Universidade Federal de Viçosa

Dissertação de Mestrado

Naiara Aparecida de Faria

# Um estudo sobre Números Irracionais e Transcendentes

Florestal
Minas Gerais – Brasil
2019

Naiara Aparecida de Faria

# UM ESTUDO SOBRE NÚMEROS IRRACIONAIS E TRANSCENDENTES

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título *Magister Scientiae*.

Florestal
Minas Gerais – Brasil
2019

**Ficha catalográfica preparada pela Biblioteca da Universidade Federal de Viçosa - Câmpus Florestal**

T

F155e
2019

Faria, Naiara Aparecida de, 1991-
Um estudo sobre números irracionais e transcendentes / Naiara Aparecida de Faria. – Florestal, MG, 2019.
viii, 68f. ; 29 cm.

Inclui anexo.
Orientador: Danielle Franco Nicolau Lara.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f. 68.

1. Matemática: Estudo e ensino. 2. Números irracionais. 3. Números transcendentes. I. Universidade Federal de Viçosa. Instituto de Ciências Exatas e Tecnológicas. Mestrado Profissional em Matemática. II. Título.

512.7

NAIARA APARECIDA DE FARIA

# UM ESTUDO SOBRE NÚMEROS IRRACIONAIS E TRANSCENDENTES

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título *Magister Scientiae*.

APROVADA: 26 de fevereiro de 2019.

Jeanne Carmo Amaral Dias

Luiz Gustavo Perona
(Coorientador)

Danielle Franco Nicolau Lara
(Orientadora)

# Dedicatória

Dedico esse trabalho aos meus familiares, ao meu noivo, e aos meus amigos do PROFMAT.

# Agradecimentos

Primeiramente a Deus que permitiu que tudo isso acontecesse, ao longo da minha vida.

Aos meus pais, Geraldo Magela de Faria e Berenice Nazareth de Oliveira Faria, por toda dedicação e o amor incondicional que tiveram comigo, durante esses dois anos.

Ao meu noivo, Henrique Ferreira Teixeira pelo apoio, incentivo, amor e paciência durante essa jornada.

A minha orientadora Dr. Danielle Franco Nicolau Lara, pelo empenho, sabedoria e dedicação.

Aos meus irmãos, Magno, Marília e Vitor pelo carinho e a compreensão.

As minhas amigas e meus familiares, que nos momentos de minha ausência dedicadas ao estudo.

A minha cunhada, Mariana pelo incentivo e o seu carinho.

Ao meu sogro Sirilo, e a minha sogra Maria Tereza, pela sabedoria e o incentivo.

Aos meus colegas de curso, pelo companheirismo e perseverança.

# Biografia

Meu nome é Naiara Aparecida de Faria, nasci no dia 09 de setembro de 1991. Aos três anos de idade, começo a dar os primeiros sinais de que minha profissão não poderia ser outra.

Seria professora quando adulta, pois minhas bonecas eram minhas alunas, e passava o dia todo brincando de escolinha.

Em 2009, quando finalizei o ensino médio, prestei vestibular na Universidade Federal de Viçosa - Campus Florestal, no qual me formei em 2014, onde já lecionava no Instituto Educacional Saber. Durante a graduação participei do projeto "OPAM" (Olhar Pedagógico Para a Aprendizagem em Matemática ), coordenado pela minha orientadora Danielle, no qual tenho muito que agradecer, por me incentivar e colaborar para minha qualificação como docente. Em 2017 iniciei o Mestrado Profissional PROFMAT, na mesma Universidade onde conclui minha graduação. Tenho um enorme carinho por toda a equipe docente da instituição, no qual sempre me acolheu com carinho e amor.

# Resumo

FARIA, Naiara Aparecida de, M.Sc., Universidade Federal de Viçosa, fevereiro de 2019. **Um estudo sobre Números Irracionais e Transcendentes**. Orientadora: Danielle Franco Nicolau Lara. Coorientador: Luiz Gustavo Perona Aráujo.

O presente trabalho tem como objetivo fazer uma abordagem na construção dos conjuntos numéricos, e uma exposição sobre a irracionalidade de certos números reais, a construção dos transcendentes e a transcendência dos números: $\pi$, e o número de Euler $e$. Para melhor entender esse trabalho será feita algumas abordagens de conteúdos da Teoria dos Números (como critérios de divisibilidade, números primos, entre outros) , a teoria de conjuntos (enumerabilidade) e conceitos do Cálculo Diferencial e Integral de uma variável real.

# Abstract

FARIA, Naiara Aparecida de, M.Sc., Universidade Federal de Viçosa, February, 2019. **A study on Irrational and Transcendent Numbers**. Adviser: Danielle Franco Nicolau Lara. Co-adviser: Luiz Gustavo Perona Aráujo.

This assignment aims to make na approach on the construction of the numerical sets, and an exhibition about the irrationality of some certain real numbers, the construction of the trascendents and the transcendence of the numbers : $\pi$ and the Euler number $e$.

To better unsderstand this assignment, some approaches of the content of the Numbers of Theory will be made (such as divisibility criteria, prime numbers, etc) , the sets theory (enumerability) and concepts of Differential and Intefgral Calculus of a real variable.

# Sumário

# 1 Introdução

Os números e a matemática nasceram e se desenvolveram juntos, tanto nas atividades práticas do homem e da sociedade, quanto a formalização dos conjuntos numéricos.

Um marco importante em relação aos números se deu na escola Pitagórica, quando surgiu o problema da incomensurabilidade. Dois segmentos são incomensuráveis, se é possível encontrar uma "parte" que caiba um número inteiro de vezes em ambos. Ainda que cada segmento possa ser dividido em partes muito pequenas, nem sempre dois segmentos são comensuráveis. Este conceito foi estudado por muitos matemáticos, mas não se obteve uma definição formal, para tais números. Foi a primeira vez que apareceu na história os números irracionais. Este trabalho trará um estudo sobre números irracionais, os quais definimos como números reais não racionais. Para entendê-los precisamos compreender o que é um número real e o que significa não ser racional. Portanto é necessário um estudo sobre os conjuntos numéricos. A construção dos Números Inteiros, denotado por $\mathbb{Z}$, e dos Números Racionais, denotado por $\mathbb{Q}$, é realizado pelo uso de classes de equivalências, e os Números Naturais, denotado por $\mathbb{N}$, teve sua construção axiomática. O alemão Richard Dedekind $(1831 - 1916)$ no início de sua carreira como professor, ao lecionar a disciplina de Cálculo Diferencial, percebeu a importância da formalidade de todos os números. A partir desse momento inciou uma pesquisa para a formalização dos Números Reais, desenvolveu o estudo por meio de Cortes, que tem como nome "Corte de Dedekind" e a notação, para o conjunto de todos os cortes, é $\mathbb{R}$, e aos números irracionais, denotamos por $\mathbb{R}\backslash\mathbb{Q}$.

Os números satisfazem algumas propriedades, ao estudá-los podemos classificá-los, por exemplo, como: algébrico ou transcendente. Um número é algébrico se é solução de uma equação de coeficientes inteiros, caso contrário esse número é dito transcendente. Não podemos falar de números irracionais sem estudarmos os números transcendentes, pois são exemplos importantes de números irracionais.

Matemáticos famosos, desde o século XVIII ficaram fascinados com uma parte da teoria dos números: a transcendência de alguns números. A definição de números transcendentes é do século XVIII. Segundo Euler, esses números " transcendem " o poder das operações algébricas. Somente em 1844, Liouville apresentou os primeiros exemplos de um número transcendente. Ele encontrou uma propriedade que era satisfeita por todos os números algébricos, e assim o número que não satisfizesse tal propriedade, seria, necessariamente transcendente.

Alguns anos mais tarde, em 1874, Cantor provou a enumerabilidade do conjunto dos números algébricos, e como consequência, temos que o conjunto dos números transcendentes não é enumerável.

Mostrar que um número é transcendente não é uma tarefa fácil, somente em 1874 que C. Hermite demonstrou a transcendência do número $e$. Em 1882, F. Lindemann demonstrou que o número $\pi$ é transcendente. Embora o número $\pi$ seja a razão do comprimento do círculo com o seu diâmetro, esse número é irracional, como demonstrado por J. H. Lambert, em 1761 pela primeira vez.

A esse campo da teoria dos números transcendentes, grandes matemáticos deram suas contribuições, como : Euler, Liouville, Cantor, Weierstrass, Lindemann, Hermite, Hilbert, Siegel, Lambert, Gelfond, Schneider, Hurwitz, Borel, Mahler, Markoff e Veblen.

Em 1900, foi realizado em Paris, o segundo Congresso Internacional de Matemática, evento em que David Hilbert pronunciou uma conferência, na qual apresentou uma lista de 23 problemas que, ao seu ver, ocupariam os matemáticos das gerações seguintes, alguns desses envolvendo números transcendentes.

Vale ressaltar que, apesar de $\pi$ e $e$ serem transcendentes, ainda hoje não sabemos se $\pi + e$ ou $\pi.e$ são transcendentes, dentre outros números cuja transcendência aparentam ser naturais.

# 2

# Conjuntos Numéricos

Neste capítulo, descreveremos a construção dos conjuntos numéricos como os Naturais, Inteiros, Racionais e Reais.

Os primeiros registros de representação numérica foi em um osso, encontrado em Ishango, na África, e datado entre vinte mil e dez mil anos antes de Cristo. Normalmente, associa-se a história dos números à necessidade de contagem, relacionada a problemas de subsistência, de acordo com [12].

Por volta de 2000 anos antes de Cristo, na Babilônia, eles começaram a realizar cálculos com a base sexagesimal posicional, no qual havia símbolos para representar os 60 números.

Os algarismos arábicos, também chamados indo-árabicos, foram criados e desenvolvidos pela Civilização do Vale do Indo. Considera-se que este sistema de numeração é um dos grandes avanços da área da Matemática. A chegada da numeração indo-arábica à Europa é atribuída ao matemático italiano Leonardo Piza. Entretanto, a formalidade do conjunto dos números naturais ocorreu com os axiomas do italiano Peano somente por volta de 1900.

Para o método axiomático a resposta consta de duas partes: primeiro, simplesmente aceitar alguns termos da teoria sem uma explicação formal de seu significado, os chamados conceitos primitivos, e, introduzir alguns axiomas, ou seja, certas afirmações que são consideradas verdadeiras sem necessidade de demonstração.

## 2.1 Conjunto dos Números Naturais

Nesta seção apresentaremos a construção formal do conjunto dos naturais, feita por volta de 1900, por Peano. Para maiores informações o leitor pode consultar [1].

**Os axiomas:**

$P_1$: zero é um número natural.

$P_2$: Se $a$ é um número natural, então $a$ tem um único sucessor que também é um número natural.

$P_3$: Zero não é sucessor de nenhum número natural.

$P_4$: Dois números naturais que tem sucessores iguais são eles próprios, iguais.

$P_5$: Se uma coleção S de números naturais contém o zero e, também, o sucessor de todo elemento de S, então S é o conjunto de todos os números naturais.

Adotaremos as seguintes notações: 0 para indicar o zero, $s(a)$ para indicar o sucessor de um número natural $a$. Isto posto, os axiomas de Peano, podem assim ser enunciados:

$P_1$: $0 \in \mathbb{N}$;

$P_2$: a $\in \mathbb{N} \Longrightarrow s(a) \in \mathbb{N}$;

$P_3$: $a \in \mathbb{N} \Longrightarrow s(a) \neq 0$;

$P_4$: $s(a) = s(b) \Longrightarrow a = b$;

$P_5$: Se $S \subset \mathbb{N}$ e $0 \in S$. Para todo $a \in S$, tem-se $s(a) \in S$. Então, $S = \mathbb{N}$

O axioma $\mathrm{P}_1$ garante que $\mathbb{N} \neq \varnothing$ . Em $\mathrm{P}_4$ deve-se subentender a unicidade de $s(a)$. Do axioma $\mathrm{P}_4$ decorre que $a \neq b \Longrightarrow s(a) \neq s(b)$, o que é óbvio pois $s(a) = s(b)$ implica $a = b$. O axioma $\mathrm{P}_5$ chama-se axioma da indução completa.

### 2.1.1 Adição no Conjunto dos Números Naturais

A.1 $m + 0 = m$

A.2 $m + s(n) = s(m + n)$

Pela definição acima temos:

1. A soma de um número arbitrário com o zero: $m + 0 = m$.

2. Soma de $m \in \mathbb{N}$ com $s(0)$, que é $m + s(0) = s(m + 0) = s(m)$.

Temos ainda que,

$$m + s(s(0)) = s(m + s(0)) = s(s(m))$$

e assim sucessivamente. A formalização desse processo se dá através do Princípio da Indução e nos mostra que a soma $m + n$ está bem definida, para todo par $m, n$ de números naturais.

De fato, para cada $m$ natural fixado arbitrariamente, definimos o conjunto $S_m = \{n \in \mathbb{N}; m + n$ está bem definida$\}$. Temos que $0 \in S_m$ e se $k \in S_m$, então $s(k) \in S_m$, pois $m + s(k) = s(m + k)$. Logo, pelo quinto axioma de Peano, $S_m = \mathbb{N}$. Como $m$ é arbitrário, $S_m = \mathbb{N}\ \forall\ m \in \mathbb{N}$, ou seja, $m + n$ está definida para todo par $(m,\, n)$ de naturais, o que nos diz que a condição acima definida é de fato uma operação em $\mathbb{N}$.

Em $m + n = p; m$ e $n$ são as parcelas e $p$ a soma. Adotaremos a seguinte notação:

- $s(0) = 1$;

- $s(1) = 2$;

- $s(2) = 3$.

E assim, sucessivamente.

**Proposição 2.1:** Para todo natural $m$, tem-se $s(m) = m + 1$ e $s(m) = 1 + m$. Portanto, $m + 1 = 1 + m$.

*Demonstração.* Para a primeira igualdade, temos de A.1 que $m + 1 = m + s(0) = s(m + 0) = s(m)$. Para a segunda igualdade, consideremos o conjunto $A = \{m \in \mathbb{N}; s(m) = 1 + m\}$. Claramente, $0 \in A$, pois de A.2 $s(0) = 1 = 1 + 0$. Seja $m \in A$. Vamos mostrar que $s(m) \in A$. De fato, como $s(m) = 1 + m$, temos que:

$$s(s(m)) = s(1 + m) = 1 + s(m).$$

Isto é, $s(m) \in A$. Assim, temos $A = \mathbb{N}$. □

**Teorema 2.1:** Sejam $m, n$ e $p$ números naturais arbitrários. As afirmações abaixo são válidas:

1. Existência do elemento neutro aditivo: $0 + n = n + 0 = n$. A demonstração segue diretamente da Definição A.1.

2. Propriedade Comutativa da adição: $n + m = m + n$.

   *Demonstração.* Faremos pelo método de indução sobre $m$.
   Se $m = 0$, temos $n + 0 = 0 + n$.
   Suponhamos que $n + m = m + n$. Observe que, $n + s(m) = s(n + m) = s(m + n) = m + s(n)$. E portanto, é válido a propriedade comutativa. □

3. Propriedade associativa da adição: $m + (n + p) = (m + n) + p$.

   *Demonstração.* Provaremos por indução sobre $p$.
   Se $p = 0$: $m + (n + 0) = m + n = (m + n) + 0$.
   Suponhamos que $(m + n) + r = m + (n + r)$ para algum $r \in \mathbb{N}$. Então, $(m + n) + s(r) = s((m + n) + r) = s(m + (n + r)) = m + s(n + r)$. E portanto, $m + (n + r) = (m + n) + r$ é válido, para todo $r \in \mathbb{N}$. Concluímos assim que é válida a associatividade. □

4. Propriedade do cancelamento da adição: $m + p = n + p \Longrightarrow m = n$

   *Demonstração.* Provaremos por indução sobre $p$.
   Se $p = 0 \Longrightarrow m + 0 = n + 0 \Longrightarrow m = n$.
   Suponhamos que $m + p = n + p \Longrightarrow m = n$, para algum $p \in \mathbb{N}$. Façamos agora: $m + s(p) = n + s(p) \Longrightarrow s(m + p) = s(n + p) \Longrightarrow m + p = n + p$. Logo, $m = n$. □

### 2.1.2 Multiplicação no Conjunto dos Números Naturais

**Definição 2.1:** A multiplicação de dois números, $m$ e $n$, é denotada por $m \cdot n$ e definida da seguinte maneira:

M.1 $m \cdot 0 = 0$

M.2 $m \cdot (n + 1) = mn + m$

Adotaremos a notação de justaposição para a multiplicação:

$$m \cdot n = mn$$

O teorema abaixo nos mostrará as propriedades da multiplicação.

**Teorema 2.2:** Para $m, n$ e $p$ naturais arbitrários, valem as proposições abaixo:

1. Existência do elemento neutro multiplicativo: $1 \cdot n = n \cdot 1 = n$.

   *Demonstração.* Temos que $n \cdot 1 = n(0+1) = n \cdot 0 + n \cdot 1 = 0 + n = n$. Mostraremos por indução em $n$, que $1 \cdot n = n$. Temos : $1 \cdot 0 = 0$, por definição e, sob a hipótese de que $1 \cdot n = n$, obtemos $1 \cdot (n+1) = 1 \cdot n + 1 = n + 1$. □

2. distributividade: $m \cdot (n+p) = mn + mp$ e $(m+n)p = mp + np$.

   *Demonstração.* Mostraremos por indução sobre $p$.
   Se $p = 0$, temos $m \cdot (n+0) = m \cdot n = m \cdot n + 0 = m \cdot n + m \cdot 0$ e $(m+n) \cdot 0 = 0 = 0 + 0 = m \cdot 0 + n \cdot 0$. Suponhamos que $n(m+p) = mn + np$ e $(m+n)p = mp + np$, para algum $p \in \mathbb{N}$. De M.2 temos,

$$\begin{aligned} m(n + (p+1)) &= m((n+p)+1) \\ &= m(n+p) + m \\ &= (mn + mp) + m \\ &= mn + (mp + m) \\ &= mn + (m(p+1)) \end{aligned}$$

   E portanto $m(n+p) = mn + np$, $\forall\ p \in \mathbb{N}$. Analogamente, obtemos que $(m+n)p = mp + np$. □

### 2.1.3 Relação de Ordem no Conjunto dos Números Naturais

Neste capítulo mostraremos a existência de uma relação de ordem em $\mathbb{N}$. Uma relação é dita de ordem em $\mathbb{N}$ se satisfaz as seguintes propriedades:

1. Reflexiva;
2. Anti simétrica;
3. Transitiva.

**Definição 2.2:** Dizemos que $a$ é menor ou igual a $b$ com $a, b \in \mathbb{N}$ se existe $u \in \mathbb{N}$ tal que $b = a + u$, e usamos a seguinte notação: $a \leqslant b$.

Se $b = a + v$, $v \neq 0$, então $a < b$ ($a$ é menor que $b$).

**Teorema 2.3:** Para $a, b$ e $c$ números naturais, valem as propriedades abaixo:

1. $a \leqslant a$, $\forall\ a \in \mathbb{N}$ (Reflexiva)

   Temos que $a = a + 0$, e portanto, $a \leqslant a$.

2. $a \leqslant b$ e $b \leqslant a \Longrightarrow a = b$ (Anti-simétrica)

   Por hipótese $b = a + u$ e $a = b + v$, em que $u, v \in \mathbb{N}$. Sendo assim, $a = (a + u) + v = a + (u + v)$, pela lei do cancelamento $u + v = 0$. daí, $u = v = 0$, e portanto $a = b$.

3. $a \leqslant b$ e $b \leqslant c \Longrightarrow a \leqslant c$ (Transitiva)

   Por hipótese $b = a+u$ e $c = b+v$, em que $u$,$v \in \mathbb{N}$. Sendo assim, $c = a+(u+v)$, concluímos assim que $a \leqslant c$.

4. Para quaisquer $a, b \in \mathbb{N}$, $a \leqslant b$ ou $b \leqslant a$.

   Para cada $b \in \mathbb{N}$ seja $S_b$ o subconjunto de $\mathbb{N}$ formado pelos elementos $n$ para os quais se verifica ao menos uma das seguintes condições:

   $(a)$ existe $u \in \mathbb{N}$ tal que $b = n + u$;

   $(b)$ existe $v \in \mathbb{N}$ tal que $n = b + v$.

   Como para $n = 0$ a sentença $(a)$ se verifica com $u = b$, então $0 \in S_b$. Seja $r \in S_b$. Se $r = b$, então $s(r) = s(b) = b + 1$ e portanto $s(r) \in S_b$, já que verifica $(b)$. Suponhamos agora $b = r + u$, $u \neq 0$; então $u = s(v) = v + 1$, para algum $v \in \mathbb{N}$, e daí, $b = r + (v + 1) = s(r) + v$, ou seja, $s(r)$ satisfaz $(a)$ e portanto pertence a $S_b$. Finalmente, se $r = b + v, v \neq 0$, então $s(r) = s(b+v) = b + s(v)$, o que significa que $s(r) \in S_b$, pois cumpre a condição de $(b)$. Donde $S_b = \mathbb{N}$ e, por isso, para todo $b \in \mathbb{N}$, qualquer que seja o número natural $a$, ou $b = a + u$ ou $a = b + v$. Ou seja, $a \leqslant b$ ou $b \leqslant a$.

5. $a \leqslant b \Longrightarrow a + c \leqslant b + c$, $\forall\ \ c \in \mathbb{N}$ (Compatibilidade da adição)

   Por hipótese $a \leqslant b$, então $b = a + u$, com $u \in \mathbb{N}$. Dado $c \in \mathbb{N}$, temos que $b + c = a + c + u$, e portanto, $a + c \leqslant b + c$.

6. $a \leqslant b \Longrightarrow ac \leqslant bc, \forall c \in \mathbb{N}$ (Compatibilidade com a multiplicação)

   Por hipótese $b = a + u$, para algum $u \in \mathbb{N}$. Donde $bc = (a + u)c = ac + uc$, do que resulta $ac \leqslant bc$.

Assim a relação "$\leqslant$" é uma relação de ordem total em $\mathbb{N}$.

## 2.2 Conjunto dos Números Inteiros

Nesta seção trataremos sobre a construção dos Números Inteiros.

**Números Negativos: Origens**

Os algarismos que usamos hoje em dia surgiram na Índia, no século VII, e sua difusão pelo mundo se deve, em grande parte, aos árabes. A escrita desses símbolos foi se modificando ao longo do tempo, e a forma moderna mal se assemelha à original. Importa, porém que foi da Índia, quando o Ocidente estava mergulhado na estagnação da primeira fase do período medieval. Coube também aos hindus a introdução na matemática dos números negativos. O objetivo era indicar débitos.

Ao introduzirem os números negativos, os hindus, não tinham nenhuma preocupação de ordem teórica. Na verdade, os progressos matemáticos verificados na Índia, por essa época, ocorreram quase que por acaso e em boa parte devido ao descompromisso com o rigor e a formalidade. A aceitação e o entendimento pleno dos números negativos foi um processo longo. Como já mencionado, os números foram surgindo de acordo com a necessidade de contagem do homem, precisava de números para representar débitos, surgindo assim os números negativos, e portanto o conjunto dos números inteiros.

**Os Números Inteiros: Construção**

A formalização dos números inteiros é dada por uma relação de equivalência em $\mathbb{N} \times \mathbb{N}$. Uma relação $R$ de um conjunto $A$ é uma relação de equivalência se satisfaz três propriedades listadas a seguir.

1. Reflexiva, ou seja, $a \in A$ então $aRa$ $\forall a \in A$;
2. Simétrica, ou seja, $a, b \in A$, $aRb$ então $bRa$ $\forall a, b \in A$;
3. Transitiva, ou seja, $a, b, c \in A$, $aRb$ e $bRc$ então $aRc$, $\forall a, b, c \in A$.

Vamos agora definir uma relação no conjunto $\mathbb{N} \times \mathbb{N}$, dos pares ordenados com entradas em $\mathbb{N}$.

A seguinte relação $\sim$ definida por: para quaisquer $(a,\, b)$ e $(c,\, d) \in \mathbb{N} \times \mathbb{N}$, temos que:

$(a,\, b) \sim (c,\, d) \Leftrightarrow a + d = b + c$.

É fácil ver que para a relação $\sim$ valem as seguintes propriedades:

1. $\sim$ *Reflexiva:* pois , como para todo $(a,\, b) \in \mathbb{N} \times \mathbb{N}$, se verifica $a + b = b + a$.
2. $\sim$ *Simétrica:* ou seja, se $(a,\, b) \sim (c,\, d)$, então $(c,\, d) \sim (a,\, b)$.
3. $\sim$ *Transitiva:* pois, se $(a,\, b) \sim (c,\, d)$ e $(c,\, d) \sim (e,\, f)$ então $(a,\, b) \sim (e,\, f)$.

E assim, $\sim$ determina uma partição em $\mathbb{N} \times \mathbb{N}$ em classes de equivalência. Para cada $(a,\, b) \in \mathbb{N} \times \mathbb{N}$ indicaremos por $\overline{(a,\, b)}$ a classe de equivalência determinada por $(a,\, b)$ $\in \mathbb{N} \times \mathbb{N}$ e o conjunto quociente será denotado por $\mathbb{Z}$.

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$$

A classe de equivalência determinada por $(a,\, b) \in \mathbb{N} \times \mathbb{N}$, é o conjunto:

$$\begin{aligned} \overline{(a,\, b)} &= \{(x,\, y) \in \mathbb{N} \times \mathbb{N} \mid (x,\, y) \sim (a,\, b)\} \\ &= \{(x,\, y) \in \mathbb{N} \times \mathbb{N} \mid x + b = y + a\} \end{aligned}$$

**Exemplo 2.2.1:**

$$\overline{(1,\, 3)} = \{(x,\, y) \in \mathbb{N} \times \mathbb{N} \mid x + 3 = 1 + y\}$$
$$\overline{(1,\, 3)} = \{(0,\, 2); (1,\, 3); (2,\, 4) \ldots\}$$

O conjunto das classes de equivalência é o conjunto quociente:

$$\mathbb{N} \times \mathbb{N}/\sim = \{\overline{(a, b)} \mid (a, b) \in \mathbb{N} \times \mathbb{N}\}$$

### 2.2.1 Adição no Conjunto dos Números Inteiros

Nesta subseção definiremos a adição no conjunto dos números inteiros e suas propriedades.

**Definição 2.3:** Sejam $m = \overline{(a, b)}$ e $n = \overline{(c, d)}$ elementos quaisquer de $\mathbb{Z}$. Chama-se soma de $m$ com $n$, indicada por $m + n$, o elemento de $\mathbb{Z}$ definido por:

$$m + n = \overline{(a + c, b + d)}$$

A relação dada por: $(m, n) \longmapsto m + n$ é uma aplicação, bem definida, isto é, independente da escolha do representante de $m$ e $n$, de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$ e, portanto é uma operação sobre $\mathbb{Z}$. A essa operação chama-se adição em $\mathbb{Z}$.

Para a adição em $\mathbb{Z}$ valem as seguintes propriedades: Associativa, comutativa, existência do elemento neutro, existência do simétrico. De fato, para $m = \overline{(a, b)}$, $n = \overline{(c, d)}$ e $r = \overline{(e, f)}$ elementos de $\mathbb{Z}$, temos:

1. Associativa:

$$(m + n) + r = \overline{(a + c, b + d)} + \overline{(e, f)} = \overline{((a + c) + e,\ (b + d) + f)} =$$

$$\overline{(a + (c + e),\ b + (d + f))} = \overline{(a + b)} + \overline{(c + e,\ d + f)} =$$

$$\overline{(a, b)} + (\overline{(c, d)} + \overline{(e, f)}) = m + (n + r)$$

2. Comutativa:

$$m + n = \overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)} =$$

$$\overline{(c + a, d + b)} = \overline{(c, d)} + \overline{(a, d)} = n + m.$$

3. Existe elemento neutro: é a classe $\overline{(0, 0)}$. De fato, para qualquer $\overline{(a, b)} \in \mathbb{Z}$:

$$\overline{(a, b)} + \overline{(0, 0)} = \overline{(a + 0, b + 0)} = \overline{(a, b)}.$$

   Usaremos a notação $0 = \overline{(0, 0)}$.

4. Todo $m = \overline{(a, b)}$ admite oposto (simétrico aditivo). Ou seja, para todo $m \in \mathbb{Z}$ existe $m' \in \mathbb{Z}$ de modo que $m + m' = 0$. Usaremos a notação: $-m = m'$. Como,

$$\overline{(a, b)} + \overline{(b, a)} = \overline{(a + b, b + a)} = 0$$

$$\text{então: } m = \overline{(a, b)} \Longrightarrow -m = \overline{(b, a)}.$$

A existência do simétrico nos possibilita definir a subtração em $\mathbb{N}$ que nada mais é que a adição com o simétrico.

### 2.2.2 Subtração no Conjunto dos Números Inteiros

Para cada par de elementos $m, n \in \mathbb{Z}$, chama-se diferença ou subtração entre $m$ e $n$ e indica-se por $m - n$ o elemento $m + (-n) \in \mathbb{Z}$. Ou seja:

$$m - n = m + (-n).$$

Assim, posto que $m - n \in \mathbb{Z}$, quaisquer que sejam $m, n \in \mathbb{Z}$, a relação dada por:

$$(m,\, n) \longmapsto m - n$$

é uma aplicação bem definida de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$ ou seja, é uma operação sobre $\mathbb{Z}$, dito operação oposta à adição.

### 2.2.3 Multiplicação no Conjunto dos Números Inteiros

**Definição 2.4:** Sejam $m = \overline{(a,\, b)}$ e $n = \overline{(c,\, d)}$ elementos quaisquer de $\mathbb{Z}$. Chama-se produto de $m$ por $n$ e indica-se por $mn$ ou $(m \cdot n)$ o elemento de $\mathbb{Z}$ definido por :

$$mn = \overline{(ac + bd,\, ad + bc)}. \tag{2.1}$$

A relação: $(m,\, n) \longmapsto mn$, é uma aplicação de $\mathbb{Z} \times \mathbb{Z}$ em $\mathbb{Z}$ e, por isso, uma operação sobre $\mathbb{Z}$. Trata-se, da multiplicação em $\mathbb{Z}$, da qual destacamos as propriedades a seguir. Lembrando que os produtos $ac, bd, ad, bc$ em (2.1) são multiplicações em $\mathbb{N}$.

1. Associativa: $m(nr) = (mn)r$, para quaisquer $m, n, r \in \mathbb{Z}$. Seja $m = \overline{(a,\, b)}$, $n = \overline{(c,\, d)}$ e $r = \overline{(e,\, f)}$. Então,

$$\begin{aligned} m \cdot (nr) &= \overline{(a,\, b)(ce + df,\, cf + de)} \\ &= \overline{(ace + adf + bcf + bde,\, acf + ade + bce + bdf)} \\ &= \overline{(e(ac + bd) + f(ad + bc),\, f(ac + bd) + e(ad + bc))} \\ &= \overline{(ac + bd,\, ad + bc)(e,\, f)} = (mn)r \end{aligned}$$

2. Comutativa: De fato, se $m = \overline{(a,\, b)}$ e $n = \overline{(c,\, d)}$ são elementos quaisquer de $\mathbb{Z}$, então:

$$mn = \overline{(ac + bd,\, ad + bc)} = \overline{(ca + db,\, cb + da)} = nm$$

3. Existe elemento neutro: é a classe (1, 0), à qual indicaremos apenas por 1.

$$\forall\ \overline{(a,\, b)} \in \mathbb{Z} \Longrightarrow \overline{(1,\, 0)} \cdot \overline{(a,\, b)} = \overline{(1 \cdot a + 0 \cdot b,\, 1 \cdot b + 0 \cdot a)} = \overline{(a,\, b)}$$

4. Lei do anulamento do produto: Se $m, n \in \mathbb{Z}$ e $mn = 0$, então $m = 0$ ou $n = 0$.

Vamos supor que, $m = \overline{(a,\, 0)}$ e $n = \overline{(0,\, b)}$, então $mn = \overline{(0,\, ab)} = \overline{(0,\, 0)}$. Daí $0 + 0 = ab + 0$ ou $ab = 0$ (em $\mathbb{N}$), o que implica $a = 0$ ou $b = 0$. Donde $m = 0$ ou $n = 0$.

5. Distributiva: Para quaisquer $m, n, r \in \mathbb{Z}$, $m(n + r) = mn + mr$.

### 2.2.4 Relação de Ordem no Conjunto dos Números Inteiros

Observe que toda classe de equivalência $\overline{(a,\, b)}$ pode ser representada com $a = 0$ ou $b = 0$. De fato, se $a < b$. $\exists\ \ c \in \mathbb{N}$ tal que $\overline{(a,\, b)} = \overline{(0,\, c)}$ , basta tomar $c = b - a$ e $b - a > 0$, logo $b - a \in \mathbb{N}$. E, se $a > b$, $\overline{(a,\, b)} = \overline{(0,c)}$, onde $c = a - b$.

Da forma como foi construído o conjunto dos números inteiros, nós não conseguimos associar esse conjunto ao que utilizamos hoje. Para que essa associação seja fácil de identificar um número inteiro, como números positivos e negativos, fazemos a seguinte associação descrita abaixo.

$$\overline{(c,\, 0)} = +c$$
$$\overline{(0,\, c)} = -c$$
$$\overline{(0,\, 0)} = 0$$

Com esta notação, conseguimos visualizar o conjunto dos números inteiros, como utilizamos corriqueiramente, por exemplo:

$$\overline{(5,\, 3)} = \overline{(2,\, 0)} = +2$$
$$\overline{(3,\, 5)} = \overline{(0,\, 2)} = -2$$
$$\overline{(4,\, 3)} = \overline{(1,\, 0)} = +1$$
$$\overline{(3,\, 4)} = \overline{(0,\, 1)} = -1$$
$$\overline{(0,\, 0)} = 0$$

O que torna mais claro, quais são os números do conjunto dos números inteiros. E portanto, denotando $\mathbb{N} \times \mathbb{N}/\sim$ por $\mathbb{Z}$ temos:

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

Seja $m \in \mathbb{Z}$ , temos $m = \overline{(a,\, 0)}$ ou $m = \overline{(0,\, a)}$ , para algum $a \in \mathbb{N}$. Façamos:

$$\{0, +1, +2, \ldots\} = \mathbb{Z}_+ \quad \text{e} \quad \{\ldots, -2, -1{,}0\} = \mathbb{Z}_-$$

Os elementos de $\mathbb{Z}_+$ são ditos inteiros não negativos e os de $\mathbb{Z}_-$ inteiros não positivos. Todo elemento $m \in \mathbb{Z}_+^* = \{+1, +2, +\ 3, \ldots\}$ é chamado inteiro positivo, e todo $m \in \mathbb{Z}_-^* = \{\ldots, -3, -2, -1\}$ é dito inteiro negativo. É fácil ver que os conjuntos citados acima são fechados para a soma.

**Definição 2.5:** Sejam $m, n \in \mathbb{Z}$. Diz-se que $m$ é menor que ou igual a $n$ e anota-se

$m \leq n$ se $\exists\ r \in \mathbb{Z}_+$ tal que $n = m + r$.

Neste caso também podemos escrever $n \geq m$, o que se lê : "$n$ é maior que ou igual a $m$".

Se $\exists\ r \in \mathbb{Z}_+^*$ tal que, $n = m + r$, então $m$ é dito menor do que $n$, e denotamos por $m < n$. É equivalente dizer que $n$ é maior que $m$ e denotamos por $n > m$.

Em particular $0 \leq r, \forall\ \ r\ \in \mathbb{Z}_+$, pois $r = 0 + r$; e $s \leq 0, \forall\ \ s\ \in \mathbb{Z}_-$, já que $0 = s + (-s)$. Também: $0 < r$, para todo $r \in \mathbb{Z}_+^*$ e $r < 0$ para todo $r \in \mathbb{Z}_-^*$.

Vejamos agora as propriedades mais importantes da relação $\leq$ sobre $\mathbb{Z}$, considere $m, n$ e $q \in \mathbb{Z}$.

1. Reflexiva: $m \leq m, \forall\ m \in \mathbb{Z}$. Pois $m = m + 0$ e $0 \in \mathbb{Z}$

2. Anti-Simétrica: Vamos supor $m \leq n$ e $n \leq m$.

   Então $m = n + r_1$, onde $r_1 = \overline{(a, 0)}$, para algum $a \in \mathbb{N}$, e $n = m + r_2$, onde $r_2 = \overline{(b, 0)}$, sendo $b$ um elemento de $\mathbb{N}$. Então,

   $$m = n + r_1 = (m + r_2) + r_1 = m + (r_1 + r_2) = m + \overline{(a + b, 0)}$$

   o que implica, pela lei do cancelamento da adição:

   $$\overline{(a + b, 0)} = \overline{(0, 0)}.$$

   Daí $a + b = 0$ em $\mathbb{N}$, e portanto $a = b = 0$. Donde $r_1 = r_2 = 0$ e $m = n$.

3. Transitiva: $m \leq n$ e $n \leq q \Longrightarrow\ m \leq q$

   Como $m \leq n$, então existe $r_1 \in \mathbb{Z}_+$, tal que $n = m + r_1$, e $n \leq q$, existe $r_2 \in \mathbb{Z}_+$ tal que $q = n + r_2$, somando o oposto de $r_2$ em ambos os termos, temos que: $q - r_2 = n$, daí $q - r_2 = m + r \Longrightarrow q = m + (r_1 + r_2) \Longrightarrow m \leq q$, para quaisquer $m, n \in \mathbb{Z}$ e $r_1 + r_2 \in \mathbb{Z}_+$.

4. $m \leq n$ ou $n \leq m$.

   Vamos supor $m = \overline{(a, 0)}$ e $n = \overline{(b, 0)}$. Se $a \leq b$, então $b = a + c$, para algum $c \in \mathbb{N}$, e portanto, $n = \overline{(b, 0)} = \overline{(a + c, 0)} = \overline{(a, 0)} + \overline{(c, 0)} = m + \overline{(c, 0)}$ o que garante a relação $m \leq n$. Se ao contrário, ocorresse $b \leq a$, então valeria $n \leq m$. O caso $m = \overline{(0, a)}$ e $n = \overline{(0, b)}$ pode ser encaminhado da mesma forma. Finalmente, seja $m = \overline{(a, 0)}$ e $n = \overline{(0, b)}$. Então $m = \overline{(a, 0)} = \overline{(a + b, 0)} = \overline{(0,b)} + \overline{(a + b,0)} = n + \overline{(a + b, 0)}$ de onde segue $n \leq m$. Uma consequência das considerações anteriores é que: $m \in \mathbb{Z}_-$ e $n \in \mathbb{Z}_+ \Longrightarrow m \leq n$.

5. Compatibilidade com adição: Se $m \leq n$, então $m + p \leq n + p$, para todo $p \in \mathbb{Z}$

   De fato, da hipótese segue que $m + r = n$ , para algum $r \in \mathbb{Z}_+$. Assim, para todo $p \in \mathbb{Z} : n + p = (m + r) + p = (m + p) + r$. Donde: $m + p \leq n + p$.

6. Compatibilidade com a multiplicação: $m \leq n$ e $0 \leq p \Longrightarrow\ mp \leq np$.

   Por hipótese $n = m + r$, onde $r = \overline{(a, 0)}$ para algum $a \in \mathbb{N}$. Supondo $p = \overline{(b, 0)}$, como $pn = pr$, onde $pr = \overline{(ab, 0)} \in \mathbb{Z}_+$, então $pm \leq pn$

## 2.3 O Conjunto dos Números Racionais

Um número $n$ é dito racional, se é possível escrever esse número na forma de uma fração, ou seja, $n = \dfrac{a}{b}$, com $a$ e $b \in \mathbb{Z}$ e $b \neq 0$. De acordo com [12], os egípcios desenvolveram um sistema de numeração e uma escrita mais ou menos na mesma época que os babilônios, ou seja, por volta do ano 300 antes de Cristo. Segundo alguns estudiosos, os primeiros conceitos de fração surgiram no Egito. Os egípcios usavam um conceito que, para nós, equivale às frações unitárias, da forma $\frac{1}{n}$. Os egípcios interpretavam uma fração somente com uma parte da unidade. Por isso, utilizavam apenas as frações unitárias, isto é, com numerador igual a 1. Para escrever as frações unitárias, colocavam um sinal oval alongado sobre o denominador.

As únicas frações em que usavam de forma que o numerador era diferente de 1 era as frações $\frac{2}{3}$ e $\frac{3}{4}$. Veremos aqui a formalidade da construção do conjunto dos números racionais.

### 2.3.1 A Construção dos Números Racionais

Seja $\mathbb{Z}^* = \{m \in \mathbb{Z}; m \neq 0\}$ e consideremos sobre:

$$\mathbb{Z} \times \mathbb{Z}^* = \{(m, n), m \in \mathbb{Z} \text{ e } n \in \mathbb{Z}^*\}$$

a relação $\sim$ definida por:

$$(m, n) \sim (p, q) \text{ se, e somente se, } mq = np.$$

Para $\sim$, valem as três propriedades que caracterizam uma relação de equivalência, ou seja:

1. $(m, n) \sim (m, n)$, para todo $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$ `(reflexiva)`
2. $(m, n) \sim (p, q) \Longrightarrow (p, q) \sim (m, n)$ `(simétrica)`
3. $(m, n) \sim (p, q)$ e $(p, q) \sim (r, s) \Longrightarrow (m, n) \sim (r, s)$ `(transitiva)`

A demonstração da relação ser reflexiva e simétrica ocorre diretamente da definição de $\sim$. Apresentaremos aqui apenas a demonstração da transitividade. Por hipótese, temos : $mq = np$ e $ps = qr$. Multiplicando a primeira dessas igualdades por $s$ e a segunda por $n$, resulta: $mqs = nps$ e $nps = nqr$. Daí, $msq = nqr$ e usando a lei do cancelamento em $\mathbb{Z}$, temos que $ms = nr$. E portanto, $(m, n) \sim (r, s)$.

Logo a relação $\sim$ determina sobre $\mathbb{Z} \times \mathbb{Z}^*$ uma partição em classes de equivalência. Para cada par $(m,n) \in \mathbb{Z} \times \mathbb{Z}^*$, a classe de equivalência à qual esse elemento pertence será indicada por $\dfrac{m}{n}$ ou $m/n$.

$$\frac{m}{n} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^*; (x, y) \sim (m, n)\} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^*; nx = my\}.$$

Por exemplo:

$$\frac{1}{3} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z}^*; 3x = 1y\} = \{( 1, 3); (2, 6); (-1, -3); \ldots\}.$$

Devido à propriedade reflexiva, é claro que $(m,\, n) \in \frac{m}{n}$ para todo $(m,\, n) \in \mathbb{Z} \times \mathbb{Z}^*$. Além disso, como $\frac{m}{n} = \frac{r}{s} \Longleftrightarrow (m{,}n) \sim (r{,}s)$, então $\frac{m}{n} = \frac{r}{s} \Longleftrightarrow ms = nr$.

Por exemplo:

$$\frac{1}{3} = \frac{2}{6} = \frac{-1}{-3} = \cdots$$

Assim, cada elemento de $\mathbb{Q}$ admite infinitas representações $\frac{m}{n}$ $(m \in \mathbb{Z}, n \in \mathbb{Z}^*)$.

Dois elementos $a,\, b \in \mathbb{Q}$ sempre admitem representações de denominadores iguais. De fato, se $a = \frac{m}{n}$ e $b = \frac{r}{s}$ então, $\frac{m}{n} = \frac{ms}{ns}$ e $\frac{r}{s} = \frac{nr}{ns}$ pois $m(ns) = n(ms)$ e $r(ns) = s(nr)$.

Os elementos de $\mathbb{Q}$ são chamados números racionais. Definimos a adição, multiplicação e a relação de ordem, ainda neste capítulo.

**Definição 2.6:** Denotamamos por $\mathbb{Q}$, e denominamos por conjunto dos números racionais, o conjunto quociente de $\mathbb{Z} \times \mathbb{Z}^*$ pela relação $\sim$, isto é,

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* \sim = \left\{ \frac{m}{n}; m \in \mathbb{Z} \text{ e } n \in \mathbb{Z}^* \right\}.$$

Uma fração $\dfrac{p}{q}$ que representa a mesma classe de $\dfrac{m}{n}$, $\dfrac{p}{q} = \dfrac{m}{n}$ é chamada de fração equivalente a $\dfrac{m}{n}$.

### 2.3.2 Adição no Conjuntos dos Números Racionais

**Definição 2.7:** Sejam $a = \frac{m}{n}$ e $b = \frac{r}{s}$ elementos de $\mathbb{Q}$. Chama-se soma de $a$ com $b$, indicada por $a + b$ o elemento de $\mathbb{Q}$ definido da seguinte maneira:

$$a + b = \frac{ms}{ns} + \frac{nr}{ns} = \frac{ms + nr}{ns}$$

De fato, a operação

$$\mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$$

$$(a,\, b) \longmapsto a + b, \text{ está bem definida.}$$

Mostraremos que a soma $a + b$ independe da fração equivalente escolhida para definir $a$ e $b$. Se $a = \frac{m}{n} = \frac{m'}{n'}$ , e $b = \frac{r}{s} = \frac{r'}{s'}$ , então $mn' = nm'$ e $rs' = sr'$. Multiplicando a primeira dessas igualdades por $ss'$ e a segunda por $nn'$ e somando membro a membro as relações obtidas:

$$msn's' + rns'n' = msm's' + nsr'n'$$

ou seja,

$$(ms + rn)n's' = ns(m's' + r's')$$

o que garante,
$$\frac{ms+rn}{ns} = \frac{m's'+r'n'}{n's'}.$$
Portanto, a correspondência $(a,\ b) \longmapsto a+b$ é uma aplicação e trata-se de uma operação sobre $\mathbb{Q}$, à qual chamaremos adição em $\mathbb{Q}$ e que possui as seguintes propriedades, que podem ser facilmente verificadas.

1. $(a+b)+c = a+(b+c)$, $\forall a, b, c \in \mathbb{Q}$ `(associativa)`.

2. $a+b = b+a, \forall a, b \in \mathbb{Q}$ `(comutativa)`.

3. Existe elemento neutro: é classe de equivalência $\frac{0}{1} = \frac{0}{2} = \cdots$, que indicamos por 0 apenas. De fato, $\frac{m}{n} + \frac{0}{1} = \frac{m.1+0.n}{n.1} = \frac{m.1}{n.1} = \frac{m}{n}$ para todo $\frac{m}{n} \in \mathbb{Q}$.

4. Todo $a \in \mathbb{Q}$ admite simétrico aditivo (oposto) em $\mathbb{Q}$: Se $a = \frac{m}{n}$, então $-a = \frac{-m}{n}$, pois:
$$\frac{m}{n} + \frac{-m}{n} = \frac{mn+(-m)n}{nn} = \frac{0}{nn} = 0.$$

**Definição 2.8:** Se $a, b \in \mathbb{Q}$ denomina-se diferença entre $a$ e $b$, e indica-se por $a-b$, o seguinte elemento de $\mathbb{Q}$: $a-b = a+(-b)$. Como $(-b) \in \mathbb{Q}$, para todo $b \in \mathbb{Q}$, então $(a,b) \longmapsto a-b$, uma operação sobre $\mathbb{Q}$, á qual chamaremos subtração em $\mathbb{Q}$.

### 2.3.3 Multiplicação no Conjuntos dos Números Racionais

**Definição 2.9:** Chamamos produto de $a = \dfrac{m}{n} \in \mathbb{Q}$ por $b = \dfrac{r}{s} \in \mathbb{Q}$ o elemento:
$$ab = a \cdot b = \frac{mr}{ns} \in \mathbb{Q}$$
o qual, pode-se mostrar, que não depende da escolha do representante da fração equivalente tomadas para $a$ e $b$.

A multiplicação em $\mathbb{Q}$ é uma operação definida por:
$$(a,\ b) \longmapsto ab, \text{ para quaisquer } (a,\ b) \in \mathbb{Q} \times \mathbb{Q}.$$
que possui as seguintes propriedades:

1. $a(bc) = (ab)c$ , $\forall a$,$b$ e $c \in \mathbb{Q}$ `(associativa)`.

2. $ab = ba$, $\forall a$,$b \in \mathbb{Q}$ `(comutativa)`.

3. Existe o elemento neutro: é a classe $\dfrac{1}{1} = \dfrac{2}{2} = \dfrac{3}{3} = \ldots$ que indicaremos simplesmente por 1. De fato: $\dfrac{m}{n} \cdot \dfrac{1}{1} = \dfrac{m.1}{n.1} = \dfrac{m}{n}$ para todo $\dfrac{m}{n} \in \mathbb{Q}$.

4. Todo $a \in \mathbb{Q}$ , $a \neq 0$, admite simétrico multiplicativo `(inverso)`: se $a = \dfrac{m}{n}$ com $m \neq 0$ temos $\dfrac{n}{m} \in \mathbb{Q}$ e, $\dfrac{m}{n} \cdot \dfrac{n}{m} = \dfrac{mn}{nm} = 1$, e $\dfrac{n}{m}$ é o inverso de $\dfrac{m}{n}$. Indicaremos

por $a^{-1}$ o inverso de $a$, então se $a = \dfrac{m}{n}, a \neq 0 \Longrightarrow a^{-1} = \dfrac{n}{m}$. Disso decorre também que se $a \neq 0$:

$$(a^{-1})^{-1} = \left(\frac{n}{m}\right)^{-1} = \frac{m}{n} = a.$$

Outro fato importante no que se refere aos inversos é que se $a$ e $b$ são elementos não nulos de $\mathbb{Q}$: $(ab)^{-1} = a^{-1}b^{-1}$. De fato, como $(ab)(a^{-1}b^{-1}) = (aa^{-1})(bb^{-1}) = 1$, então, $a^{-1}b^{-1}$ é o inverso de $ab$.

**Definição 2.10:** Entendemos por divisão em $\mathbb{Q}$ a operação $\mathbb{Q} \times \mathbb{Q}^*$ em $\mathbb{Q}$ definida por:$(a, b) \longmapsto ab^{-1}$.

O elemento $ab^{-1}$ é chamado quociente de $a$ por $b$ e pode ser indicado por $a\colon b$. Por exemplo, se $a = \dfrac{2}{3}$ e $b = \dfrac{1}{5}$, então: $a\colon b = \dfrac{2}{3} \cdot \left(\dfrac{1}{5}\right)^{-1} = \dfrac{2}{3} \cdot \dfrac{5}{1} = \dfrac{10}{3}$.

Para a divisão em $\mathbb{Q}$ vale a seguinte propriedade: se $a, b, c \in \mathbb{Q}$ e $c \neq 0$, então:

$$(a + b)\colon c = a\colon c + b\colon c$$

De fato, se $c = \dfrac{r}{s}$, $(r, s \in \mathbb{Z}^*)$, então:

$$(a + b)\colon c = (a + b) \cdot \frac{s}{r} = a \cdot \frac{s}{r} + b \cdot \frac{s}{r} = a\colon \frac{r}{s} + b\colon \frac{r}{s} = a\colon c + b\colon c.$$

### 2.3.4 Relação de Ordem no Conjunto dos Números Racionais

Seja $a = \dfrac{m}{n} \in \mathbb{Q}$. Como $a = \dfrac{m}{n} = \dfrac{-m}{-n}$, pois $m(-n) = n(-m)$, sempre podemos considerar, para todo $a \in \mathbb{Q}$, uma representação em que o denominador seja maior que zero (em $\mathbb{Z}_+^*$).

Nessa subseção, considere sempre os elementos de $\mathbb{Q}$ representados com denominadores positivos. Sejam $a$ e $b$ elementos de $\mathbb{Q}$, com $a = \dfrac{m}{n}$ e $b = \dfrac{r}{s}$.

Nessas condições, diz-se que $a$ é menor que ou igual a $b$, e escreve-se $a \leqslant b$, se $ms \leqslant nr$ (obviamente esta última relação é considerada em $\mathbb{Z}$). Equivalente a dizer que $b$ é maior que ou igual a $a$ e anotar $b \geqslant a$. Com as mesmas hipóteses, se $ms < nr$, diz-se que $a$ é menor que $b$ (notação: a < b) ou que $b$ é maior que $a$. Usando a notação: $b > a$

**Exemplo 2.3.1:**

$$\frac{-2}{3} < \frac{1}{4}, \text{ pois } -8 < 3.$$

$$\frac{5}{6} < \frac{4}{5}, \text{ pois } 25 > 24.$$

Um elemento $a = \dfrac{m}{n} \in \mathbb{Q}$ , diz positivo se $a \geqslant 0$. Lembrando que $0 = \dfrac{0}{1}$ , então:

$$a \geqslant 0 \Longleftrightarrow \frac{m}{n} \geqslant \frac{0}{1} \Longleftrightarrow m \geqslant 0.$$

Mostraremos a seguir que a relação $\leqslant$, conforme a definição acima, é uma relação de ordem sobre $\mathbb{Q}$, compatível com a adição e a multiplicação definidas. Dados $a = m/n$, $b = r/s$ e $c = p/q$ números racionais, temos:

1. $a \leqslant a$ `(reflexiva)`. Evidentemente, pois $mn \leqslant nm$.

2. $a \leqslant b$ e $b \leqslant a$ `(anti-simétrico)` Como $ms \leqslant nr$ e $rn \leqslant sm$ (em $\mathbb{Z}$), então $ms = nr$. Logo, $\dfrac{m}{n} = \dfrac{r}{s}$.

3. $a \leqslant b$ e $b \leqslant c \Longrightarrow a \leqslant c$ `(transitiva)`

   De fato, como $ms \leqslant nr$ e $rq \leqslant sp$, multiplicando a primeira dessas relações por $q > 0$ e a segunda por $n > 0$:

   $$msq \leqslant nqr \text{ e } rqn \leqslant spn.$$

   Usando a transitividade de $\leqslant$ em $\mathbb{Z}$, $msq \leqslant spn$. E uma vez que $s > 0$, pode-se concluir que $mq \leqslant pn$. Logo, $\frac{m}{n} \leqslant \frac{p}{q}$

4. $a \leqslant b$ ou $b \leqslant a$. Evidentemente, pois em $\mathbb{Z}$ : $ms \leqslant nr$ ou $nr \leqslant ms$.

5. $a \leqslant b \Longrightarrow a + c \leqslant b + c$ ( $\leqslant$ é compatível com a adição de $\mathbb{Q}$). De fato, como por hipótese $ms \leqslant nr$, então $msq^2 \leqslant nrq^2$, e daí:

   $$msq^2 + pnsq \leqslant nrq^2 + psnq$$

   ou seja,

   $$(mq + pn)sq \leqslant nq(rq + ps).$$

   Donde,

   $$\frac{m}{n} + \frac{p}{q} = \frac{mq + np}{nq} \leqslant \frac{rq + ps}{sq} = \frac{r}{s} + \frac{p}{q}$$

6. $a \leqslant b$ e $0 \leqslant c \Longrightarrow a \cdot c \leqslant b \cdot c$ ($\leqslant$ é compartível com a multiplicação em $\mathbb{Q}$).

   Por hipótese, $ms \leqslant nr$ e $p \geqslant 0$ (além de $n, s, q > 0$). Assim $pq \geqslant 0$ e portanto, $(ms)(pq) \leqslant (nr)(pq)$, ou, $(mp)(sq) \leqslant (nq)(rp)$, onde, $sq > 0$ e $nq > 0$.
   Logo, $\dfrac{m}{n} \cdot \dfrac{p}{q} = \dfrac{mp}{nq} \leqslant \dfrac{rp}{sq} = \dfrac{r}{s} \cdot \dfrac{p}{q}$

## 2.4 Os Números Não Racionais - Números Reais

Um marco importante na história dos números, ocorreu na escola Pitagórica, por volta do século VI antes de Cristo, quando um integrante dessa escola, percebeu que os lados e a diagonal de um quadrado de lado igual a um, eram segmentos não comensuráveis. A esse conceito, chamamos de segmentos incomensuráveis.

**Definição 2.11:** Os segmentos $AB$ e $CD$, são ditos *comensuráveis*, quando um terceiro $(EG)$, cabe um número $n$ e $m$ de vezes, respectivamente , nos segmentos $AB$ e $CD$, com $n$, $m \in \mathbb{N}^*$.

Essa ideia nos permite comparar dois segmentos de reta da seguinte maneira: dados dois segmentos, $AB$ e $CD$, dizer que a razão de seus comprimentos (faremos aqui um abuso de linguagem, ao denotar o comprimento de $AB$, por $AB$ também): $AB/CD$ é o número racional $m/n$, significa que existe um terceiro segmento $EF$, submúltiplo comum desses dois, satisfazendo: $AB$ é $m$ vezes $EF$ e $CD$ é $n$ vezes $EF$.

Tal ideia, citada acima, abalou muitos pitagóricos, uma vez que acreditavam que existia uma harmonia interna no mundo, governada pelos números naturais. E foi em sua própria comunidade, através de um figura geométrica, veio a descoberta da existência de números incomensuráveis, primeira menção aos números irracionais.

No decorrer deste e dos próximos capítulos, vamos aprender que os números reais podem ser classificados não apenas como racionais e irracionais, mas também em duas outras categorias. Uma categoria contém os chamados números algébricos, isto é, números que são soluções de equações algébricas com coeficientes inteiros, e uma outra contém todos os demais números, sendo esses chamados números transcendentes. Porém mencionaremos imediatamente que alguns números algébricos são racionais e outros irracionais, mas todos números transcendentes são irracionais.

### 2.4.1 A construção dos Números Reais - $\mathbb{R}$

O conceito de um número não racional, se deu pelo conceito de um segmento não comensurável.

Os matemáticos alemães Cantor e Dedekind, construíram os números reais a partir dos números racionais por métodos diferentes, respectivamente conhecidos por classes de Equivalência de sequências de Cauchy e por Cortes de Dedekind. Neste trabalho apresentaremos a construção dos números reais, através do Corte de Dedekind.

O que faremos será a construção dos números reais, com o rigor matemático. Tendo como ponto de partida o conjunto dos números racionais com suas propriedades algébricas e aritméticas, de forma análoga aos outros conjuntos numéricos citados em seções anteriores. Definiremos a noção de corte devido a Dedekind. E a esse conjunto de cortes, chamaremos de conjunto dos números reais.

Descreveremos aqui essa teoria. Para maiores informações, o leitor pode recorrer a referência [2].

**Definição 2.12:** Um conjunto $\alpha$ de números racionais, diz-se um *corte* se satisfazer as seguintes condições:

1. $\varnothing \neq \alpha \neq \mathbb{Q}$;
2. Se $r \in \alpha$ e $s < r$ (s racional), então $s \in \alpha$;
3. em $\alpha$ não existe elemento máximo.

**Exemplo 2.4.1:** O Conjunto A $= \left\{ x \in \mathbb{Q} \mid x < \dfrac{1}{2} \right\}$ é um corte, pois se $s < x$ e $x \in A$, então $s < x < \dfrac{1}{2}$. Por transitividade, $s < \dfrac{1}{2}$ e $s \in A$.

**Exemplo 2.4.2:** O Conjunto B $= \left\{ x \in \mathbb{Q} \mid x > \dfrac{1}{2} \right\}$ não é um corte, pois não satisfaz o segundo item da definição de corte.

**Definição 2.13:** Um conjunto não vazio $X \subset \mathbb{R}$ é dito limitado superiormente se existe $b \in \mathbb{R}$ tal que $x \leqslant b$ para todo $x \in X$. Neste caso, dizemos que $b$ é uma cota superior de $X$.

Como veremos a seguir, todo corte é um subconjunto de $\mathbb{Q}$ limitado superiormente.

**Proposição 2.2:** Sejam $\alpha$ um corte e $r \in \mathbb{Q}$. Então, $r$ é uma cota superior de $\alpha$ se, e somente se, $r \in \mathbb{Q} \setminus \alpha$.

*Demonstração.* Se $r$ é cota superior de $\alpha$, então $r$ não pode pertencer a $\alpha$, caso contrário $r$ seria elemento máximo de $\alpha$, contradizendo o terceiro item Definição 2.12 . Reciprocamente, se $r \in \mathbb{Q} \backslash \alpha$, então $r$ é cota superior de $\alpha$, pois, caso contrário haveria $s \in \alpha$ tal que $r < s$, o que, pelo segundo item da Definição 2.12, obrigaria $r$ a pertencer a $\alpha$, uma contradição. □

**Proposição 2.3:** Se $r \in \mathbb{Q}$ e $\alpha = \{x \in \mathbb{Q} \mid x < r\}$, então $\alpha$ é um corte e $r$ é a menor cota superior de $\alpha$.

*Demonstração.* A proposição é válida para os dois primeiros itens da definição de corte. Quanto ao terceiro item de 2.12, basta observar que se $s \in \alpha$, então $s < \dfrac{s+r}{2} < r$ e, como $\dfrac{s+r}{2} \in \mathbb{Q}$, então $\dfrac{s+r}{2} \in \alpha$. Assim, $s$ não é elemento máximo de $\alpha$. Esse argumento também mostra que $r$ é a menor cota superior, que podemos chamar de supremo. □

Seja $A$ um corte de Dedekind tal que existe $m \in \mathbb{Q}$ com $m$ sendo o supremo de $A$. Dizemos que $m$ é o elemento separador entre os conjuntos $A$ e $\mathbb{Q} \backslash A$. Nem todo corte de Dedekind possui supremo em $Q$, como mostra o exemplo seguinte.

**Exemplo 2.4.3:** Um conjunto $B = \{x \in \mathbb{Q}; x \leqslant 0 \text{ ou } x > 0 \text{ e } x^2 < 2\}$ é um corte de Dedekind, mas não possui supremo em $\mathbb{Q}$.

*Demonstração.* Mostraremos que as propriedades da definição de corte é verdadeira, logo após que o conjunto $A$ não possui supremo.

1. $A \neq \varnothing$, pois $1 > 0$ e $1^2 < 2$ e daí $1 \in A$;
2. $A \neq \mathbb{Q}$, pois $2 \in \mathbb{Q}$ mas $2 \notin A$, uma vez que $2^2 > 2$;
3. Sejam $x, y \in \mathbb{Q}$ tal que $x \in A$ e $y < x$. Se $y \leqslant 0$ então $y \in A$. Se $y > 0$ e então $0 < y < x$ nos dá $0 < y^2 < x^2 < 2$ e daí $y^2 < 2$, ou seja, $y \in A$. Em qualquer caso tem-se $y \in A$.
4. Se $x \in A$ é um número menor ou igual a zero então $1 > x$. Isso mostra que 1 é um elemento de $A$ maior do que $x$. Por fim, se $x \in A$ é um número positivo então $2 - x^2 > 0$. Assim, tomando $n > \dfrac{2x+1}{2-x^2}$ obtemos,

$$\begin{aligned}
&n > \frac{2x+1}{2-x^2} && \Longrightarrow \\
&n(2-x^2) > 2x+1 && \Longrightarrow \\
&2n - nx^2 > 2x+1 && \Longrightarrow \\
&nx^2 + 2x + 1 < 2n && \Longrightarrow \\
&\left(x + \frac{1}{n}\right)^2 < 2.
\end{aligned}$$

Sendo $x$ um racional, segue que $x + 1/n$ é racional maior do que $x$ tal que o quadrado é menor do que 2. Isso mostra que $\left(x + \dfrac{1}{n}\right)^2 \in A$, ou seja, $A$ não possui elemento máximo, e portanto $A$ é um corte de Dedekind.

□

**Definição 2.14:** Os cortes do tipo da proposição anterior são denominados cortes racionais e se representam por $r^*$.

$$r^* = \{x \in \mathbb{Q} \mid x < r\}$$

**Notação:** Denotaremos por $C$ o conjunto de todos os cortes.

### 2.4.2 Relação de Ordem e Operações com Cortes

**Definição 2.15:** Sejam $\alpha, \beta \in C$. Dizemos que $\alpha$ é menor do que $\beta$ e escrevemos $\alpha < \beta$ quando $\beta \setminus \alpha \neq \varnothing$. Neste caso dizemos também que $\beta > \alpha$, ou seja, ($\beta$ é maior do que $\alpha$).

**Exemplo 2.4.4:** $7^* > \left(\dfrac{1}{2}\right)^*$, pois $2 \in 7^* \setminus \left(\dfrac{1}{2}\right)^*$.

**Exemplo 2.4.5:** $(-1)^* < 0^*$, pois $\dfrac{-1}{2} \in 0^* \setminus (-1)^*$.

Podemos definir também "menor ou igual" dizendo que $\alpha \leqslant \beta$ se $\alpha < \beta$ ou $\alpha = \beta$. Analogamente definimos "maior ou igual". Note que $\alpha \leqslant \beta$ é equivalente a $\alpha \subset \beta$.

**Definição 2.16:** Se $\alpha \in C$ e $\alpha > 0^*$, $\alpha$ chama-se corte positivo. Se $\alpha < 0^*$, $\alpha$ é dito corte negativo. Se $\alpha \geqslant 0^*$, $\alpha$ chama-se corte não negativo e se $\alpha \leqslant 0^*$, $\alpha$ chama-se não positivo.

**Teorema 2.4:** (Tricotomia) Para $\alpha, \beta \in C$, temos uma e apenas uma das possibilidades a seguir ocorre.

$$\alpha = \beta \quad \text{ou} \quad \alpha < \beta \quad \text{ou} \quad \alpha > \beta.$$

*Demonstração.* É claro que $\alpha = \beta$ exclui as outras duas possibilidades, pela definição de igualdade de conjuntos. De modo análogo, as possibilidades $\alpha < \beta$ ou $\alpha > \beta$ claramente excluem $\alpha = \beta$. Será apresentado aqui que as desigualdades também se excluem mutuamente. Suponhamos o contrário, isto é, que $\alpha < \beta$ e $\alpha > \beta$ ocorram simultaneamente. Então, existem $r \in \beta \setminus \alpha$ e $s \in \alpha \setminus \beta$. Como $r \in \beta$ e $s \notin \beta$ resulta $r < s$, analogamente, como $s \in \alpha$ e $r \notin \alpha$ resulta $s < r$, contradizendo a lei da tricotomia em $\mathbb{Q}$. Concluímos que no máximo uma das três possibilidades ocorre. Para mostrar que uma delas necessariamente ocorre, temos que $\alpha = \beta$ ou $\alpha \neq \beta$. Se $\alpha = \beta$ nada há a provar. Suponhamos que $\alpha \neq \beta$, então $\alpha \setminus \beta \neq \varnothing$ ou $\beta \setminus \alpha \neq \varnothing$ (pois, caso contrário, $\alpha = \beta$). No primeiro caso, $\beta < \alpha$ e, no segundo caso $\alpha < \beta$. □

**Teorema 2.5:** Sejam $\alpha, \beta \in C$. Se $\gamma = \{a + b \mid a \in \alpha \ \text{ e } \ b \in \beta\}$, então $\gamma \in C$.

*Demonstração.* Verificaremos que $\gamma$ satisfaz as três condições da Definição 2.12. É fácil ver que atende ao primeiro item da definição, já que $\gamma \neq \varnothing$ (uma vez que $\alpha$ e $\beta$ são diferentes de vazio).

1. Sejam $t \in \mathbb{Q} \setminus \alpha \Longrightarrow t > a, \forall a \in \alpha$ e $u \in \mathbb{Q} \setminus \beta \Longrightarrow u > b, \forall b \in \beta$. Então $t + u > a + b, \forall a \in \alpha$ e $b \in \beta$. Logo, $t + u \notin \gamma$ e $\gamma \neq \mathbb{Q}$.
2. Sejam $a \in \gamma$ e $b < a$ ($b$ racional). Sabemos que $b \in \gamma, a$ é do tipo $p + q$, com $p \in \alpha$ e $q \in \beta$. Como $b < p + q$, podemos escrever $b = p + q'$ com $q' \in \mathbb{Q}$ e $q' < q$ e, portanto, $q' \in \beta$. Logo, $b = p + q'$ em que $p \in \alpha$ e $q' \in \beta$ isto é, $b \in \gamma$.
3. Se $a \in \gamma$, existe $b \in \gamma$ com $b > a$. Temos: $a = p + q$ com $p \in \alpha$ e $q \in \beta$. Como existe $p' \in \alpha$ com $p' > p$, o racional $s = p' + q \in \gamma$ e é maior do que $a$.

□

**Definição 2.17:** Para $\alpha, \beta \in C$, definimos $\alpha + \beta$ como sendo o corte do teorema anterior, ou seja,

$$\alpha + \beta = \{a + b \mid a \in \alpha \ \text{ e } \ b \in \beta\}.$$

**Teorema 2.6:** A adição em $C$ é comutativa, associativa e tem $0^*$ como elemento neutro.

*Demonstração.* A comutatividade e a associatividade são herdadas das propriedades análogas da adição em $\mathbb{Q}$. Para mostrar que $\alpha + 0^* = \alpha, \forall \alpha \in C$, vamos verificar as duas inclusões: $\alpha + 0^* \subset \alpha$ e $\alpha \subset \alpha + 0^*$. Seja $a \in \alpha + 0^*$. Então $a = p + q$, com $p \in \alpha$ e $q \in 0^*$, isto é, $q < 0$. Assim, $a < p \in \alpha$ e, portanto, $a \in \alpha$. Logo, $\alpha + 0^* \subset \alpha$. Seja agora $a \in \alpha$, tomando $b \in \alpha$ com $b > a$, podemos expressar $a$ como $a = b + (a - b)$, onde $a - b < 0$ e, portanto, ele pertence $0^*$ e $\alpha \subset \alpha + 0^*$. □

**Teorema 2.7:** Seja $\alpha \in C$. Existe um único $\beta \in C$ tal que $\alpha + \beta = 0^*$. Como nos casos dos inteiros e racionais, tal $\beta$ denota-se por $-\alpha$ e se chama de simétrico (ou inverso aditivo) de $\alpha$.

*Demonstração.* Suponhamos $\alpha + \beta_1 = \alpha + \beta_2 = 0^*$. Vale ressaltar que a adição de cortes é comutativa e associativa. Obtemos assim, $\beta_2 = \beta_2 + 0^* = \beta_2 + (\alpha + \beta_1) = (\beta_2 + \alpha) + \beta_1 = 0^* + \beta_1 = \beta_1$. E portanto, existe um único $\beta \in C$, tal que $\alpha + \beta = 0^*$. Agora para construir o simétrico de $\alpha$, tomaremos $\alpha \in C$. O candidato a $-\alpha$ é o conjunto obtido pelos negativos dos elementos que estão fora de $\alpha$, com exceção da eventual cota superior mínima de $\alpha$. Mais precisamente, seja $\beta = \{p \in \mathbb{Q} | -p$ é cota superior NÃO mínima de $\alpha\}$. No caso geral, não temos necessariamente cortes racionais e, então, o símbolo $(-\alpha)^*$ pode não fazer sentido. Mostraremos que $\beta$ é um corte e que $\alpha + \beta = 0^*$. Analisaremos as três condições da definição de corte. Observe que satisfaz ao primeiro item da Definição 2.12, já que $\alpha + \beta \neq \varnothing$, pois $\beta$ é o oposto de $\alpha$, o que explica o segundo item da Definição 2.12, quanto ao terceiro item da Definição 2.12,tomemos $a \in \beta$. Queremos encontrar $b > a$ em $\beta$. Como $-a$ é cota superior de $\alpha$ mas não é mínima, então existe $t \in \mathbb{Q}$, $-t < -a$, tal que $-t$ é cota superior de $\alpha$, e portanto, $-t < -a$, tal que $-t \notin \alpha$. Seja $b = \dfrac{a+t}{2}$. Temos: $-t < -b < -a$, de modo que $-b$ é cota superior de $\alpha$ mas não é mínima, logo $a \in \beta$ e $b > a$ como queríamos. Vamos verificar agora que $\alpha + \beta = 0^*$. Seja $t \in \alpha + \beta$. Então $t = a + b$, com $a \in \alpha$ e $b \in \beta$. Como $-b \notin \alpha$, então $-b > a$, de modo que $0 > a + b = t$, ou seja, $t \in 0^*$. Reciprocamente, suponhamos que $t \in 0^*$, isto é, $t < 0$. Sejam $r \in \alpha$ e $r' \notin \alpha$, tais que $r' - r = -t$, segue que $t = r + (-r')$, com $r \in \alpha$ e $-r' \in \beta$, ou seja, $t \in \alpha + \beta$. □

**Definição 2.18:** Como nos casos de $\mathbb{Z}$ e $\mathbb{Q}$, definimos a subtração em $C$ por $\alpha - \beta = \alpha + (-\beta), \forall \alpha, \beta \in C$.

A proposição seguinte, cuja demonstração segue imediatamente das definições, nos mostra algumas propriedades. Para maiores informações, o leitor pode verificar em [2].

**Proposição 2.4:** Para $\alpha, \beta, \gamma \in C$, vale:

1. $-(-\alpha) = \alpha$;
2. $-\alpha + \beta = \beta - \alpha$;
3. $\alpha - (-\beta) = \alpha + \beta$;
4. $-\alpha - \beta = -(\alpha + \beta)$;
5. $\alpha - (\beta + \gamma) = \alpha - \beta - \gamma$.

**Teorema 2.8:** (Compatibilidade da relação de ordem com a adição) Sejam $\alpha, \beta, \gamma \in C$ tais que $\alpha \leqslant \beta$. Então $\alpha + \gamma \leqslant \beta + \gamma$.

*Demonstração.* $\alpha \leqslant \beta \Longleftrightarrow \alpha \subset \beta$. Seja $t \in \alpha + \gamma$, isto é, $t = a + b$, com $a \in \alpha$ e $s \in \gamma$. Como $\alpha \subset \beta$, então $a \in \beta$ e $t = a + b \in \beta + \gamma$ ou seja, $\alpha + \gamma \subset \beta + \gamma$. Portanto, $\alpha + \gamma \leqslant \beta + \gamma$. $\square$

Considere agora dois cortes positivos, $\alpha \geqslant 0^*, \beta \geqslant 0^*$. Considere o conjunto

$$\gamma = \mathbb{Q}^*_- \cup \{a \in \mathbb{Q} |\ a = pq\}$$

com $p \in \alpha$ e $q \in \beta$, $p, q \geqslant 0$. Veremos que um corte e $\gamma \geqslant 0^*$. De fato, observe que $-1 \in \gamma$, assim $\gamma \neq \varepsilon$. Sejam agora $r \in \gamma$ e $s < r$. Se $s < 0$, então $s \in \gamma$. Suponhamos $s \geqslant 0$ e, portanto, $r > 0$. Pela definição de $\gamma$ existem $p \in \alpha$ e $q \in \beta$ tais que $r = p \cdot q$, $p \geqslant 0$ e $q \geqslant 0$. Como $r > 0$ segue que $p > 0$. Seja $t = s/p$, temos $t < q$, pois se fosse $q \leqslant t, pq \leqslant pt$, ou seja, $r \leqslant s$. Então $t \leqslant q$ e $t \in \beta$. Daí, $s \in \gamma$, pois $s = pt$. Por fim, para o terceiro item da definição de corte, dado $r \in \gamma$, se $r < 0$ basta tomar $s = r/2$ que $s > r$ e $s \in \gamma$. Se $r \geqslant 0, r \in \gamma$ implica em $r = pq$ com $p \in \alpha$ e $q \in \beta, p \geqslant 0$ e $q \geqslant 0$. Existem $t \in \alpha$ e $u \in \beta$ tal que $p < t$ e $q < u$. Logo, $r = pq < tu$ e tome $s = tu \in \gamma$ e $s > r$.

**Definição 2.19:** O Corte $\gamma$ definido acima é dito produto ou multiplicação de $\alpha$ e $\beta$ e será denotado por $\gamma = \alpha \cdot \beta$ ou simplesmente $\gamma = \alpha \cdot \beta$.

**Definição 2.20:** Dado $\alpha \in C$, definimos o valor absoluto de $\alpha$ (ou o módulo de $\alpha$), representado por $|\alpha|$, do seguinte modo:

$$|\alpha| = \begin{cases} \alpha, & \text{se} \quad \alpha \geqslant 0^* \\ -\alpha, & \text{se} \quad \alpha < 0^* \end{cases}$$

Temos abaixo a definição de produto.

**Definição 2.21:** Sejam $\alpha, \beta \in C$. Definimos $\alpha \cdot \beta$ por,

$$\alpha \cdot \beta = \begin{cases} |\alpha||\beta|, & \text{se} \quad 0^* \subset \alpha \quad \text{e} \quad 0^* \subset \beta \\ -|\alpha||\beta|, & \text{se} \quad 0^* \subset \alpha \quad \text{e} \quad \beta \subsetneq 0^* \\ -|\alpha||\beta|, & \text{se} \quad \alpha \subsetneq 0^* \quad \text{e} \quad 0^* \subset \beta \\ |\alpha||\beta|, & \text{se} \quad \alpha \subsetneq 0^* \quad \text{e} \quad \beta \subsetneq 0^* \end{cases}$$

O teorema a seguir traz algumas propriedades da multiplicação, para maiores informações o leitor pode encontrar em [2]

**Teorema 2.9:** A multiplicação de cortes é comutativa, associativa, tem $1^*$ como elemento neutro e, se $\alpha, \beta, \gamma \in C$, vale:

1. $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ (distributividade) ;

2. $\alpha \cdot 0^* = 0^*$;

3. se $\alpha \leqslant \beta$ e $\gamma \geqslant 0^*$, então $\alpha\gamma \leqslant \beta\gamma$;

4. se $\alpha \leqslant \beta$ e $\gamma < 0^*$, então $\alpha\gamma \geqslant \beta\gamma$;

5. se $\alpha \neq 0^*$ em $C$, existe um único $\beta \in C$ tal que $\alpha\beta = 1^*$. Esse corte chama-se inverso de $\alpha$ e é denotado por $\alpha^{-1}$.

Concluímos que $C$ é munido de duas operações e uma relação de ordem, obedecendo às mesmas leis aritméticas dos racionais. Assim, $C$ é um corpo ordenado. Em particular define-se também a divisão em $C$, $\alpha \div \beta = \alpha \cdot \beta^{-1}$, e adota-se a notação de fração: $\frac{\alpha}{\beta}$. Além disso, a aplicação $j : \mathbb{Q} \longrightarrow C$ dada por $j(r) = r^*$ é injetora e preserva a adição, multiplicação e ordem. De fato $j(r) = j(s)$ implica em $r^* = s^*$ e então, $r = s$. Dessa maneira, temos que $j(\mathbb{Q})$ é uma cópia de $\mathbb{Q}$ em $C$, sendo $j(\mathbb{Q})$ precisamente o conjunto dos cortes racionais.

**Definição 2.22:** O conjunto $C$ dos cortes será, a partir de agora, denominado de conjunto dos números reais, e denotado por $\mathbb{R}$. Os cortes racionais serão identificados, via a injeção $j$, com os números racionais. Todo corte que não for racional será denominado número irracional.

No conjunto dos números racionais o corte do Exemplo 2.4.3 não possui elemento de separação. Assim, para Dedekind, deveria ser criado um número no caso $\sqrt{2}$, como elemento de separação entre os conjuntos $A$ e $\mathbb{Q} \backslash A$.

**Notação:** A identificação de $j(\mathbb{Q})$ com $\mathbb{Q}$ nos permite escrever $\mathbb{Q} \subset \mathbb{R}$. O conjunto $\mathbb{R} \backslash \mathbb{Q}$ representa o conjunto dos números irracionais.

## 2.5 A enumerabilidade dos conjuntos numéricos

Descreveremos a enumerabilidade dos Conjuntos Numéricos, tratados nas seções anteriores. Este capítulo será baseado em teorias encontradas nos livros [10] e [7].

**Definição 2.23:** Um conjunto $A$ é *enumerável* se seus elementos puderem ser postos em correspondência biunívoca com os números naturais. Mais precisamente, $A$ é enumerável se existir uma função bijetiva, $f : \mathbb{N} \longrightarrow A$.

**Exemplo 2.5.1:** O conjunto dos números pares positivos é enumerável: tome $f(n) = 2n$.

**Exemplo 2.5.2:** O conjunto dos números ímpares (positivos) é enumerável: tome $f(n) = 2n - 1$.

**Exemplo 2.5.3:** O conjunto $\mathbb{Z}$ é enumerável: olhe a tabela abaixo:

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

**Exemplo 2.5.4:** O conjunto dos números racionais é enumerável. Mostraremos primeiramente que o conjunto dos racionais positivos é enumerável. Olhe o quadro abaixo.

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

Observe que todos os números da forma $p/q$ com $p, q \in \mathbb{N}$ e $q \neq 0$ aparecerão no quadro acima. Se o percorremos seguindo as flexas teremos uma ordenação desse conjunto, o qual vale dizer, a função $f$ será $f(n) = n$-ésimo elemento que encontraremos seguindo as flexas. Assim, mostramos que o conjunto $\mathbb{Q}_+^* = \{x \in \mathbb{Q} : x > 0\}$ é enumerável. A enumerabilidade de $\mathbb{Q}$ segue-se do Teorema abaixo, lembrando que $\mathbb{Q} = \mathbb{Q}_+^* \cup \mathbb{Q}_-^* \cup \{0\}$, onde $\mathbb{Q}_-^* = \{x \in \mathbb{Q} : x < 0\}$.

**Teorema 2.10:**

1. A união de um conjunto finito com um conjunto enumerável é enumerável;
2. A união de dois conjuntos enumeráveis é enumerável;
3. A união de um número finito de conjuntos enumeráveis é enumerável;
4. A união de um conjunto enumerável de conjuntos finitos é enumerável;
5. A união de um conjunto enumerável de conjuntos enumeráveis é enumerável.

*Demonstração.* A demonstração dos dois primeiros itens será feito de acordo com Djairo [3].

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

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

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

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

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

3. Sejam $A_1, A_2, \ldots, A_n$ conjuntos enumeráveis, queremos mostrar que

$$A_1 \cup A_2 \cup \ldots \cup A_n$$

é enumerável, $\forall\ n\ \mathbb{N}$. Para isso usamos o Princípio de Indução Finita.

a) $n = 1$ é válida pois $A_1$ é enumerável.

b) $n = 2$ é válida pelo item (2).

**Hipótese de Indução:** Suponha que seja válida para $k$ ou seja, se $A_1, A_2, \ldots, A_k$ são enumeráveis então $A_1 \cup \ldots \cup A_k$ é enumerável. Provaremos se a propriedade é válida para $k + 1$.

Observe que:

$$A_1 \cup A_2 \cup \ldots \cup A_k \cup A_{k+1} = (A_1 \cup A_2 \cup \ldots \cup A_k) \cup A_{k+1}$$

Considerando $A = A_1 \cup A_2 \cup \ldots \cup A_k$, então.

$$A_1 \cup A_2 \cup \ldots \cup A_k \cup A_{k+1} = A \cup A_{k+1}$$

Temos que $A$ é enumerável, por hipótese de indução, e pelo item (2) $A \cup A_{k+1}$ é enumerável. Logo, pelo princípio da Indução Finita, temos que (3) é válida.

4. Agora, considerando $\{A_1, A_2, \ldots, A_n, \ldots\}$ um conjunto enumerável onde cada $A_j$ é um conjunto finito, para qualquer $j \in \mathbb{N}$.Queremos mostrar que a união de conjuntos finitos é enumerável, o item (4). Suponha que $A_1 = \{a_{11}, a_12, \ldots, a_{1k_1}\}$, $A_2 = \{a_{21}, a_{22}, \ldots, a_{2k_2}\}$, ..., $A_n = \{a_{n1}, a_{n2}, \ldots, a_{nk_n}\}$. Então:

$$A_1 \cup A_2 \cup \ldots A_n = \{a_{11}, \ldots, a_{1k_1}, a_{21}, \ldots, a_{2k_2}, \ldots, a_{n1}, \ldots, a_{nk_n}, \ldots\}$$

Defina a seguinte correspondência entre $A_1 \cup A_2 \cup \ldots \cup A_n \ldots \subset \mathbb{N}$.

$$\begin{array}{ccccccccccccc} a_{11}, & \ldots, & a_{1k_1}, & a_{21}, & \ldots, & a_{2k_2}, & \ldots, & a_{n1}, & \ldots, & a_{nk_n} & \ldots \\ \updownarrow & & \updownarrow & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & \\ 1, & \ldots, & k_1, & k_1 + 1, & \ldots, & k_1 + k_2 & \ldots, & k_1 + \cdots + k_{n-1} + 1 & \ldots, & k_1 + \cdots + K_{n_1} + k_n & \ldots \end{array}$$

Logo, $A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots$ é enumerável.

5. Seja $\{A_1, A_2, \ldots\}$ um conjunto enumerável onde cada $A_i$ é um conjunto enumerável para qualquer $i \in \mathbb{N}$. Suponha que:

$$A_1 = \{a_{11}, a_{12}, \ldots\}, \quad A_2 = \{a_{21}, a_{22}, \ldots\}, \quad \ldots, \quad A_n = \{a_{n1}, a_{n2}, \ldots\}$$

Disponha os elementos de $A_1, A_2, \ldots, A_n$ como a tabela

$$\begin{array}{lll} a_{11}, & a_{12}, & \ldots \\ a_{21}, & a_{22}, & \ldots \\ \vdots & \vdots & \\ a_{n1}, & a_{n2}, & \ldots \\ \vdots & \vdots & \end{array}$$

Formando flechas como feito em $\mathbb{Q}^+$ definimos $f$ dada por $f(n) = n-$ésimo elemento que encontramos seguindo as flechas. Dessa forma definimos uma correspondência biunívoca entre $A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots$ e consequentemente provamos que é um conjunto enumerável.

□

O próximo teorema dirá sobre a enumerabilidade dos números reais.

**Teorema 2.11:** O conjunto $\mathbb{R}$ dos números reais não é enumerável.

*Demonstração.* Demonstraremos que o conjunto dos números reais $x \in [0,1)$, não é enumerável, em consequência, teremos que $\mathbb{R}$ não é enumerável. Note que os números $x \in [0, 1)$ tem uma representação decimal da forma

$$0, a_1 a_2 a_3 \ldots \tag{2.2}$$

onde $a_j$ é um dos algarismos $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Alguns números tem duas representações da forma (2.2) por exemplo, $\frac{1}{4} = 0{,}25000\ldots = 0{,}25$ ou $0{,}24444\ldots$

Para tais números, escolhemos a representação decimal que termina, ou seja, a finita. Suponhamos que os demais decimais do tipo (2.2) ou que os números reais no intervalo [0,1), formam um conjunto enumerável, como mostra na tabela abaixo.

$$\begin{array}{lllll} 0, & a_{11}, & a_{12}, & a_{13} & \ldots \\ 0, & a_{21}, & a_{22}, & a_{23}, & \ldots \\ 0, & a_{31}, & a_{32}, & a_{33}, & \ldots \\ & & \vdots & & \ldots \end{array}$$

Agora forme o decimal $0{,}b_1b_2b_3\ldots$ do seguinte modo: todos os $b'_{is}$ são diferentes de 0 ou 9 e $b_1 \neq a_{nm}$. Logo $0{,}b_1b_2b_3\ldots$ não está na tabela acima, o que é um absurdo, já que é um número real entre 0 e 1. $\square$

# 3

# Números Irracionais

No Capítulo 2 definimos o conjunto dos números irracionais que é o conjunto dos reais não racionais e é representado por $\mathbb{R}\backslash\mathbb{Q}$. Neste capítulo daremos alguns exemplos de números irracionais. Alguns exemplos e demonstrações serão feitas de acordo como Ivan Niven [11].

**Exemplo 3.0.1:** $\sqrt{5}$ é um número irracional.

**Afirmação:** Se $p^2$ é múltiplo de 5, então $p$ é múltiplo de 5

Suponhamos que $p$ não seja múltiplo de 5. Então, $p = 5q + r$, com $q \in \mathbb{Z}$ e $0 < r < 5$. Daí,

$$\begin{array}{ll} p^2 = (5q+r)^2 & \Longrightarrow \\ p^2 = 25q^2 + 10qr + r^2 & \Longrightarrow \\ p^2 = 5(5q^2 + 2qr) + r^2 & \Longrightarrow \\ p^2 = 5t + r^2 & \end{array}$$

onde $t = (5q^2 + 2qr) \in \mathbb{Z}$. Estudemos o resto $r$, $0 < r < 5$

- $r = 1$

  $$p^2 = 5t + 1$$

  Neste caso, $p^2$ não seria múltiplo de 5

- $r = 2$

  $$p^2 = 5t + 4$$

  Neste caso, $p^2$ não seria múltiplo de 5

- $r = 3$

  $$p^2 = 5t_1 + 4$$

  Neste caso, $p^2$ não seria múltiplo de 5

- $r = 4$

  $$p^2 = 5t_2 + 1$$

  Neste caso, $p^2$ não seria múltiplo de 5

  Chegando assim que $p^2$ não é múltiplo de 5, o que é um absurdo. Logo, se $p^2$ é múltiplo de 5, concluímos que $p$ é múltiplo de 5.

Vamos mostrar que $\sqrt{5}$ é irracional. Suponhamos por absurdo que $\sqrt{5}$ seja um número racional. Logo, existem $p, q \in \mathbb{N}$, com $q \neq 0$ e $mdc(p, q) = 1$, tal que

$$\begin{array}{ll} \sqrt{5} = p/q & \Longrightarrow \\ (\sqrt{5})^2 = (p/q)^2 & \Longrightarrow \\ 5 = p^2/q^2 & \Longrightarrow \\ 5q^2 = p^2 & \end{array}$$

Temos que $p^2$ é múltiplo de 5. Logo, $p$ é múltiplo de 5. Consequentemente , $p$ pode ser escrito como $5k$, para $k \in \mathbb{Z}$. Substituindo $p$ por $5k$, teremos:

$$\begin{array}{ll} 5q^2 = (5k)^2 & \Longrightarrow \\ 5q^2 = 25k^2 & \Longrightarrow \\ q^2 = 5k^2 & \end{array}$$

Concluímos que $q^2$ é múltiplo de 5, ou seja, $q$ é múltiplo de 5. Ou seja, $p$ e $q$ são múltiplos de 5, o que é um absurdo, já que por hipótese $p$ e $q$ são primos entre si.

**Proposição 3.1:** Temos que, $\sqrt{p}$ com $p$ primo é um número irracional.

*Demonstração.* Suponhamos por absurdo que $\sqrt{p}$ é um número racional. Logo, existem $a, b \in \mathbb{N}$, com $b \neq 0$ e $mdc(a, b) = 1$, tal que

$$\begin{array}{ll} \sqrt{p} = a/b & \Longrightarrow \\ p = a^2/b^2 & \Longrightarrow \\ b^2p = a^2 & \end{array}$$

$a^2$ é múltiplo de $p$, daí $a$ é múltiplo de $p$, consequentemente $a = kp$, para $k \in \mathbb{Z}$, daí,

$$\begin{array}{ll} b^2p = (kp)^2 & \Longrightarrow \\ b^2p = k^2p^2 & \Longrightarrow \\ b^2 = k^2p & \end{array}$$

Concluímos que $b^2$ é múltiplo de $p$, daí $b$ é múltiplo de $p$, o que é um absurdo, pois por hipótese $a$ e $b$ são primos entre si. Logo, $\sqrt{p}$, com $p$ primo é irracional. □

De acordo com a Proposição 3.1, temos que os números $\sqrt{2}$ e $\sqrt{3}$ são números não racionais.

**Exemplo 3.0.2:** O número $\sqrt{2}+\sqrt{3}$ não é racional.

*Demonstração.* Suponhamos por absurdo que o número $\sqrt{2}+\sqrt{3}$ seja racional. Logo, existem $p, q \in \mathbb{N}$, com $q \neq 0$ e $mdc(p, q) = 1$, tal que

$$\begin{array}{ll} \sqrt{2}+\sqrt{3} = p/q & \Longrightarrow \\ (\sqrt{2}+\sqrt{3})^2 = (p/q)^2 & \Longrightarrow \\ 2+2\sqrt{2}\cdot\sqrt{3}+3 = (p/q)^2 & \Longrightarrow \\ \sqrt{6} = \dfrac{1}{2}\left(\dfrac{p^2}{q^2}-5\right) & \end{array}$$

**Afirmação:** $\sqrt{6} \notin \mathbb{Q}$.

Suponhamos por absurdo que $\sqrt{6} \in \mathbb{Q}$, então existem $a$ e $b \in \mathbb{N}$ com $mdc(a, b) = 1$ e $b \neq 0$, tal que

$$\begin{array}{ll} \sqrt{6} = a/b & \Longrightarrow \\ (\sqrt{6})^2 = (a/b)^2 & \Longrightarrow \\ 6 = a^2/b^2 & \Longrightarrow \\ 6b^2 = a^2 & \end{array}$$

E portanto $a$ é múltiplo de 6. Sendo assim, $a = 6k$. Assim,

$$\begin{array}{ll} (6k)^2 = 6b^2 & \Longrightarrow \\ 36k^2 = 6b^2 & \Longrightarrow \\ 6k^2 = b^2 & \end{array}$$

Ou seja, $b$ é múltiplo de 6. Absurdo, pois $mdc(a, b) = 1$. Logo, $\sqrt{6} \notin \mathbb{Q}$.

Observe que $\dfrac{1}{2}\left(\dfrac{p^2}{q^2}-5\right) \in \mathbb{Q}$, sendo assim, $\sqrt{6} \in \mathbb{Q}$. O que é um absurdo. Logo, $\sqrt{2}+\sqrt{3}$ é irracional. □

Para apresentarmos mais exemplos de irracionais, daremos algumas definições importantes como a de números transcendentes e números algébricos.

## 3.1 Número Algébrico e Número Transcendente

Qualquer solução de uma equação polinomial da forma:

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

onde os coeficientes $a_i's$ são inteiros, é chamado um *número algébrico.*

Assim, um número $\alpha \in \mathbb{R}$ é algébrico se existir uma equação polinomial com coeficientes inteiros, da qual $\alpha$ seja raiz. Qualquer número racional, $\alpha = p/q$, é algébrico, porque $\alpha$ é a raiz da equação

$$qx - p = 0 \tag{3.2}$$

Um número que não seja algébrico é chamado *transcendente.*

**Exemplo 3.1.1:** Um número real $\beta$ é dito transcendente, então esse número $\beta$ é irracional, isso segue de (3.2) pelo fato de que todo número real racional é algébrico.

Como citado acima, todos os números racionais são algébricos. Será todos números reais algébricos? A resposta é não. A existência dos números transcendentes foi demonstrada por G. Cantor e será apresentada no final desta seção.

**Exemplo 3.1.2:** O número $\sqrt{5}$ é algébrico, pois é solução da equação $x^2 - 25 = 0$

**Proposição 3.2:** A soma de dois números algébricos é algébrico.

*Demonstração.* Sejam $\alpha$ e $\beta$ números algébricos. Logo, existem equações polinomiais,

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0 \tag{3.3}$$

$$x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0 = 0 \tag{3.4}$$

com coeficientes racionais, tais que $\alpha$ seja raiz de (3.3) e $\beta$ seja raiz de (3.4). De (3.3) obtemos:

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0 \tag{3.5}$$

isto é, $\alpha^n$ está expresso como uma combinação linear de $1, \alpha, \ldots, \alpha^{n-1}$, usando coeficientes racionais. Multiplicando (3.5) por $\alpha$ e substituindo $\alpha^n$, obtido na expressão pelo seu valor de (3.5), obtemos $\alpha^{n+1}$ expresso como uma combinação linear dos mesmos $1, \alpha, \ldots, \alpha^{n-1}$, usando-se coeficientes racionais. De modo análogo podemos exprimir as potências $\beta^k$, para $k = m, m+1, \ldots$, como combinações lineares de $1, \beta, \ldots, \beta^{m-1}$ usando coeficientes racionais. Nosso objetivo agora é 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

$$1, \alpha + \beta, (\alpha + \beta)^2, \ldots, (\alpha + \beta)^{mn} \tag{3.6}$$

Desenvolvendo as várias potências $\alpha^j$, $j \geqslant n$ e $\beta^k$, $k \geqslant m$, obtemos que os números de (3.6) onde os $x_i's$ são $mn$ números $\alpha^j\beta^k$. Logo, existem racionais $r_0, r_1, \ldots, r_{mn}$ tais que,

$$r_0 + r_1(\alpha + \beta) + \cdots + r_{mn}(\alpha + \beta)^{mn} = 0 \tag{3.7}$$

o que mostra que $\alpha + \beta$ satisfaz uma equação polinomial de grau $mn$ com coeficientes racionais. E portanto $\alpha + \beta$ é algébrico. $\square$

**Proposição 3.3:** O produto de dois números algébricos é algébrico.

*Demonstração.* Segue as mesmas linhas da demonstração anterior. Em (3.6) entretanto, consideramos as potências $1, \alpha\beta, (\alpha\beta)^2, \ldots, (\alpha\beta)^{mn}$ e assim iremos concluir que o produto de dois números algébricos é algébrico. □

**Proposição 3.4:** O simétrico, $-\alpha$, de um número algébrico $\alpha$ é algébrico.

*Demonstração.* Se $\alpha$ é algébrico, então $-\alpha$ é raiz de uma equação

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

ou seja, $-\alpha$ é algébrico. □

**Proposição 3.5:** O inverso, $\alpha^{-1}$, de um número algébrico $\alpha \neq 0$ é algébrico.

*Demonstração.* Se $\alpha$ satisfaz a equação (3.1), e $\alpha \neq 0$, então $\alpha^{-1}$ satisfaz a equação,

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

e fica demonstrado o que queríamos. □

**Teorema 3.1:** O conjunto de todos os números algébricos é enumerável.

A demonstração dos dois primeiros itens segue de acordo com Djairo [3].

*Demonstração.* Dado um polinômio com coeficientes inteiros

$$P(x) = a_n x^n + \cdots + a_1 x + a_0 \tag{3.8}$$

definimos sua altura como sendo o número natural

$$|P(x)| = |a_n| + \cdots + |a_1| + |a_0| + n. \tag{3.9}$$

Pelo Teorema Fundamental da Álgebra, [5] temos que $P(x)$ em (3.8) tem $n$ raízes complexas. Todas, algumas ou nenhuma podem ser reais. O número de polinômios do tipo (3.8) com uma dada altura é apenas um número finito. Observe que é para essa afirmação que incluímos a parcela $n$ na definição de altura em (3.9). Portanto, as raízes de todos os polinômios com uma altura dada formam um conjunto finito. Sabemos que conjuntos finitos são enumeráveis, a seguir observamos que o conjunto de todas as raízes de todos os polinômios de todas as alturas formam um conjunto enumerável, pois é a união de um conjunto enumerável de conjuntos finitos. □

**Teorema 3.2:** Existem números transcendentes.

*Demonstração.* Do Teorema 3.1 temos que o conjunto dos números algébricos é enumerável. Como foi mostrado no Teorema 2.11 o conjunto dos números reais ($\mathbb{R}$) não é enumerável. Então o conjunto dos números transcendentes não deve ser enumerável. Caso contrário, se o conjunto dos números transcendentes fosse enumerável, teríamos de acordo com o Teorema 2.10 que $\mathbb{R}$ seria enumerável, como a união de dois conjuntos enumeráveis. Segue que o conjunto dos números transcendentes não é enumerável, portanto diferente de vazio. □

## 3.2 Raízes Racionais de equações polinomiais

Nesta seção veremos alguns procedimentos que nos auxiliam a encontrar raízes racionais de uma equação polinomial com coeficientes inteiros. Ao mesmo tempo nos fornece uma maneira simples para saber se $\alpha \in \mathbb{R}$ é transcendente, e portanto, irracional.

**Teorema 3.3:** Consideremos uma equação polinomial qualquer com coeficientes inteiros:

$$c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0 \tag{3.10}$$

Se essa equação tiver raiz racional $a/b$, com $a/b$ uma fração irredutível, então $a$ é um divisor de $c_0$ e $b$ é um divisor de $c_n$.

*Demonstração.* Seja $a/b$ uma raiz da equação (3.10). Isso significa que vale a igualdade abaixo. Substituindo $x$ por $a/b$:

$$c_n\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0 \tag{3.11}$$

Multiplicando ambos os termos por $b^n$, obtemos:

$$c_n a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n = 0 \tag{3.12}$$

que pode ser escrita como:

$$c_n a^n = -c_{n-1}a^{n-1}b - \cdots - c_1 ab^{n-1} - c_0 b^n$$

ou

$$c_n a^n = b(-c_{n-1}a^{n-1} - \cdots - c_1 ab^{n-2} - c_0 b^{n-1})$$

Isso mostra que $b$ é um divisor de $c_n a^n$. Temos que $mdc(a,\, b) = 1$, então $mdc(a^n,\, b) = 1$, ou seja, $b$ e $a^n$ são primos entre si, e portanto, $b$ divide $c_n$. Reescreveremos a equação (3.12) como

$$c_0 b^n = a(-c_n a^{n-1} - \cdots - c_1 b^{n-1}).$$

Isso mostra que $a$ é divisor de $c_0 b^n$. Como $mdc(a,\, b) = 1$ então $mdc(a,\, b^n) = 1$, concluímos assim que $a$ é divisor de $c_0$. □

**Corolário 3.1:** Consideremos uma equação da forma:

$$x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_2 x^2 + c_1 x + c_0 = 0$$

com coeficientes inteiros. Se essa equação possuir uma raiz racional, ela será um inteiro, além do mais, essa raiz inteira será um divisor de $c_0$.

*Demonstração.* Consideremos uma raiz racional $a/b$. Podemos supor que $b$ seja um inteiro positivo, porque se $b$ for negativo poderíamos absorver o sinal menos em $a$. De acordo com o último teorema, $b$ é um divisor de $c_n$, e portanto, um divisor de 1, logo, devemos ter $b = +1$, pois excluímos valores negativos para $b$. Consequentemente, qualquer raiz racional será da forma $a/1$ e, portanto, um inteiro $a$. Ainda pelo último teorema, sabemos que $a$ será um divisor de $c_0$ e isso completa a demonstração do corolário. $\square$

No próximo exemplo veremos como o Teorema 3.3 nos auxilia a encontrar números irracionais.

**Exemplo 3.2.1:** O número $\sqrt[3]{3}$ é irracional.

*Demonstração.* O número $\sqrt[3]{3}$ é uma raiz de $x^3 - 3 = 0$. De acordo com o Corolário 3.1, se essa equação tivesse uma raiz racional, seria um inteiro, divisor de 3. Os divisores de 3 são: $+1, -1, +3, -3$. Mas nenhum desses é uma raiz pois:
$1^3 - 3 = -2$; $(-1)^3 - 5 = -6$; $3^3 - 3 = 24$; $(-3)^3 - 3 = -30$, ou seja, nenhum divisor de 3 é raiz dessa equação. Portanto, $x^3 - 3 = 0$ não tem raízes racionais e $\sqrt[3]{3}$ é irracional. $\square$

Generalizando o exemplo acima, temos o seguinte corolário.

**Corolário 3.2:** Um número da forma $\sqrt[n]{a}$, com $a$ e $n$ inteiros positivos, ou é irracional ou é um inteiro; no segundo caso, $a$ é uma $n$-ésima potência de um inteiro.

*Demonstração.* O resultado decorre do Corolário 3.1, porque $\sqrt[n]{a}$ é uma raiz de $x^n - a = 0$, e se essa equação tiver uma raiz racional, ela terá que ser um inteiro. Além do mais, se $\sqrt[n]{a}$ for um inteiro, digamos $k$, então $a = k^n$. $\square$

## 3.3 O número $e$ é Irracional

Um número irracional cuja verificação não é imediata, é o número $e$. Nesta seção apresentaremos a demonstração que será baseada no livro de Djairo [3].

O número $e$ aparece no estudo da função logarítmica, e é definido pela área abaixo da curva $y = \dfrac{1}{x}$ de área igual a 1, com $x > 0$. Temos que:

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots \tag{3.13}$$

Suponha que $e$ fosse um número racional, isto é, $e = \frac{p}{q}$ , com p, q $\in \mathbb{N}$, primos entre si. Segue que

$$\frac{p}{q} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{q!}\right) = \sum_{k=q+1}^{\infty} \frac{1}{j!} \tag{3.14}$$

Agora, faremos uma estimativa do segundo membro:

$$\sum_{j=q+1}^{\infty} \frac{1}{j!} = \frac{1}{q!}\left(\frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \cdots\right) \tag{3.15}$$

$$< \frac{1}{q!}\left(\frac{1}{q+1} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + \cdots\right) \tag{3.16}$$

A expressão entre parênteses no último membro de (3.16) é uma série geométrica da forma $\sum_{n=1}^{\infty} r^n$ , com para $0 < r < 1$, e tem a soma igual a $r/(1-r)$. Usando esse fato obtemos:

$$\sum_{j=q+1}^{\infty} \frac{1}{j!} < \frac{1}{q!}\frac{1}{q} \tag{3.17}$$

Daí,

$$0 < \frac{p}{q} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{q!}\right) < \frac{1}{q!}\frac{1}{q} \tag{3.18}$$

sendo assim,

$$0 < q!\left(\frac{p}{q} - 1 - \frac{1}{1!} - \frac{1}{2!} - \cdots - \frac{1}{q!}\right) < \frac{1}{q} \tag{3.19}$$

O termo do meio é inteiro pois q! cancela todos os denominadores das frações presentes. Mas isso é impossível, pois sendo $1/q \leq 1$ a última expressão diria que o termo médio é um inteiro positivo estritamente menor que 1. O absurdo provém da hipótese feita inicialmente que $e$ fosse um número racional. Logo, $e$ é irracional.

## 3.4 O número $\pi$ é Irracional

O número $\pi$, razão do comprimento pelo diâmetro de um círculo, é um dos números irracionais mais conhecidos. O objetivo dessa seção é demonstrar que o número $\pi$ é irracional, seguiremos as orientações de Djairo, em [3]. Para isso consideremos a função,

$$f(x) = \frac{x^n(1-x)^n}{n!} \tag{3.20}$$

**Lema 3.1:** $D^k f(0)$ é um número inteiro para qualquer $k = 0,1,2,\ldots$ onde $D^k$ representa a k-ésima derivada de $f$, e $D^0 f = f$

*Demonstração.* Vamos utilizar a chamada fórmula de Leibniz para as derivadas de um produto de duas funções $g$ e $h$,

$$D^k(gh) = \sum_{j=0}^{k} \binom{k}{j} D^j g D^{(k-j)} h. \tag{3.21}$$

Note que a função $f(x)$ em (3.20) pode ser escrita como o produto das funções $g(x)= \frac{x^n}{n!}$ e $h(x)= (1-x)^n$. Logo aplicando (3.21) temos:

$$D^k f = \frac{1}{n!}\sum_{j=0}^{k}\binom{k}{j} D^j x^n D^{(k-j)}(1-x)^n \tag{3.22}$$

$\square$

Observe agora que:

$$D^j x^n|_{x=0} = \begin{cases} 0, & \text{se} \quad j < n \\ n!, & \text{se} \quad j = n \\ 0, & \text{se} \quad j > n \end{cases} \tag{3.23}$$

Já que, $D^1 x^n = nx^{n-1}, D^2 x^n = n(n-1)x^{n-2}, \ldots, D^j x^n = n(n-1)\ldots(n(j-1))x^{n-j}$, se $j < n$. Substituindo (3.23) em (3.21) segue que

$$D^k f(0) = 0 \text{ se } k \neq n$$

e que,

$$D^k f(0) = \frac{1}{n!}\binom{k}{n} n! D^{(k-n)}(1-x)^n|_{x=0} = 0, \text{ se } k > n. \tag{3.24}$$

Ou teremos,

$$D^k f(0) = \frac{1}{n!}\binom{k}{n} n! D^{(k-n)}(1-x)^n|_{x=0} = 1, \text{ se } k = n. \tag{3.25}$$

As derivadas $D^{k-n}(1-x)|_{x=0}$ é zero, para $k > n$, assim a equação (3.24) é facilmente calculada. Como os coeficientes binominais são inteiros segue que a expressão no segundo membro de (3.24) é um inteiro. Portanto, como $D^k f(0)$ é um número inteiro para qualquer $k = 0,1,2,\ldots$

**Lema 3.2:** $D^k f(1)$ é um número inteiro para qualquer $k = 0,1,2,\ldots$

*Demonstração.* Segue diretamente do lema anterior, e vale observar que:

$$f(1-x) = f(x)$$

pois,

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

De fato, como $D^k f(1-x)= (-1)^k D^k f(x)$, temos para $x$=0, que

$$D^k f(1) = D^k f(0)$$

Como $D^k f(0)$ é um número inteiro segue que $D^k f(1)$ também é um inteiro. $\square$

**Teorema 3.4:** $\pi$ é um número irracional.

*Demonstração.* Suponha que $\pi^2 = \dfrac{p}{q}$, em que $\dfrac{p}{q}$ é uma fração irredutível. Com essa suposição queremos encontrar um absurdo, mostrando assim que $\pi^2$ não é racional e consequentemente, $\pi$ não é racional, pois o quadrado de um número racional necessariamente é racional. Para isso, defina a função:

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

Podemos escrever $F(x)$ da seguinte maneira,

$$F(x) = \sum_{j=0}^{n} (-1)^j \pi^{2n-2j} D^{2j} f(x)$$

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

Como consequência dos Lemas 3.1 e 3.2, também da hipótese $\pi^2 = \dfrac{p}{q}$ , temos que $F(0)$ e $F(1)$ são números inteiros pois:

$$F(0) = q^n \left[ \left(\frac{p}{q}\right)^n f(0) - \left(\frac{p}{q}\right)^{n-1} D^2 f(0) + \cdots + (-1)^n D^{2n} f(0) \right] =$$

$$= -q^n \frac{p^{n-1}}{q^{n-1}} D^2 f(0) + \cdots + (-1)^n q^n D^{2n} f(0) =$$

$$= -qp^{(n-1)} D^2 f(0) + \cdots + (-1)^n q^n D^{2n} f(0)$$

e,

$$F(1) = -qp^{(n-1)} D^2 f(1) + \cdots + (-1)^n q^n D^{2n} f(1).$$

Agora, observe que,

$$\{F'(x) \operatorname{sen} \pi x - \pi F(x) \cos \pi x)\}' =$$

$$F''(x) \operatorname{sen} \pi x + F'(x) \pi \cos \pi x - \pi F'(x) cos \pi x + \pi^2 F(x) \operatorname{sen} \pi x =$$

$$F''(x) \operatorname{sen} \pi x + \pi^2 F(x) \operatorname{sen} \pi x,$$

onde $F'$ representa a derivada. Calculando $F''(x)$ temos,

$$F'(x) = q^n \{\pi^{2n} D^1 f(x) - \pi^{2n-2} D^3 f(x) + \cdots + (-1)^n D^{2n+1} f(x)\}, \text{ e}$$

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

Assim,

$$\{F'(x) \operatorname{sen}(\pi x) - \pi F(x) \cos(\pi x)\}' =$$

$$= \operatorname{sen}(\pi x)[q^n \{\pi^{2n} D^2 f(x) - \pi^{2n-2} D^4 f(x) + \cdots + (-1)^{n-1} D^{2n} f(x) + (-1)^n D^{2n+2} f(x)\}$$

$$+q^n\{\pi^{2n+2}f(x) - \pi^{2n}D^2f(x) + \pi^{2n-2}D^4f(x) + \cdots + (-1)^n\pi^2D^{2n}f(x)\}]$$
$$= \operatorname{sen}(\pi x)q^n\{(-1)^nD^{2n+2}f(x) + \pi^{2n+2}f(x)\}$$

De acordo com (3.24), podemos concluir que $\operatorname{sen}(\pi x)q^n\{(-1)^nD^{2n+2}f(x)\} = 0$. Sendo assim,

$$\{F'(x)\operatorname{sen}\pi x - \pi F(x)\cos\pi x)\}' = \operatorname{sen}(\pi x)q^n \cdot \pi^{2n} \cdot \pi^2 \cdot f(x).$$

E portanto,

$$\{F'(x)\operatorname{sen}(\pi x) - \pi F(x)\cos(\pi x)\}' = (F''(x) + \pi^2F(x))\operatorname{sen}(\pi x) = p^n\pi^2f(x)\operatorname{sen}(\pi x) \tag{3.26}$$

Agora, aplicamos o Teorema Fundamental do Cálculo que diz: "Se $g : [0,1] \to \mathbb{R}$ é uma função derivável em $(0, 1)$, então $\int_0^1 g'(x)dx = g(1) - g(0)$ ."

Use esse teorema para a função $g(x) = F'(x)\operatorname{sen}(\pi x) - \pi F(x)\cos(\pi x)$. Obtemos, então, em virtude de (3.26), que

$$p^n\pi^2\int_0^1 f(x)\operatorname{sen}(\pi x)dx = \pi F(1) + \pi F(0),$$

ou seja,

$$\pi p^n \int_0^1 f(x)\operatorname{sen}(\pi x)dx = F(1) + F(0) \tag{3.27}$$

A ideia para finalizar a demonstração é a seguinte: o lado direito de (3.27) é um inteiro, pois $F(1)$ e $F(0)$ são inteiros, se mostrarmos que para algum $n \in \mathbb{N}$ conveniente, o lado esquerdo de (3.27) é um número positivo estritamente menor que 1, teremos o absurdo procurado!

Note que para $0 < x < 1$, temos, $0 < x^n < 1$. E é claro que $0 < x \Longrightarrow 1 < x + 1 \Longrightarrow 1 - x < 1$, e portanto, $(1 - x)^n < 1$. E portanto,

$$0 < f(x) = \frac{x^n(1-x)^n}{n!} < \frac{x^n}{n!} < \frac{1}{n!} \tag{3.28}$$

Usando a desigualdade (3.28) em (3.27) temos,

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

onde a última igualdade foi obtida fazendo-se a integração indicada. Para $n$ muito grande $\dfrac{p^n}{n!} = 0$, ou seja, $\lim_{n\to\infty}\dfrac{p^n}{n!} = 0$, a demonstração que esse limite converge para zero, pode ser verificada em [6], assim podemos tomar um $n \in \mathbb{N}$ tal que $2p^n/n! < 1$, e nosso objetivo está atingido. □

Note que para esta prova não mencionamos a definição de $\pi$. Mas usamos algumas propriedades,um exemplo, que $\operatorname{sen}\pi = 0$.

# 4 Números Transcendentes

No estudo de números irracionais, usamos o conceito de números algébricos que nos auxiliam em alguns exemplos. Dois importantes números irracionais, o número $\pi$ e o número $e$, não são algébricos. Nesta seção mostraremos a transcendência desses números.

## 4.1 Os Números de Liouville

No capítulo anterior foi demonstrado que existem números transcendentes, mas não foi apresentado um exemplo de um número transcendente. Somente em 1851, que o matemático francês Liouville, apresentou um conjunto de números transcendentes que recebem o nome de números de Liouville. Usando esse resultado será possível escrever explicitamente alguns números transcendentes. Para este estudo, usaremos alguns conceitos da referência [8].

**Definição 4.1:** Diz-se que um número algébrico $\alpha$ é de grau $n$ se ele for raiz de uma equação polinomial de *grau* $n$ com coeficientes inteiros, e se não existir uma equação desse tipo, de menor grau, da qual $\alpha$ seja raiz.

Os números racionais coincidem com os números algébricos de grau 1, pois $\alpha$ racional da forma $\alpha = p/q$ é raiz de $qx - p = 0$.

**Definição 4.2:** Dizemos que um polinômio não constante $f(x)$ é irredutível em $\mathbb{Z}[x]$ (ou irredutível sobre $\mathbb{Z}$) se é impossível expressar $f(x)$ como o produto $g(x) \cdot h(x)$ de dois polinômios $g(x)$ e $h(x)$ em $\mathbb{Z}[x]$ cujos graus são ambos maiores ou iguais a 1.

**Exemplo 4.1.1:** o número $\sqrt[3]{2}$ tem grau 3, pois é raiz de $x^3 - 2 = 0$, que é irredutível em $\mathbb{Z}$. E portanto $\sqrt[3]{2}$ é dito um número algébrico de grau 3.

**Definição 4.3:** Um número real $\alpha$ é aproximável na ordem $n$ por racionais se existirem uma constante $c > 0$ e uma sequência $(p_j/q_j)$ de racionais diferentes, com $q_j > 0$ e $mdc(p_j, q_j) = 1$, tais que

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{c}{q_j^n} \tag{4.1}$$

Uma observação que podemos fazer é que se um número $\alpha$ for aproximável na ordem $n$, então ele é aproximável em qualquer ordem $k$, com $k < n$. Pela desigualdade (4.1) segue que :

$$\left|\alpha - \frac{p_j}{q_j}\right| < c \tag{4.2}$$

o que mostra que a sequência $(q_j)$ não se mantém limitada. De fato, temos que,

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

Suponha $(q_j)$ é limitada, isto é, $q_j \leqslant M$. Daí,

$$|\alpha q_j - p_j| < cq_j \leqslant cM$$

$$|p_j| - |\alpha q_j| \leqslant cM$$

$$|p_j| \leqslant cM + \alpha|q_j| \leqslant cM + |\alpha cM| \leqslant (|\alpha| + 1)Mc$$

Absurdo, pois existem infinitos $p_j/q_j$. Logo, $q_j$ é ilimitada. Ou seja, se $(q_j)$ fosse limitada, $(p_j)$ seria limitada. Mas $(p_j/q_j)$ são diferentes e existem finitos $(p_j/q_j)$.

Note que a sucessão de racionais apresentada na Definição 4.2 converge para $\alpha$. E sabemos que tais sequências sempre existem, para qualquer que seja o real $\alpha$. De fato, podemos, pois concluir que $q_j \to +\infty$. Logo,

$$\lim_{j\to\infty}\left(\frac{p_j}{q_j}\right) = \alpha \tag{4.3}$$

**Exemplo 4.1.2:** Todo número racional é aproximável na ordem 1, e não é aproximável na ordem $k$, para $k > 1$.

*Demonstração.* De acordo com o Teorema de Bézout, que pode ser encontrado em [9], temos que se $p/q$ um número racional, com $q > 0$ e $mdc(p, q) = 1$. Sendo assim, existem $x_0, y_0 \in \mathbb{Z}$ tais que,

$$px_0 - qy_0 = 1 \tag{4.4}$$

Veremos que a equação,

$$px - qy = 1 \tag{4.5}$$

tem um número infinito de soluções. De fato,

$$x_t = x_0 + qt, \qquad y_t = y_0 + pt \tag{4.6}$$

para qualquer $t \in \mathbb{Z}$, satisfazem (4.5), isto é,

$$px_t - qy_t = 1. \tag{4.7}$$

Fixe $k \in \mathbb{N}$, tal que $k > -x_0/q$ e considere as sucessões $\{x_j\}, \{y_j\}$ definidas a partir de (4.6), por

$$x_j = x_0 + q(k+j), \qquad y_j = y_0 + p(k+j), j \in \mathbb{N}. \tag{4.8}$$

Pela restrição posta em $K$, temos $x_j > q_j$ e daí $x_j > 0$, pois $q > 0$. Agora, afirmamos que

$$\frac{y_j}{x_j} \neq \frac{j_j^{'}}{x_j^{'}} \text{ se } j \neq j^{'}. \tag{4.9}$$

Suponhamos que há igualdade dos racionais, em (4.9). Usando (4.6) e (4.4), concluímos que $j = j^{'}$. Em virtude de (4.7), os $x_j^{'}s$ e $y_j^{'}s$, definidos em (4.8), satisfazem a desiguldade,

$$\left|\frac{p}{q} - \frac{y_j}{x_j}\right| = \frac{1}{qx_j} < \frac{2}{x_j}, \tag{4.10}$$

o que mostra que $p/q$ é aproximável na ordem 1.

Para qualquer racional $v/u \neq p/q$, com $u > 0$, tem-se

$$\left|\frac{p}{q} - \frac{v}{u}\right| = \frac{|pu - qv|}{qu} \geqslant \frac{1}{qu}. \tag{4.11}$$

Se $p/q$ fosse aproximável na ordem 2, teríamos a existência de $c > 0$, e de uma sucessão de racionais $v_j/u_j$ diferentes, tais que,

$$\left|\frac{p}{q} - \frac{v_j}{u_j}\right| < \frac{c}{u_j^2}. \tag{4.12}$$

De (4.11) e (4.12), segue que $1/qu_j < c/u_j^2$, ou seja, $u_j < qc$. Isso, porém, não é possível, pois $u_j \longrightarrow +\infty$. Logo, $p/q$ não é aproximável na ordem 2, e portanto, em nenhuma ordem superior. □

**Exemplo 4.1.3:** Todo número irracional é aproximável na ordem 2.

Alguns números irracionais também podem ser aproximáveis em ordem superior a 2. O próximo teorema nos dará informações específicas sobre essas ordens de aproximação.

A demonstração do exemplo acima, pode ser verificada em [3]. Podemos nos perguntar sobre a constante $c$ da Definição 4.3. Se $\lambda$ é um número irracional existe uma constante $c > 0$ tal que a desigualdade abaixo se verifica para um número infinito de racionais $p/q$ distintos:

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

De acordo com Djairo, [3], o matemático Hurwitz mostrou que a menor constante $c$

que serve para todos irracionais na desigualdade acima é $1\sqrt{5}$.

**Teorema 4.1:** Seja $\alpha$ um número algébrico real de grau $n$. Então, existe uma constante $A > 0$ tal que, para todo racional $p/q$, é válida a relação

$$\left|\alpha - \frac{p}{q}\right| > \frac{A}{q^n}, \ \forall \ \ p/q \ \ \in \mathbb{Q}, \ \ \text{com } q \ \geqslant 1$$

*Demonstração.* Como $\alpha$ é algébrico de grau $n$, ele é raiz de uma equação polinomial da forma:

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{4.13}$$

Em que $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, com $f(x) = 0$, existe $\delta > 0$ tal que, no intervalo $[\alpha - \delta, \ \alpha + \delta]$ a única raiz de $f(x) = 0$ é $\alpha$. ( A existência de tal valor $\alpha$ se segue do fato de a equação polinomial ter no máximo $n$ raízes reais: portanto $\alpha$ pode ser qualquer número menor das distâncias de $\alpha$ às demais raízes reais). Dado $p/q \ \ \in \ \ \mathbb{Q}$, temos duas possibilidades:

1. $p/q \notin [\alpha - \delta, \ \alpha + \delta]$, então $\left|\alpha - \dfrac{p}{q}\right| > \delta \geqslant \dfrac{\delta}{q^n}$
2. $p/q \ \ \in \ \ [\alpha - \delta, \ \alpha + \delta]$. A função $f$ é contínua em $[\alpha - \delta, \ \alpha + \delta]$ e derivável no intervalo $(\alpha - \delta, \ \alpha + \delta)$. Logo, pelo Teorema do Valor Médio, existe um $\xi \in (\alpha - \delta, \alpha + \delta)$, tal que,

$$f'(\xi) = \frac{f(\alpha) - f(p/q)}{(\alpha - p/q)}.$$

Utilizando a última igualdade e o fato de $f(\alpha) = 0$, obtemos que

$$\left|f\left(\frac{p}{q}\right)\right| = |f'(\xi)|\left|\alpha - \frac{p}{q}\right|.$$

Como $f'$ é contínua no intervalo fechado com extremos $\alpha - \delta$ e $\alpha + \delta$, observe que $f'$ é um polinômio de grau $n - 1$, então, $|f'(x)| \leqslant M, \ \forall \ \ x$ no intervalo de $[\alpha - \delta, \ \alpha + \delta]$. Assim,

$$\left|f\left(\frac{p}{q}\right)\right| = |f'(\xi)|\left|\alpha - \frac{p}{q}\right| \leqslant M \cdot \left|\alpha - \frac{p}{q}\right|$$

Sabemos que $0 \neq \left|f\left(\dfrac{p}{q}\right)\right|$, e que,

$$\left|f\left(\frac{p}{q}\right)\right| = \left|a_0 + a_1\frac{p}{q} + \cdots + a_n\frac{p^n}{q^n}\right|$$

$$= \left|\frac{a_0 q^n + a_1 q^{n-1} p + \cdots + a_n p^n}{q^n}\right| = \frac{|a_0 q + \cdots + a_n q^n|}{q^n} \geqslant \frac{1}{q^n}.$$

Daí,

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

tomando $A =$ mínimo $\{\delta, 1/M\}$, temos:

$$\left|\alpha - \frac{p}{q}\right| > \frac{A}{q^n} \quad \forall \;\; p/q \quad \in \quad \mathbb{Q}.$$

□

Agora, podemos definir o chamado número de Liouville, o primeiro exemplo de números transcendentes.

**Definição 4.4:** Um número real $\alpha$ é chamado um número de Liouville se existir uma sequência $(p_j/q_j)$ de racionais todos distintos, onde $p_j, q_j \in \mathbb{Z}$, com $q_j > 0$ e $mdc(p_j,\ q_j) = 1$, tais que satisfaçam

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

**Teorema 4.2:** Todo número de Liouville é transcendente.

*Demonstração.* Suponha que $\alpha$ é Liouville e algébrico de grau $n$. De acordo com o Teorema 4.1, temos que existe $(p_j/q_j)$ tais que:

$$\frac{A}{q_j^n} < \left|\alpha - \frac{p_j}{q_j}\right|, \forall \;\; j \geqslant 1.$$

E pela definição de números de Liouville, temos que existe $(p_j/q_j)$ tais que :

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

Então,

$$\frac{A}{q_j^n} < \frac{1}{q_j^j} \Longrightarrow q_j^{n-j} < A.$$

Absurdo, pois $(q_j)$ é ilimitada. Logo, todo número de Liouville é transcendente.

□

**Lema 4.1:** Seja $\alpha$ um número real tal que

$$\left|\alpha - \frac{v_j}{u_j}\right| < \frac{1}{u_j^j},$$

onde $\{v_j/u_j\}$ é uma sucessão de racionais diferentes com $u_j > 0$. Então $\alpha$ é um número de Liouville.

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

$$\frac{p_j}{q_j} = \frac{v_j}{u_j}.$$

Então,

$$\left|\alpha - \frac{p_j}{q_j}\right| = \left|\alpha - \frac{v_j}{u_j}\right| < \frac{1}{u_j^j} < \frac{1}{q_j^j},$$

o que prova que $\alpha$ é um número de Liouville. $\square$

Como já mencionado em (3.1.1) que todo número real transcendente é não racional, por esse fato, segue que um número real $\alpha$ de Liouville é irracional.

**Exemplo 4.1.4:** Seja

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} \tag{4.14}$$

Consideremos a sucessão de racionais definida por:

$$\frac{v_j}{u_j} = \sum_{k=1}^{j} \frac{1}{10^{k!}}.$$

Temos,

$$\left|\alpha - \frac{v_j}{u_j}\right| = \sum_{k=j+1}^{\infty} \frac{1}{10^{k!}} = \frac{1}{10^{(j+1)!}}\left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + \cdots\right) \tag{4.15}$$

A expressão em parêntese é majorada por

$$1 + \frac{1}{10} + \frac{1}{10^2} + \cdots = \frac{10}{9}.231$$

Logo, o último membro de (4.15) é marjorada por

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

e portanto,

$$\left|\alpha - \frac{v_j}{u_j}\right| < \frac{1}{(10^{j!})^j}.$$

Como $u_j = 10^{j!}$, segue-se que $\alpha$ definido em (4.14) é um número de Liouville.

**Exemplo 4.1.5:** Qualquer número da forma

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

onde $a_k$ é qualquer um dos algarismos de 1 a 9, é um número de Liouville.

## 4.2 A transcendência do número $e$

Mostramos que o número $e$ é irracional na seção 3.3. Demonstraremos nesta seção que o número $e$ é transcendente. Saber se um dado número é transcendente, é, em geral, uma questão muito difícil, talvez por esse motivo, a demonstração do número $e$ foi um desafio aos matemáticos até o século XIX. Em 1873, o matemático francês C. Hermite demonstrou a transcendência do número $e$. A demonstração original de Hermite sofreu simplificações sucessivas por matemáticos famosos como Jordan (1882), Markhoff (1883), Rouché (1883), Weierstrass (1885), Hilbert (1893), Hurwitz (1893) e Veblen (1904), entre outros. A demonstração que será apresentada é baseada em Hurwitz. Sendo assim, consideremos $P(x)$ um polinômio de grau $r$. Defina a função,

$$F(x) = P(x) + P'(x) + \cdots + P^{(r)}(x) \tag{4.16}$$

onde $P^{(r)}$ representa a derivada de ordem $r$ de $P$. Temos que,

$$\frac{d}{dx}(e^{-x}F(x)) = -e^{-x}P(x).$$

De fato, observamos que $\frac{d}{dx}(e^{-x}F(x)) = \frac{d}{dx}(e^{-x})F(x) + \frac{d}{dx}(F(x))e^{-x}$

$$= -e^{-x}F(x) + e^{-x}(P'(x) + P"(x) + \cdots + P^r(x) + P^{r+1})$$

$$= e^{-x}(-P(x) - P'(x) - \cdots - P^r(x) + P"(x) + \cdots + P^r(x) + P^{r+1}(x))$$

$$= e^{-x}(-P(x) + P^{r+1}(x)) = e^{-x}(-P(x)) = -e^{-x}P(x).$$

**Proposição 4.1:**

$$F(k) - e^k F(0) = -ke^{k(1-\theta_k)}P(k\theta_k),\ \forall k > 0,\ \text{ e } \ 0 < \theta_k < 1 \tag{4.17}$$

*Demonstração.* Seja $G(x) = e^{-x}F(x)$, temos que $G$ é contínua e derivável em $\mathbb{R}$, em particular em $[0, k]$. Pelo Teorema do Valor Médio, existe $c \in (0, k)$, tal que $G'(c) = \dfrac{G(k) - G(0)}{(k-0)}$, chamando $c = k\theta_k$ e $0 < \theta_k < 1$. Assim,

$$G(k) - G(0) = G'(k\theta_k).(k-0)$$

$$e^{-k}F(k) - e^{-0}F(0) = -ke^{-k\theta_k}F(k\theta_k) + e^{-k\theta_k}F'(k\theta_k)$$

$$F(k) - e^k F(0) = -ke^{k(1-\theta_k)} F(k\theta_k) + e^{k(1-k\theta_k)} F'(k\theta_k)$$
$$F(k) - e^k F(0) = -ke^{k(1-\theta_k)} [F(k\theta_k) - F'(k\theta_k)]$$
$$F(k) - e^k F(0) = -ke^{k(1-\theta_k)} P(k\theta_k)$$

Para todo $k > 0$ e $0 < \theta_k < 1$. □

Agora seja $\varepsilon_k = F(k) - e^k F(0)$, sendo assim,

$$\varepsilon_k = -ke^{k(1-\theta_k)} P(k\theta_k) \tag{4.18}$$

e suponha que $e$ seja algébrico, isto é, existem inteiros $c_0, c_1, \ldots, c_n$ (podemos tomar $c_0 > 0$) tais que

$$c_n e^n + \cdots + c_1 e + c_0 = 0. \tag{4.19}$$

Note que:

$$c_0 F(0) + c_1 F(1) + \cdots + c_n F(n) = c_1 \varepsilon_1 + \cdots + c_n \varepsilon_n. \tag{4.20}$$

De fato, partindo de que $F(k) - e^k F(0) = -ke^{k(1-\theta_k) P(k\theta_k)}$ temos que $\varepsilon_k = F(k) - e^k F(0)$, isto é, $F(k) - \varepsilon_k = e^k F(0), \forall k > 0$. Assim,

$$[c_0 F(0) + c_1 F(1) + \cdots + c_n F(n)] - [c_1 \varepsilon_1 + \cdots + c_n \varepsilon_n]$$
$$= c_n [F(n) - \varepsilon_n] + \cdots + c_1 [F(1) - \varepsilon_1] + c_0 F(0)$$
$$= c_n e^n F(0) + \cdots + c_1 e^1 F(0) + c_0 F(0)$$
$$= F(0)[c_n e^n + \cdots + c_1 e + c_0] = F(0).0 = 0.$$

Concluímos assim que é válida a igualdade (4.20).

Considere agora o polinômio

$$P(x) = \frac{1}{(p-1)!} x^{p-1} (1-x)^p \ldots (n-x)^p. \tag{4.21}$$

Em que $p$ é um número primo tal que $p > n$, $p > c_0$, e $n$ e $c_0$ são números dados em (4.19). A ideia agora é demonstrar que o lado esquerdo de (4.20) é um inteiro não divisível por $p$, enquanto o lado direito é menor que 1 em valor absoluto. Isso dará o absurdo. Agora será mencionado alguns conceitos matemáticos importantes para concluir que o lado esquerdo de (4.20) é um inteiro não divisível por $p$.

**Lema 4.2:** Seja $Q(x) = \sum_{j=0}^{r} a_j x^j$ um polinômio com coeficientes inteiros, e seja $p < r$. Então

$$Q^{(i)}(x) = \sum_{j=i}^{r} \frac{j!}{(j-i)!} a_j x^{j-i}, i \leqslant r. \tag{4.22}$$

Utilizando o Lema 4.2 é possível mostrar que $\dfrac{1}{(p-1)!}Q^{(i)}(x)$, para $i \geqslant p$, é um polinômio com coeficientes inteiros divisíveis por $p$.

Antes façamos alguns exemplos, para $r = 4$.

$$Q(x) = \sum_{j=0}^{4} a_j x^j = a_0x^0 + a_1x^1 + a_2x^2 + a_3x^3 + a_4x^4$$

$$Q^{(1)}(x) = a_1 + 2a_2x^{2-1} + 3a_3x^{3-1} + 4a_4x^{4-1}$$

$$Q^{(2)}(x) = 2a_2 + 2 \cdot 3a_3x + 3 \cdot 4a_4x^2$$

$$Q^{(3)}(x) = 2 \cdot 3a_3 + 2 \cdot 34a_4x$$

$$Q^{(4)}(x) = 1 \cdot 2 \cdot 3 \cdot 4a_4x^0.$$

Logo, podemos escrever

$$Q^{(1)}(x) = \sum_{j=1}^{4} \frac{j!}{(j-i)!} a_j x^{j-1}$$

Provaremos por Indução a expressão para $Q^{(1)}(x)$. Verificaremos se $Q^{(1)}(x)$ é válida.

$$Q^{(1)}(x) = [Q(x)]'$$

$$\left(\sum_{j=0}^{r} a_j x^j\right)' = (a_0x^0 + a_1x^1 + \cdots + a_rx^r)' = (1a_1x^{1-1} + 2a_2x^{2-1} + \cdots + ra_rx^{r-1}) =$$

$$\frac{1!}{(1-1)!}a_1x^{1-1} + \frac{2!}{(2-1)!}a_2x^{2-1} + \cdots + \frac{r!}{(r-1)!}a_rx^{r-1} = \sum_{j=1}^{r} \frac{j!}{(j-1)!} a_j x^{j-1}$$

portanto $Q^{(1)}$ é válida.

`Hipótese de Indução:` Suponha que $Q^{(k)}(x)$ é válida. Se,

$$Q^{(k)}(x) = \sum_{j=k}^{r} \frac{j!}{(j-k)!} a_j x^{j-k}$$

Então

$$Q^{(k+1)}(x) = \sum_{j=k+1}^{r} \frac{j!}{(j-k)!} (j-k) a_j x^{j-(k+1)}$$

$$= \sum_{j=k+1}^{r} \frac{j!}{(j-(k+1))!} a_j x^{j-(k+1)}.$$

Logo, a expressão para $Q^{(k+1)}(x)$ é válida. Pelo Princípio da Indução Finita é válido a expressão para $Q^{(i)}(x)$, $i \leqslant r$ e $r \in \mathbb{N}$.

Mostraremos agora que $\dfrac{1}{(p-1)!}Q^{(i)}(x)$, para $i \geqslant p$, é um polinômio com coeficientes inteiros, tal que os seus coeficientes sejam divisíveis por $p$. Observe que, $(i \leqslant r)$,

$$\frac{1}{(p-1)!}Q^{(i)}(x) = \frac{1}{(p-1)!}\sum_{j=i}^{r}\frac{j!}{(j-i)!}a_j x^{j-i} = \sum_{j=i}^{r}\frac{1}{(p-1)!}\cdot\frac{j!}{(j-i)!}a_j x^{j-i} =$$

$$\sum_{j=i}^{r}\frac{i\cdot(i-1)\ldots p\cdot j!}{i\cdot(i-1)\ldots p(p-1)!(j-1)!}a_j x^{j-i} =$$

$$\sum_{j=i}^{r}\frac{i\cdot(i-1)\ldots p\cdot j!}{i!(j-i)!}a_j x^{k-i} = \sum_{j=i}^{r} i\ldots p\binom{j}{i}a_j x^{j-i}$$

Note que $\binom{j}{i} \in \mathbb{Z}, i, \ldots, p \in \mathbb{Z}$ o fator de $p$ aparece pelo menos uma vez no produto $i\ldots p\binom{j}{i}$ e $i, \ldots, p\binom{j}{i}a_j$ são inteiros divisíveis por $p$. Ou seja, os coeficientes de $\dfrac{1}{(p-1)!}Q^{(i)}(x)$ são inteiros divisíveis por p.

**Lema 4.3:** Considere o polinômio $P(x)$ definido em (4.21). Temos que $P(x)$ é da forma:

$$P(x) = \frac{(n!)^p}{(p-1)!}x^{p-1} + \frac{b_0}{(p-1)!}x^p + \cdots \tag{4.23}$$

*Demonstração.* Temos que $P(x) = \dfrac{1}{(p-1)!}x^{p-1}(1-x)^p \ldots (n-x)^p$. Observe que:

$$(1-x)^p = 1 + p(-x) + \cdots + \binom{p}{i}(-x)^i + \cdots + (-x)^p \tag{4.24}$$

$$(2-x)^p = 2^p + p2^{p-1}(-x) + \cdots + \binom{p}{i}2^{p-1}(-x)^i + \cdots + (-x)^p \tag{4.25}$$

$$(3-x)^p = 3^p + p3^{p-1}(-x) + \cdots + \binom{p}{i}3^{p-1}(-x)^i + \cdots + (-x)^p \tag{4.26}$$

$$\vdots$$

$$(n-x)^p = n^p + pn^{p-1}(-x) + \cdots + \binom{p}{i}n^{p-i}(-x)^i + \cdots + (-x)^p \tag{4.27}$$

Note que o produto dos termos de (4.24), (4.25), ..., (4.27) é um polinômio de grau $np$ e o termo independente $1\cdot 2^p\cdot 3^p\ldots n^p = (n!)^p$. Assim,

$$(1-x)^p\ldots(n-x)^p = (n!)^p + b_0x + b_1x^2 + \cdots + b_{np-1}x^{np}.$$

E dessa maneira,

$$P(x) = \frac{x^{p-1}}{(p-1)!}(n!)^p + \frac{b_0 x^p}{(p-1)!} + \cdots$$

□

Além disso, $P^{(i)}(k) = 0; k = 1, \ldots, n;\ \ i < p$ e $P^{(p-1)}(0) = (n!)^p$, e $P^{(i)}(0) = 0$, $i < p - 1$. De fato, note que por $P(x) = \frac{1}{(p-1)!}x^{p-1}(1-x)^p \ldots (n-x)^p$, teremos:

$$P^1(x) = \frac{1}{(p-1)!}(p-1)x^{p-2}(1-x)^p + \cdots + \left(\frac{1}{(p-1)!}x^{p-1}\right)(1-x)^p \ldots p(n-x)^{p-1}.$$

Observe que as derivadas $i-$ ésimas para $i < p$ assim como $P^{(1)}$ serão somas de parcelas que são produtos de termos, no qual, em cada parcela aparecerá $(k-x)^{p-i}$, para $k = 1, \ldots, r$. Logo, $P^{(i)}(k) = 0$, para $k = 1, \ldots, n$. Ainda, veja que:

$$P^{(p-1)}(x) = \frac{(n!)^p}{(p-1)!}(p-1)! + \frac{b_0}{(p-1)!}p \cdot (p-1) \ldots 2x + \ldots$$

$$P^{(p-1)}(x) = (n!)^p + b_0 px + \cdots$$

$$P^{(p-1)}(0) = (n!)^p.$$

Para $i < p - 1$, todas as parcelas de $P^{(i)}(x)$ possuem a variável $x$, já que o termo de menor grau em $P(x)$ possui grau $p - 1$. Logo, $P^{(i)}(0) = 0$, para $i < p - 1$.

Usando os Lemas 4.2 e 4.3 vamos mostrar que $F(k)$, para $k = 1, \ldots, n$ é um inteiro divisível por $p$. E também que $F(0)$ é um inteiro não divisível por $p$. Para isto, lembremos que $F(x) = P(x) + P'(x) + \cdots + P^{(r)}(x)$.

Seja $Q(x) = x^{p-1}(1-x)^p \cdot (2-x)^p \ldots (n-x)^p$. Assim temos $Q(x) = n!x^{p-1} + b_0 x^p + \cdots + b_n x^{p+n \cdot p-1} \in \mathbb{Z}[x]$ onde $\partial Q =$ grau $(Q(x)) = (n+1) \cdot p - 1 = r > p$. Logo, $Q(x)$ satisfaz o Lema 4.2 e $P(x) = \frac{1}{(p-1)!} \cdot Q(x)$. Para $i \geqslant p$, $P^{(i)}(x) = \frac{1}{(p-1)!}Q^{(i)}(x)$ é um polinômio com coeficientes inteiros divisíveis por $p$. Donde, para $i \geqslant p, P^{(i)}(k)$ é um número inteiro divisível por $p$, para todo $k \in \mathbb{Z}$ e, em particular, para $k = 1, \ldots, n$. Qualquer que seja o caso, temos que $P(k)^{(i)}$ é um inteiro divisível por $p$, para $k = 1, \ldots, n$ onde $0 \leqslant i \leqslant r = p + n \cdot p - 1$. Logo, $F(k) = P(k) + P'(k) + \cdots + P^{(r)}$ é um inteiro divisível por $p$, $\forall k \in 1, \ldots, n$. Agora, $F(0) = P(0) + P'(0) + \cdots + P^{(p-2)}(0) + P^{(p-1)}(0) + P^{(p)}(0) + \cdots + P^{(r)}(0)$. Pelo Lema 4.3, $F(0) = (n!)^p + P^{(p)}(0) + \cdots + P^{(r)}(0)$. Sabemos que $P^{(i)}(0)$ é um número inteiro divisível por $p$, para $i \geqslant p$ e $k = 0$, o qual vimos acima. Portanto, $p$ divide $P^{(p)}(0) + \cdots + P^{(r)}(0)$, uma vez que $p$ divide $P^{(p)}(0), \ldots, P(0)$. Mas como $p$ não divide $(n!)^p$, pois $p$ é primo e $p > n$, então $p$ não divide $(n!)^p + P^{(p)}(0) + \cdots + P^{(r)}(0)$, ou seja, $F(0)$ é um inteiro não divisível por $p$.

**Proposição 4.2:** Temos que $c_0 F(0) + c_1 F(1) + \cdots + c_n F(n)$ é um inteiro não divisível por $p$. (Os coeficientes $c_{is}$ foram definidos na expressão 4.19, $0 < c_0 < p$.)

*Demonstração.* Tome $d_k = c_k F(k)$. Para $k = 1, \dots, n$ e $d_k$ é um inteiro divisível por $p$ e $d_0 = c_0 F(0)$ é um inteiro não divisível por $p$, já que $F(0) < c_0 < p$. Logo, $\sum_{k=0}^{n} d_k$ não é divisível por $p$, mas $\sum_{k=0}^{n} d_k = d_0 + d_1 + \cdots + d_n = c_0F(0) + c_1F(1) + \cdots + c_nF(n)$. Portanto, $c_0F(0) + c_1F(1) + \cdots + c_nF(n)$ é um inteiro não divisível por $p$. □

Agora, mostraremos que $|c_1\epsilon_1 + \cdots + c_n\epsilon_n| < 1$, como já mencionado anteriormente chegaremos em um absurdo, pois da equação (4.20) teremos que o lado esquerdo é um número inteiro, e o lado direito tem módulo menor do que 1.

Observe que os $\varepsilon_k$, definido em (4.18) e calculados para o polinômio $P(x)$, definido em (4.21) têm a forma,

$$\epsilon_k = -ke^{k(1-\theta_k)}\frac{1}{(p-1)!}(k\theta_k)^{p-1}(1-k\theta_k)^p \dots (n-k\theta_k)^p. \tag{4.28}$$

Usando a definição de $\epsilon_k$ em (4.28), então,

$$|\epsilon_k| = \left| -ke^{k(1-\theta_k)}\frac{1}{(p-1)!}(k\theta_k)^{p-1}(1-k\theta_k)^p \dots (n-k\theta_k)^p \right|$$

$$= \frac{1}{(p-1)!}|-k||e^{k(1-\theta_k)}||(k\theta_k)^{p-1}||(1-k\theta_k)^p| \dots |(n-k\theta_k)^p|$$

$$\leqslant \frac{1}{(p-1)!}ne^{n(1-\theta_k)}|n\theta_k|^{p-1}|1-\theta_k|^p \dots |n-\theta_k|^p$$

$$\leqslant \frac{1}{(p-1)!}ne^n n^{p-1} = \frac{e^n n^p}{(p-1)!} \leqslant \frac{e^n n^p (n!)^p}{(p-1)!}.$$

Assim, $|\epsilon_k| \leqslant \dfrac{e^n n^p (n!)^p}{(p-1)!}$

Além disso, temos que, $|c_1\epsilon_1 + \cdots + c_n\epsilon_n| \leqslant |c_1\epsilon_1| + \cdots + |c_n\epsilon_n|$
$\leqslant |c_1|\dfrac{e^n n^p (n!)^p}{(p-1)!} + \cdots + |c_n|\dfrac{e^n n^p (n!)^p}{(p-1)!} = (|c_1| + \cdots + |c_n|)\dfrac{e^n n^p (n!)^p}{(p-1)!}$.

Para $p$ um número suficientemente grande temos:

$$|c_1\epsilon_1 + \cdots + c_n\epsilon_n| \leqslant (|c_1| + \cdots + |c_n|)\frac{e^n n^p (n!)^p}{(p-1)!} < 1.$$

Agora temos ferramentas suficientes para concluir sobre a transcendência do número $e$.

Supondo que o número $e$ é algébrico, existem inteiros $c_0, c_1, \dots, c_n$ (com $c_0 > 0$) tais que $c_ne^n + \cdots + c_1e + c_0 = 0$, temos que $c_0F(0) + \cdots + c_nF(n) = c_1\epsilon_1 + \cdots + c_n\epsilon_n$, e $c_0F(0) + \cdots + c_nF(n)$ é um inteiro não divisível por $p$, porém temos que nessas condições que $|c_1\epsilon_1 + \cdots + c_n\epsilon_n| < 1$, o que é um absurdo, já que um número inteiro não nulo tem módulo sempre maior ou igual a um. O absurdo foi supor que $e$ é um número algébrico.

Terminando, assim, a prova de $e$ ser transcendente.

## 4.3 A transcendência do número $\pi$

O método usado por Hermite para demonstrar a transcendência de $e$ foi estendido por Lindemann, em 1882, para demonstrar a transcendência do número $\pi$. Como a demonstração do número $e$ passou por algumas alterações apresentadas por alguns matemáticos, como citado na seção 4.2, o mesmo ocorreu com o número $\pi$. A demonstração da transcendência de $\pi$, que será apresentada nesta seção, é baseada na demonstração feita por R. Moritz. Como consequência do fato de que o número $\pi$ é transcendente, fica provado que o problema da quadratura do círculo tem resposta negativa. Esse problema é conhecido há muitos anos e consiste em saber se é possível, com régua e compasso, construir um quadrado cuja área seja igual a de um círculo dado.

Para a demonstração que o número $\pi$ é transcendente será utilizado alguns recursos de Análise Complexa.

**Teorema 4.3:** O número $\pi$ é transcendente.

Suponhamos, por contradição, que $\pi$ seja um número algébrico. Logo, $i\pi$, uma vez que $i = \sqrt{-1}$ seria também algébrico, como um produto de dois números algébricos. Então $i\pi$ seria raiz de uma equação polinomial com coeficientes inteiros:

$$P_1(x) = 0 \tag{4.29}$$

O polinômio em (4.29) além da raiz $\alpha_1 = i\pi$, possui outras raízes, digamos $\alpha_2, \ldots, \alpha_n$. Como $e^{i\pi} = -1$, temos que o produto $(1 + e^{\alpha_1})(1 + e^{\alpha_2}) \ldots (1 + e^{\alpha_n}) = 0$. Assim,

$$\prod_{j=1}^{n} (1 + e^{\alpha_j}) = 0 \tag{4.30}$$

Note que ao desenvolvermos o produto indicado em (4.30), obteremos uma expressão da forma um mais o somatório de exponenciais, para maiores informações o leitor pode verificar no capítulo de Polinômios Simétricos em [3] cujos expoentes são:

$$\alpha_1, \alpha_2, \cdots, \alpha_n \tag{4.31}$$

$$\alpha_i + \alpha_j, \quad para \quad todos \quad i < j \tag{4.32}$$

$$\alpha_i + \alpha_j + \alpha_k, \quad para \quad todos \quad i < j < k \tag{4.33}$$

$$\vdots$$

$$\alpha_1 + \cdots + \alpha_n \tag{4.34}$$

Observemos que o número de termos em (4.31) é $n$, em (4.32) é $\binom{n}{2}$, em (4.33) é $\binom{n}{3}$ , ... , em (4.34) é $\binom{n}{n} = 1$ , em que $\binom{n}{m}$ são coeficientes binomiais, isto é,

$\binom{n}{m} = \dfrac{n!}{m!(m-n)!}$ para $0 \leqslant m \leqslant n$.

Agora, como $\alpha_1, \ldots, \alpha_n$ satisfazem uma equação polinomial de grau $n$ com coeficientes inteiros. Segue que,

$(a)$ os números em (4.32) satisfazem uma equação polinomial de grau $\binom{n}{2}$ com coeficientes inteiros.

$$P_2(x) = 0 \tag{4.35}$$

$(b)$ os números em (4.33) satisfazem uma equação polinomial de grau $\binom{n}{3}$ com coeficientes inteiros.

$$P_3(x) = 0$$

e assim sucessivamente.

Logo, os números (4.31) e (4.34) satisfazem uma equação polinomial

$$P_1(x) \ldots P_n(x) = 0 \tag{4.36}$$

com coeficientes inteiros e cujo grau é $n + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n - 1$. Como alguns dos números em (4.31) $\cdots$ (4.34) podem se anular, podemos supor que $m$ deles sejam diferentes de zero e representamos por $\beta_1, \ldots, \beta_m$. Logo, simplificando em (4.36) os fatores da forma $x^q$, para $q > 0$, caso haja, (e haverá se $2^n - 1 > m$) obtemos que $\beta_1, \ldots, \beta_m$ são raízes de uma equação na forma:

$$R(x) = cx^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0 = 0 \tag{4.37}$$

com coeficientes inteiros.

A seguir, efetuamos o produto de (4.30) e obtemos

$$k + e^{\beta_1} + \cdots + e^{\beta_m} = 0 \tag{4.38}$$

Considere o polinômio,

$$P(x) = \frac{e^s}{(p-1)!} x^{p-1} (R(x))^p \tag{4.39}$$

onde $s = mp - 1$ e $p$ é um número primo a ser escolhido posteriormente. O grau de $P$ é $r = s + p$. Seja agora

$$F(x) = P(x) + P'(x) + \cdots + P^{(s+p)}(x) \tag{4.40}$$

segue que

$$\frac{d}{dx}(e^{-x}F(x)) = -e^{-x}P(x). \tag{4.41}$$

**Teorema 4.4:** Seja $f : \mathbb{C} \longrightarrow \mathbb{C}$ uma função analítica e sejam $z_1, z_2 \in \mathbb{C}$. Então:

$$|f(z_2) - f(z_1)| \leqslant 2|z_2 - z_1| sup\{f'(z_1 + \lambda(z_2 - z_1)) : 0 \leqslant \lambda \leqslant 1\} \tag{4.42}$$

Aplicando o Teorema 4.4 à função $f(z) = e^{-z}F(z)$, temos

$$|e^{-\beta_j}F(\beta_j) - F(0)| \leqslant 2|\beta_j| sup\{e^{-\lambda\beta_j}P(\lambda\beta_j)| : 0 \leqslant \lambda \leqslant 1\} \tag{4.43}$$

para $j = 1, \cdots, m$. Fazendo

$$\epsilon_j = 2|\beta_j| \sup\{|e^{(1-\lambda)\beta_j}P(\lambda\beta_j)| : 0 \leqslant \lambda \leqslant 1\} \tag{4.44}$$

obtemos de (4.43) que

$$|F(\beta_j) - e^{\beta_j}F(0)| \leqslant \varepsilon_j \tag{4.45}$$

Utilizando (4.38) e a expressão (4.45) para $j = 1, \ldots, m$ obtemos:

$$|KF(0) + \sum_{j=1}^{m} F(\beta_j)| \leqslant \sum_{j=1}^{m} \varepsilon_j \tag{4.46}$$

Mostraremos, agora, que o lado esquerdo de (4.46) é um inteiro não nulo, e que o lado direito, para $p$ conveniente, é menor que 1.

Devemos, então, calcular as várias derivadas de $P(x)$ nos pontos: $0, \beta_1, \ldots, \beta_m$. O polinômio $P(x)$ definido em (4.39) é da forma

$$P(x) = \frac{c^s}{(p-1)!}\{c_0^p x^{p-1} + bx^p + \cdots\}$$

Logo,

$$P^{(i)}(0) = 0, \text{para} i < p - 1 \quad \text{e} \quad P^{(p-1)}(0) = c^s c_0^p \tag{4.47}$$

Por outro lado, segue-se diretamente de (4.39) que

$$P^{(i)}(\beta_j) = 0, i < p, j = 1, \ldots, m. \tag{4.48}$$

uma vez que nas derivadas $P^{(i)}(x)$, para $i$ e $p$ a expressão $R(x)$ é fator comum, e $R(\beta_j) = 0$

Para as derivadas de ordem $i \geqslant p$ e de (4.39), concluímos que os coeficientes de

$$P^{(i)}(x), i \geqslant p, \tag{4.49}$$

são inteiros divisíveis por $pc^s$.

Logo, de (4.47) e (4.49) obtemos

$$F(0) = c^s c_0^p + pc^s k_0, \tag{4.50}$$

onde $K_0$ é um inteiro, cujo valor não importa para os nossos propósitos. Para os demais $F(\beta_j)$ observamos que

$$\sum_{j=1}^{m} F(\beta_j) = \sum_{j=1}^{m} \sum_{i \geqslant p} P^{(i)}(\beta_j) = \sum_{i \geqslant p} \sum_{j=1}^{m} P^{(i)}(\beta_j) \tag{4.51}$$

Agora, na expressão

$$\sum_{j=1}^{m} P^{(i)}(\beta_j) \tag{4.52}$$

para cada $i$ fixado, com $p \leqslant i \leqslant s+p$. Por (4.49) o polinômio $P^{(i)}$ tem coeficientes inteiros divisíveis por $pc^s$. Além disso, como $P$ tem grau $s+p$, segue- se que $P^{(i)}$ tem grau $s+p-i \leqslant s$, pois $p \leqslant i$. Logo, a expressão (4.52) pode ser escrita como

$$\sum_{j=1}^{m} P^{(i)}(\beta_j) = pc^s Q(\beta_1, \ldots, \beta_m), \tag{4.53}$$

onde $Q(\beta_1, \ldots, \beta_m)$ é um polinômio nos $\beta_i's$ de grau menor ou igual a $s$, com coeficientes inteiros. Observe que $Q(\beta_1, \ldots, \beta_m)$ é um polinômio simétrico nos $\beta_i's$ com coeficientes inteiros. Logo, existe um polinômio $G(\sigma_1, \ldots, \sigma_m)$ de grau menor ou igual a $s$ com coeficientes inteiros e onde $\sigma_1, \ldots, \sigma_m$, tal que

$$Q(\beta_1, \ldots, \beta_m) = G(\sigma_1, \ldots, \sigma_m). \tag{4.54}$$

Por outro lado, temos

$$\sigma_1 = c^{-1}c_{m-1}, \sigma_2 = c^{-1}c_{m-2}, \ldots, \sigma_m = c^{-1}c_0 \tag{4.55}$$

Logo, de (4.53) ,(4.54) e (4.55) segue que a expressão (4.52) é um inteiro divisível por p. Voltando a (4.51) concluímos que

$$\sum_{j=1}^{m} F(\beta_j) = pk_1 \tag{4.56}$$

onde $k_1$ é um inteiro qualquer. A seguir, usando (4.50) e (4.56) obtemos que o lado esquerdo de (4.46) é um inteiro da forma

$$|kc^s c_0^p + pk| \tag{4.57}$$

onde $k = c^s k_0 + k_1$. Agora escolhemos um número primo $p$ de modo que ele seja maior que $k, c$ e $c_0$. Portanto, o inteiro de (4.57) não é divisível por $p$, e , consequentemente, é um inteiro não nulo.

Para concluir a demonstração, necessitamos fazer a estimativa do termo do lado direito de (4.46). Seja,

$$M = max(|\beta_1|, \ldots, |\beta_m|)$$

Logo,

$$\varepsilon_j \leqslant 2Me^M \frac{|c|^s}{(p-1)!} \sup\{|\lambda\beta_j|^{p-1}|R(\lambda\beta_j)|^p : 0 \leqslant \lambda \leqslant 1\} \tag{4.58}$$

onde usamos que $0 \leqslant \lambda \leqslant 1$. Seja a seguir,

$$N = max\{|R(z)| : |z| < m\}$$

a qual usada em (4.58) fornece

$$\epsilon_j \leqslant 2Me^M \frac{|c|^s}{(p-1)!} M^{p-1} N^p$$

como o fatorial domina qualquer exponencial, isto é,

$$\lim_{x\to\infty} \frac{A^n}{n!} = 0$$

para qualquer $A > 0$, segue que, para $p$ suficientemente grande, podemos fazer $\epsilon_j < \frac{1}{m+1}$. Logo,

$$\sum_{j=1}^{m} \epsilon_j \leqslant \frac{m}{m+1} < 1 \tag{4.59}$$

A expressão (4.59) juntamente com o fato que o lado esquerdo de (4.46) é inteiro não nulo resulta em um absurdo. Logo, $\pi$ é transcendente.

# 5

# Algumas Curiosidades

## 5.1 O Sétimo Problema de Hilbert

O Segundo Congresso Internacional de Matemática, realizado em Paris no ano 1900, ficou célebre na história da Matemática, porque foi nele que David Hilbert pronunciou uma conferência, na qual apresentou uma lista de 23 problemas que, a seu ver, ocupariam os matemáticos das gerações seguintes. O discurso de Hilbert foi bem mais do que expor uma coleção de questões matemáticas, ele esboçou sua filosofia da matemática e propôs problemas importantes, que até os dias de hoje, são uma fonte inesgotável de perguntas tocando diversos campos da matemática.

Hilbert foi um alemão brilhante em matemática. Dotado de uma inteligência fina e enorme capacidade de trabalho, fez contribuições marcantes nas áreas de Álgebra, Geometria, Análise e Fundamentos de Matemática. Portanto, quando expôs em Paris seus 23 problemas, nas mais diversas áreas, ele o fazia com autoridade respeitada.

O sétimo problema, o quarto apresentado oralmente, consistia em estabelecer se certos números eram transcendentes. Assim, por exemplo, não se sabia na época se $\sqrt{2}^{\sqrt{2}}$ era transcendente ou algébrico. A inclusão desse problema na lista dos 23 revela a importância que Hilbert atribuia.

Em 1929, Gelfond provou que o número $\sqrt{2}^{i\sqrt{2}}$ é transcendente. Em seguida, Siegel provou que $\sqrt{2}^{\sqrt{2}}$ é transcendente. Mais alguns anos e Gelfond (1934) e Schneider (1935), independente, provaram um teorema que decide a transcendência dos números mencionados acima e muitos outros. A seguir, enunciaremos esse resultado, cuja a demonstração não é simples.

**Teorema 5.1:** (Gelfond-Schneider) Sejam $\alpha$ e $\beta$ números algébricos (reais ou complexos). Se $\alpha \neq 0$, $\alpha \neq 1$ e $\beta$ não for um número racional (real), então $\alpha^{\beta}$ é transcendente.

**Corolário 5.1:** O número $e^{\pi}$ é transcendente.

*Demonstração.* Como $e^{\pi i} = \cos(\pi) + i\,\mathrm{sen}(\pi) = -1$ (relação de Euler), então $(e^{\pi i})^{-i} = (-1)^{-i}$. Logo $e^{\pi} = (e^{\pi i})^{-i} = (-1)^{-i}$ é transcendente, pelo Teorema 5.1. □

O número $e^\pi$ é chamado de constante de Gelfond. Quanto aos números $\pi^e, e^e$ e $\pi^\pi$ ainda não se sabe se são ou não transcendentes.

## 5.2 Soma e Produto de Números Transcendentes

**Teorema 5.2:** Sejam $\alpha$ e $\beta$ números transcendentes, então pelo o 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 $2\alpha$ seria algébrico. Absurdo, pois por hipótese $\alpha$ é transcendente. Portanto, pelo o menos um desses números $(\alpha+\beta)$ e $(\alpha-\beta)$ é transcendente. □

Observe que fazendo $\alpha = \pi$ e $\beta = e$, temos que pelo o 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.

**Teorema 5.3:** Sejam $\alpha$ e $\beta$ números transcendentes, então pelo o 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 $\alpha^2+\beta^2$ seja algébrico, pois é o resultado da diferença entre dois números 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. Contradizendo a hipótese. E portanto, pelo o menos um dos números $(\alpha+\beta)$ ou $(\alpha\cdot\beta)$ é transcendente. □

## 5.3 A Conjectura de Schanuel

Esta seção será descrita de acordo com o livro [8].

Um corpo é um conjunto não vazio munido de duas operações ditas + (soma) e $\cdot$ (multiplicação) que possui as seguintes propriedades: comutatividade, associatividade, elemento neutro (0) e simétricos aditivos, elemento neutro e inverso multiplicativo (para elementos diferentes de zero), além da distributividade da multiplicação em relação a adição. Exemplos de corpos são: $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$. Uma extensão $L$ de um corpo $K$ é um corpo tal que $L \supset K$. Se todo $\alpha \in L$ é algébrico sobre $K$, dizemos que $L$ é uma extensão algébrica, caso contrário dizemos que a extensão é transcendente, e usamos a seguinte notação: $L|_K$.

Se $L|_K$, podemos enxergar $L$ como espaço vetorial sobre $K$. Assim, $L$ tem uma dimensão sobre $K$. A essa dimensão damos o nome de grau de extensão $L|_K$ e denotamos por $[L:K]$. É possível mostrar que $L|_K$ é finita ($[L:K] < \infty$) se e somente se $L|_K$ é uma extensão algébrica.

Seja $L|_K$ uma extensão transcendente, isto é, $[L:K] = \infty$. Um conjunto $B \subseteq L$ é dito de base de transcendência de $L|_K$, se $B$ é algebricamente independente sobre $K$, isto é, $B = \{\alpha_1, \dots, \alpha_n\}$ com $p(\alpha_1, \dots, \alpha_n) \neq 0$, $\forall\, p(x) \in k[x_1, \dots, x_n]$ e $L|_{B(K)}$ é uma extensão algébrica, ou equivalente, e $B$ é o conjunto algebricamente independente (sobre $K$) maximal relativo à inclusão. 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 $L|_K$, como a cardinalidade de $B$. Denotamos por $grtr(L|_K) = grtr_k(L) = \#B$. Se $L|_K$ é algébrico, então $grtr(L|_K) = 0$.

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

$$grtr(\mathbb{Q}(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n})|\mathbb{Q}) \geqslant n.$$

A Conjectura de Schanuel é, sem dúvida, o grande resultado a ser provado em Teoria dos Transcendente. A motivação de tal conjectura de Schanuel é que se for demonstrada, fica provado alguns problemas em aberto. Apresentaremos aqui, em particular uma consequência dessa conjectura.

**Teorema 5.4:** Se a Conjectura de Schanuel é verdadeira então $e$ e $\pi$ são algebricamente independentes sobre $\overline{\mathbb{Q}}$, então $e + \pi$ e $e\pi$ são números transcendentes. Onde $\overline{\mathbb{Q}}$ representa o Conjunto dos Números Algébricos.

*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 racionais linearmente independentes, esse fato segue diretamente da transcendência de $\pi$ logo,

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

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

$\square$

Vale ressaltar que, mesmo depois de muitos anos da prova da transcendência de $e$ e $\pi$, até hoje não se sabe se $e\pi$ e $e + \pi$ são ambos transcendentes. Na verdade, só se sabe que pelo o menos um dos números $e\pi$ ou $e + \pi$ é transcendente.

# 6

# Uma proposta didática na prática da sala de aula

Uma proposta didática na apresentação de uma aula no nono ano, seria o estudo dos conjuntos numéricos com destaque nos Números Irracionais. De acordo com a Base Nacional Comum Curricular (BNCC) [4], o Ensino Básico tem como proposta que os alunos do nono ano já saibam identificar um número irracional, tal como fazer as operações básicas com tais números. Uma das habilidades que o aluno deve atingir é saber localizar um número irracional na reta, e suas operações aritméticas. Infelizmente não é tratado de maneira formal, na maioria das vezes um número irracional é dito para os alunos, apenas como um número que não pode ser escrito na forma de uma fração, e nem sempre mostrando como demonstrar que um número é ou não irracional. Os alunos apresentam dificuldade em operar tais números, por exemplo em soma de números irracionais, muitos ao efetuar por exemplo, $\sqrt{2}+\sqrt{3}$ fazem $\sqrt{2+3}=\sqrt{5}$, o que é falso. Talvez a formalidade não seja de desconhecimento apenas do aluno, mas até mesmo do professor, uma vez que tal conceito não é exposto no material didático do ensino regular. Números Reais ainda é um tema presente no ensino de maneira superficial, quando se refere à formalização de tal conjunto. Com o passar dos anos, houve uma melhora nos livros didáticos de Matemática, porém persiste a ausência de formalidade na abordagem de certos conceitos. Dessa maneira, duas atividades foram elaboradas, afim de melhorar esse quadro.

## 6.1 Descrição da Primeira Atividade

A primeira atividade, que está no anexo A, foi organizada da seguinte maneira:

- Tema: Números irracionais.
- Objetivo: Apresentar exemplos de números irracionais, com a demonstração formal.
- Carga horária: Duas aulas de 50 minutos cada.
- Material Didático: Texto produzido pela professora, quadro e pincel.

- Avaliação: Participação dos alunos.

A aula ocorreu no dia 16 de maio de 2018, e pela primeira vez, eles estabeleceriam um contato com a demonstração pelo método da contradição, além de entenderem melhor o conceito de um número irracional. Essa atividade teve a duração de dois horários consecutivos, ou seja, 100 minutos. Alguns assuntos como o conjunto dos Números Reais, os alunos já conheciam, pois já aprenderam em aulas anteriores.

Por causa da dificuldade da maioria dos alunos sobre as operações em $\mathbb{R}\backslash\mathbb{Q}$ foi necessário explicar com mais detalhes, mesmo assim muitas dúvidas persistiram. Por isso decidimos planejar uma segunda atividade com foco principal nas operações entre números irracionais e a construção de $\mathbb{R}$.

Iniciamos a aula, definindo os Números Racionais, como números que podem ser escritos como frações nas quais o numerador e o denominador são números inteiros e o denominador é diferente de zero. Dos números racionais, alguns são classificados como dízimas periódicas, exemplo o número 0,121212..., que pode ser escrito como 12/99, os números exatos também são classificados como números racionais, uma vez que se $p$ um número inteiro, temos $p = p/1$. Concluímos essa parte inicial dizendo que há números decimais que não são exatos e nem dízimas periódicas, tais números, são chamados de Números Irracionais.

Algumas operações com esses números, como a demonstração da irracionalidade é um tema que os alunos sentem dificuldade. Por isso, nesta aula lecionada, nos preocupamos em mostrar aos alunos a demonstração da irracionalidade de alguns números, por exemplo do número $\sqrt{2}$.

O plano de aula foi elaborado para cada exercício conduzir os alunos a chegarem em suas próprias conclusões. Assim, esta foi uma aula investigativa, onde cada aluno pesquisava e conjecturava. Em sala de aula, foi abordado o conceito de segmentos incomensuráveis, antes de trabalhar a demonstração dos números irracionais citado no Anexo A, retratando o surgimento dos números irracionais, na época de Pitágoras. Além de estudar esses conceitos, a atividade teve o intuito retratar a formalização dos conjuntos numéricos.

Os alunos participaram ativamente. Conseguiram concluir a demonstração da irracionalidade de $\sqrt{2}$. Eles se surpreenderam, uma vez que nunca tiveram contato com a demonstração de um número irracional.

### 6.1.1 Descrição da Segunda Atividade

A segunda atividade, apresentada no Anexo A, foi organizada da seguinte maneira:

- Tema: Conceitos Importantes dos Números Reais.
- Objetivo: Manipular as operações aritméticas de números irracionais, e a formalização do Conjunto dos Números Reais.
- Carga horária: Duas aulas de 50 minutos cada.
- Material Didático: Texto produzido pela professora, quadro e pincel.
- Avaliação: Participação dos alunos.

A aula foi elaborada pensando na dificuldade encontrada pela maioria dos alunos. Ao nos depararmos com os números reais no ensino básico, observamos que certos números são mais difíceis a compreensão de suas operações do que outros. É por esse fato, que a segunda atividade foi aplicada, inicialmente em analisar o conhecimento prévio dos alunos, sobre números irracionais. Assim os alunos do nono ano tiveram a oportunidade de adquirir conhecimento sobre as operações entre números irracionais, sanando várias dúvidas. O objetivo dessa atividade é mostrar que embora as operações como soma e multiplicação sejam feitas em $\mathbb{R}\backslash\mathbb{Q}$, elas não são fechadas no conjunto dos números irracionais, e devemos ter um cuidado ao fazer as operações. Essa aula teve duração de 100 minutos.

Muitos alunos ao somar $\sqrt{5}+\sqrt{7}$ colocam como resultado $\sqrt{12}$, um resultado incorreto. Analisando tais fatores, nos propusemos a usar as aulas para apresentar aos alunos as propriedades aritméticas desses números. Para isso optamos em iniciar a aula explicando como foi o surgimento dos números irracionais, na época do matemático Pitágoras. Trabalhamos também a formalização do conceito do conjunto dos números reais ($\mathbb{R}$), que na maioria dos livros didáticos, há apenas a definição como união dos conjuntos dos números: Racionais e Irracionais, abordando o conceito novo para os estudantes, que é "Corte de Dedekind" . Ao relatar da origem dos números irracionais, como segmentos não comensuráveis, fica mais claro ao aluno o conceito de número irracional. Os alunos participaram da aula, fazendo perguntas e resolvendo as atividades propostas.

# 7
# Conclusões

O estudo dos números transcendentes mostra a existência de uma área da Matemática ainda com muitas questões em aberto. Em particular os números: $e\pi$, $e+\pi$, $e^e$ e $\pi^\pi$ continua em aberto saber se esses números são transcendentes ou algébricos, apesar de ter demonstrado neste trabalho que $\pi$ e $e$ são transcendentes nada podemos afirmar dos números citados acima.

No decorrer deste trabalho foi realizado um estudo da formalização dos conjuntos numéricos. Além do estudo, houve uma preocupação de tal apresentação desses números no ensino fundamental. Devido a esse fato foi elaborado atividades para expor de forma clara para os alunos do nono ano. É notável a presença dos números reais no ensino básico e no ensino superior tão quanto a sua relevância para o ensino aprendizagem da matemática. Na maioria das vezes ao apresentar um número irracional ele é dito como um número que não é racional. Pensando em toda essa situação, a aula elaborada que está em anexo neste trabalho, era uma forma de apresentar o conceito de um número irracional, através de uma visão vinculada ao teorema de Pitágoras, como por exemplo mostrar que a diagonal de um quadrado de lado um, representa um número irracional. Alguns alunos pela primeira vez, passavam a ter contato com uma demonstração matemática pelo método do absurdo, ao demonstrarem que em particular o número $\sqrt{2}$ é irracional.

Neste trabalho, usamos algumas ferramentas como propriedades algébricas, o cálculo diferencial e integral de uma e duas variáveis, além do estudo de Cortes de Dedekind. Para tais questões já mencionadas que são problemas em aberto, talvez seria necessário de alguma teoria mais avançada, para a resolução desses problemas.

# A

# Anexos

Aqui estão anexadas as duas atividades aplicada no nono ano, cuja descrição se encontra no capítulo 6.

Universidade Federal de Viçosa
*Campus* Florestal

Naiara Aparecida de Faria
Orientadora: Danielle Lara

**Atividade- Profmat**
**Números Reais**

Todo número Racional, pode ser escrita como:

Você sabia que $\sqrt{2} \in \mathbb{R} \backslash \mathbb{Q}$?

**Vamos provar?**
Se $\sqrt{2}$ fosse racional, então $\sqrt{2}$ poderia ser escrito na forma de uma fração. Escreva $\sqrt{2}$ na forma de uma fração irredutível. Ou seja,

$\sqrt{2} = \dfrac{a}{b}$ com $b \neq 0$

1. O que podemos fazer para eliminar a raiz quadrada?

   Faça conta.

2. Qual foi o resultado obtido?

3. Qual a conclusão do resultado obtido acima?

4. Se $a^2$ é par, o que podemos concluir sobre $a$?

5. Como podemos escrever $a$?

6. Substitua o valor de $a$ na equação acima, e faça os cálculos.

7. O que podemos concluir de $b$?

8. Isso faz sentindo? Uma vez que $a$ e $b$ são primos entre si?

*Conclusão:*

**Agora é a sua vez!**

Universidade Federal de Viçosa
de Viçosa

Universidade Federal de Viçosa
*Campus* Florestal

Naiara Aparecida de Faria
Orientadora: Danielle Lara

Mostre que o número $\sqrt{3}$ não é racional.

Você conhece o número $\pi$?

Esse número é racional?

Você conseguiria usar o mesmo argumento de $\sqrt{3}$ para mostrar isso?

Universidade Federal de Viçosa
*Campus* Florestal

Naiara Aparecida de Faria
Orientadora: Danielle Lara

**Atividade- Profmat**
**Conceitos Importantes do Conjunto dos Números Reais $\mathbb{R}$**

1. Quando se fala de um número racional, quais são os números que você pensa?

2. Quando se fala de um número irracional, quais são os números que você pensa?

Vamos fazer uma atividade envolvendo os números irracionais?
Qual o resultado de $\sqrt{3} + \sqrt{2}$? Seria $\sqrt{3+2} = \sqrt{5}$? Vamos verificar? Utilizando uma calculadora, verifique os valores abaixo:

$\sqrt{3} =$

$\sqrt{2} =$

$\sqrt{3} + \sqrt{2} =$

$\sqrt{5} =$

Você estava correto na sua soma acima?
Vamos verificar o valor de $\sqrt{3} + \sqrt{6}$. Seria $\sqrt{3+6}$? Use uma calculadora para verificar.

Um matemático, chamado Dedekind preocupado com a formalização dos Números Irracionais, fez um estudo sobre tais números e criou a seguinte definição:

**Definição 1** *Um conjunto A diz- se um corte se satisfazer as seguintes condições:*

1. $\varnothing \neq A \neq \mathbb{Q}$
2. *Se* $r \in A$, *e* $s < r$ *(s racional), então* $s \in A$
3. *Em A não possui elemento máximo.*

Considere o conjunto $B = \left\{ x \in \mathbb{Q}; x < \frac{1}{2} \right\}$
Todo elemento menor do que $1/2 \in \mathbb{Q}$ pertence ao conjunto $B$?
O Conjunto acima é chamado Corte.
A formalidade do conjunto dos Números Reais foi realizado pelo matemático alemão Dedekind, através de cortes de conjuntos racionais.

# Bibliografia


[1] Domingues, H. H. *Fundamentos de Aritmética.* Atual Editora. Fundamentos de Matemática. CIP, 1991, p. 151.

[2] Ferreira, J. *A construção dos Números.* Textos universitários. SBM, 2013. URL: https://books.google.com.br/books?id=GFmynQAACAAJ.

[3] Figueiredo, D. G. de. *Números Irracionais e Transcendentes.* 2011.

[4] Filho, M. *Base Nacional Comum Curricular.* Ministério da Educação, 2018. URL: http://basenacionalcomum.mec.gov.br/wp-content/uploads/2018/02/bncc-20dez-site.pdf.

[5] Hefez, A. e Villela, M. L. T. *Polinômios e Equações Algébricas.* 1ª Ed. Coleção Profmat. SBM, 2012, p. 269.

[6] Lima, E. L. *Análise Real.* 1ª Ed. Coleção matemática universitária. SBM, 2017, p. 198.

[7] Lima, E. L. *Números e Funções Reais.* 1ª Ed. Coleção Profmat. SBM, 2013, p. 289.

[8] Marques, D. *Teoria dos números transcendentes.* Textos universitários. SBM, 2013. URL: https://books.google.com.br/books?id=cV1gAQAACAAJ.

[9] Martinez, F. et al. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro.* Projeto Euclides. IMPA, 2010. URL: https://books.google.com.br/books?id=q5z3kQEACAAJ.

[10] Neves, W. *Uma Introduçao A Analise Real.* UFRJ EDITORA. URL: https://books.google.com.br/books?id=p98nvgAACAAJ.

[11] Niven, I. *Numeros Racionais E Irracionais.* Colecao fundamentos da matematica elementar. Sociedade Brasileira de Matematica, 1984. URL: https://books.google.com.br/books?id=L7y1HAAACAAJ.

[12] Roque, T. e Carvalho, J. B. P. de. *Tópicos de História da Matemática.* 2ª Ed. Coleção Profmat. SBM, 2012, p. 452.