos os pontos do seu domínio. (Aos interessados em aprofundar os conhecimentos sobre classes de funções, derivadas de ordem superior e polinômio de Taylor, recomendamos a referência [10], capítulo 9.)

(2.3), segue que:

$$\frac{p}{q} = \left(1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + ... + \frac{1}{q!}\right) + \frac{1}{(q+1)!} + ... \Rightarrow$$

$$0 < \frac{p}{q} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + ... + \frac{1}{q!}\right) = \frac{1}{(q+1)!} + \frac{1}{(q+2)!} + ... \Rightarrow$$

$$\sum_{j=q+1}^{\infty} \frac{1}{j!} \tag{2.4}$$

mas observe que,

$$\frac{1}{(q+1)!} = \frac{1}{(q+1)q!}$$

$$\frac{1}{(q+2)!} = \frac{1}{(q+2)(q+1)q!}$$

$$\frac{1}{(q+3)!} = \frac{1}{(q+3)(q+2)(q+1)q!}$$

assim,

$$\sum_{j=q+1}^{\infty} \frac{1}{j!} =$$

$$\frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \frac{1}{(q+3)!} + ... =$$

$$\frac{1}{q!}\left(\frac{1}{(q+1)} + \frac{1}{(q+2)(q+1)}\right) + ... \leq$$

$$\frac{1}{q!}\left(\frac{1}{(q+1)} + \frac{1}{(q+2)^2} + \frac{1}{(q+1)^3}\right) + ... \tag{2.5}$$

pois

$$(q+1) < (q+2) < (q+3) < ... \Rightarrow$$

$$... < \frac{1}{(q+3)} < \frac{1}{(q+2)} < \frac{1}{(q+1)}$$

logo

$$\frac{1}{(q+2)(q+1)} < \frac{1}{(q+1)(q+1)} = \frac{1}{(q+1)^2},$$

$$\frac{1}{(q+3)(q+2)(q+1)} < \frac{1}{(q+1)(q+1)(q+1)} = \frac{1}{(q+1)^3},$$

e assim sucessivamente...

Agora, note que

$$\left(\frac{1}{(q+1)} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + ...\right)$$

é a soma dos termos de uma progressão geométrica infinita

$$\left(\frac{1}{(q+1)}, \frac{1}{(q+1)^2}, \frac{1}{(q+1)^3}, ...\right)$$

cujo primeiro termo é $\left(\frac{1}{(q+1)}\right)$ e a razão é $\left(\frac{1}{(q+1)}\right)$. Logo essa soma é igual a

$$\frac{\frac{1}{(q+1)}}{1-\left(\frac{1}{(q+1)}\right)} = \frac{1}{(q+1)}\frac{(q+1)}{q} = \frac{1}{q}$$

ou seja,

$$\left(\frac{1}{(q+1)} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + ...\right) = \frac{1}{q} \tag{2.6}$$

substituindo (2.6) em (2.5) segue que

$$\sum_{j=q+1}^{\infty} \frac{1}{j!} < \frac{1}{q}\frac{1}{q!} \tag{2.7}$$

substituindo (2.7) em (2.4),

$$0 < \frac{p}{q} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + ... + \frac{1}{q!}\right) < \frac{1}{q!}\frac{1}{q}$$

$$0 < q!\left(\frac{p}{q} - 1 - \frac{1}{1!} + \frac{1}{2!} - ... - \frac{1}{q!}\right) < \frac{1}{q} \leq 1$$

Observe que o segundo termo da esquerda para a direita da desigualdade acima é um número inteiro pois, $p, q \in \mathbb{Z}$, valem as leis do fechamento na multiplicação e adição temos:

$$q!\left(\frac{p}{q} - 1 - \frac{1}{1!} + \frac{1}{2!} - ... - \frac{1}{q!}\right) =$$

$$q!\left(\frac{(q-1)!(p-q)! - q! - ... - 1}{q!}\right) =$$

$$((q-1)!(p-q)! - q! - ... - 1),$$

Mas isso é um absurdo, já que é impossível ter um número inteiro positivo menor que 1. O absurdo foi supor que e é um número racional. Portanto e é um número irracional.

2.5 Irracionalidade de π

Há milênios que o que o número π intriga e ao mesmo tempo encanta as mentes dos curiosos e estudiosos. Sua presença no mundo antigo, no sentido de aproximações, vai desde os registros na Babilônia, marcando presença nos papiros egípcios e posteriormente, aparecendo nas paginas do antigo testamento. Também devemos ressaltar o destaque que tal número ganhou no mundo grego, principalmente pelos aos trabalhos do grande matemático Arquimedes de Siracusa, que obteve aproximações consideráveis através de polígonos regulares. Outra presença marcante de π, foi no famoso problema da quadradura do círculo.

Prosseguindo na escala do tempo, a busca por aproximações do π continuou a motivar diversos estudiosos, principalmente por este números está presente diversos campos da matemática e do conhecimento, como por exemplo: na teoria das probabilidades geométricas , astronomia, hidrografia e em diversos fenômenos periódicos, etc.

Porém, havia uma questão importantíssima sem resposta, o número π é irracional? Essa questão foi respondida primeiramente pelo matemático francês Johann Heinrich Lambert que utilizou em sua demonstração a teoria das frações contínuas vinculada a função trigonométrica tangente.

A seguir, apresentaremos a demonstração de autoria do matemático canadense Ivan Níven, disponível na referência [4], que sofreu bastante influência dos métodos de C. Hermite utilizados na prova da transcendência do número e.

Começaremos com seguintes passos:

LEMA 1. *Dado o polinômio* $f(x) = \dfrac{x^n(1-x)^n}{n!}$, *se* $0 < x < 1$, *então*

$$0 < f(x) < \frac{1}{n!}.$$

Prova. Para $0 < x < 1$, temos que $0 < x^n < 1$ e $0 < (1-x)^n < 1$. Logo,

$$0 < x^n \cdot (1-x)^n < 1$$

Multiplicando a última desigualdade por $\dfrac{1}{n!}$, obtemos

$$0 < \frac{x^n \cdot (1-x)^n}{n!} < \frac{1}{n!}$$

Portanto $0 < f(x) < \dfrac{1}{n!}$, para todo $0 < x < 1$. Para cada $n \in \mathbb{Z}, n \geq 0$ consideremos a função polinomial

$$f_n(x) = \frac{1}{n!}x^n \cdot (1-x)^n, x \in \mathbb{R}.$$

LEMA 2. $f_n^{(k)}(0)$ *e* $f_n^{(k)}(1) \in \mathbb{Z}$ *para todo* $k \in \mathbb{N}$.

Prova. Observe que $f_n^{(k)}(x)$ é obtida a partir do produto $x^n(1-x)^n$. Portanto, seu grau varia de n a $2n$. Assim, $f_n(x)$ pode ser escrita na forma

$$f_n(x) = \frac{1}{n!}\sum_{i=n}^{2n} c_i x_i, \text{ com } c_i \in \mathbb{Z}$$

Para provarmos o lema proposto, será necessário analisar os possíveis valores de $f_n^{(k)}(0)$ e $f_n^{(k)}(1)$. Note que

- Se $k < n$, então $f_n^{(k)}(0) = 0$ pois f_n é aplicada no ponto $x = 0$.
- Se $k > 2n$, então $f_n^{(k)}(0) = 0$ pois o grau de f_n é $2n$.

Observe ainda que

$$f_n(x) = \sum_{i=n}^{2n} c_i x^i = \frac{1}{n!}[c_n x^n + c_{n+1}x^{n+1} + ... + c_{2n}x^{2n}]$$

Então para $n \leq k \leq 2n$, temos

$$f_n^{(n)}(x) = \frac{1}{n!}[n!c_n + \overbrace{(n+1)!c_{n+1}x + ... + \frac{(2n)!}{n!}c_{2n}x^n}^{\text{termos envolvendo } x}]$$

$$f_n^{(n+1)}(x) = \frac{1}{n!}[(n+1)!c_{n+1} + \overbrace{(n+2)!c_{n+2}x + ... + \frac{(2n)!}{(n-1)!}c_{2n}x^{n-1}}^{\text{termos envolvendo } x}]$$

$$\vdots$$

$$f_n^{(2n)}(x) = \frac{1}{n!}[(2n)!c_{2n}]$$

Assim, temos que

$$f_n^{(n)}(0) = c_n,$$

$$f_n^{(n+1)}(0) = (n+1)c_{n+1}$$

$$\vdots$$

$$f_n^{(2n)}(0) = (2n)(2n-1)...(n+1)c_{2n}$$

Então, podemos concluir que $f_n^{(n)}(0)$ é inteiro para todo $k \in \mathbb{Z}$. Além disso, podemos perceber que

$$f_n(x) = f_n(1-x),$$

logo,

$$f_n^{(k)}(x) = (-1)^k f_n(1-x),$$

e, portanto,

$$f_n^{(k)}(1) = (-1)^k f_n^{(k)}(0).$$

Assim, $f_n^{(k)}(1)$ também é um inteiro para todo o k.

LEMA 3. *Se a é qualquer número e $\varepsilon > 0$, então para n suficientemente grande*

$$\frac{a^n}{n!} < \varepsilon.$$

Prova. Para provar esse resultado, observe que, se $n > 2a$, então

$$\frac{a^{n+1}}{(n+1)!} = \frac{a}{n+1}\frac{a^n}{n!} < \frac{1}{2}\frac{a^n}{n!}.$$

Agora, seja $\mathbf{n_0}$ qualquer número natural com $\mathbf{n_0 \geq 2a}$. Então, qualquer que seja $\frac{a^{n_0}}{(n_0)!}$, as seguintes desigualdades podem ser satisfeitas:

$$\frac{a^{n_0+1}}{(n_0+1)!} < \frac{1}{2} \cdot \frac{a^{n_0}}{n_0!}$$

$$\frac{a^{n_0+2}}{(n_0+2)!} < \frac{1}{2} \cdot \frac{a^{n_0+1}}{(n_0+1)!} < \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{a^{n_0}}{n_0!}$$

$$\vdots$$

$$\frac{a^{n_0+k}}{(n_0+k)!} < \left(\frac{1}{2}\right)^k \cdot \frac{a^{n_0}}{n_0!}.$$

Se k é tão grande que $\frac{a^{n_0}}{(n_0)! \cdot \varepsilon} < 2^k$, então

$$\frac{a^{n_0+k}}{(n_0+k)!} < \varepsilon.$$

Teorema 1. *π^2 é irracional.*

Prova. Suponha que π^2 é racional. Então, $\pi^2 = \frac{p}{q}$, onde $p, q \in \mathbb{Z}$ com $q \neq 0$ e considere os seguintes polinômios:

$$f(x) = \frac{x^n(1-x)^n}{n!}$$

e

$$F(x) = q^n[\pi^{2n}.f(x) - \pi^{2n-2}.f^{(2)}(x) + ... + (-1)^n f^{(2n)}(x)]$$

Do Lema 2, concluímos que $F(0)$ e $F(1)$ são inteiros. Agora, observe que

$$[F^{(1)}(x)\sin(\pi x) - \pi F(x)\cos(\pi x)]' =$$

$$F^{(2)}(x)\sin(\pi x) + F^{(1)}(x)\pi\cos(\pi x) - [F^{(1)}(x)\pi\cos(\pi x) + F(x)\pi^2(-\sin(\pi x))] =$$

$$F^{(2)}(x)\sin(\pi x) + F(x)\pi^2\sin(\pi x)$$

Além disso,

$$F^{(2)}(x) = q^n[\pi^{2n}f^{(2)}(x) - \pi^{2n-2}f^{(4)}(x) + ... + (-1)^n\pi^2 f^{(2n+2)}(x)]$$

$$\pi^2 F(x) = q^n[\pi^{2n+2}f(x) - \pi^{2n}f^{(2)}(x) + ... + (-1)^n\pi^2 f^{(2n)}(x)]$$

Note que $f^{(2n+2)}(x) = 0$, pois o grau de $f(x)$ é $2n$. Logo,

$$F^{(2)}(x)\sin(\pi x) + F(x)\pi^2\sin(\pi x) = q^n\pi^{2n}\pi^2 f(x)\sin(\pi x) = p^n\pi^2\sin(\pi x).$$

Assim,

$$p^n\pi^2 \int_0^1 \sin(\pi x) f(x)dx = [F^{(1)}(x)\sin(\pi x) - \pi F(x)\cos(\pi x)]\,\big|_0^1$$

Portanto,

$$p^n\pi^2 \int_0^1 \sin(\pi x) f(x)dx = \pi[F(1) + F(0)],$$

isto é,

$$p^n\pi \int_0^1 \sin(\pi x) f(x)dx = F(1) + F(0). \tag{2.8}$$

Como já foi mostrado $F(1) + F(0)$ é inteiro. Agora, do Lema 1 e da expressão 2.8, temos

$$0 < \pi p^n \int_0^1 \sin(\pi x) f(x)dx < \frac{\pi p^n}{n!} \int_0^1 \sin(\pi x) f(x)dx.$$

Mas,

$$\int_0^1 \sin(\pi x) f(x)dx = -\frac{\cos(\pi x)}{\pi}\,\big|_0^1 = \frac{2}{\pi}.$$

Logo,

$$0 < \pi p^n \int_0^1 \sin(\pi x) f(x)dx < \frac{2p^n}{n!}.$$

Do Lema 3 podemos tomar n tal que $\dfrac{2p^n}{n!} < 1$. Mas, o lado direito da expressão 2.8 é um inteiro e

$$0 < p^n\pi \int_0^1 \sin(\pi x) f(x)dx < 1,$$

o que corresponde a uma contradição, pois não há inteiros entre 0 e 1.

Corolário 1. *O número π é irracional.*

Prova. Suponha que π é racional, então existem $a, b \in \mathbb{Z}$, com $b \neq 0$ de modo que $\pi = \dfrac{a}{b}$ é irredutível. Então $\pi^2 = \dfrac{a^2}{b^2}$ também racional, o que contraria o teorema anterior. Logo, π é irracional.

Capítulo 3

Uma Outra Forma de Enxergar os Números Reais

A seguir, com base na ótima referência [5], definiremos o conjunto dos números algébricos e apresentaremos algumas de suas propriedades . Consequentemente, definiremos também, o conjunto dos números transcendentes. Porém, sem entrar em muitos detalhes nesse ultimo caso.

3.1 Números algébricos

Qualquer solução de uma equação polinomial da forma

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0, \tag{3.1}$$

onde os coeficientes a_i's são inteiros, é chamado *número algébrico*. Portanto, um número α é algébrico se pudermos fabricar uma equação polinomial com coeficientes inteiros, da qual α seja raiz. A equação polinomial minimal ou o polinômio minimal de α é o polinômio primitivo[1]de menor grau que tem α como raiz. Nesse caso, o grau de α é definido como o grau do seu polinômio minimal.

Exemplo 1. *$\sqrt{2}$ é raiz de $x^2 - 2 = 0$.*

Exemplo 2. *$\frac{1+\sqrt{5}}{2}$ é raiz de $x^2 - x - 1 = 0$.*

Exemplo 3. *$\sqrt{2} + \sqrt{3}$ é raiz de $x^4 - 10x^2 + 1 = 0$.*

Exemplo 4. *i é raiz de $x^2 + 1 = 0$ (mas nosso foco são os números reais).*

Exemplo 5. *Todo número racional $\frac{a}{b}$ com $a, b \in \mathbb{Z}$ e $b \neq 0$ é raiz de $bx - a = 0$.*

[1]Um polinômio em $\mathbb{Z}_{[x]}$ é chamado **primitivo** se seus coeficientes são primos entre si.

Alguns autores denotam o conjunto dos números algébricos por $\bar{\mathbb{Q}}$, por influência do fecho algébrico[2].

Um número que não é algébrico é dito **transcendente** e alguns autores o denotam o conjunto dos números transcendentes por $\mathbf{T}$.

3.2 A existência de números transcendentes

A existência de números transcendentes pode ser demonstrada como o fez G. Cantor. Para tal necessitamos de alguns conceitos.

Definição 1. *Um conjunto A é **enumerável** se seus elementos podem ser postos em correspondência biunívoca com os números naturais. Mais precisamente, A é enumerável se existir uma função bijetiva (isto é, função $1-1$ e sobre) $f : \mathbb{N} \to A$.*

Exemplo 6. *O conjunto dos números pares (positivos) é enumerável: tome $f(n) = 2n$.*

Exemplo 7. *O conjunto dos números ímpares (positivos) é enumerável: tome $f(n) = 2n - 1$.*

Exemplo 8. *O conjunto $\mathbb{Z}$ é enumerável: olhe a tabela abaixo*

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

Podemos também exibir essa bijeção através da seguinte função $f : \mathbb{N} \to \mathbb{Z}$:

$$f(n) = \begin{cases} \frac{n}{2}, & \text{se } n \text{ é par;} \\ -\frac{n-1}{2}, & \text{se } n \text{ é ímpar.} \end{cases}$$

Exemplo 9. *O conjunto dos números racionais é enumerável. Mostremos primeiramente que o conjunto dos racionais positivos é enumerável. Olhe o quadro a seguir:*

[2]Dado um corpo F, dizemos que uma extensão E de F é um fecho algébrico de F quando E é uma extensão algébrica que é algebricamente fechada, isto é, contém todas as raízes de polinômios com coeficientes em F. Para mais conceitos algébricos recomendamos a referência [7].

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

Observe que todos os números da forma $\frac{p}{q}$ com $p, q \in \mathbb{N}$ e $q \neq 0$ aparecerão no quadro acima. Se o percorremos seguindo as flechas teremos uma ordenação desse conjunto, o que vale dizer, a função f será $f(n) = n$-ésimo elemento que encontraremos seguindo as flechas. Assim, mostramos que o conjunto $\mathbb{Q}^+ = \{x \in \mathbb{Q}; x > 0\}$ é enumerável que $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup 0$, onde $\mathbb{Q}^- = \{x \in \mathbb{Q} : x < 0\}$.

Teorema 1.

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

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

Prova: (i) Seja $A = \{a_1, ..., a_n\}$ o conjunto finito e $B = \{b_1, b_2, ...\}$ o conjunto enumerável. O conjunto $A \cup B$ é enumerável. De fato a correspondência biunívoca entre $A \cup B$ e $\mathbb{N}$ será assim:

$$
\begin{array}{ccccccc}
a_1 & ,..., & a_n, & b_1, & b_2, & ... \\
\updownarrow & & \updownarrow & \updownarrow & \updownarrow & \\
1 & ,..., & n, & n+1, & n+2, & ...
\end{array}
$$

(ii) Se $A = \{a_1, a_2, ...\}$ e $B = \{b_1, b_2, ...\}$ são dois conjuntos enumeráveis, então $A \cup B$ é enumerável, bastando fazer a correspondência biunívoca definida abaixo

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

ou seja, $f(a_n) = 2n - 1$ e $f(b_n) = 2n$.

O leitor poderá produzir a demonstração do resultado seguinte que generaliza o Teorema $1(ii)$.

Teorema 1(iii). *A união de um número finito de conjuntos enumeráveis é enumerável.*

Para demonstrar o resultado abaixo, basta colocar os conjuntos um após o outro.

Teorema 1(iv). *A união de um conjunto enumerável de conjuntos finitos é enumerável.*

Finalmente, a generalização do Teorema 1 (iv):

Teorema 1(v). *A união de um conjunto enumerável de conjuntos enumeráveis é enumerável.*

Prova: Sejam $A_1 = \{a_{11}, a_{12}, a_{13}, ...\}$, $A_2 = \{a_{21}, a_{22}, a_{23}, ...\}$,..., $A_n = \{a_{n1}, a_{n2}, a_{n3}, ...\}$,... os conjuntos. Escreva-os na tabela

$$\begin{array}{cccc} a_{11}, & a_{12}, & a_{13}, & ... \\ a_{21}, & a_{22}, & a_{23}, & ... \\ a_{21}, & a_{22}, & a_{23}, & ... \\ \vdots & \vdots & \vdots & \end{array}$$

e proceda como na demonstração que $\mathbb{Q}^+$ é enumerável.

Observação: Se A é enumerável e $B \subset A$ é um conjunto infinito, então B é também enumerável. Imediato.

O conceito de conjunto enumerável é importante, porque existem conjuntos infinitos que não são enumeráveis.

Teorema 2. *O conjunto* $\mathbb{R}$ *dos números dos reais não é enumerável.*

Prova: Demonstraremos que o conjunto dos números reais $x \in [0, 1)$, isto é, $0 \leq x < 1$, não é enumerável. E em virtude da observação acima seguir-se-á que $\mathbb{R}$ também não é enumerável. Ora, os números $x \in [0, 1)$ têm uma representação decimal da forma

$$0, a_1 a_2 a_3 ..., \tag{3.2}$$

onde a_j é um dos algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8, ou 9. Alguns números têm duas representações da forma 3.1. Exemplo: $\frac{1}{2}$ é

$$0,500... \text{ ou } 0,49999...$$

Para tais números, escolhemos a representação decimal que "termina". Em outras palavras, eliminamos as decimais 3.2 que a partir de uma certa ordem todos os elementos são

9. Suponhamos agora que as decimais 3.2, ou, o que dá no mesmo, que os reais do intervalo $[0, 1)$ formam um conjunto enumerável:

$$0, a_{11}a_{12}a_{13}...0, a_{21}a_{22}a_{23}...0, a_{31}a_{32}a_{33}... \tag{3.3}$$

Agora, forme a seguinte decimal

$$0, b_1b_2b_3...$$

do seguinte modo: todos os b_is são diferentes de 0 ou 9 e

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

É claro que

$$0, b_1b_2b_3 \neq 0, a_{n1}a_{n2}a_{n3}...$$

para todo n, pois $b_n \neq a_{nn}$. Logo $0, b_1b_2b_3...$ não está na tabela 3.3, o que é absurdo.

Teorema 3. *O conjunto de todos números algébricos é enumerável.*

Prova: Dado um polinômio com coeficientes inteiros

$$P(x) = a_nx^n + ... + a_1x + a_0 \tag{3.4}$$

definimos sua altura como sendo o número natural

$$|P| = |a_n| + ... + |a_1| + |a_0| + n. \tag{3.5}$$

O teorema fundamenta da álgebra nos diz que $P(x) = 0$, com $P(x)$ dado em 3.4, tem exatamente n raízes complexas. Agora o número de polinômios do tipo 3.4 com uma dada altura é apenas um número finito. (Observe que é para essa afirmação que incluímos a parcela n na definição da altura em 3.5). Portanto., as raízes de todos os polinômios de uma dada altura formam um conjunto finito. A seguir observamos que o conjunto de todas as raízes de todos os polinômios de todas as alturas formam um conjunto enumerável, pois ele é a união de um conjunto enumerável de conjuntos finitos.

Teorema 4. *Existem números transcendentes.*

Prova: Do Teorema 3 segue-se que o conjunto dos algébricos reais é enumerável. Como o conjunto $\mathbb{R}$ é não enumerável, então o conjunto dos transcendentes reais deve ser não enumerável. De fato, se não o fosse obteríamos, usando o Teorema 1(ii), que $\mathbb{R}$ seria enumerável como união de dois conjuntos enumeráveis.

3.3 A aritmética dos números algébricos

As seguintes propriedades serão demonstradas a seguir.

(i) A soma de dois números algébricos é algébrico.

(ii) O produto de dois números algébricos é algébrico.

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

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

Demonstração de (iii): Se α é algébrico, então ele é raiz de uma equação do tipo 3.1 do início deste capítulo. Portanto $-\alpha$ é raiz da equação

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

Demonstração de (iv): Se α satisfaz a equação 3.1, e $\alpha \neq 0$, então α^{-1} satisfaz à equação

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

As demonstrações de (i) e (ii) são mais delicadas. Vamos necessitar de um fato sobre formas lineares com coeficientes racionais. Uma *forma linear* com coeficientes racionais é uma expressão da forma

$$X = q_1 x_1 + ... + q_n x_n,$$

onde $q_1, ..., q_n \in \mathbb{Q}$. (Os x_is são chamados indeterminadas; se o leitor quiser, pense-os como números reais fixados). O resultado sobre formas lineares que necessitaremos é o seguinte.

LEMA 1. *Dadas $n+1$ formas lineares*

$$X_1 = q_{11} x_1 + ... + q_{1n} x_n \vdots X_{n+1} = q_{n+1,1} x_1 + ... + q_{n+1,n} x_n \tag{3.6}$$

elas são linearmente dependentes sobre racionais, isto é, existem $r_1, ..., r_{n+1} \in \mathbb{Q}$, com alguns (ou todos) diferentes de zero, tais que

$$r_1 X_1 + ... + r_{n+1} X_{n+1} = 0. \tag{3.7}$$

A demonstração desse lema pode ser encontrada em diversos livros de álgebra linear.

Demonstração de (i): Seja α e β números algébricos. Logo, existem equações polinomiais

$$x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0 \tag{3.8}$$

$$x^m + b_{m-1}x^{m-1} + ... + b_1x + b_0 = 0 \tag{3.9}$$

com coeficientes racionais (atenção: a equação 3.1 tem coeficientes inteiros; as equações acima são obtidas dividindo-se a equação 3.1 pelo coeficiente líder), tais que α seja raiz de 3.8 e β seja raiz de 3.9. De 3.8 obtemos

$$\alpha^n = -a_{n-1}\alpha^{n-1} - ... - a_1\alpha - a_0, \tag{3.10}$$

isto é α^n está expresso como uma combinação linear de $1, \alpha, ..., \alpha^{n-1}$, usando coeficientes racionais. Multiplicando-se 3.10 por α e substituindo-se o α^n, obtido na expressão pelo seu valor em 3.10, obtemos α^{n+1} expresso como uma combinação linear dos mesmos $1, \alpha, ..., \alpha^{n-1}$, usando-se coeficientes racionais.

De modo análogo podemos exprimir as potências β^k, para $k = m$, $m + 1$,..., como combinações lineares de $1, \beta, ..., \beta^{m-1}$ usando-se coeficientes racionais.

Nosso objetivo agora será mostrar que $\alpha + \beta$ satisfaz uma equação polinomial de grau mn com coeficientes racionais, implicando então que $\alpha + \beta$ seja algébrico. Com isso em vista considere os $mn + 1$ números

$$1, \alpha + \beta, (\alpha + \beta)^2, ..., (\alpha + \beta)^{mn}. \tag{3.11}$$

Desenvolvendo as várias potências, e usando-se o que se viu acima sobre a representação das potências α^j, $j \geq n$ e β^k, $k \geq m$, obtemos que os números em 3.11 podem ser expressos como combinações lineares dos mn números $\alpha^j\beta^k$, $0 \leq j \leq n-1$, $0 \leq k \leq m-1$, usando-se coeficientes racionais. Agora, aplicamos o Lema 1: os X_is são os $mn + 1$ números de 3.11, os x_is são os mn números $\alpha^j\beta^k$. Logo, existem racionais $r_0, r_1, ..., r_{mn}$ tais que

$$r_0 + r_1(\alpha + \beta) + ... + r_{mn}(\alpha + \beta)^{mn} = 0$$

, o que mostra que $\alpha + \beta$ satisfaz uma equação polinomial de grau mn com coeficientes racionais. Terminou a demonstração de (i): soma de algébricos é algébrico.

Demonstração de (ii): Segue as mesmas linhas da demonstração anterior. Em 3.11, entretanto, consideramos as potências

$$1, \alpha\beta, (\alpha\beta)^2, ..., (\alpha\beta)^{mn}$$

.

As propriedades i,ii, iii e iv permitem classificar o conjunto dos números algébricos como um corpo.

Exemplo: Lembrando que $\sqrt{2}$ é raiz de $x^2 - 2 = 0$ e $\sqrt{3}$ é raiz de $x^2 - 3 = 0$, então temos que $\sqrt{2} + \sqrt{3}$ é raiz de $x^4 - 10x^2 + 1 = 0$ e $\sqrt{6}$ é raiz de $x^2 - 6 = 0$.

Nos capítulos a seguir apresentaremos e comprovaremos a transcendência de alguns números reais.

Capítulo 4

O Teorema de Liouville: Nasce a Teoria dos Números Transcendentes

Neste capítulo, tomando como base a referência [13], abordaremos o Teorema de Liouville, que foi resultado que historicamente iniciou a teoria transcendente. Apresentaremos também um classe de números conhecida como números de Liouville e consequentemente, exibiremos o primeiro número comprovadamente transcendente, a constante de Liouville.

4.1 O Teorema de Liouville

A ideia de Liouville para construir números transcendentes era ingênua, mas eficaz: encontrar uma propriedade que é satisfeita por todos os algébricos. Depois, bastava construir um número que não satisfizesse tal propriedade.

Teorema 5.1 (Liouville). *Seja α uma raiz real de um polinômio irredutível $P(x) \in \mathbb{Z}[x]$ de grau $n \geq 2$. Então, existe uma constante positiva $c(\alpha)$ tal que*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n}, \tag{4.1}$$

para todo racional $\frac{p}{q}$. Uma escolha conveniente para essa constante é

$$c(\alpha) := \frac{1}{1 + \max_{|t-\alpha|\leq 1} |P'(t)|}. \tag{4.2}$$

Demonstração. Com a escolha de $c(\alpha)$ em (4.2), se tivermos $|\alpha - \frac{p}{q}| \geq 1$, o teorema é válido pois $1 \geq \frac{c(\alpha)}{q}$. Para o caso $|\alpha - \frac{p}{q}| < 1$, observe que, como $P(x)$ é irredutível sobre $\mathbb{Z}$, ele será irredutível também sobre $\mathbb{Q}$ (Lema de Gauss, referência [13], p. 15) e assim

$P(\frac{p}{q}) \neq 0$, o que implica $|q^n P(\frac{p}{q})| \geq 1$, visto que $q^n P(\frac{p}{q})$ é inteiro não nulo. Pelo Teorema do Valor Médio (referência [6], p. 225), existe $t \in \mathbb{R}$ entre α e $\frac{p}{q}$, tal que

$$\left|P\left(\frac{p}{q}\right)\right| = \left|P(\alpha) - P\left(\frac{p}{q}\right)\right| = \left|\alpha - \frac{p}{q}\right| \cdot |P'(t)|.$$

Portanto

$$q^n |P'(t)| \left|\alpha - \frac{p}{q}\right| = q^n \left|P\left(\frac{p}{q}\right)\right| \geq 1$$

e assim

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{q^n \cdot (1 + |P'(t)|)} \geq \frac{1}{q^n (1 + \max_{|t-\alpha|\leq 1} |P'(t)|)} = \frac{c(\alpha)}{q^n},$$

onde usamos que $|t - \alpha| \leq |\frac{p}{q} - \alpha| \leq 1$.

Podemos dizer que α é uma raiz isolada do intervalo no intervalo considerado na demonstração anterior.

Observe que, por 4.1, a função $f(x) = \frac{c(\alpha)}{x^n}$ é uma medida de irracionalidade para α.

Exemplo 2. Alguns valores particulares de $c(\alpha)$ são:

$$c(\sqrt{3}) = \frac{2\sqrt{3}}{3} - 1 \text{ e } c(\sqrt{2} + \sqrt{3}) = \frac{1}{1 + 24\sqrt{2} + 16\sqrt{3}}$$

.

4.2 Os números de Liouville

Como o conjunto dos números racionais é denso na reta real, então todo número real pode ser aproximado por racionais. no entanto, existem algumas aproximações que são mais efetivas ou "boas", onde podemos estimar de fato o erro da aproximação.

Definição 1. *Um número real α é aproximável na ordem n por racionais, se existirem uma constante $C > 0$ e uma sequência $\left(\frac{p_j}{q_j}\right)_{j\geq 1}$ de racionais distintos, com $q_j > 1$ e $mdc(p_j, q_j) = 1$ tais que*

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{C}{q_j^n}, \tag{4.3}$$

Podemos dizer que um número real é bem aproximado por racionais se é aproximável na ordem n por racionais. indicamos uma leitura ao Capítulo 5 de [5], para uma classificação dos números reais em relação a essa aproximação. Em particular, foi provado em [5] o famoso Teorema de Dirichlet (ou Teorema da Aproximação de Dirichlet, já que existem

vários importantes resultados devidos a Johann Peter Gustav Lejeune Dirichlet): *Se $\alpha \in \mathbb{R}$ é um número irracional, então existem infinitos racionais $\frac{p}{q}$, com $q \geq 1$, tais que*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Este é um dos resultados fundamentais em *aproximação diofantina* (que é o ramo da matemática que estuda a aproximação de números reais por racionais).

Em um certo sentido, o Teorema de Liouville diz que um número algébrico irracional não pode ser *bem aproximado* por racionais. Portanto, Liouville construiu uma classe de números que são muito bem aproximados por racionais.

Definição 2. *Um número real α é chamado número de Liouville se existir uma sequência de racionais $(\frac{p_j}{q_j})_{j\geq 1}$, com $q_j > 1$, tal que*

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j}, \text{ para todo } j \geq 1.$$

O conjunto dos números de Liouville é denotado por $\mathbb{L}$.

Proposição 1. *A sequência $(q_j)_{j\geq 1}$ é ilimitada.*

Demonstração. Suponha o contrário, então existe $M > 0$, tal que $q_j \leq M$, para todos $j \geq 1$. Como $|\alpha - \frac{p_j}{q_j}| < 1$, obtemos

$$|p_j| - |q_j\alpha| < |q_j\alpha - p_j| < q_j,$$

o que implica uma ilimitação para $(p_j)_{j\geq 1}$, pois $|p_j| < (|\alpha| + 1)M$. Mas isso contraria o fato de que a sequência $(\frac{p_j}{q_j})_{j\geq 1}$ ser infinita.

Corolário 1. *Todo número de Liouville é irracional.*

Demonstração. Suponha por absurdo que $\frac{p}{q} \in \mathbb{Q}$ é um número de Liouville. Então existem infinitos $\frac{p_j}{q_j}$, diferentes de $\frac{p}{q}$, tais que

$$\frac{1}{q_j^j} > \left|\frac{p}{q} - \frac{p_j}{q_j}\right| = \left|\frac{pq_j - p_jq}{qq_j}\right| \geq \frac{1}{|q|q_j}.$$

Assim $q_j^{j-1} < |q|$, contrariando a ilimitação de $(q_j)_j$.

Exemplo 1. O número

$$\sum_{n=1}^{\infty} 10^{-n!} = 0.11000100000000000000000010000...$$

é um número de Liouville. Este número é conhecido como a *constante de Liouville*.

Exemplo 2. Generalizando o exemplo anterior, se $b \geq 2$ é um inteiro, então $\alpha = \sum_{n=0}^{\infty} a_n b^{-n!}$ é um número de Liouville, para toda escolha de $a_n \in \{1, ..., b-1\}$. De fato, escolha $q_j = b^{j!}$ e $p_j = \sum_{n=1}^{j} a_n b^{j!-n!}$. Então

$$\begin{aligned} \left|\alpha - \frac{p_j}{q_j}\right| &= \sum_{n=j+1}^{\infty} a_n b^{-n!} \leq (b-1) \sum_{n=j+1}^{\infty} b^{-n!} \\ &< (b-1) \sum_{n=j+1}^{\infty} b^{-n!} = \frac{b}{b^{(j+1)!}} < \frac{1}{q_j^j}. \end{aligned}$$

O próximo resultado consolida o método de Liouville

Teorema 2. *Todo número de Liouville é transcendente.*

Demonstração. Pelo corolário 1, um número de Liouville α não pode ser racional. Daí suponha que α é algébrico de grau $n > 1$. Então pelo Teorema 1 segue-se que a relação 4.1 será válida para todo número racional. Em particular, para os $\frac{p_j}{q_j}$ da definição 2. Assim, teríamos

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

Daí, $q_j^{j-n} < \frac{1}{c(\alpha)}$, para todo $j \geq 1$, contrariando a ilimitação da sequência $(q_j^{j-n})_j$. Portanto α não pode ser algébrico.

Como consequência imediata, os números nos exemplos 2 e 3 são transcendentes.

Uma pergunta bem perspicaz é se a recíproca do teorema anterior é verdadeira, isto é, existem números transcendentes que não são números de Liouville? A resposta é sim! Um exemplo de número transcendente que não é de Liouville é o número e. Esta comprovação pode ser encontrada em [8], pp. 13-14.

Capítulo 5

Um Pouco Mais Sobre Mundo Transcendente

Neste penúltimo capítulo, tendo como referências [8], [13] e [14], exibiremos alguns dos mais importantes resultados da teoria transcendente. Começando pela transcendência dos números e e π vistas como consequências do teorema de Hermite-Lindemann. Serão também apresentados algumas operações entre transcendentes, além de outros poderosos resultados como por exemplo o teorema de Gelfond-Schneider, o teorema de Baker e o mais famoso problema em aberto, a conjectura de Schanuel. Em todo texto deste capítulo, $\log x$ denotará o logaritmo natural de x, ou seja, o logaritmo na base e.

5.1 A transcendência de π e de e

Em 1873 , Charles Hermite estabeleceu a transcendência do número e, e em 1884, Ferdinand Von Lindemann generalizou os métodos de Hermite e provou que e^{α} é transcendente para todo α algébrico não nulo. A consequência mais relevante desse teorema é a transcendência do π.

5.1.1 O teorema de Hermite-Lindemann

Teorema 1 (Hermite-Lindemann). *Se $\alpha_1, ..., \alpha_m$ são números algébricos distintos, então $e^{\alpha_1}, ..., e^{\alpha_m}$ são linearmente independentes sobre o corpo dos números algébricos.* (Uma demonstração pode ser vista na referência [13], apêndice A).

Quando $m = 2$, $\alpha_1 = 0$ e $\alpha_2 = \alpha \in \overline{\mathbb{Q}}$, não nulo, nós obtemos o seguinte caso particular que é conhecido como Teorema de Lindemann.

Corolário 1 *Se α é algébrico não nulo, então e^{α} é transcendente.*

Existe uma formulação equivalente ao Teorema de Hermite-Lindemann que é chamado Teorema de Lindemann-Weierstrass.

Teorema 2 (Lindemann-Weierstrass). *Se $\alpha_1, ..., \alpha_n$ são números algébricos linearmente independentes sobre $\mathbb{Q}$, então $e^{\alpha_1}, ..., e^{\alpha_n}$ são algebricamente independentes*[1]*.*

A seguir apresentaremos consequências importantes do teorema de Hermite-Lindemann.

Proposição 1. *Os seguintes números são transcendentes:*

1. e;

2. $\sin\alpha$, $\cos\alpha$, $\tan\alpha$, $\sinh\alpha$, $\cosh\alpha$, $\tanh\alpha$, *para todo* $\alpha \in \overline{\mathbb{Q}}^*$;

3. π;

4. $\log\alpha$, $\arcsin\alpha$, *e em geral as funções inversas do item (2), para todo* $\alpha \in \overline{\mathbb{Q}}$, $\alpha \notin \{0, 1\}$.

Para demonstrações específicas da transcendência de e e de π, sugerimos uma leitura dos capítulos 6 e 7 da referência [5].

Demonstração. (1) Faça $\alpha = 1$ no Teorema de Lindemann.

(2) Note que,

$$\begin{aligned}
2i(\sin\alpha)e^0 + (-1)e^{i\alpha} + e^{-i\alpha} &= 0,\\
2(\cos\alpha) + (-1)e^{i\alpha} + (-1)e^{-i\alpha} &= 0,\\
(i\tan\alpha - 1)e^{i\alpha} + (i\tan\alpha + 1)e^{-i\alpha} &= 0,\\
2(\sinh\alpha)e^0 + (-1)e^{\alpha} + e^{-\alpha} &= 0,\\
2(\cosh\alpha)e^0 + (-1)e^0 + (-1)e^{-\alpha} &= 0,\\
(\tanh\alpha - 1)e^{\alpha} + (\tanh\alpha + 1) &= 0.
\end{aligned}$$

Supondo $\alpha \neq 0$, então $i\alpha \neq 0$. Portanto, pelo Teorema de Hermite-Lindemann,

$$\sin\alpha,\ \cos\alpha,\ \tan\alpha,\ \sinh\alpha,\ \cosh\alpha,\ \tanh\alpha,$$

[1]Em álgebra abstrata, um subconjunto S de um corpo L é algebricamente independente sobre um subcorpo K se os elementos de S não satisfazem nenhuma equação polinomial não-trivial com coeficientes em K. Isto significa que para toda série finita $\alpha_1, ..., \alpha_n$ de elementos de S, não sendo dois idênticos, e todo polinômio distinto de zero $P(x_1, ..., x_n)$ com coeficientes em K, temos $P(\alpha_1, ..., \alpha_n) \neq 0$. Em particular, um conjunto de um elemento α é algebricamente independente sobre K se e somente se α é transcendente sobre K.

são números transcendentes.

(3) Se π fosse algébrico, então $i\pi \in \overline{\mathbb{Q}}^*$. Logo, $e^{i\pi}$ é transcendente, mas $e^{i\pi} = -1$. Portanto, π é transcendente.

(4) Suponha que $\log \alpha \in \overline{\mathbb{Q}}$. Pelo Teorema Lindemann $e^{\log \alpha}$ é transcendente, mas $e^{\log \alpha} = \alpha \in \overline{\mathbb{Q}}$, essa contradição mostra que $\log \alpha \notin \overline{\mathbb{Q}}$. De modo análogo, usando o item (2), mostramos que as funções inversas das funções do item (2) assumem valores transcendentes em $\alpha \in \overline{\mathbb{Q}} - \{0, 1\}$.

Observação: Não se conhece se o conjunto $\{\pi, e\}$ é algebricamente independente sobre $\mathbb{Q}$.

5.2 Soma e produto de números transcendentes

Apresentaremos a seguir alguns resultados operatórios envolvendo números transcendentes. As seguintes questões são levantadas na referência [13], p. 78.

Fato 1: Sejam α e β números transcendentes, então pelo menos um dos números $(\alpha+\beta)$ ou $(\alpha - \beta)$ é transcendente.

Demonstração: Suponha que $(\alpha + \beta)$ e $(\alpha - \beta)$ sejam ambos algébricos, logo a soma desses números, que resulta em 2α, teria que ser algébrico pois o conjunto dos números algébricos é um corpo, porém, 2α é transcendente, contradição. Portanto pelo menos um desses números $(\alpha + \beta)$ e $(\alpha - \beta)$ é transcendente.

Observe que fazendo $\alpha = \pi$ e $\beta = e$, temos que pelo menos um dos números $(\pi + e)$ ou $(\pi - e)$ é transcendente. Na verdade, provar a transcendência de cada um desses números ainda é um problema em aberto.

Fato 2: Sejam α e β números transcendentes, então pelo menos um dos números $(\alpha+\beta)$ ou $(\alpha \cdot \beta)$ é transcendente.

Demonstração: Suponha que $(\alpha + \beta)$ e $(\alpha \cdot \beta)$ sejam ambos algébricos, e sabemos dos estudos de produtos notáveis que: $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta$ o que implica que $\alpha^2 + \beta^2$ é algébrico pois é resultado da diferença entre dois algébricos já que por hipótese $(\alpha + \beta)$ e $(\alpha\beta)$ são algébricos logo, $(\alpha + \beta)^2 = (\alpha + \beta)(\alpha + \beta)$ e $(2\alpha\beta)$ também são algébricos devido as propriedades de corpo.

Temos também a seguinte relação:

$(\alpha-\beta)^2 = \alpha^2+\beta^2-2\alpha\beta$ o que implica que $(\alpha-\beta)^2$ é algébrico pois resulta da diferença

de dois algébricos $\alpha^2 + \beta^2$ (provado anteriormente) e $2\alpha\beta$ consequência da hipótese. Como $(\alpha - \beta)^2$ é algébrico, consequentemente temos que a raiz quadrada desse número também é algébrico (o módulo também seria), portanto $(\alpha - \beta)$ também seria algébrico, o que contraria o Fato 1 pois teríamos $(\alpha + \beta)$ e $(\alpha - \beta)$ ambos algébricos, logo, pelos menos um dos números $(\alpha + \beta)$ ou $(\alpha\beta)$ é transcendente.

Observe que fazendo $\alpha = \pi$ e $\beta = e$, temos agora que pelo menos um dos números $(\pi + e)$ ou (πe) é transcendente.

Fato 3: Sejam α, β, e θ ambos transcendentes, será que sempre teremos pelo menos um dos números $(\alpha + \beta + \theta)$ ou $(\alpha\beta\theta)$, transcendente?

A resposta é não! Pois basta tomar $\alpha = e + i\sqrt{\frac{27}{e} - e^2}$, $\beta = \alpha = e - i\sqrt{\frac{27}{e} - e^2}$, (onde $i = \sqrt{-1}$) e $\theta = -2e$ que teremos os seguintes resultados: $(\alpha + \beta + \theta) = 2e - 2e = 0$ $(\alpha\beta\theta) = (e^2 + \frac{27}{e} - e^2)(-2e) = -54$.

Ambos os resultados são algébricos.

Observação: Apesar de estarmos tratando de números reais, o conceito de número algébrico pode ser estendido para os complexos e ressaltamos que um número complexo é transcendente quando pelo menos a parte real ou a parte imaginária é um número transcendente.

Por fim vamos ao último fato.

Fato 4: Sejam α, β, θ e λ ambos números transcendentes, será que sempre teremos pelo menos um dos números $(\alpha + \beta + \theta + \lambda)$ ou $(\alpha\beta\theta\lambda)$, transcendente?

A resposta também é não. Basta tomar $\alpha = \pi$, $\beta = -\pi$, $\theta = \frac{1}{\pi}$ e $\lambda = -\frac{1}{\pi}$ que teremos os seguintes resultados:

$$\begin{cases} (\alpha + \beta + \theta + \lambda) = 0, \\ (\alpha\beta\theta\lambda) = 1. \end{cases}$$

5.3 O Teorema de Gelfond-Schneider

Em 1900, no Congresso Internacional de Matemática em Paris, o matemático alemão David Hilbert propôs uma lista de 23 problemas. Até esse momento todos eram problemas abertos, e vários deles acabaram se tornando muito influentes na matemática do século XX. O sétimo prblema de Hilbert pergunta se o número α^β, onde α é algébrico (diferente de zero e um) e β é algébrico (não racional), é transcendente. Essa questão foi resolvida em 1934 por A. O. Gelfond e independentemente em 1935 por T. Schneider.

Teorema 1. *(Gelfond-Schneider) Seja* $\alpha \in \bar{\mathbb{Q}} - \{0,1\}$ *e* $\beta \in \bar{\mathbb{Q}} - \mathbb{Q}$. *Então* α^β *é transcendente.* (Uma demonstração pode ser vista na referência [13], apêndice B).

Resultados imediatos:

Os números: $2^{\sqrt{2}}$ (constante de Gelfond-Schneider), i^i e $\sqrt[3]{7}^{\sqrt{10}}$ são transcendentes.

Note-se que β não pode ser racional ou transcendente: se β for racional, então α^β será algébrico; do mesmo modo, existem valores transcendentes de β (por exemplo, $\beta = \log_\alpha 10$ $\beta = \log_\alpha 10$) para os quais $\alpha^\beta \alpha^\beta$ será algébrico (nesse exemplo, $\alpha^\beta = 10$ $\alpha^\beta = 10$).

Corolário 1. e^π *é transcendente.*

Demonstração. Como $e^{\pi i} = -1$ (relação de Euler), então $(e^{\pi i})^{-i} = (-1)^{-i}$, logo $e^\pi = (-1)^{-i}$ é transcendente pelo Teorema de Gelfond-Schneider.

Teorema 2. *Dados* α_1, α_2, $\beta 1$ *e* $\beta_2 \in \overline{\mathbb{Q}^*}$, *se* $\log \alpha_1$, $\log \alpha_2$ *linearmente independentes sobre* $\mathbb{Q}$. *Então*

$$\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 \neq 0.$$

Vamos provar a equivalência, suponhamos o Teorema de Gelfond-Schneider e sejam α_1, α_2, $\beta 1$ e $\beta_2 \in \overline{\mathbb{Q}^*}$, com

$$\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 = 0$$

e $\log \alpha_1$, $\log \alpha_2$ linearmente independentes sobre $\mathbb{Q}$, então temos que $(\frac{\beta_1}{\beta_2} \log \alpha_1 = -\log \alpha_2)$, ou seja, $\alpha^{(\frac{\beta_1}{\beta_2})} = -\alpha^{-1} \in \overline{\mathbb{Q}}$, então por G.-S. temos que $(\frac{\beta_1}{\beta_2}) \in \mathbb{Q}$, o que contraria a hipótese que $\log \alpha_1$, $\log \alpha_2$ linearmente independentes sobre $\mathbb{Q}$, logo

$$\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 \neq 0.$$

Reciprocamente, suponha o Teorema anterior e sejam $\alpha \in \overline{\mathbb{Q}} - \{0,1\}$ e $\beta \in \overline{\mathbb{Q}} - \mathbb{Q}$, suponha que $\gamma = \alpha^\beta \in \overline{\mathbb{Q}}$, então

$$\log \gamma - \beta \log \alpha = 0,$$

logo $\beta \in \mathbb{Q}$ pelo Teorema anterior, o que é uma contradição, pois supomos que $\beta \in \overline{\mathbb{Q}} - \mathbb{Q}$, logo $\alpha^\beta \notin \overline{\mathbb{Q}}$, o que completa a demonstração da equivalência.

5.4 O Teorema de Baker

Vimos na formulação equivalente ao Teorema de Gelfond-Schneider que para α_1, α_2 números algébricos não nulos, sua independência linear sobre $\mathbb{Q}$ e $\overline{\mathbb{Q}}$ são equivalentes. Foi

conjecturado que esse resultado seria válido para uma quantidade arbitrária de logaritmos. Essa conjectura foi provada por A. Baker em 1966 (e lhe rendeu a medalha Fields em 1970).

Teorema 1. (Baker). *Dados* $\alpha_1, ..., \alpha_n$ *números algébricos, não nulos, tais que* $\log \alpha_1$,..., $\log \alpha_n$ *são linearmente independentes sobre* $\mathbb{Q}$. *Então* 1, $\log \alpha_1$,...,$\log \alpha_n$ *são linearmente independentes sobre* $\overline{\mathbb{Q}}$. (Uma demonstração pode ser vista na referência [13], apêndice C).

Vamos apresentar uma das importantes consequências do Teorema de Baker.

Teorema 2. *Dados* $\alpha_1, ..., \alpha_n$ *números algébricos, não nulos, e* $\beta_1, ..., \beta_n$ *números algébricos tais que*

$$\gamma = \beta_1 \log \alpha_1 + ... + \beta_n \log \alpha_n \neq 0.$$

Então γ *é um número transcendente.*

Demonstração: Basta-nos mostrar que se $\alpha_1, ..., \alpha_n, \beta_0, \beta_1, ..., \beta_n$ são números algébricos, com $\alpha_j \neq 0$, $1 \leq j \geq n$ e $\beta_0 \neq 0$. então

$$\beta_0 + \beta_1 \log \alpha_1 + ... + \beta_n \log \alpha_n \neq 0.$$

Procedemos por indução em n. O caso $n = 1$ segue do fato que $\log \alpha$ é transcendente para $\alpha \in \overline{\mathbb{Q}}$ pelo Teorema de Lindemann. Assuma a validade para $n < m$, onde $m \in \mathbb{Z}$; mostraremos então o resultado para $n = m$.

Se $\log \alpha_1, ..., \log \alpha_m$ são linearmente independentes sobre $\mathbb{Q}$, o resultado segue-se do Teorema de Baker. Assim, suponha que existem $\rho_1, ..., \rho_m \in \mathbb{Q}$, não todos os nulos, e tais que

$$\rho_1 \log \alpha_1 + ... + \rho_m \log \alpha_m = 0.$$

Sem perda de generalidade, suponha $\rho_1 \neq 0$. Entretanto, para $\alpha_0 = 0$, temos que

$$\begin{aligned} \rho_1 \sum_{k=0}^{m} \beta_k \log \alpha_k &= \rho_1(\beta_0 +) - \beta_r(\rho_1 \log \alpha_1 + ... + \rho_m \log \alpha_m) \\ &= \beta'_0 + \beta'_1 \log \alpha_1 + ... + \beta'_m \log \alpha_m, \end{aligned}$$

onde

$$\beta'_0 = \rho_r \beta_0, \beta'_j = \rho_r \beta_j - \rho_j \beta_r \text{ para } 1 \leq j \geq m.$$

Daí,

$$\rho_r(\beta_0 + \beta_1 \log \alpha_1 + ... + \beta_m \log \alpha_m) = \beta'_0 + \beta'_1 \log \alpha_1 + ... + \beta'_m \log \alpha_m. \tag{5.1}$$

Note que $\beta'_0 \neq 0$ e $\beta'_r = 0$, então, por hipótese de indução, o lado direito de 5.1 é não nulo e como $\rho_r \neq 0$, segue-se que

$$\beta_0 + \beta_1 \log \alpha_1 + ... + \beta_m \log \alpha_m \neq 0.$$

5.5 A Conjectura de Schanuel

Seja $L\mid_K$ uma extensão transcendente, isto é, $[L:K]=\infty$. Um conjunto $\mathcal{B}\subseteq L$ é dito *base de transcendência* de $L\mid_K$, se $\mathcal{B}$ é algebricamente independente sobre K e $L\mid_{K(\mathcal{B})}$ é uma extensão algébrica, ou equivalentemente, $\mathcal{B}$ é o conjunto algebricamente independente (sobre K) maximal relativo à inclusão, cuja existência é garantida via lema de Zorn. Pode-se provar que quaisquer duas bases de transcendência de uma extensão têm a mesma cardinalidade. Assim podemos definir o *grau de transcendência* de uma extensão $L\mid_K$, como cardinalidade de $\mathcal{B}$. denotamos por grtr$(L\mid_K)$=grtr$_K(L)$= $\#\mathcal{B}$. Se $L\mid_K$ é algébrico, então grtr$(L\mid_K)$= 0.

Vamos agora, usando essa nomenclatura, apresentar a importante Conjectura de Schanuel que diz

Conjectura 1 (Schanuel). *Se $x_1,...,x_n\in\mathbb{C}$ são linearmente independentes sobre $\mathbb{Q}$, então*

$$grtr(\mathbb{Q}(x_1,...,x_n),e^{x_1},...,e^{x_n}\mid_{\mathbb{Q}})\geq n.$$

A Conjectura de Schanuel é, sem dúvida, o grande resultado a ser provado em Teoria Transcendente. A motivação da Conjectura de Schanuel parece vir de alguns resultados já sabidos. Por exemplo, quando $n=1$ temos que se $\alpha\neq 0$, então, pelo Teorema de Lindemann, pelo menos um dos números α e e^{α} é transcendente, assim grtr$(\mathbb{Q}(\alpha,e^{\alpha})\mid_{\mathbb{Q}})\geq 1$. No caso de n arbitrário, essa conjectura está resolvida apenas para $\{x_1,...,x_n\}\subset\overline{\mathbb{Q}}$, usando o Teorema de Lindemann-Weierstrass.

Vamos agora apresentar algumas das implicações da Conjectura de Schanuel, em particular vamos ver que muitos dos números que acreditamos ser números transcendentes, mas ainda não sabemos provar, podem ter a transcendência obtida via Conjectura de Schanuel, além disso vamos ver que os teoremas que enunciamos podem ser vistos como consequência dessa conjectura.

Teorema 1.*Se a Conjectura de Schanuel for verdadeira, então e e π são algebricamente independentes sobre $\overline{\mathbb{Q}}$, em particular $e+\pi$ e $e\pi$ são números transcendentes.*

Demonstração: Suponha que a Conjectura de Schanuel é verdadeira, e considere $x_1=1$ e $x_2=i\pi$, temos que x_1 e x_2 são linearmente independentes sobre $\overline{\mathbb{Q}}$, esse fato segue

diretamente da transcendência de π, logo

$$\begin{aligned} 2 &\leq grtr(\mathbb{Q}(1, i\pi, e, e^{i\pi})) \\ &= grtr(\mathbb{Q}(1, i\pi, e, -1)) \\ &= grtr(\mathbb{Q}(\pi, e)) \\ &\leq 2 \end{aligned}$$

donde e, π são algebricamente independentes, ou seja, $p(e, \pi) \notin \mathbb{Q}$ para todo $p(x, y) \in \overline{\mathbb{Q}}[x, y] \setminus \{0\}$, em particular, $e\pi$, $e + \pi$ são transcendentes.

Por fim vamos ver, baseados na referência [8], que a Conjectura de Schanuel implica os teoremas clássicos apresentados acima

(I) Conjectura de Schanuel $\Rightarrow$ Teorema de Lidemann-Weierstrass: Essa implicação é imediata tomando $x_1 = \alpha_1, ..., x_n = \alpha_n$. Note que, pela equivalência, temos que a conjectura implica o Teorema de Hermite-Lidemann.

(II) Conjectura de Schanuel $\Rightarrow$ Teorema de Gelfond-Schneider: Nós mostramos que o Teorema de Gelfond-Schneider é equivalente ao Teorema 2 de 5.3, que por sua vez é uma consequência direta da Conjectura de Schanuel tomando $x_1 = \log \alpha_1$, $x_2 = \log \alpha_2$ que, por hipótese, são linearmente independentes em $\overline{\mathbb{Q}}$.

(III) Conjectura de Schanuel $\Rightarrow$ Teorema de Baker: Aqui tomamos $x_1 = \log \alpha_1, ..., x_n = \log \alpha_n$ e o resultado também segue naturalmente.

Então podemos ver que os resultados clássicos, caso a Conjectura de Schanuel se mostre verdadeira, são corolários imediatos dela, o que justifica sua grande importância na Teoria dos Números Transcendentes. Mas é importante ressaltar que a Conjectura de Schanuel não é o passo final nessa teoria, mesmo com a demonstração da conjectura, ainda existem muitos problemas em aberto, como por exemplo os números $\zeta(2n+1)$, para $n > 1$ (imagens de valores ímpares da função zeta de Riemann, referência [13], p. 4). Com isso queremos deixar mais do que um pequeno histórico de uma teoria, mas com um convite, um convite a essa teoria relativamente recente, porém, com grandes desafios.

5.6 Novamente sobre o teorema de Gelfond-Schneider

Levantaremos agora, com base na empolgante referência [11], algumas questões a respeito das raízes da equação $2^x = x^2$ e mostraremos uma aplicação do teorema de Gelfond-

Schneider em tal questão.

Exemplo 1. *Quais são as raízes da equação* $2^x = x^2$*?*

Duas dessas raízes são evidentes: $x = 2$ e $x = 4$. Mas, traçando os gráficos das funções $y = 2^x$ e $y = x^2$, constatamos que há uma raiz negativa, como se vê na figura 5.1.

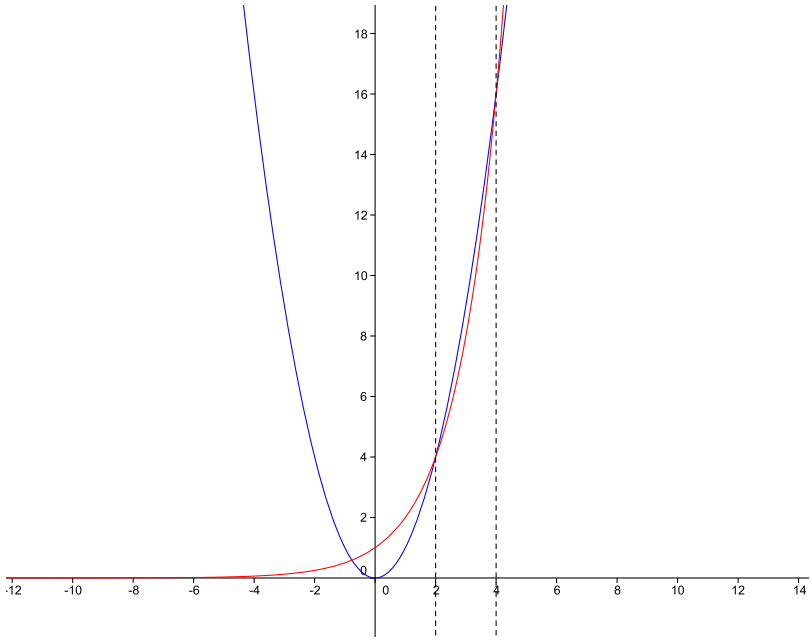

Figura 5.1:

Prosseguindo a análise, são inevitáveis as seguintes perguntas:

1º) Tal raiz é um número racional ou irracional?

2º) É possível obtê-la por um processo puramente algébrico?

O problema de determinar as raízes da equação $2^x = x^2$ me tem sido proposto várias vezes, em diferentes ocasiões. A curiosidade que ele suscita talvez se deva ao fato de que as pessoas se sentem inseguras quando, para resolver uma equação, precisam apelar para os execráveis "métodos numéricos".

Estamos condicionados a preferir métodos "algébricos", fórmulas assim a da equação do 2º grau, ou artifícios específicos para cada equação que enfrentamos. Ao adotarmos este ponto de vista, entretanto, estamos esquecendo duas coisas:

a) Uma "fórmula fechada", como a que existe para equações do 2º, 3º e 4º graus, é muitas vezes uma vitória ilusória; nem sequer nos dá uma ideia da ordem de grandeza das coisas;

b) Todo processo de resolução de uma equação recai, mais cedo ou mais tarde, num cálculo numérico que dará o resultado final, com a aproximação desejada.

No caso em questão, a raiz da equação $2^x = x^2$ pode ser obtida, de modo simples, pelo método das aproximações sucessivas, como mostraremos no final desta seção. O resultado é $x = -0,7666646959$, com 10 algarismos decimais exatos.

A primeira resposta é negativa, isto é, a raiz negativa da equação proposta é um número irracional. Isto se prova por absurdo.

Suponhamos que $\frac{p}{q}$ fosse uma fração *irredutível* positiva tal que $2^{-\frac{p}{q}} = (-\frac{p}{q})^2$. Eliminando os denominadores e elevando ambos membros, à potência q, teríamos então $2^p \cdot p^{2q} = q^{2p}$.

Ora, se p for ímpar, o primeiro membro desta última igualdade é um inteiro que contém um número ímpar de fatores iguais a 2 enquanto o segundo membro contém um número par (talvez zero) de fatores 2. Se, entretanto, p for par então q será ímpar, logo o primeiro membro é divisível por 2 mas o segundo não é. De qualquer maneira, tem-se uma contradição: não existe número racional $r = \frac{p}{q} > 0$ tal que $2^{-r} = (-r)^2$.

A segunda pergunta equivale a indagar se a nossa solução negativa é um número algébrico.

A resposta à segunda pergunta também é NÃO. A raiz negativa da equação $2^x = x^2$ não pode ser obtida por métodos puramente algébricos porque é um número transcendente.

Para provar isto, vamos ter que utilizar o Teorema de Gelfond-Schneider, que relembrando o enunciado, nos diz o seguinte:

Se a, b são números algébricos e b é irracional, então a^b é transcendente (exceto, evidentemente, quando $a = 0$ ou $a = 1$).

Ora, 2 é claramente algébrico e, como vimos, a raiz negativa x de nossa equação é irracional. Se fosse algébrico então, pelo Teorema de Gelfond-Schneider, 2^x seria transcendente. Mas se x é algébrico, x^2 também será. Logo não pode ser $2^x = x^2$.

Agora vejamos como calcular numericamente a raiz negativa da equação $2^x = x^2$:

Consideremos a função $f : [0, +\infty) \to [0, +\infty)$, definida por $f(x) = 2^{-\frac{x}{2}}$. Se o número $a \geq 0$ for tal que $f(a) = a$, então $-a$ será a raiz negativa de $2^x = x^2$.

Para resolver equações da forma $f(x) = x$, existe um método, chamado "das aproximações sucessivas", que funciona muito bem quando a derivada da função f cumpre uma condição do tipo $|f'(x)| \leq \lambda < 1$, onde λ é constante.

No nosso caso, temos $f'(x) = \frac{1}{2} \log 2 \cdot e^{-\frac{x}{2}}$. Olhando numa tabela, vemos que o logaritmo natural de 2 é $0,69$. Logo, podemos escrever $\lambda = \dfrac{\log 2}{2}$ e ter certeza de que $0 < \lambda < 1$.

Portanto $|f'(x)| \leq \lambda < 1$ para todo $x \geq 0$.

O "método das aproximações sucessivas"opera assim: começamos como qualquer número $x_0 \geq 0$. A sequência de aproximações sucessivas

$$x_1 = f(x_0), x_2 = f(x_1), ..., x_{n+1} = f(x_n), ...$$

convergirá para um limite $a \geq 0$, o qual é a única solução da equação $f(x) = x$.

Então $-a$ será a única solução negativa de $2^x = x^2$. Usando uma calculadora que tenha a tecla x^y, e começando com $x_0 = 0$, obtemos as aproximações sucessivas

$$\begin{aligned} x_1 &= 1 \\ x_2 &= f(x_1) = 0,7071067811, \\ x_3 &= f(x_2) = 0,7826540277, ..., \\ x_{18} &= 0,7666646959 \end{aligned}$$

e partir daí, vêm $x_{18} = x_{19} = x_{20}$ etc.

Isto significa que aproximações melhores para a solução procurada só podem ser obtidas com 11 ou mais casas decimais, enquanto nossa calculadora só tem 10. Na verdade, x_{18} é uma excelente aproximação para tal raiz; até mesmo exagerada para a maioria dos usos.

Capítulo 6

A Transcendência e a Construção Geométrica

Neste último capítulo citaremos os três problemas clássicos da geometria grega antiga e enfatizaremos a impossibilidade da quadradura do círculo com régua e compasso ao modo grego, comprovada com a transcendência do número π. As referências deste capítulo são [15] e [18].

6.1 Três Problemas Famosos de Construção

A teoria dos números algébricos e transcendentes possibilitou aos matemáticos resolver três problemas geométricos, bem conhecidos, que provinham da antiguidade. Estes três problemas, conhecidos sob os nomes de "duplicação do cubo", "trissecção de um ângulo"e "quadratura do círculo", consistem em efetuar as seguintes construções, usando apenas régua e compasso[1]:

(1) "Duplicar o cubo"significa construir um cubo de volume igual ao dobro do volume de um cubo dado. Apesar de o cubo ser uma figura da geometria do espaço, o problema é, realmente, de geometria plana, pois, tomarmos como unidade de comprimento a aresta do cubo dado 6.1, o problema se reduz à construção de um segmento de comprimento $\sqrt[3]{2}$, porque este seria o comprimento da aresta de um cubo cujo volume fosse o dobro do volume do cubo dado.

[1]K. T. "régua", neste contexto, significa "régua sem escala".

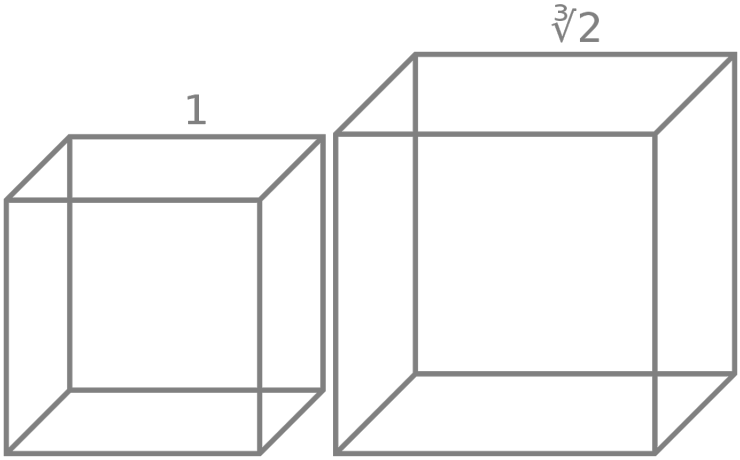

Figura 6.1:

(2) "Trissectar um ângulo"significa descobrir um processo, usando apenas régua e compasso, para dividir qualquer ângulo em três partes iguais. Existem ângulos especiais, como por exemplo os de 45^o e 90^o, que podem ser trissectados apenas com o uso de régua e compasso; mas, o assim chamado, ângulo "geral"não pode ser dividido em três ângulos iguais com os instrumentos permitidos.

(3) "Quadratura do Círculo"significa construir um quadrado cuja área seja igual à de um cubo ou, de modo equivalente, construir um círculo de área igual à de um quadrado dado.

Sabe-se que tais construções são impossíveis, isto é, elas não podem ser efetuadas pelos métodos de construção da Geometria Euclidiana, usando apenas régua e compasso. Muitos amadores continuam tentando encontrar soluções para estes problemas, não sabendo que seus esforços serão em vãos. Apesar de estes amadores estarem cientes que nenhum matemático conseguiu efetuar estas construções, aparentemente eles não sabem que a impossibilidade de tais construções já foi demonstrada. O que muitos dos matemáticos amadores conseguem, de tempo em tempo, é uma solução aproximada de um destes problemas, mas nunca uma solução exata. A distinção aqui é clara: o problema da duplicação do cubo, por exemplo, consiste em descrever uma construção, com instrumentos de desenho teoricamente perfeitos, de um segmento, não de comprimento quase igual a $\sqrt[3]{2}$, mas sim, exatamente igual a $\sqrt[3]{2}$. Não será solução do problema, por exemplo, a construção de um segmento de comprimento $10(8-\sqrt{62})$, apesar de os números $10(8-\sqrt{62})$ e $\sqrt[3]{2}$ coincidirem até a sexta casa decimal.

Um mal-entendido especial ocorre no caso do problema da trissecção de um ângulo. É possível trissectar qualquer ângulo se for permitido fazer marcas na régua. Deste modo, só podemos falar de impossibilidade da trissecção de um ângulo geral, entendendo que os processos de construção permitem apenas o uso de compasso e de uma régua *sem marcas*.

Por causa da considerável confusão que cerca estes três problemas clássicos, daremos agora uma noção, a grosso modo, de como demonstrar a impossibilidade destas construções. Não poderemos dar demonstrações completas porque os detalhes se tornam bastante técnicos. Mesmo assim, esperamos tornar o assunto plausível. Se algum leitor quiser se aprofundar, existe uma apostila completa da trissecção do ângulo e da duplicação do cubo no livro de R. Courant e H. Robbins, "O que é Matemática!". A demonstração da impossibilidade da quadratura de um círculo é muito mais difícil do que as outras duas demonstrações.

Como é possível demonstrar a impossibilidade destas construções? O primeiro passo é obter alguma noção sobre que comprimentos podem ser construídos com régua e compasso, a partir de um comprimento unitário dado. Afirmamos, sem demonstrar (quem estiver familiarizado com construções geométricas perceberá que a afirmação é razoável) que, dentre os comprimentos que podem ser construídos, estão sucessões de raízes quadradas aplicadas a números racionais, como por exemplo,

$$\sqrt{2}, \sqrt{1+\sqrt{2}}, \sqrt{5-3\sqrt{1+\sqrt{2}}}, \sqrt{1+\sqrt{5-3\sqrt{1+\sqrt{2}}}}. \tag{6.1}$$

Estes números são todos algébricos. Os quatro números acima, são raízes, respectivamente, das equações

$$x^2 - 2 = 0 \tag{6.2}$$

$$x^4 - 2x^2 - 1 = 0 \tag{6.3}$$

$$x^8 - 20x^6 + 132x^4 - 320x^2 + 94 = 0 \tag{6.4}$$

$$x^{16} - 8x^{14} + 8x^{12} + 64x^{10} - 98x^8 - 164x^6 + 200x^4 + 224x^2 - 113 = 0 \tag{6.5}$$

Escolhamos uma delas, digamos 6.4, e verifiquemos a afirmação acima. Comecemos com

$$x = \sqrt{5-3\sqrt{1+\sqrt{2}}}.$$

Elevado ao quadrado, obtemos

$$x^2 = 5 - 3\sqrt{1+\sqrt{2}}.$$

Mudando um termo de membro e, novamente, elevando ao quadrado, obtemos

$$\begin{aligned} x^2 - 5 &= -3\sqrt{1+\sqrt{2}}, \\ x^4 - 10x^2 + 25 &= 9 + 9\sqrt{2}, \\ x^4 - 10x^2 + 16 &= 9\sqrt{2} \end{aligned}$$

e, elevado novamente ao quadrado ambos os membros, chegamos a 6.4.

Não apenas são os números 6.1 raízes das equações 6.2 e 6.5, mas nenhum desses números é raiz de algumas equação, com coeficientes inteiros, de menor grau. Consideremos o número $\sqrt{1+\sqrt{2}}$, por exemplo. Ele satisfaz a eq. 6.4 de grau 4, mas não satisfaz nenhuma equação de grau 3, 2 ou 1, com coeficientes inteiros. (Não vamos provar esta afirmação.) Sempre que um número algébrico for raiz de uma equação de grau π, com coeficientes inteiros, dizemos tratar-se de um número *algébrico de grau n*. Assim, os números 6.1 são números algébricos de graus 2, 4, 8 e 16, respectivamente. Isto sugere o seguinte fato básico sobre comprimentos que podem ser construídos pelos métodos da Geometria Euclidiana.

Teorema 1 (Sobre Construções Geométricas). *Começando com um segmento de comprimento unitário, qualquer comprimento que possa ser construído com régua e compasso é um número algébrico de grau* 1*, ou* 2*, ou* 4*, ou* 8*, ..., isto é, um número algébrico de grau igual a um potência de* 2*.*

Se o leitor aceitar a validade deste resultado, poderemos mostrar porque as três famosas construções são impossíveis[2].

Comecemos com a duplicação do cubo. Como vimos, ao enunciar o problema, trata-se de construir um segmento de comprimento $\sqrt[3]{2}$ a partir de um segmento unitário. Mas será que $\sqrt[3]{2}$ é um comprimento construtível? Ele satisfaz a equação

$$x^3 - 2 = 0 \tag{6.6}$$

e isto sugere ser $\sqrt[3]{2}$ um número algébrico de grau 3. De fato isto é assim e para demonstração basta verificar que $\sqrt[3]{2}$ não satisfaz nenhuma equação de grau 1 ou 2, com coeficientes inteiros. Apesar de a demonstração não ser difícil, ela é um pouca artificiosa e vamos deixá-la para a próxima seção.

Sendo $\sqrt[3]{2}$ um número algébrico de grau 3, pelo Teorema Sobre Construções Geométricas, enunciado acima, ele não será construtível. Daí concluímos ser impossível duplicar o cubo.

[2]O leitor deverá lembrar que este teorema implica o seguinte: números algébricos de grau n, onde n não é uma potência de 2, *não* são construtíveis com régua e compasso; também números transcendentes não são construtíveis com régua e compasso.

Consideremos, a seguir, o problema da trissecção de um ângulo. Para mostrar que a trissecção é impossível, basta mostrar que um certo ângulo não pode ser trissectado com o uso somente de régua e compasso. O ângulo específico que vamos considerar é o de 60^o. Trissectar um ângulo de 60^o significa construir um ângulo de 20^o, o que, por sua vez, consiste em construir, a partir de um dado segmento unitário, um segmento de comprimento igual a $\cos 20^o$. Para ver isto, consideremos um triângulo de base 1, cujos ângulos de base sejam 60^o e 90^o, como na 6.2. Temos, assim, um triângulo ABC, com base $AB = 1$, ângulo $BAC = 60^o$, ângulo $ABC = 90^o$. No lado AC escolhamos o ponto D tal que o ângulo $DAB = 20^o$. Da trigonometria elementar, sabemos que

$$AD = \frac{AD}{1} = \frac{AD}{AB} = \sin 20^o.$$

Portanto, a trissecção de um ângulo de 60^o se resume na construção de um segmento

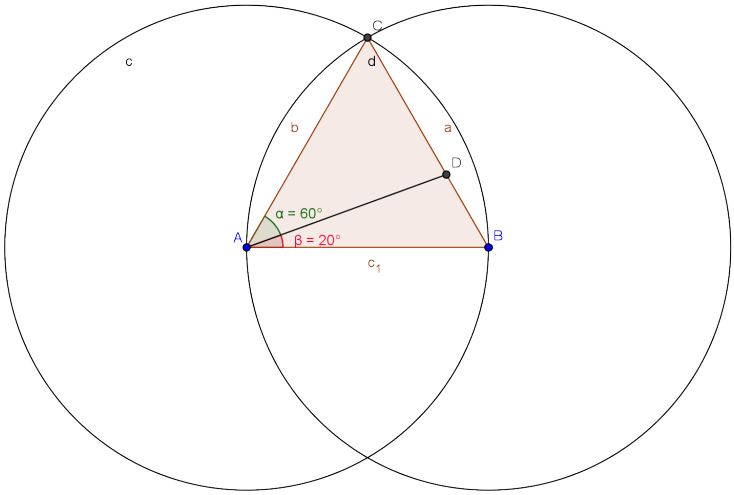

Figura 6.2:

de comprimento igual a $\sec 20^o$, o que, por sua vez, equivale a construir um segmento de comprimento $\cos 20^o$ porque $\cos 20^o$ e $\sec 20^o$ são recíprocos um do outro e sabe-se bem que se um segmento for construtível, o segmento de comprimento recíproco também o será.

Então a questão passa a ser: Pode-se construir um segmento de comprimento $\cos 20^o$ a partir de um segmento dado de comprimento 1? Sabemos que $\cos 20^o$ é raiz de uma equação $8x^3 - 6x - 1 = 0$ (consequência da relação fundamental trigonométrica e da fórmula do arco triplo), isto é, de uma equação de grau 3. Além do que, afirmamos (sem demonstrar, pois trata-se de um resultado mais profundo) que $\cos 20^o$ não satisfaz nenhuma equação de grau 1 ou 2, com coeficientes de grau 3 e pelo Teorema Sobre Construções Geométricas, $\cos 20^o$

não é construtível. Assim, a trissecção de um ângulo de 60º, com régua e compasso, é impossível.

Finalmente, consideremos o problema da quadratura do círculo. Dado um círculo qualquer, podemos considerar seu raio como unidade de comprimento. Com essa unidade, a área do círculo será π unidades de área. Um quadrado de mesmo tamanho teria lado de comprimento $\sqrt{\pi}$. Portanto o problema da quadratura do círculo consiste em construir um segmento de comprimento $\sqrt{\pi}$ a partir de um comprimento unitário dado. Na teoria das construções geométricas é bem conhecido que se pode construir um segmento de comprimento a^2 a partir de segmentos de comprimentos 1 e a. Portanto, se fosse possível construir um segmento de comprimento $\sqrt{\pi}$ também seria possível construir um segmento de comprimento π.

Mas, no capítulo anterior verificamos que π é um número transcendente, isto é, π não é um número algébrico. O Teorema Sobre Construções Geométricas diz ser impossível a construção de um segmento de comprimento π. Portanto, a construção necessária para a "quadratura do círculo"é impossível.

Bibliografia

[1] ÁVILA, Geraldo; **Olhando mais de Cima: Eudoxo, Dedekind, Números Reais e Ensino de Matemática**. Revista do Professor de Matemática, Rio de Janeiro, RJ, n.7, p.5-10,1985.

[2] ÁVILA, Gerald;. **Introdução à Análise Matemática**. Ed. Edgard Blücher, 1999.

[3] BOYER, Carl Benjamin; **História da matemática**. 11. ed. São Paulo: Edgard Blucher, 1974.

[4] DANTAS, Marcelo Rodrigues Nunes; **Sobre o número Pi**. Dissertação de Mestrado Profissional - PROFMAT, CCEN-UFPB, 63 p. João Pessoa-PB: UFPB, 2013.

[5] FIGUEIREDO, D. G.; **Números Irracionais e Transcendentes**, 3ª ed., Rio de Janeiro: SBM, 2011.

[6] GUIDORIZZI, Hamilton Luiz; **Um curso de cálculo**. Vol. 1, 5ª ed. Rio de Janeiro: Livros Técnicos e Científicos, 2001.

[7] HEFEZ, Abramo; Curso de Álgebra. Vol.2. **Coleção Matemática Universitária**. Rio de Janeiro: SBM-IMPA, 2002.

[8] LAFETÁ, Anna Carolina; SILVA, Elaine; LELIS, Jean. **Teoria dos números transcendentes: do teorema de Liouville à conjectura de Schanuel**. Rio de Janeiro: SBM-IMPA, 2016.

[9] LIMA, Elon Lages; CARVALHO, Paulo Cezar Pinto; WAGNER, Eduardo; MORGADO, Augusto César. A Matemática do Ensino Médio. Vol. 1, 9ª ed. **Coleção do Professor de Matemática**. Rio de Janeiro: SBM-IMPA, 2006.

[10] LIMA, Elon Lages; Análise Real. Funções de Uma variável, vol.1, 9ª ed., **Coleção Matemática Universitária**, Rio de janeiro: IMPA, 2007.

[11] LIMA, Elon Lages; **Meu Professor de Matemática e outras histórias**, 6ª Ed., Rio de Janeiro: SBM, 2012.

[12] LIMA, Elon Lages; **Curso de Análise**, 14ª Ed., Rio de Janeiro: IMPA, Volume 1. 2013.

[13] MARQUES, D.; **Teoria dos Números Transcendentes**, 1ª ed., Rio de Janeiro: SBM, 2013.

[14] MURTY, M. Ram; RATH, Purusottam; **Transcendental Numbers**. New York: Springer, 2014.

[15] NÍVEN, Ivan; **Números: Racionais e Irracionais**. Coleção Fundamentos da Matemática Elementar. 1.ed. Rio de Janeiro, RJ: Sociedade Brasileira de Matemática, 1984.

[16] SILVA, Elaine Cristine de Souza; **Alguns resultados relacionados a números de Liouville**. Dissertação de mestrado, PPGM da UNB, 74 p. Brasília: UNB, 2015.

[17] VASCONCELOS, Getúlio de Assis; **A Irracionalidade e Transcendência do Número** e, Dissertação de Mestrado Profissional-PROFMAT, Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas. 39p., Rio Claro-SP:UNESP,2013.

[18] WAGNER, E.; **Construções Geométricas**. 6ª edição. Coleção do Professor de Matemática. Rio de Janeiro: SBM , 2007.