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

SEBASTIÃO PONTES MASCARENHAS

A IRRACIONALIDADE E TRANSCENDÊNCIA DOS NÚMEROS

FORTALEZA
2017

SEBASTIÃO PONTES MASCARENHAS

A IRRACIONALIDADE E TRANSCENDÊNCIA DOS NÚMEROS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. José Othon Dantas Lopes.

FORTALEZA

2017

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

M361i Mascarenhas, Sebastião Pontes.
A Irracionalidade e Transcendência dos Números / Sebastião Pontes Mascarenhas. – 2017.
79 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Programa de Pós-Graduação em Matemática, Fortaleza, 2017.
Orientação: Prof. Dr. José Othon Dantas Lopes.

1. Irracionalidade. 2. Transcendência. 3. Liouville. I. Título.

CDD 510

SEBASTIÃO PONTES MASCARENHAS

A IRRACIONALIDADE E TRANSCENDÊNCIAS DOS NÚMEROS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Aprovada em: ___/___/_____.

BANCA EXAMINADORA

_____
Prof. Dr. José Othon Dantas Lopes (Orientador)
Universidade Federal do Ceará (UFC)

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

_____
Prof. Dr. Ângelo Papa Neto
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

Aos meus pais, esposa e família.

AGRADECIMENTOS

Aos meus pais, por toda a dedicação e amor incondicionais que tiveram comigo e meus irmãos para que pudéssemos trilhar o caminho dos estudos, educação e trabalho. A minha mãe, Maria Zulene Pontes Mascarenhas, por ter me apresentado às primeiras letras e números, estudando ao meu lado até que eu pudesse caminhar sozinho. Ao meu pai, Sebastião Teles Mascarenhas, pelo exemplo de homem dedicado ao trabalho e à família, fazendo todo o esforço para que meus irmãos e eu pudéssemos nos dedicar exclusivamente aos estudos.

Aos meus irmãos, Maria do Socorro P. Mascarenhas, Maria Irislene P. Mascarenhas, José Cleidson P. Mascarenhas e Liédja Maria P. Mascarenhas, pela amizade e companheirismo que sempre nos uniu em todos os momentos. Em especial, a Liédja, pelo incentivo e pelas horas que dispensou na organização dessa dissertação.

A minha mulher, Jovelina de Carvalho Portela Mascarenhas, pelo carinho, amor e paciência que mostrou durante as horas mais difíceis dessa jornada.

Aos meus filhos, Karl Breno de Carvalho Mascarenhas e Karen Anne de Carvalho Mascarenhas, pela dedicação com que abraçam os estudos, pela educação e respeito familiar e pelo o amor que recebo deles.

Ao meu orientador, Prof. Dr. José Othon Dantas Lopes, pelo empenho, compromisso e sabedoria durante a condução do desenvolvimento desse trabalho.

Aos professores Dr. José Valter Lopes Nunes e Dr. Ângelo Papa Neto, participantes da banca examinadora, pelo tempo dedicado e pelas valiosas colaborações e sugestões.

Aos professores que contribuíram no decorrer do curso, pelo esforço na transmissão de novos conhecimentos em suas disciplinas.

A todos os colegas de curso, pelo companheirismo e perseverança nos finais de semana.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), pelo apoio financeiro.

À Universidade Federal do Ceará, pela estrutura física, funcionários e professores disponibilizados aos alunos na realização desse curso.

Ao Prof. Dr. Silvano Dias Bezerra de Menezes (in memoriam), pela persistência com que me cobrava a realização desse curso.

Ao Prof. Marcondes Jamacaru, pela revisão ortográfica que possibilitou melhor entendimento desse trabalho.

Enfim, agradeço a todos que direta ou indiretamente contribuíram para a realização do mestrado PROFMAT.

“Conheço muitos que não puderam quando deviam, porque não quiseram, quando podiam.”

Francois Rebelais

RESUMO

O presente trabalho é uma exposição voltada à verificação da irracionalidade de certos números reais, à construção de certos números transcendentes (em especial, os números de Liouville) e à transcendência de e, π e outros números. O entendimento das demonstrações presentes nesse trabalho envolve alguns conhecimentos básicos em teoria dos números (divisibilidade, máximo divisor comum, números primos, etc), teoria dos conjuntos (enumerabilidade), Cálculo Diferencial e Integral em uma variável real, um pouco de funções de duas variáveis e alguns fatos sobre convergência de sequências e séries. Como consequência, veremos a solução do antigo problema da quadratura de um círculo, isto é, a possibilidade ou não da construção com régua e compasso de um quadrado, cuja área equivale-se à área de um círculo de raio dado.

Palavras-chave: Números racionais e irracionais. Números algébricos e transcendentes. O número de Euler (e). O número π. Números de Liouville.

ABSTRACT

This present work is an explanation orientated for the check of the irracionality of some real numbers, for the construction of some transcendents numbers (in especial, the Liouville´s numbers) and for the transcendency of e, π and anothers numbers. The understanding of the presents demonstrations in this work involves some basics knowledge in theory of numbers (divisibility, highest divisor common, number prime, etc), theory of conjunct (enumerate), Differential and Integral Calculation in a real variable, a few of functions of two variables e some facts about convergence of sequences and series. As a consequence, will be seen the solution of the old problem of the quadrature of a circle, that is, a possibility ou not of the construction with ruler and compass of a square, whose area be equal to area of a circle radius gived.

Keywords: Racional and irracional numbers. Algebraic and transcendent numbers. The Euler's number (e). The number π. Liouville's numbers.

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{R}$	Conjunto dos números reais
$\mathbb{C}$	Conjunto os números complexos
$\max K$	Maior elemento de K
$a \mid b$	a divide b
$a \nmid b$	a não divide b
$mdc(a, b)$	Máximo divisor comum entre a e b
$mmc(a, b)$	Mínimo múltiplo comum entre a e b
$n!$	Fatorial de n
$\binom{m}{k}$	Coeficiente binomial de m, tomados k a k
$\log x$	Logaritmo natural de x
f'	Derivada da função f
$f^{(n)}$	n-èsima derivada da função f
$D^n f$	n-èsima derivada da função f
$K[x_1, \dots, x_n]$	Polinômios nas variáveis $x_1, \dots, x_n$ com coeficientes em K
$\sup K$	Supremo dos elementos de K
$\# K$	Quantidade de elementos (cardinalidade) de K
$K[x]$	Polinômio na variável x com coeficientes em K
∂P	Grau do polinômio P
$\overline{\mathbb{Q}}$	Conjunto dos números algébricos
(a_j)	Sequência dos números a_j
$\{a_j\}$	Conjunto dos números a_j
$[x]$	Parte inteira do número real x

SUMÁRIO

1 INTRODUÇÃO

Desde meados do século XVIII, o estudo dos números transcendentes forma uma área central da teoria dos números: a teoria dos números transcendentes. Essa teoria vive um grande paradoxo: se quase todos os números são transcendentes, por que demonstrar a transcendência de um dado número é, em geral, uma tarefa tão complicada?

É possível afirmar que a teoria dos números transcendente é pouco conhecida, apesar de ser uma área onde grandes matemáticos deram contribuição, como por exemplo, Euler, Liouville, Cantor, Weierstrass, Lindemann, Hermite, Hilbert, Siegel, Lambert, Gelfond, Schneider, Hurwitz, Borel, Mahler, Markoff e Veblen. Isso provavelmente é devido ao fato de que seus métodos são difíceis e, além disso, falta a existência de teoremas fundamentais como os que aparecem em outras áreas da Matemática.

Espera-se que esse material seja uma continuação natural do livro Números Irracionais e Transcendentes do professor Djairo Guedes de Figueiredo, o qual é mencionado nas Referências Bibliográficas.

A palavra transcendente, frequentemente atribuída a Leibniz, significa, segundo Euler, que os números transcendentes extrapolam (excedem, transcendem) ao poder de serem obtidos através de simples operações algébricas.

O estudo dos números transcendentes provém de diversos problemas, tais como: a antiga questão grega da quadratura do círculo; as pesquisas de Liouville e Cantor; investigações de Hermite sobre a função exponencial; o sétimo problema da famosa lista dos 23 problemas de Hilbert e as formas lineares em logaritmos devidas a Baker.

A teoria dos números transcendentes vive um intrigante dilema: enquanto que, essencialmente, todos os números são transcendentes, estabelecer a transcendência de um número particular é uma tarefa bastante complicada. O principal obstáculo é que um número transcendente é definido não pelo que ele é, mas pelo que não é.

2 OS NÚMEROS INTEIROS ALGÉBRICOS

Definição 1) Um número real α é dito um *inteiro algébrico* se for solução de uma equação polinomial da forma

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

onde os coeficientes $a_0, a_1, \ldots, a_{n-1}$ são números inteiros e $n \geq 1$. Ou seja, α é raiz de um polinômio $f(x)$ não nulo, mônico e pertencente ao anel de polinômios $\mathbb{Z}[x]$. Assim, qualquer número inteiro b é um inteiro algébrico, pois é a raiz do polinômio

(2.2) $f(x) = x - b$

Exemplo 1) Se p é um número inteiro primo, então os números irracionais $\sqrt{p}$ e $-\sqrt{p}$ são inteiros algébricos, pois são as raízes do polinômio

(2.3) $f(x) = x^2 - p.$

Exemplo 2) Se p e q são números inteiros primos, então o número irracional $\sqrt{p + \sqrt{q}}$ é um inteiro algébrico, pois é uma raiz do polinômio

(2.4) $f(x) = x^4 - 2p.x^2 + (p^2 - q).$

Apesar de nos restringirmos ao estudo dos inteiros algébricos que sejam números reais, podemos expandir essa definição para os números complexos.

Exemplo 3) Os Números complexos $i = \sqrt{-1}$ e seu simétrico $-i$ são inteiros algébricos, pois são as raízes do polinômio

(2.5) $f(x) = x^2 + 1$

uma vez que i satisfaz à condição de $i^2 = -1$ em sua definição.

Teorema 1) Seja α um número real. Se α é um inteiro algébrico, então α é um número inteiro ou α é um número irracional.

Demonstração: Seja α um inteiro algébrico. Suponhamos, por contradição, que $\alpha = \frac{p}{q}$, onde $p \in \mathbb{Z}$, $q \in \mathbb{N}$, $q > 1$, p e q primos entre si. Isto é, α é um número racional que não é inteiro ($\alpha \in \mathbb{Q}$ e $\alpha \notin \mathbb{Z}$). Como α é uma solução de uma equação do tipo (1.1), aplicando $\alpha = \frac{p}{q}$ em tal equação, temos:

(2.6) $\frac{p^n}{q^n} + a_{n-1}.\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1.\frac{p}{q} + a_0 = 0$, de onde obtemos

(2.7) $p^n = -a_{n-1}.p^{n-1}.q - a_{n-2}.p^{n-2}.q^2 - \cdots - a_1.p.q^{n-1} - a_0.q^n$, ou ainda

(2.8) $p^n = q.(-a_{n-1}.p^{n-1} - a_{n-2}.p^{n-2}.q - \cdots - a_1.p.q^{n-2} - a_0.q^{n-1})$.

Como $(-a_{n-1}.p^{n-1} - a_{n-2}.p^{n-2}.q - \cdots - a_1.p.q^{n-2} - a_0.q^{n-1})$ é um número inteiro, então q divide p^n. Seja r um fator primo de q. Obviamente, $r \neq 1$ e $r = q$ se q for primo. Assim, r é número primo e r divide p^n. Pelos teoremas de divisibilidade da Aritmética, r divide p. Com isso, r divide p e q, contrariando o fato deles serem primos entre si. O absurdo provém de admitirmos que $\alpha \in \mathbb{Q}$ com $\alpha \notin \mathbb{Z}$ satisfizesse a equação (2.1). Portanto, se α é um inteiro algébrico real, então α é um número inteiro ($\alpha \in \mathbb{Z}$) ou α é um número irracional ($\alpha \in (\mathbb{R} - \mathbb{Q})$). ■

3 A IRRACIONALIDADE DO NÚMERO DE EULER (e)

O número e, conhecido como número de Euler, que aparece no estudo da função logarítmica, é definido como o único número real satisfazendo a igualdade log $e = 1$, visto que a função $log : (0 , \infty) \rightarrow \mathbb{R}$, dada por $log\ x = \int_1^x \frac{dt}{t}$ é bijetiva. A constante e pode também ser escrita como um limite, uma série e um número que faz a delimitação de uma região plana cuja área tem valor numérico igual a 1.

- $e = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n$

- $e = \sum_{n=0}^{\infty} \frac{1}{n!} = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + ...$

- e = número real, maior que 1, cuja região plana limitada pelos gráficos da curva $f(x) = \frac{1}{x}$ para $x > 0$ e das retas $y = 0$, $x = 1$ e $x = e$ tenha área igual a 1.

No estudo de séries de funções e em textos de cálculo temos que

(3.1) $e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$, $-\infty < x < \infty$. Em particular, obtemos que

(3.2) $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$

Suponha que e fosse um número racional, isto é, $e = \frac{p}{q}$ onde, $p, q \in \mathbb{N}$ e são primos entre si. De (3.2) segue-se

(3.3) $\frac{p}{q} - (1 + \frac{1}{1!} + \frac{1}{2!} + ... + \frac{1}{q!}) = \sum_{j=q+1}^{\infty} \frac{1}{j!}$.

Agora, faremos uma estimativa do segundo membro de (3.3) :

(3.4)

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

.

A expressão entre parênteses no último membro de (3.4) é uma série geométrica da forma $\sum_{n=1}^{\infty} r^n$, onde r = $\frac{1}{1+q}$ e portanto tem soma igual a $\frac{r}{1-r}$, já que $0 < r < 1$. Daí, $\frac{r}{1-r} = \frac{1}{q}$ e usando este fato em (3.4) obtemos a relação

(3.5)

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

.

Aplicando a estimativa (3.5) na equação (3.3) temos que

$0 < \frac{p}{q} - (1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{q!}) < \frac{1}{q!}\,\frac{1}{q}$. Multiplicando ambos os membros por $q!$ segue-se a expressão

(3.6) $0 < q!.(\frac{p}{q} - 1 - \frac{1}{1!} - \frac{1}{2!} - \ldots - \frac{1}{q!}) < \frac{1}{q}$

Observando a relação (3.6), notamos que o termo intermediário é um número inteiro, pois $q!$ cancela todos os denominadores das frações aí presentes. Mas isso é impossível, pois sendo $\frac{1}{q} \leq 1$ a relação (3.6) diria que o termo médio é um número inteiro estritamente positivo e menor que 1. O fato absurdo provém da hipótese feita inicialmente que e fosse um número racional. Portanto, e é um número irracional.■

A irracionalidade de e pode também ser concluída do fato mais geral, (a ser provado no Capítulo 7), que e é um número transcendente.

4 A IRRACIONALIDADE DO NÚMERO π

Mostraremos neste capítulo que π é um número irracional. A irracionalidade de π foi, possivelmente, demonstrada pela primeira vez pelo francês J. H. Lambert, em 1761, usando frações contínuas. A demonstração de irracionalidade de π , que daremos a seguir, é devida a I. Niven, em artigo publicado no Bulletin of the American Mathematical Society, 53 (1947), pág. 509, o qual usou um método desenvolvido por Hermite para provar a transcendência do número e; conforme veremos no Capítulo 7 do presente trabalho.

Apresentaremos a seguir dois resultados envolvendo derivadas sucessivas da função $f: \mathbb{R} \rightarrow \mathbb{R}$ definida por

(4.1) $f(x) = \frac{x^n.(1-x)^n}{n!}$, onde n é um número inteiro positivo fixo.

Afirmação 1) Seja $D^k f$ a função que representa a k-ésima derivada de f onde $D^0 f = f$. Então, $D^k f\ (0)$ é um número inteiro para qualquer k = 0,1,2,...

Demonstração: Nos cursos de Cálculo, utilizamos a chamada fórmula de Leibnitz para as derivadas de um produto de duas funções, g e h:

(4.2)

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

onde k = 0,1,2,...

A demonstração da fórmula (4.2) pode ser feita sem muita dificuldade através do Princípio de Indução Finita. Vale lembrar que $\binom{k}{j}$ são os coeficientes do Binômio de Newton, definidos por $\binom{k}{j} = \frac{k!}{j!.(k-j)!}$, os quais são sempre números naturais positivos.

Aplicando (4.2) para a função definida em (4.1) temos

(4.3)

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

onde k = 0,1,2,... e $n \in \mathbb{N}$ fixo.

Observemos as seguintes derivadas:

(4.4) $$D^j g = \begin{cases} n.(n-1)\ldots(n-j+1).x^{n-j} & se\ j < n \\ n! & se\ j = n \\ 0 & se\ j > n \end{cases}$$

para $g(x) = x^n$.

(4.5) $$D^j h = \begin{cases} (-1)^j.n.(n-1)\ldots(n-j+1).(1-x)^{n-j} & se\ j < n \\ (-1)^n.n! & se\ j = n \\ 0 & se\ j > n \end{cases}$$

para $h(x) = (1-x)^n$.

De (4.4), obtemos que $D^j g(0) = \begin{cases} n! & se\ j = n \\ 0 & se\ j \neq n \end{cases}$ e $D^j g(1) \in \mathbb{Z}_+$.

De (4.5), obtemos que $D^j h(1) = \begin{cases} (-1)^n.n! & se\ j = n \\ 0 & se\ j \neq n \end{cases}$ e $D^j h(0) \in \mathbb{Z}$.

De (4.3) e das escolhas de $g(x)$ e $h(x)$ acima temos

(4.6)

$$D^k f = \frac{1}{n!} \cdot \sum_{j=0}^{k} \binom{k}{j} . D^j g . D^{k-j} h$$

onde k = 0,1,2,... e $n \in \mathbb{N}$ fixo.

Se $j \neq n$, temos $D^j g(0) = 0$.

Daí, $D^k f(0) = \frac{1}{n!} . \binom{k}{n} . n!. D^{k-n} h(0) = \binom{k}{n} . D^{k-n} h(0) \in \mathbb{Z}$, desde que $k \geq n$.

Caso tenhamos $k < n$, como j ∈ $\{0,1,\dots,k\}$, temos $j < n$ e logo $D^j g(0) = 0$ para todo $j \in \{0,1,\dots,k\}$. Assim, $D^k f(0) = 0 \in \mathbb{Z}$. Portanto, em qualquer caso, temos que $D^k f(0) \in \mathbb{Z}$ para todo $k = 0, 1, 2, \dots$ ■

Afirmação 2) Seja $D^k f$ a função que representa a k-ésima derivada de f onde $D^0 f = f$. Então, $D^k f\,(1)$ é um número inteiro para qualquer $k = 0, 1, 2, \dots$

Demonstração: Utilizando (4.6) e fatos decorrentes de (4.4) e (4.5), se $k - j \neq n$ temos $D^{k-j} h(1) = 0$ e logo $D^k f(1) = \frac{1}{n!}.\binom{k}{k-n}.D^{k-n} g(1).(-1)^n.n! = (-1)^n\binom{k}{k-n}.D^{k-n} g(1) = (-1)^n\binom{k}{n}.D^{k-n} g(1) \in \mathbb{Z}$, desde que $k \geq n$.

Caso tenhamos $k < n$, como j ∈ $\{0,1,\dots,k\}$, temos $j < n$ e logo $k - j \in \{0,1,\dots,k\}$. Daí, $k - j \leq k < n$, ou seja, $k - j \neq n$ e assim $D^{k-j} h(1) = 0$ para todo $j \in \{0,1,\dots,k\}$. Portanto, $D^k f(1) = 0 \in \mathbb{Z}$. Com isso, em qualquer situação, temos que $D^k f(1) \in \mathbb{Z}$ para todo $k = 0, 1, 2, \dots$ ■

Agora, de volta ao nosso objetivo, suponha que π fosse um número racional. Assim, π^2 também é um número racional, ou seja, $\pi^2 = \frac{p}{q}$ onde $p, q \in \mathbb{N}$ e são primos entre si.

Defina a função F: $\mathbb{R} \to \mathbb{R}$ pela expressão

(4.7) $F(x) = q^n.\{(\pi^{2n}.f(x) - \pi^{2n-2}.D^2 f(x) + \cdots + (-1)^{n-1}.\pi^2.D^{2n-2} f(x) + (-1)^n.D^{2n} f(x)\} = q^n.\sum_{i=0}^{n}(-1)^i.\pi^{2(n-i)}.D^{2i} f(x)$ onde $n \in \mathbb{N}$ é fixo.

Notemos que $q^n.\pi^{2k} = q^n.\frac{p^k}{q^k} = q^{n-k}.p^k \in \mathbb{N}$, se $k \leq n$.

Este fato e as Afirmações 1 e 2 garantem

(4.8) $F(0)$ e $F(1)$ são números inteiros.

Adotando a representação ' e " para as derivadas primeira e segunda de $F(x)$, isto é, $F' = D^1 F$ e $F'' = D^2 F$, obtemos

(4.9) $\{F'(x).\sin\pi x - \pi.F(x).\cos\pi x\}' = F''(x).\sin\pi x + \pi^2.F(x).\sin\pi x =$
$= \{F''(x) + \pi^2.F(x)\}.\sin\pi x.$

Efetuando um cálculo imediato obtemos as igualdades:

$$F''(x) + \pi^2.F(x) = q^n.\sum_{i=0}^{n}(-1)^i.\pi^{2(n-i)}.D^{2(i+1)}f(x) + \pi^2.F(x) =$$

$$= q^n.\ \sum_{i=0}^{n}(-1)^i.\pi^{2(n-i+1)}.D^{2i}f(x) + \pi^2.F(x) =$$

$$= q^n.\pi^{2n}.\pi^2.f(x) + (-1)^n.q^n.1.D^{2n+2}\,f(x) =$$

$$= p^n.\pi^2.f(x)$$

pois $q^n.\pi^{2n} = p^n$ e $D^{2n+2}\,f(x) = 0$ já que $f(x)$ é um polinômio de grau $2n$. Consequentemente,

(4.10) $\{F'(x).\sin\pi x - \pi.F(x).\cos\pi x\}' = p^n.\pi^2.f(x).\sin\pi x.$

O Teorema Fundamental do Cálculo Diferencial e Integral diz: "Se g: $[0,1] \to \mathbb{R}$ é uma função continuamente derivável em $[0,1]$, então $\int_0^1 g'(x).dx = g(1) - g(0)$". Usando esse teorema para a função $g(x) = F'(x).\sin\pi x - \pi.F(x).\cos\pi x$ e usando a relação (4.10) obtemos

$$\int_0^1 g'(x).dx = \int_0^1 p^n.\pi^2.f(x).\sin\pi x\,.dx$$

$$g(1) - g(0) = p^n.\pi^2.\int_0^1 f(x).\sin\pi x\,.dx$$

$$p^n.\pi^2.\int_0^1 f(x).\sin\pi x\,.dx = \pi.F(1) - \pi.F(0)$$

(4.11)

$$\pi . p^n . \int_0^1 f(x) . \sin \pi x . dx = F(1) - F(0) \in \mathbb{Z}$$

Observemos que o lado direito de (4.11) é um número inteiro em virtude de (4.8) e a igualdade é verdade para todo $n \in \mathbb{N}$.

Note que para $0 < x < 1$, temos que $0 < x^n < 1$ e $0 < (1-x)^n < 1$.

Logo, $0 < x^n . (1-x)^n < 1$, implicando em $0 < \frac{x^n . (1-x)^n}{n!} < \frac{1}{n!}$, ou seja,

(4.12) $0 < f(x) < \frac{1}{n!}$ para todo $n \in \mathbb{N}$.

Vejamos agora a igualdade da integração

(4.13)

$$\int_0^1 \sin \pi x . dx = -\frac{1}{\pi} . [\cos \pi x]_0^1 = -\frac{1}{\pi} . [\cos \pi - \cos 0] = \frac{2}{\pi}$$

Usando as desigualdades (4.12) e a integração (4.13) em (4.11) temos

(4.14)

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

Como $\lim_{n \to \infty} \frac{p^n}{n!} = 0$, podemos escolher convenientemente um $n \in \mathbb{N}$ tal que $\frac{2 . p^n}{n!} < 1$. Portanto, existe $n \in \mathbb{N}$ tal que $\pi . p^n . \int_0^1 f(x) . \sin \pi x . dx = F(1) - F(0) \in \mathbb{Z}$ e satisfaz a desigualdade

(4.15) $$0 < \pi . p^n . \int_0^1 f(x) . \sin \pi x . dx = F(1) - F(0) < 1$$

Desta forma, chegamos a um fato absurdo, proveniente da hipótese inicial que π fosse um número racional. Assim, π é um número irracional. ■

5 OS NÚMEROS ALGÉBRICOS E TRANSCENDENTES

Definição 1) Dado $\alpha \in \mathbb{R}$, diz-se que α é um *número algébrico* se existir um polinômio $P(x) = a_n.x^n + a_{n-1}.x^{n-1} + \cdots + a_1.x + a_0$ onde os coeficientes $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ tal que $P(\alpha) = 0$. Ou seja, α é algébrico se pudermos construir uma equação polinomial com coeficientes inteiros da qual α seja raiz.

Qualquer número racional, $\alpha = \frac{p}{q}$ onde $p, q \in \mathbb{Z}$, é um número algébrico, pois α é raiz da equação $q.x - p = 0$.

Na verdade, a Definição 1 pode ser estendida para um número $\alpha \in \mathbb{C}$. Assim, o número complexo $\alpha = i$ é um número algébrico, pois α é raiz da equação $x^2 + 1 = 0$ já que $i^2 = -1$.

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

A existência de números transcendentes pode ser demonstrada como fez o matemático G. Cantor. Para tal demonstração, necessitamos de alguns conceitos e resultados sobre conjuntos enumeráveis, os quais enunciaremos a seguir, sem que nos debrucemos sobre esses fatos.

Definição 2) Um conjunto A é dito *enumerável* se seus elementos puderem ser postos em correspondência biunívoca com os números naturais. Ou seja, A é enumerável se existir uma função bijetiva $f: \mathbb{N} \to A$.

A função $f(n) = 2n$ é uma bijeção de $\mathbb{N}$ no conjunto dos números pares positivos.

A função $f(n) = 2n - 1$ é uma bijeção de $\mathbb{N}$ no conjunto dos números ímpares positivos.

A função $f: \mathbb{Z} \to \mathbb{N}$ definida por $f(n) = \begin{cases} 1, \ se \ n = 0 \\ 2.n, \ se \ n > 0 \\ -2.n + 1, \ se \ n < 0 \end{cases}$ é uma bijeção, mostrando que $\mathbb{Z}$ é enumerável.

O conjunto $\mathbb{Q}$ dos *números racionais* e o conjunto $\overline{\mathbb{Q}}$ dos *números algébricos reais* são também exemplos de conjuntos enumeráveis.

Agora, enunciaremos alguns resultados referentes à enumerabilidade de conjuntos, os quais são usados na verificação da afirmação anterior, por exemplo. O leitor interessado nas demonstrações pode encontrá-las no livro Números Irracionais e Transcendentes mencionado nas Referências.

Teorema 1) A enumerabilidade de conjuntos satisfaz as seguintes propriedades:

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

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

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

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

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

(vi) Se A é um conjunto enumerável e $B \subset A$ é um conjunto infinito, então B é um conjunto enumerável.

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

Teorema 3) O conjunto de todos os números reais algébricos é enumerável.

Demonstração: Dado um polinômio com coeficientes inteiros

(5.1) $P(x) = a_n.x^n + a_{n-1}.x^{n-1} + \cdots + a_1.x + a_0$ definimos sua altura como sendo o número natural

(5.2) $|P| = |a_n| + \cdots + |a_1| + |a_0| + n.$

O Teorema Fundamental da Álgebra nos diz que $P(x) = 0$, com $P(x) = a_n.x^n + a_{n-1}.x^{n-1} + \cdots + a_1.x + a_0$, tem n raízes complexas, contando-se com a

multiplicidade de cada raiz, as quais todas, algumas ou nenhuma delas podem ser reais. Observe que a inclusão da parcela n, na definição da altura em (5.2), garante a existência de um número finito de polinômios do tipo (5.1) que tenham uma dada altura fixada. De fato, sem inclusão de n, o grau do polinômio $P(x)$ ficaria livre para assumir qualquer valor natural, já que sua altura dependeria apenas de seus coeficientes. Portanto, as raízes de todos os polinômios de uma dada altura fixa formam um conjunto finito. Ou seja, se H_j é o conjunto de todas as raízes de todos os polinômios de altura j, então H_j é um conjunto finito. Com isso observamos que o conjunto de todas as raízes de todos os polinômios de todas as alturas é dado por $H = \bigcup_{j=1}^{\infty} H_j$, que é um conjunto enumerável, pois é a união de um conjunto enumerável de conjuntos finitos. Mas H é exatamente o conjunto de todos os números algébricos em $\mathbb{C}$. Em particular, o conjunto dos números reais algébricos é enumerável, concluindo o teorema.■

Teorema 4) Existem números transcendentes.

Demonstração: Do Teorema 3 temos que o conjunto dos números algébricos reais é enumerável. Suponhamos que o conjunto dos números transcendentes reais fosse enumerável. Então, o conjunto $\mathbb{R}$ seria a união de dois conjuntos enumeráveis, que pelo Teorema 1 item (ii), garantiria que $\mathbb{R}$ é um conjunto enumerável, contrariando o Teorema 2. Logo, o conjunto dos números transcendentes reais é não enumerável, mostrando que não é vazio.■

Agora faremos um comentário sobre as operações aritméticas entre números algébricos reais. Novamente, o leitor interessado nas demonstrações pode encontrá-las no livro Números Irracionais e Transcendentes mencionado nas Referências.

Teorema 5) Sejam $\alpha, \gamma \in \mathbb{R}$ dois números algébricos. Então, as seguintes propriedades são verdadeiras:

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

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

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

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

Cabe observar que as propriedades relacionadas no Teorema 5 mostram que o conjunto dos números algébricos reais formam um subcorpo do corpo $\mathbb{R}$ dos números reais.

6 OS NÚMEROS DE LIOUVILLE

No capítulo 5, o Teorema 4 garante a farta existência de números transcendentes reais, apesar de não nos dar nenhuma técnica para reconhecê-los e nem exemplo sequer de algum desses números. Em 1851, o matemático francês J. Liouville, estabeleceu um critério para que um número real seja transcendente. Esse é o conteúdo do Teorema 5 desse capítulo e, com ele, será possível escrever explicitamente alguns números transcendentes.

Definição 1) Diz-se que um número algébrico α 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 grau menor, da qual α seja raiz.

Como exemplo, temos que os números racionais são precisamente os números algébricos de grau 1. Também é fácil ver que se $t \in \mathbb{N}$ é um número primo, então $\sqrt{t}$ é um número algébrico de grau 2, já que $\sqrt{t} \notin \mathbb{Q}$ e $\sqrt{t}$ é raiz do polinômio $P(x) = x^2 - t \in \mathbb{Z}[x]$.

Definição 2) Um número real α é dito *aproximável na ordem* n por racionais, se existirem $c > 0$ e uma sequência $\left(\frac{p_j}{q_j}\right)$ de racionais distintos, onde $p_j, q_j \in \mathbb{Z}$, com $q_j > 0$ e $mdc(p_j, q_j) = 1$, tais que satisfaçam

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

É claro que, se um número α for aproximável de ordem n, então ele é aproximável em qualquer ordem k, onde $k < n$. De fato, se $k < n$ temos que $\frac{c}{{q_j}^n} < \frac{c}{{q_j}^k} < c$ mostrando a relação

(6.2) $\left|\alpha - \frac{p_j}{q_j}\right| < c$,

o que garante que a sequência (q_j) não se mantém limitada, isto é, $q_j \to \infty$. Realmente, se (q_j) é limitada $\Rightarrow \exists\, r \in \mathbb{N}$ tal que $q_j \leq r \Rightarrow q_j \in \{1, \ldots, r\} \Rightarrow \#\{q_j\} \leq r \Rightarrow \#\{p_j\} = \infty \Rightarrow (p_j)$ não é limitada $\Rightarrow |p_j| \to \infty \Rightarrow \left|\frac{p_j}{q_j}\right| \to \infty \Rightarrow \left(\frac{p_j}{q_j}\right)$ não é limitada $\Rightarrow \left(\alpha - \frac{p_j}{q_j}\right)$ não é limitada $\Rightarrow \left|\alpha - \frac{p_j}{q_j}\right| \to \infty \Rightarrow \exists\, j \in \mathbb{N}$ tal que $\left|\alpha - \frac{p_j}{q_j}\right| > c$, contrariando a relação (6.2). Logo, (q_j) não se mantém limitada, isto é, $q_j \to \infty$.

Agora, da relação (6.1), obtemos que $0 \leq \lim_{j\to\infty} \left|\alpha - \frac{p_j}{q_j}\right| \leq \lim_{j\to\infty} \frac{c}{{q_j}^n} = 0 \Rightarrow \lim_{j\to\infty} \left|\alpha - \frac{p_j}{q_j}\right| = 0 \Rightarrow \lim_{j\to\infty} \frac{p_j}{q_j} = \alpha$. Assim, conseguimos

(6.3) $\lim_{j\to\infty} \frac{p_j}{q_j} = \alpha$

O fato de tomarmos racionais todos distintos na Definição 2 implica, em particular, que possamos tomá-los diferentes de α, mesmo no caso de α ser racional. De fato, se $\alpha \in \mathbb{Q}$, podemos ter $\alpha = \frac{p_j}{q_j}$ para algum j único, pois $\frac{p_j}{q_j} = \frac{p_i}{q_i} \Leftrightarrow i = j$. A seguir, citamos algumas relações entre os conceitos nas definições 1 e 2 acima.

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

Demonstração: Seja $\frac{p}{q}$ um número racional, com $p, q \in \mathbb{Z}$, $q > 0$ e $mdc(p, q) = 1$. Assim existem $x_0, y_0 \in \mathbb{Z}$ tais que ocorre

(6.4) $px_0 - qy_0 = 1.$

Na verdade, a equação seguinte

(6.5) $px - qy = 1$

tem um número infinito de soluções. A saber

(6.6) $x_t = x_0 + qt \ ; \ y_t = y_0 - pt$

para qualquer $t \in \mathbb{Z}$ satisfazem (6.5). De fato, é fácil ver que vale

(6.7) $px_t - qy_t = 1.$

Fixando $k \in \mathbb{N}$, tal que $k > \frac{-x_0}{q}$, considere as sequências $(x_j), (y_j)$ definidas, a partir de (6.6), por

(6.8) $x_j = x_0 + q(k+j)$; $y_j = y_0 + p(k+j)$ com $j \in \mathbb{N}$.

Pela restrição posta em k, temos $x_j > qj$ e daí $x_j > 0$, pois $q > 0$. De fato, temos $qk > -x_0 \Rightarrow x_0 + qk > 0 \Rightarrow x_0 + qk + qj > qj \Rightarrow x_0 + q(k+j) > qj \Rightarrow x_j > qj$.

Agora, mostraremos que

(6.9) $\frac{y_j}{x_j} \neq \frac{y_i}{x_i}$, se $j \neq i$.

Suponhamos que ocorra a igualdade $\frac{y_j}{x_j} = \frac{y_i}{x_i}$. Logo, $x_i y_j = x_j y_i \Rightarrow \big(x_0 + q(k+i)\big)\big(y_0 + p(k+j)\big) = (x_0 + q(k+j))(\, y_0 + p(k+i) \Rightarrow x_0 y_0 + k(px_0 + qy_0) + x_0 pj + y_0 qi = x_0 y_0 + k(px_0 + qy_0) + x_0 pi + y_0 qj \Rightarrow x_0 pj + y_0 qi - x_0 pi - y_0 qj = 0 \Rightarrow j(px_0 - qy_0) - i(px_0 - qy_0) = 0 \Rightarrow j - i = 0 \Rightarrow j = i$.

Portanto, se $j \neq i$, temos $\frac{y_j}{x_j} \neq \frac{y_i}{x_i}$.

Da igualdade (6.7), para qualquer $j \in \mathbb{N}$, temos $px_j - qy_j = 1$. Logo, os $x_j's$ e $y_j's$, definidos em (6.8), satisfazem à desigualdade

$\left|\frac{p}{q} - \frac{y_j}{x_j}\right| = \left|\frac{px_j - qy_j}{qx_j}\right| = \left|\frac{1}{qx_j}\right| = \frac{1}{qx_j} = \frac{1}{q}\frac{1}{x_j} \leq \frac{1}{x_j} < \frac{2}{x_j}$, uma vez que $q \geq 1$ e $\frac{1}{q} < 1$. Desta forma, usando $c = 2$, $n = 1$ e $\alpha = \frac{p}{q}$ para a igualdade (6.1), mostramos que $\alpha = \frac{p}{q}$ é aproximável na ordem 1.

Notemos que, para qualquer racional $\beta = \frac{v}{u}$ onde $v, u \in \mathbb{Z}$ e $u > 0$, tal que $\frac{v}{u} \neq \frac{p}{q}$, isto é, $pu - qv \neq 0$, tem-se

(6.10) $\left|\frac{p}{q} - \frac{v}{u}\right| = \left|\frac{pu-qv}{qu}\right| = \frac{|pu-qv|}{qu} \geq \frac{1}{qu}$.

Agora, se $\alpha = \frac{p}{q}$ fosse aproximável na ordem 2, teríamos a existência de uma constante $c > 0$ e de uma sequência de racionais $\left(\frac{v_j}{u_j}\right)$ distintos, tais que

(6.11) $\left|\frac{p}{q} - \frac{v_j}{u_j}\right| < \frac{c}{{u_j}^2}$.

Usando (6.10) e (6.11) nos elementos da sequência $\left(\frac{v_j}{u_j}\right)$, segue-se que $\frac{1}{qu_j} \leq \left|\frac{p}{q} - \frac{v_j}{u_j}\right| < \frac{c}{{u_j}^2}$, ou seja, $u_j < qc$. Deste modo, a sequência (u_j) é limitada, o que é um absurdo, pois $u_j \to \infty$. Logo, $\alpha = \frac{p}{q}$ não é aproximável na ordem 2, e portanto, também não é aproximável em nenhuma ordem superior. ■

Teorema 2) Todo número irracional α é aproximável na ordem 2, isto é, existe uma constante $c > 0$ tal que a desigualdade $\left|\alpha - \frac{h_j}{k_j}\right| < \frac{c}{{k_j}^2}$ se verifica para um número infinito de racionais $\frac{h_j}{k_j}$ distintos.

Demonstração: Seja α um número irracional e $n \in \mathbb{N}$. Representemos por $[x]$ a parte inteira de um número real x, isto é, o maior inteiro menor ou igual a x. Considere agora os $n + 1$ números reais

(6.12) $a_0 = 0\,, a_1 = \alpha - [\alpha]\,, a_2 = 2\alpha - [2\alpha]\,, \ldots, a_n = n\alpha - [n\alpha]$

os quais pertencem ao intervalo $[0,1) = \{x \in \mathbb{R}/0 \leq x < 1\}$. Considere em seguida a partição do intervalo $[0,1)$ em n intervalos, disjuntos dois a dois, construídos da forma seguinte:

(6.13) $\left[\frac{j}{n}, \frac{j+1}{n}\right)$ onde $j = 0,1, \ldots, n-1$.

Usando o Princípio da Casa dos Pombos, é claro que, pelo menos, dois dos números reais em (6.12) estão em um mesmo intervalo do tipo em (6.13). Digamos que eles sejam $a_{n_1} = n_1\alpha - [n_1\alpha\,]$ e $a_{n_2} = n_2\alpha - [n_2\alpha\,]$, com $0 \leq n_1 < n_2 \leq n$, para os quais temos então

(6.14) $\left|a_{n_2} - a_{n_1}\right| = |n_2\alpha - [n_2\alpha\,] - n_1\alpha + [n_1\alpha\,]| < \frac{1}{n}$.

Sejam agora $k = n_2 - n_1$ e $h = [n_2\alpha] - [n_1\alpha]$, os quais são números inteiros, com $k > 0$ e $h \geq 0$. Logo, (6.14) pode ser escrito como $|k\alpha - h| < \frac{1}{n}$ ou $\left|\alpha - \frac{h}{k}\right| < \frac{1}{nk}$. Como $0 < k < n \Rightarrow \frac{1}{n} < \frac{1}{k}$, de onde se segue

(6.15) $\left|\alpha - \frac{h}{k}\right| < \frac{1}{nk} = \frac{1}{n}\frac{1}{k} < \frac{1}{k^2}$.

Resumindo, mostramos que, para cada $n \in \mathbb{N}$, existe um racional da forma $\frac{h}{k}$, com $k < n$, para o qual (6.15) se verifica. Agora, afirmamos que (6.15) se verifica para um número infinito de racionais $\frac{h}{k}$ distintos. De fato, suponhamos que tal afirmação não seja verdade, ou seja, há apenas um número finito de racionais distintos satisfazendo (6.15), digamos, $\frac{h_1}{k_1}, \ldots, \frac{h_r}{k_r}$. Seja $\varepsilon = min\left\{\left|\alpha - \frac{h_1}{k_1}\right|, \ldots, \left|\alpha - \frac{h_r}{k_r}\right|\right\}$, o qual é positivo, já que $\alpha \notin \mathbb{Q}$. Tomemos $n \in \mathbb{N}$ tal que $\frac{1}{n} < \varepsilon$. Pelo que fizemos em (6.15), existe um racional $\frac{h}{k}$ tal que $\left|\alpha - \frac{h}{k}\right| < \frac{1}{nk} = \frac{1}{n}\frac{1}{k} \leq \frac{1}{n} < \varepsilon$. Portanto, $\frac{h}{k} \neq \frac{h_i}{k_i}$ para todo $i = 1, \ldots, r$. Isso é uma contradição, pois $\frac{h}{k}$ satisfaz (6.15). ■

Observe que o Teorema 2 nos diz que um número irracional é aproximável, pelo menos, na ordem 2. Dependendo do número irracional, ele poderá ser aproximável numa ordem superior a 2.

Hurwitz mostrou que a menor constante c que serve para todos os irracionais na desigualdade do Teorema 2 acima é $\frac{1}{\sqrt{5}}$. Ou seja, se $A < \frac{1}{\sqrt{5}}$, então existe um número irracional α tal que $\left|\alpha - \frac{p_j}{q_j}\right| > \frac{A}{{q_j}^2}$ para todos os racionais $\frac{p_j}{q_j}$, exceto para um número finito deles.

Teorema 3) Seja α um número algébrico real de grau n. Então, existe uma constante $A > 0$ tal que, para todo racional $\frac{p}{q}$, é válida a relação

(6.16) $\left|\alpha - \frac{p}{q}\right| > \frac{1}{A.q^n}$.

Para o caso particular de $n = 1$ (equivalentemente, se $\alpha \in \mathbb{Q}$), basta tomar $\frac{p}{q} \neq \alpha$ para todo $\frac{p}{q} \in \mathbb{Q}$.

Demonstração: Seja α uma solução de uma equação polinomial da forma

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

Agora, seja $d > 0$ tal que, no intervalo $[\alpha - d, \alpha + d]$ a única raiz de $f(x) = 0$ é α. (A existência de tal valor d se segue do fato de a equação polinomial ter no máximo n raízes reais: portanto d pode ser qualquer número menor que a menor das distâncias de α às demais raízes reais). A seguir observamos que a derivada $f'(x)$ é um polinômio de grau $n - 1$, e, portanto, ela é limitada em qualquer intervalo finito: seja, então, $M > 0$ tal que

(6.18) $|f'(x)| < M$, para $x \in [\alpha - d, \alpha + d]$.

Agora, para qualquer racional p/q (com $q > 0$) em $[\alpha - d, \alpha + d]$ temos, aplicando o Teorema do Valor Médio, que

$$f(\alpha) - f(p/q) = (\alpha - p/q)f'(\xi),$$

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

(6.19)

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

onde usamos a estimativa (6.18) no último passo. Para obter a desigualdade buscada, necessitamos de uma estimativa inferior para $f(p/q)$:

Como

$\alpha \neq \frac{p}{q} \in [\alpha - d, \alpha + d] \Rightarrow f\left(\frac{p}{q}\right) \neq 0 \Rightarrow$

$\Rightarrow |a_n p^n + a_{n-1} q p^{n-1} + \cdots + a_0 q^n| \in \mathbb{N} \Rightarrow |a_n p^n + a_{n-1} q p^{n-1} + \cdots + a_0 q^n| \geq 1 \Rightarrow$

(6.20)

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

Portanto, (6.19) e (6.20) nos darão a desigualdade

$$\frac{1}{q^n} \leq \left|f\left(\frac{p}{q}\right)\right| \leq M|\alpha - \frac{p}{q}|$$

ou seja

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

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

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

e como $q \geq 1$ temos $q \geq 1 \Rightarrow q^n \geq 1 \Rightarrow \frac{1}{q^n} \leq 1 \Rightarrow \frac{d}{q^n} \leq d \Rightarrow$

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

Tomamos, finalmente, $\frac{1}{A}$ igual ao menor dos números $\frac{1}{M}$ e d, e obtemos a relação (6.16) para todos os racionais $\frac{p}{q}$. Notemos que

$$\left(\frac{1}{M} \geq \frac{1}{A}\ e\ d \geq \frac{1}{A}\right) \Rightarrow \left(\frac{1}{Mq^n} \geq \frac{1}{Aq^n}\ e\ \frac{d}{q^n} \geq \frac{1}{Aq^n}\right).\blacksquare$$

Exercício: Mostre que para $x \in [\alpha - d, \alpha + d]$, temos $|x| \leq |\alpha| + d$. Use essa desigualdade para provar (6.18) a partir da forma explícita de $f'(x)$.

Solução: Utilizando a Desigualdade Triangular, se $x \in [\alpha - d, \alpha + d] \Rightarrow |x - \alpha| \leq d \Rightarrow |x| - |\alpha| \leq |x - \alpha| \leq d \Rightarrow |x| - |\alpha| \leq d \Rightarrow |x| \leq |\alpha| + d$

Utilizando a derivada de $f(x)$ e a Desigualdade Triangular, temos que

$$|f'(x)| = |na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x^1 + a_1| \leq$$
$$\leq n|a_n||x|^{n-1} + (n-1)|a_{n-1}||x|^{n-2} + \cdots + 2|a_2||x| + |a_1| \leq$$
$$\leq n|a_n|(|\alpha|+d)^{n-1} + (n-1)|a_{n-1}|(|\alpha| + d|^{n-2} + \cdots + 2|a_2|(|\alpha| + d) + |a_1|.$$

Tome $M > 0$ onde M é maior que o último termo da desigualdade acima e obtemos $|f'(x)| < M$ para $x \in [\alpha - d, \alpha + d]$.$\blacksquare$

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

Demonstração: Por contradição, suponha que existe $c > 0$ e uma sequência $\left(\frac{p_j}{q_j}\right)$ de racionais distintos, onde $p_j, q_j \in \mathbb{Z}$, com $q_j > 0$ e $mdc(p_j, q_j) = 1$, tais que satisfaçam

(6.21)

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

Para tais racionais, seguir-se-ia, de (6.16) e (6.21), que

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

Mas a última desigualdade não pode ocorrer, pois $q_j \to +\infty$. Portanto, α não é aproximável na ordem $n+1$. ■

Uma versão mais forte do Teorema 3, decorrente de um teorema de Roth-Siegel-Thue, estabelece o resultado a seguir.

Teorema 4) Seja φ um número algébrico real. Se houver uma infinidade de racionais distintos $\frac{p}{q}$, com $mdc(p,q) = 1$, $q > 0$, satisfazendo à desigualdade $\left|\varphi - \frac{p}{q}\right| \leq \frac{1}{q^v}$, então $v \leq 2$.

Segue-se do Teorema 4 que se $s > 2$, então há apenas um número finito de racionais $\frac{p}{q}$ satisfazendo à desigualdade $\left|\varphi - \frac{p}{q}\right| \leq \frac{1}{q^s}$ para todo número algébrico φ. Esse resultado gera mais uma consequência que relatamos a seguir. Dados um número algébrico φ e um número $\varepsilon > 0$, existe uma constante $D > 0$ tal que $\left|\varphi - \frac{p}{q}\right| \geq \frac{D}{q^{2+\varepsilon}}$ para qualquer número racional $\frac{p}{q}$.

Vale alertar que o Corolário 1 não diz que um número algébrico de grau n deva ser aproximável na ordem n .

Definição 3) Um número real α é chamado um *número de Liouville* se existir uma sequência $\left(\frac{p_j}{q_j}\right)$ 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

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

Observe que a potência de q_j é j, ou seja, é um valor variável e não fixo (igual a n) como na Definição 2. Além disso, o numerador da fração do lado direito é o valor $c = 1$.

Teorema 5) Todo número de Liouville é transcendente.

Demonstração: Suponhamos, por contradição, que um certo número de Liouville α seja algébrico, digamos de grau n. Então, pelo Teorema 3, segue-se que a relação (6.3) é válida para todo racional. Em particular, para os $\frac{p_j}{q_j}$ da Definição 3. Assim, obtemos as desigualdades $\frac{1}{A.{q_j}^n} < \left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{{q_j}^j}$, de onde tiramos que ${q_j}^{j-n} < A$. Como $q_j \to \infty$, existe j suficientemente grande tal que $q_j > A$ e $j \geq n + 1$. Para tal j vale que ${q_j}^{j-n} \geq q_j > A$, de onde chegamos ao fato absurdo de $A < {q_j}^{j-n} < A$. Portanto, o número α é transcendente.■

Corolário 2) Seja α um número real tal que $\left|\alpha - \frac{v_j}{u_j}\right| < \frac{1}{{u_j}^j}$, onde $\left(\frac{v_j}{u_j}\right)$ é uma sequência de racionais, todos distintos com $u_j > 0$, onde agora não exigimos a condição de $mdc(v_j, u_j) = 1$. Então, α é um número de Liouville.

Demonstração: Considere a sequência $\left(\frac{p_j}{q_j}\right)$ com $q_j > 0$ e $mdc(p_j, q_j) = 1$ definida por $\frac{p_j}{q_j} = \frac{v_j}{u_j}$. Neste caso, temos $q_j \leq u_j \Rightarrow {q_j}^j \leq {u_j}^j \Rightarrow \frac{1}{{u_j}^j} \leq \frac{1}{{q_j}^j}$. Então, $\left|\alpha - \frac{p_j}{q_j}\right| = \left|\alpha - \frac{v_j}{u_j}\right| < \frac{1}{{u_j}^j} \leq \frac{1}{{q_j}^j}$, provando que α é um número de Liouville. ■

Exemplo 1) Considere o número α definido pela expressão

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

Mostre que α é um número de Liouville.

Demonstração: Considere a sequência de racionais definida por

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

Assim, $\frac{v_j}{u_j} = \sum_{k=1}^{j} \frac{1}{10^{k!}}$ corresponde a uma soma de frações cujo mínimo múltiplo comum (mmc) é igual a $10^{j!}$, ou seja, $u_j = 10^{j!}$.

Temos que

$$\left|\alpha - \frac{v_j}{u_j}\right| = \sum_{k=j+1}^{\infty} \frac{1}{10^{k!}} = \frac{1}{10^{(j+1)!}} . \left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + \frac{1}{10^{(j+3)!-(j+1)!}} + \cdots\right)$$

.

A expressão em parênteses é majorada por $1 + \frac{1}{10} + \frac{1}{10^2} + \cdots = \frac{10}{9}$, pois corresponde a soma infinita dos termos de uma progressão geométrica.

Como $(j+1)! = (j+1).j! = j.j! + j!$, temos $\frac{1}{10^{(j+1)!}} = \frac{1}{(10^{j!})^{j}.10^{j!}}$.

Logo, a igualdade acima sofre a seguinte majoração:

$$\left|\alpha - \frac{v_j}{u_j}\right| = \sum_{k=j+1}^{\infty} \frac{1}{10^{k!}} = \frac{1}{10^{(j+1)!}} . \left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + \frac{1}{10^{(j+3)!-(j+1)!}} + \cdots\right) <$$

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

Enfim, chegamos a $\left|\alpha - \frac{v_j}{u_j}\right| < \frac{1}{(10^{j!})^{j}} = \frac{1}{{u_j}^{j}}$, uma vez que $u_j = 10^{j!}$.

Pelo Corolário 2,

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

é um número de Liouville.■

Observe o formato que o número acima adquire:

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} = \frac{1}{10^1} + \frac{1}{10^2} + \frac{1}{10^6} + \frac{1}{10^{24}} + \cdots$$

ou

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} = 0{,}110001000000000000000000001\ldots$$

Exemplo 2) Qualquer número da forma $\alpha = \sum_{k=1}^{\infty} \frac{a}{10^{k!}}$ onde a é qualquer um dos algarismos de 1 a 9, é um número de Liouville.

Demonstração:

$$\alpha = \sum_{k=1}^{\infty} \frac{a}{10^{k!}} \leq \sum_{k=1}^{\infty} \frac{9}{10^{k!}} = 9.\sum_{k=1}^{\infty} \frac{1}{10^{k!}}$$

onde $a \in \{1,2,\ldots,9\}$. Considere a sequência de números racionais definida por

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

Analogamente ao que fizemos no Exemplo 1, majoramos

$$9.\left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + \frac{1}{10^{(j+3)!-(j+1)!}} + \cdots\right) < 9.\frac{10}{9} = 10$$

Assim, obtemos

$$\left|\alpha - \frac{v_j}{u_j}\right| = \sum_{k=j+1}^{\infty} \frac{a}{10^{k!}} = \frac{1}{10^{(j+1)!}} .9.\left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + \frac{1}{10^{(j+3)!-(j+1)!}} + \cdots\right) <$$

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

Enfim, novamente chegamos a $\left|\alpha - \frac{v_j}{u_j}\right| < \frac{1}{(10^{j!})^{j}} = \frac{1}{{u_j}^{j}}$, uma vez que $u_j = 10^{j!}$. Pelo Corolário 2,

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

é um número de Liouville.■

Observe o formato que o número acima adquire:

$$\alpha = \sum_{k=1}^{\infty} \frac{a}{10^{k!}} = \frac{a}{10^1} + \frac{a}{10^2} + \frac{a}{10^6} + \frac{a}{10^{24}} + \cdots$$

ou

$$\alpha = \sum_{k=1}^{\infty} \frac{a}{10^{k!}} = 0, aa000a00000000000000000a \ldots$$

Os exemplos acima são os únicos números reais cuja transcendência foi demonstrada. Nos próximos capítulos, faremos a verificação de que os números irracionais e e π são transcendentes.

7 A TRANSCENDÊNCIA DO NÚMERO *e*

O número de Euler e mencionado no Capítulo 4 e no qual verificamos sua irracionalidade, é agora questionado sobre sua transcendência. Saber se um número é transcendente, é, em geral, uma questão muito difícil. Talvez por isso mesmo a questão se torna desafiadora, e, via de regra, a solução é um belo arranjo matemático. No Capítulo 9, veremos que nenhum segmento cujo comprimento seja um número transcendente (e também muitos segmentos cujos comprimentos sejam números algébricos) pode ser construído com régua e compasso. Esse fato nos dá uma aplicação prática à questão da transcendência de um dado número.

A transcendência do número e permaneceu sem solução até o século XIX, quando em 1873, o matemático francês C. Hermite marcou época ao demonstrar esse fato. 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). A demonstração que apresentaremos a seguir é baseada na realizada por Hurwitz.

A demonstração de que e é um número transcendente seguirá uma sequência de exercícios propostos a seguir, acompanhados de suas devidas soluções ou referências para suas justificativas.

Exercício 1) Seja $P(x)$ um polinômio de grau r. Defina a função

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

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

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

Demonstração: $F'(x) = P'(x) + \cdots + P^{(r)}(x)$, pois $P^{(r+1)}(x) = 0$.
Note que $F'(x) = F(x) - P(x)$. Assim, temos que

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

Portanto,

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

Exercício 2) Use o Teorema do Valor Médio para a função

$$G(x) = e^{-x}.F(x)$$

e mostre que

(7.2) $F(k) - e^{k}.F(0) = -k.e^{k(1-\theta_k)}.P(k.\theta_k)$

para todo $k > 0$, onde θ_k é um número entre 0 e 1.

Demonstração: $G(x)$ é uma função continuamente derivável em $\mathbb{R}$. Aplicando o Teorema do Valor Médio no intervalo $[0, k]$ com $k \in \mathbb{N}$, temos que existe θ_k com $0 < \theta_k < 1$ tal que $G(k) - G(0) = (k - 0).\ G'(0 + \theta_k.(k - 0)) = k.G'(k.\theta_k)$. Logo,

$$e^{-k}.F(k) - F(0) = -k.e^{-k.\theta_k}.P(k.\theta_k)$$

Multiplicando por e^{k} temos

$$F(k) - e^{k}.F(0) = -k.e^{k(1-\theta_k)}.P(k.\theta_k)$$

para todo $k > 0$ e $0 < \theta_k < 1$.■

Exercício 3) Considere a expressão

(7.3) $\varepsilon_k = -k.e^{k(1-\theta_k)}.P(k.\theta_k)$ onde $k = 1, \dots, n$.

Suponha que e seja um número algébrico, isto é, existem números inteiros $c_0, c_1, \dots, c_n$ (podemos tomar $c_0 > 0$) tais que

(7.4) $c_n.e^{n} + \cdots + c_1.e + c_0 = 0$

Mostre que vale a igualdade

(7.5) $c_0 . F(0) + c_1 . F(1) + \cdots + c_n . F(n) = c_1 . \varepsilon_1 + \cdots + c_n . \varepsilon_n$

Demonstração: De (7.2) temos ε_k= - $k . e^{k(1-\theta_k)} . P(k . \theta_k) = F(k)$ - $e^k . F(0)$, isto é, $F(k)$ - $\varepsilon_k = e^k . F(0)$, para todo k > 0. Assim,

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

donde segue-se a igualdade (7.5).■

Considere o polinômio

(7.6) $P(x) = \frac{1}{(p-1)!} . x^{p-1} . (1-x)^p . (2-x)^p \ldots . (n-x)^p$, sendo p um número primo tal que $p > n$, $p > c_0$, onde n e c_0 são dados em (7.4). A ideia agora é demonstrar que para tal polinômio $P(x)$, o lado esquerdo de (7.5) é um número inteiro não divisível por p, enquanto o lado direito é menor que 1 em valor absoluto. Isso será um absurdo.

Exercício 4) Seja $Q(x) = \sum_{j=0}^{r} a_j . x^j$ um polinômio com coeficientes inteiros e $p < r$ um número natural. Mostre que

(7.7)

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

Utilizando (7.7), mostre que para $i \geq p$ obtemos $\frac{1}{(p-1)!} . Q^{(i)}(x)$ no formato de um polinômio com coeficientes inteiros divisíveis por p.

Demonstração: A fórmula (7.7) é obtida sem dificuldades pela aplicação do princípio de indução finita e deixamos a cargo do leitor. Agora, sejam $p \in \mathbb{N}$ com $p \leq i \leq r$ e $j \in \{i, \ldots, r\}$. Logo temos

$$\frac{1}{(p-1)!}.Q^{(i)}(x) =$$

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

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

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

Exercício 5) Considere o polinômio $P(x)$ definido em (7.6). Mostre que $P(x)$ é da forma

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

Mostre que valem:

(7.9) $P^{(i)}(k) = 0$ para $k = 1, \ldots, n$ e $i < p$

(7.10) $P^{(p-1)}(0) = (n!)^p$ e $P^{(i)}(0) = 0$ para $i < p-1$.

Demonstração:

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

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

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

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

concluindo (7.8).

Agora temos

$$P^{(i)}(x) = \frac{1}{(p-1)!}.\sum_{j=0}^{i}\binom{i}{j}.D^j[x^{p-1}].\ D^{i-j}[\big((1-x)\dots(n-x)\big)^p]$$

Se $i < p \Rightarrow i \leq p-1 \Rightarrow i-j \in \{0,1,\dots,p-1\} \Rightarrow D^{i-j}[\big((1-x)\dots(n-x)\big)^p]$ contém o fator $(1-x)\dots(n-x)$ em sua derivação, pelo menos uma vez. Logo,

$P^{(i)}(k) = 0$ para $k = 1,\dots,n$ e $i < p$, concluindo (7.9).

Observe que $P^{(p-1)}(x) = (n!)^p + \frac{d_0}{(p-1)!}.x^1 + \cdots + \frac{d_{n.p-1}}{(p-1)!}.x^{n.p}$ .Daí, chegamos a $P^{(p-1)}(0) = (n!)^p$.

Se $i < p-1 \Rightarrow i \leq p-2 \Rightarrow j \leq i \leq p-2 \Rightarrow D^j[x^{p-1}]$ contém o fator x em sua derivação, pelo menos uma vez. Logo, $D^j[x^{p-1}](0) = 0$ para todo $j = 0,1,\dots,i$. Portanto, $P^{(i)}(0) = 0$ para $i < p-1$, finalizando (7.10).■

Exercício 6) Use os Exercícios 4 e 5 para mostrar que $F(k)$, para $k = 1,\dots,n$, é um inteiro divisível por p. Mostre também que $F(0)$ é um inteiro não divisível por p. (Use o fato que $(n!)^p$ não é divisível por p, uma vez que $p > n$ e p é primo.

Demonstração: Seja $Q(x) = x^{p-1}.(1-x)^p.(2-x)^p \dots .(n-x)^p$. Assim, temos $Q(x) = n!.x^{p-1} + b_0.x^p + \cdots + b_{n.p-1}.x^{p+n.p-1} \in \mathbb{Z}[x]$ onde $\partial Q = grau\big(Q(x)\big) = n.p-1 := r > p$. Logo, $Q(x)$ satisfaz o Exercício 4 e $P(x) = \frac{1}{(p-1)!}.Q(x)$ na equação (7.8). Para $i \geq p$, $P^{(i)}(x) = \frac{1}{(p-1)!}.Q^{(i)}(x)$ é um polinômio com coeficientes inteiros divisíveis por p. Donde, para $i \geq p$, $P^{(i)}(k)$ é um número

inteiro divisível por p, para todo $k \in \mathbb{Z}$ e, em particular, para $k = 1, \dots, n$. Porém, para $i < p$, $P^{(i)}(k) = 0$ para $k = 1, \dots, n$. Qualquer que seja o caso, temos que $P^{(i)}(k)$ é um número inteiro divisível por p, para $k = 1, \dots, n$ onde $0 \leq i \leq r := p + n.p - 1$.

Logo, $F(k) = P(k) + P'(k) + \cdots + P^{(r)}(k)$ é um número inteiro divisível por p, $\forall\, k \in \{1, \dots, n\}$.

Agora, $F(0) = P(0) + P'(0) + \cdots P^{(p-2)}(0) + P^{(p-1)}(0) + P^{(p)}(0) + \cdots + P^{(r)}(0)$. Pelo Exercício 5, $F(0) = (n!)^p + P^{(p)}(0) + \cdots + P^{(r)}(0)$. Sabemos que $P^{(i)}(0)$ é um número inteiro divisível por p, para $i \geq p$ e $k = 0$ no que vimos acima. Portanto, p divide $P^{(p)}(0) + \cdots + P^{(r)}(0)$, uma vez que p divide $P^{(p)}(0), \dots, P^{(r)}(0)$. 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.■

Exercício 7) Utilize o Exercício 6 e a maneira como o primo p foi escolhido para mostrar que $c_0.F(0) + c_1.F(1) + \dots + c_n.F(n)$ é um número inteiro não divisível por p.

Demonstração: Como $p \mid F(1), \dots, F(n) \Rightarrow p \mid c_1.F(1), \dots, c_n.F(n) \Rightarrow p \mid c_1.F(1) + \cdots + c_n.F(n)$. Fizemos a escolha de p primo com $o < c_0 < p$. Se supormos que $p \mid c_0.F(0) + c_1.F(1) + \cdots + c_n.F(n)$, então $p \mid c_0.F(0)$, acarretando que $p \mid c_0$ ou $p \mid F(0)$. Mas, pelo Exercício 6, $p \nmid F(0)$, restando a possibilidade de $p \mid c_0$, impondo a condição de $p \leq c_0$. Isso é um absurdo, pois $o < c_0 < p$. Portanto, $c_0.F(0) + c_1.F(1) + \dots + c_n.F(n)$ é um número inteiro não divisível por p.■

Exercício 8) Observe que os ε_k, definidos em (7.3), e calculados para o polinômio $P(x)$, definido em (7.6), têm a forma

(7.11) $\varepsilon_k = -k.e^{k(1-\theta_k)}.\frac{1}{(p-1)!}.(k.\theta_k)^{p-1}.(1-k.\theta_k)^p.(2-k.\theta_k)^p \dots .(n-k.\theta_k)^p.$

Usando (7.11) e o fato de que $0 < \theta_k < 1$, mostre que vale

(7.12) $|\varepsilon_k| \leq \frac{e^n.n^p.(n!)^p}{(p-1)!}$, para $k = 1, \dots, n$.

Demonstração: Aplicando $x = k.\theta_k$ no polinômio $P(x)$ de (7.6) e substituindo esse valor em (7.3), obtemos a expressão desejada

$$\varepsilon_k = -k.e^{k(1-\theta_k)}.\frac{1}{(p-1)!}.(k.\theta_k).^{p-1}.(1-k.\theta_k)^p.(2-k.\theta_k)^p \ldots.(n-k.\theta_k)^p.$$

Temos $1 \leq k \leq n$ e $0 < \theta_k < 1 \Rightarrow 0 < k.\theta_k < k \leq n \Rightarrow -k < -k.\theta_k < 0$ $\Rightarrow 0 < k - k.\theta_k < k \leq n \Rightarrow e^{k-k.\theta_k} < e^n$. Além disso, como $-k.\theta_k < 0 \Rightarrow j - k.\theta_k < j$, para $j = 1, \ldots, n$. Com isso, temos a relação $(1-k\theta_k)^p.(2-k\theta_k)^p \ldots.(n-k\theta_k)^p = [(1-k\theta_k)(2-k\theta_k)\ldots(n-k\theta_k)]^p < (1.2\ldots n)^p = (n!)^p$. Além disso, $k\theta_k < n \Rightarrow (k\theta_k)^{p-1} < n^{p-1}$. Agora, chegamos nas expressões:

$$|\varepsilon_k| = |-k|.\left|e^{k(1-\theta_k)}\right|.\left|\frac{1}{(p-1)!}\right|.|k.\theta_k|^{p-1}.|1-k.\theta_k|^p \ldots.|n-k.\theta_k|^p$$

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

$$|\varepsilon_k| < \frac{n.e^n.n^{p-1}}{(p-1)!}.1^p.2^p \ldots n^p = \frac{n.e^n.n^{p-1}}{(p-1)!}..((1.2\ldots.n)^p) = \frac{e^n.n^p}{((p-1)!)}.(n!)^p, \quad \text{para}$$

$k = 1, \ldots, n$. ■

Exercício 9) Mostre que se p for um número primo suficientemente grande, então vale

(7.13) $|c_1.\varepsilon_1 + \ldots + c_n.\varepsilon_n| < 1.$

Demonstração: Sabemos que fixado $a \in \mathbb{N}$, temos $\lim_{q\to\infty}\frac{a^q}{q!} = 0$. Por (7.12), vemos que $|\varepsilon_k| \leq \frac{e^n.(n.n!)}{((p-1)!)}.(n.n!)^{p-1}$, para $k = 1, \ldots, n$ onde n é um número natural fixo e p é qualquer primo satisfazendo a $p > n$ e $p > c_0$.

Tomando $a = n.n!$ e $q = p-1$ chegamos a

$$\lim_{p\to\infty}\frac{e^n.n^p}{\big((p-1)!\big)}.(n!)^p=\lim_{p\to\infty}\frac{e^n.(n.n!)}{\big((p-1)!\big)}.(n.n!)^{p-1}=$$

$$=e^n.(n.n!).\lim_{p\to\infty}\frac{(n.n!)^{p-1}}{(p-1)!}=e^n.(n.n!).\lim_{q\to\infty}\frac{a^q}{q!}$$

$$=e^n.(n.n!).0=0$$

Daí,

$$0\le\lim_{p\to\infty}|\varepsilon_k|\le\lim_{p\to\infty}\frac{e^n.n^p}{\big((p-1)!\big)}.(n!)^p=0$$

e logo $\lim_{p\to\infty}|\varepsilon_k|=0$,ou seja, $\lim_{p\to\infty}\varepsilon_k=0$ para $k=1,\dots,n$. Assim, fixado $k\in\{1,\dots,n\}$, existe um primo p_k suficientemente grande tal que $|\varepsilon_k|<\frac{1}{n.|c_k|}$. Seja $p=\max\{p_1,\dots,p_n\}$, isto é, p é o maior entre esses primos. Usando a desigualdade triangular e o primo p, temos $|c_1.\varepsilon_1+\cdots+c_n.\varepsilon_n|\le|c_1|.|\varepsilon_1|+\cdots+|c_n|.|\varepsilon_n|<|c_1|.\frac{1}{n.|c_1|}+\cdots+|c_n|.\frac{1}{|c_n|}=\frac{1}{n}+\cdots+\frac{1}{n}=1.$■

Portanto, utilizando o Exercício 7, a equação (7.5), juntamente com $|c_1.\varepsilon_1+\cdots+c_n.\varepsilon_n|<1$, temos que $c_1.\varepsilon_1+\cdots+c_n.\varepsilon_n=0$. Logo, $p\mid c_1.\varepsilon_1+\cdots+c_n.\varepsilon_n\Rightarrow p\mid c_0.F(0)+c_1.F(1)+\cdots+c_n.F(n)$, o que é um absurdo pelo que vimos no Exercício 7. Tal contradição é proveniente do fato de supormos que e seja um número algébrico. Concluímos, então, que e é um número transcendente.■

8 POLINÔMIOS SIMÉTRICOS

Se $t_1, \dots, t_n \in \mathbb{C}$ e são raízes de um polinômio $P(x)$, então esse polinômio é da forma

(8.1) $$P(x) = (x - t_1), \dots, (x - t_n).$$

Claro que podemos supor que o coeficiente líder de $P(x)$ é igual a 1.

Desenvolvendo o produto indicado em (8.1) obtemos

(8.2) $$P(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n ,$$

Onde

(8.3.1)
$$s_1 = \sum_{j=1}^{n} t_j$$

(8.3.2)
$$s_2 = \sum_{i<j} t_i t_j$$

(8.3.3)
$$s_3 = \sum_{i<j<k} t_i t_j t_k$$

⋮ ⋮

(8.3.n) $$s_n = t_1 t_2 \dots t_n$$

Os polinômios (8.3.1), (8.3.2), ..., (8.3.n) são chamados os *polinômios simétricos elementares em* $t_1, \dots, t_n$.

Exemplos:

1) $(n = 1)$. Neste caso, há um único polinômio simétrico elementar, $s_1 = t_1$.

2) ($n = 2$). Os polinômios simétricos elementares neste caso são

$$s_1 = t_1 + t_2\,, \qquad s_2 = t_1 t_2$$

3) ($n = 3$). Neste caso os polinômios simétricos elementares são

$$s_1 = t_1 + t_2 + t_3, \quad s_2 = t_1 t_2 + t_1 t_3 + t_2 t_3, \quad s_3 = t_1 t_2 t_3$$

Uma *permutação* dos inteiros $1, 2, \dots, n$, é uma função bijetiva (isto é, 1-1 e sobre) do conjunto $\{1, 2, \dots, n\}$ nele próprio:

$$\sigma: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} \qquad j \rightarrow \sigma(j)$$

Exemplos:

1) Se $n = 1$ existe apenas uma permutação 1→1.

2) Se $n = 2$ existem duas permutações,

$$\begin{array}{cc} \sigma_1: 1 \rightarrow 1, & \sigma_2: 1 \rightarrow 2 \\ \quad 2 \rightarrow 2 & \quad 2 \rightarrow 1 \end{array}$$

3) Se $n = 3$ existem seis permutações,

$$\begin{array}{cccc} \sigma_1: 1 \rightarrow 1, & \sigma_2: 1 \rightarrow 2, & \sigma_3: 1 \rightarrow 3 & \sigma_4: 1 \rightarrow 1 \\ 2 \rightarrow 2 & 2 \rightarrow 3 & 2 \rightarrow 1 & 2 \rightarrow 3 \\ 3 \rightarrow 3 & 3 \rightarrow 1 & 3 \rightarrow 2 & 3 \rightarrow 2 \end{array}$$

$$\begin{array}{cc} \sigma_5: 1 \rightarrow 2, & \sigma_6: 1 \rightarrow 3 \\ 2 \rightarrow 1 & 2 \rightarrow 2 \\ 3 \rightarrow 3 & 3 \rightarrow 1 \end{array}$$

O leitor pode ver que, em geral, existem $n!$ permutações dos inteiros $\{1, 2, \dots, n\}$.

Consideremos agora polinômios em $t_1, t_2, \dots, t_n$ com coeficientes em um conjunto *A*. (Neste capítulo, *A* será sempre o conjunto $\mathbb{Q}$ dos racionais, ou $\mathbb{Z}$ dos inteiros). Por exemplo, os dados em (8.3.1), (8.3.2), ..., (8.3.n). Outros exemplos:

(i) $(t_1 + \cdots + t_n)^3$;

(ii) $(t_1^2 + \cdots + t_n^2)$;

(iii) $3t_1 t_3^2 t_5$.

Uma expressão como a (iii) acima é chamada um *monômio*. A forma geral de um monômio é

(8.4) $$a t_1^{k_1} t_2^{k_2} \dots t_n^{k_n},$$

onde os k_j são inteiros maiores ou iguais a 0, e $a \in A$ é seu coeficiente. O *grau* do monômio (8.4) é, por definição, o número inteiro $\sum_{j=1}^{n} k_j$. Define-se, também, o *peso* do monômio (8.4) como o inteiro $\sum_{j=1}^{n} j k_j$. Desta forma, o grau do monômio (iii) é 4, e seu peso é 12.

O *grau* de um polinômio é o máximo dos graus dos monômios que o formam. Analogamente, o *peso* de um polinômio é o máximo dos pesos dos monômios que o constituem. Assim, o grau do polinômio (i) é 3, e do polinômio (ii) é 2. O peso do polinômio (i) é $3n$, e do polinômio (ii) é $2n$. A expressão geral de um polinômio de grau m com coeficientes em A é

(8.5)

$$f(t_1, \dots, t_n) = a_{k_1 k_2 \dots k_n} \sum_{k_1 + \cdots k_n \leq m} {t_1}^{k_1} \dots {t_n}^{k_n}$$

onde os coeficientes $a_{k_1 k_2 \dots k_n}$ estão em A, além de $a_{k_1 k_2 \dots k_n}$ não serem todos nulos quando ocorrer de $k_1 + \cdots k_n = m$.

Seja σ uma permutação dos inteiros $1, \dots, n$. Dado um polinômio $f(t_1, \dots, t_n)$, a ele associamos um outro polinômio, que representamos por $f^{\sigma}(t_1, \dots, t_n)$, assim definido

(8.6) $f^{\sigma}(t_1, \dots, t_n) = f(t_{\sigma(1)}, \dots, t_{\sigma(n)})$.

Exemplos:

1) Considere $n = 2$ e a permutação σ_2 , definida acima. Se

$$f(t) = t_1^3 + 2t_1t_2 + 0{,}3\ t_2$$

então $f^{\sigma_2}(\mathrm{t}) = t_2^3 + 2t_2t_1 + 0{,}3\ t_1$.

Se tomarmos o polinômio

(8.7) $f(t_1, t_2) = (t_1+t_2)^4$

então $f^{\sigma_2}(t_1, t_2) = (t_2+t_1)^4$.

2) Considere $n = 3$ e a permutação σ_5 , definida acima. Se

$$f(t_1, t_2, t_3) = t_1^6 + 0{,}5\ t_2t_3^4 + 4\ t_1t_2^3t_3^6$$

então $f^{\sigma_5}(t_1, t_2, t_3) = t_2^6 + 0{,}5\ t_1t_3^4 + 4\ t_2t_1^3t_3^6$

Se tomarmos o polinômio

(8.8) $f(t_1, t_2, t_3) = t_1t_2 + t_1t_3 + t_2t_3$

então $f^{\sigma_5}(t_1, t_2, t_3) = t_2t_1 + t_2t_3 + t_1t_3$. Logo, $f(t_1, t_2, t_3) = f^{\sigma_5}(t_1, t_2, t_3)$.

Um polinômio $f(t_1, \dots, t_n)$ é chamado *simétrico* se

(8.9) $f^{\sigma}(t_1, \dots, t_n) = f(t_1, \dots, t_n)$

para todas as permutações σ dos inteiros $1, \dots, n$.

Exemplos:

1) Os polinômios (8.7) e (8.8) são simétricos.

2) Os polinômios simétricos elementares (8.3.1), (8.3.2),...,(8.3.n) são simétricos.

3) Qualquer polinômio $g(s_1, \dots, s_n)$ nos polinômios simétricos elementares $s_1, \dots, s_n$, com coeficientes em A, é um polinômio simétrico em $t_1, \dots, t_n$. Assim, para $n = 2$, o polinômio

$$f(t_1, t_2) = (t_1 + t_2)^3 + 4t_1t_2$$

é simétrico, pois é equivalente ao polinômio $g(s_1, s_2) = s_1^3 + 4s_2$ nos polinômios elementares s_1, s_2.

Nosso objetivo a seguir será provar a recíproca do exemplo 3 acima. Isto é, qualquer polinômio simétrico em $t_1, \dots, t_n$ é um polinômio em $s_1, \dots, s_n$.

Vejamos mais alguns polinômios que satisfazem a este fato.

Exemplos:

1) $(n = 2)$. O polinômio $f(t_1, t_2) = t_1^2 + t_2^2 + 6t_1t_2$ é simétrico, e vemos que

$$t_1^2 + t_2^2 + 6t_1t_2 = (t_1 + t_2)^2 + 4t_1t_2$$

.

Logo, o polinômio $g(s_1, s_2)$ nesse caso será $g(s_1, s_2) = s_1^2 + 4s_2$.

2) $(n = 3)$. O polinômio $f(t_1, t_2, t_3) = t_1^2 + t_2^2 + t_3^2 + t_1t_2t_3$ é simétrico, e podemos checar que

$$t_1^2 + t_2^2 + t_3^2 + t_1t_2t_3 == (t_1 + t_2 + t_3)^2 - 2(t_1t_2 + t_1t_3 + t_2t_3) + t_1t_2t_3$$

Logo, o polinômio $g(s_1, s_2, s_3)$ nesse caso será $g(s_1, s_2, s_3) = s_1^2 - 2s_2 + s_3$.

Teorema 1) Seja $f(t_1, \dots, t_n)$ um polinômio simétrico de grau d com coeficientes em *A*. Então, existe um polinômio $g(s_1, \dots, s_n)$ de peso menor ou igual a d com coeficientes em *A*, onde $s_1, \dots, s_n$ são os polinômios simétricos elementares definidos em (8.3.1), ..., (8.3.n), tal que

(8.10) $f(t_1, \dots, t_n) = g(s_1, \dots, s_n)$.

Demonstração: (Por indução em n). Para $n = 1$, o teorema é óbvio, pois nesse caso $s_1 = t_1$. Suponhamos, agora, que o teorema seja válido para polinômio em $t_1, \dots, t_{n-1}$. Representemos por $\bar{s}_1, \dots, \bar{s}_{n-1}$ os polinômios simétricos elementares em $t_1, \dots, t_{n-1}$:

(8.11.1)

$$\bar{s}_1 = \sum_{j=1}^{n-1} t_j$$

(8.11.2)

$$\bar{s}_2 = \sum t_i t_j\,, \qquad 1 \le i < j \le n-1$$

(8.11.3)

$$\bar{s}_3 = \sum t_i t_j t_k\,, \qquad 1 \le i < j < k \le n-1$$

⋮ ⋮

(8.11.n-1) $\bar{s}_{n-1} = t_1 \dots t_{n-1}$

os quais podem ser obtidos das expressões correspondentes, em (8.3.1), ..., (8.3.n) fazendo-se $t_n = 0$.

Agora, para provar que o teorema vale para polinômios em $t_1, \dots, t_n$, procedemos por indução nos graus d desses polinômios. Para $d = 0$, o resultado é trivial, pois teríamos apenas os polinômios constantes. Suponha que o resultado seja válido para polinômios de grau menor que d, e provemos que ele se verifica para polinômios de grau d. Seja, pois, $f(t_1, \dots, t_n)$ um polinômio de grau d. Pela

hipótese de indução, existe um polinômio de peso menor ou igual a d, $g_1(\bar{s}_1, \dots, \bar{s}_{n-1})$, tal que

(8.12) $f(t_1, \dots, t_{n-1}, 0) = g_1(\bar{s}_1, \dots, \bar{s}_{n-1})$

Assim $g_1(s_1, \dots, s_{n-1})$ é um polinômio em $t_1, \dots, t_n$, cujo grau é menor ou igual a d. É fácil verificar que $g_1(s_1, \dots, s_{n-1})$ é um polinômio simétrico em $t_1, \dots, t_n$. Logo,

(8.13) $f_1(t_1, \dots, t_n) = f(t_1, \dots, t_n) - g_1(s_1, \dots, s_{n-1})$

é um polinômio simétrico em $t_1, \dots, t_n$. Provaremos agora que $f_1(t_1, \dots, t_n)$ é da forma (8.14), abaixo, com f_2 de grau menor que d, para então usarmos a hipótese de indução. Vejamos: se fizermos $t_n = 0$ em (8.13), obtemos, em virtude de (8.12), que

$$f_1(t_1, \dots, t_{n-1}, 0) = 0$$

.

Consequentemente, t_n é um fator comum em $f_1(t_1, \dots, t_n)$. Agora, do fato que $f_1(t_1, \dots, t_n)$ é simétrico em $t_1, \dots, t_n$, segue-se que t_j, para todo $j = 1, \dots, n$, é fator comum de $f_1(t_1, \dots, t_n)$. Logo, como $s_n = t_1 t_2 \dots t_n$, temos

(8.14) $f_1(t_1, \dots, t_n) = t_1 t_2 \dots t_n . f_2(t_1, \dots, t_n) = s_n f_2(t_1, \dots, t_n)$

e daí se segue que o grau de f_2 é $\leq d - n < d$. Aplicando a hipótese de indução, temos que existe um polinômio $g_2(s_1, \dots, s_n)$ de peso menor ou igual a $d - n$, tal que

(8.15) $f_2(t_1, \dots, t_n) = g_2(s_1, \dots, s_n)$

Finalmente, de (8.13), (8.14) e (8.15) obtemos

$$f(t_1, \dots, t_n) = s_n g_2(s_1, \dots, s_n) + g_1(s_1, \dots, s_{n-1})$$

o que mostra que $f(t_1, \dots, t_n)$ é igual a um polinômio simétrico em $s_1, \dots, s_n$: $g(s_1, \dots, s_n) = s_n g_2(s_1, \dots, s_n) + g_1(s_1, \dots, s_{n-1})$. O peso de $g(s_1, \dots, s_n)$ é menor ou igual a d. Assim, a demonstração do Teorema 1 está concluída. ■

Observação: Nos cursos de Álgebra, vemos que o conjunto de todos os polinômios $f(t_1, \dots, t_n)$ com coeficientes em $\mathbb{Q}$, representado por $\mathbb{Q}[t_1, \dots, t_n]$, forma um anel. O conjunto dos polinômios simétricos forma um subanel. O Teorema 1 mostra que esse subanel é gerado pelos polinômios simétricos elementares.

Nosso objetivo será, agora, provar alguns fatos que serão usados no decorrer do Capítulo 9.

Teorema 2) Sejam $\alpha_1, \dots, \alpha_n$ números algébricos, tais que os polinômios simétricos elementares

(8.16.1)

$$s_1 = \sum_{j=1}^{n} \alpha_j$$

(8.16.2)

$$s_2 = \sum \alpha_i \alpha_j, \ \ 1 \leq i < j \leq n$$

⋮ ⋮

(8.16.n) $s_n = \alpha_1, \dots, \alpha_n$

sejam números racionais. Considere agora os $\binom{n}{2}$ números algébricos

(8.17) $\beta_{ij} = \alpha_i + \alpha_j, \ \ 1 \leq i < j \leq n.$

Então, os polinômios simétricos elementares associados aos $\beta_{ij}{}'s$ são também números racionais.

Demonstração: Em virtude do Teorema 1, basta provar que os polinômios simétricos elementares nos $\beta_{ij}{}'s$ são polinômios simétricos nos $\alpha_j{}'s$.

Portanto, seja σ uma permutação dos inteiros $1, \dots, n$. A expressão (8.6) define uma função do conjunto dos polinômios nele próprio, função esta associada de σ. Vamos representar essa função também pela letra σ. Assim, por (8.6) temos

(8.18) $$\sigma(\alpha_j) = \alpha_{\sigma(j)}, \ j = 1, \dots, n.$$

Agora, se tivermos um polinômio qualquer em $\alpha_1, \dots, \alpha_n$ com coeficientes racionais, segue-se de (8.6) que a ação de σ sobre ele é

$$\sigma\left(\sum\nolimits_{a_{k_1 k_2 \dots k_n}} \alpha_1^{k_1} \dots \alpha_n^{k_n}\right) =$$

(8.19)

$$= \sum\nolimits_{a_{k_1 k_2 \dots k_n}} [\sigma(\alpha_1)]^{k_1} \dots [\sigma(\alpha_n)]^{k_n}$$

onde os somatórios são tomados sobre todos os inteiros $k_1, \dots, k_n \geq 0$, e tais que $k_1 + \cdots + k_n \leq m$, m sendo o grau do polinômio. A seguir, observemos que σ induz uma permutação $\hat{\sigma}$ dos $\beta_{ij}{}'s$ assim definida

(8.20) $$\hat{\sigma}(\beta_{ij}) = \hat{\sigma}(\alpha_i + \alpha_j) \stackrel{\text{def}}{=} \sigma(\alpha_i) + \sigma(\alpha_j).$$

Logo,

(8.21) $$\hat{\sigma}(\beta_{ij}) = \sigma(\beta_{ij}).$$

Para verificar que o primeiro polinômio simétrico elementar S_1 dos $\beta_{ij}{}'s$ é simétrico nos $\alpha_j{}'s$ devemos provar que $\sigma(S_1) = S_1$. Vejamos:

(8.22)

$$\sigma(S_1) = \sum \sigma(\beta_{ij}) = \sum \hat{\sigma}(\beta_{ij}) = \hat{\sigma}(S_1) = S_1$$

onde utilizamos, na última igualdade, que S_1 é simétrico nos $\beta_{ij}´s$. Para os demais polinômios simétricos elementares, $S_2, \dots, S_n$, procedemos de modo análogo ao que se fez um (8.22). Desta forma, completamos a demonstração do Teorema 2.■

O Teorema 2 implica imediatamente no resultado seguinte.

Corolário 1) Suponha que $\alpha_1, \dots, \alpha_n$ sejam raízes de um polinômio

$$P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$$

cujos coeficientes $a_1, \dots, a_n$ são números racionais. Então, os $\binom{n}{2}$ números $\alpha_i + \alpha_j$, $1 \leq i < j \leq n$, são as raízes de um polinômio de grau $\binom{n}{2}$ com coeficientes racionais.

Demonstração: A demonstração do Corolário 1 consiste em observar que se $\alpha_1, \dots, \alpha_n$ são as raízes de um polinômio de grau n, então o polinômio é da forma

$$P(x) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n$$

onde os coeficientes s_j são dados por (8.16.1), ..., (8.16.*n*).

Logo, $s_j = (-1)^j . a_j \in \mathbb{Q}$.

Realmente, como α_j é algébrico, para todo $1 \leq j \leq n$, então $\beta_{ij} = \alpha_i + \alpha_j$; $1 \leq i < j \leq n$ é algébrico. Pelo Teorema 2, os polinômios simétricos elementares associados aos $\beta_{ij}´s$ são também números racionais. Seja $\left\{\theta_1, \theta_2, \dots, \theta_{\binom{n}{2}}\right\} = \{\beta_{ij} = \alpha_i + \alpha_j ;\ 1 \leq i < j \leq n\}$ o conjunto dos $\binom{n}{2}$ números algébricos definidos acima. Sejam $\sigma_1, \sigma_2, \dots, \sigma_{\binom{n}{2}}$ os polinômios simétricos elementares associados aos $\theta_k's$, os quais são todos racionais. Daí, os $\theta_k's$ são as raízes do polinômio $T(x) = x^{\binom{n}{2}} - \sigma_1 x^{\binom{n}{2}-1} + \sigma_2 x^{\binom{n}{2}-2} - \cdots + (-1)^{\binom{n}{2}}\sigma_{\binom{n}{2}}$ onde $T(x) \in \mathbb{Q}[x]$. Logo, os $\binom{n}{2}$ números algébricos $\theta_k's = \beta_{ij}´s = \alpha_i + \alpha_j$ são as raízes de um polinômio $T(x)$ de grau $\binom{n}{2}$ com coeficientes racionais.■

Do mesmo modo, provamos o Teorema 3 e seu Corolário que enunciamos a seguir, com $j = 3, \dots, n$.

Teorema 3) Sejam $\alpha_1, \dots, \alpha_n$ números algébricos, tais que os polinômios simétricos elementares, dados em (8.16.1), ..., (8.16.n), sejam racionais. Considere agora os $\binom{n}{j}$ números algébricos

$$\beta_{k_1 \dots k_j} = \alpha_{k_1} + \dots + \alpha_{k_j} \quad , \quad 1 \leq k_1 < \cdots < k_j \leq n$$

então, os polinômios simétricos elementares associados a esses $\beta's$ são também números racionais.

Corolário 2) Se os números algébricos $\alpha_1, \dots, \alpha_n$ do teorema anterior são as raízes de um polinômio de grau n, com coeficientes racionais, então os $\binom{n}{j}$ números algébricos

$$\beta_{k_1 \dots k_j} = \alpha_{k_1} + \dots + \alpha_{k_j} \quad , \quad 1 \leq k_1 < \cdots < k_j \leq n$$

são raízes de um polinômio de grau $\binom{n}{j}$, com coeficientes racionais.

9 A TRANSCENDÊNCIA DO NÚMERO π

O método usado por Hermite para demonstrar a transcendência de e foi estendido por Lindemann, em 1882, para demonstrar a transcendência do número π. Como consequência desse fato, fica provado que o problema da quadratura do círculo tem resposta negativa. Esse problema é conhecido desde a antiguidade e consiste em saber se é possível, com régua e compasso, construir um quadrado cuja área seja igual a de um círculo dado. Debalde, os gregos e matemáticos, por gerações, tentaram resolver esse problema. Agora, podemos explicar porque tal construção não é possível.

A demonstração da transcendência de π, que daremos a seguir, é baseada naquela de R. Moritz, em Annals of Mathematics, Vol. 2 (1901), a qual, por sua vez, foi inspirada na prova de Hurwitz para a transcendência do número e.

O Teorema do Valor Médio, como aplicado no Capítulo 7, diz o seguinte: "Seja f:$[a,b]\rightarrow\mathbb{R}$ a uma função real contínua definida em um intervalo fechado $[a,b]$ com *a*, *b* $\in \mathbb{R}$. Suponha que a derivada $f'(x)$ existe para todo x no intervalo aberto (a,b). Então, existe $\lambda \in \mathbb{R}$ com $0 < \lambda < 1$ tal que

$$f(b) - f(a) = (b-a).f'(a-\lambda(b-a))".$$

Para obtermos um Teorema de Valor Médio para funções complexas, necessitamos de alguns fatos elementares sobre essas funções. Nesse ponto, deixamos de usar apenas técnicas do cálculo diferencial e integral de uma variável, e utilizaremos algo sobre funções de duas variáveis. Representamos por $\mathbb{C}$ o conjunto dos números complexos, isto é, números da forma $z = x + iy$, onde $x, y \in \mathbb{R}$. Para não delongar essa exposição, vamos admitir que o leitor saiba operar com números complexos. Uma função $f: \mathbb{C} \rightarrow \mathbb{C}$ tem derivada no ponto z se o limite abaixo existe

(9.1) $$f'(z) = \lim_{z_o \rightarrow 0} \left(\frac{f(z+z_o)-f(z)}{z_o} \right) ,$$

onde $z_0 \in \mathbb{C}$, e $f'(z)$ é chamada a *derivada* de f em z. Se uma função f tiver derivadas em todos os pontos de $\mathbb{C}$, então dizemos que ela é *analítica* em $\mathbb{C}$.

Sejam $u(x,y)$ e $v(x,y)$ as partes real e imaginária de $f(z)$, isto é,

(9.2) $f(z) = f(x,y) = u(x,y) + iv(x,y)$, *onde* $z = x + iy$.

Suponhamos que $f(z)$ seja analítica em $\mathbb{C}$ e calculemos a derivada definida em (9.1) usando valores reais para z_o, digamos $z_o = h$, obtendo

$$f'(z) = \lim_{h\to 0}\left(\frac{u(x+h\,,\ y) - u(x,y)}{h}\right) + i\lim_{h\to 0}\left(\frac{v(x+h\,,\ y) - v(x,y)}{h}\right),$$

ou seja,

(9.3) $f'(z) = u_x(x,y) + iv_x(x,y)$

(u_x e v_x representam as derivadas de $u(x,y)$ e $v(x,y)$ com relação à primeira variável x, respectivamente).

A seguir calculemos a derivada (9.1) usando valores imaginários puros para z_o, digamos $z_o = ik$, obtendo

$$f'(z) = \lim_{k\to 0}\left(\frac{u(x,\ y+k) - u(x,y)}{ik}\right) + i\lim_{k\to 0}\left(\frac{v(x,\ y+k\,,\ y) - v(x,y)}{ik}\right)$$

ou seja,

(9.4) $f'(z) = -iu_y(x,y) + v_y(x,y) = v_y(x,y) - iu_y(x,y)$

(u_y e v_y representam as derivadas de $u(x,y)$ e $v(x,y)$ com relação à segunda variável y, respectivamente).

Identificando (9.3) e (9.4), obteremos as equações de *Cauchy-Riemann*

$$u_x(x,y) = v_y\ (x,y), \quad u_y\ (x,y) = -v_x(x,y)\ ,$$

para qualquer $z = x + iy$ em $\mathbb{C}$. Resumindo: se f for *analítica* em $\mathbb{C}$, então as equações de *Cauchy-Riemann* valem em qualquer ponto de $\mathbb{C}$.

Se $f: \mathbb{C} \to \mathbb{C}$ for uma função analítica em $\mathbb{C}$ e se z_2 e z_1 forem números complexos, não é verdade, em geral, que exista $\lambda \in \mathbb{R}$, $0 < \lambda < 1$ tal que

(9.5) $f(z_2) - f(z_1) = (z_2 - z_1)\,.\,f'\left(z_1 + \lambda(z_2 - z_1)\right)$,

e isso parece ser o que Moritz usa em sua demonstração. Que esse "Teorema de Valor do Valor Médio" é falso, podemos ver através de um contra-exemplo. Seja $\mathrm{P(z)} = (z^2 - 2z + 2)(z^2 + 2z + 2)$ cujas raízes são $z_1 = 1 + i$, $z_2 = 1 - i$, $z_3 = -1 + i$, $z_4 = -1 - i$. Aplicando (9.5) aos pares de pontos $(z_1, z_2), (z_2, z_3), (z_3, z_4), (z_4, z_1)$ concluiríamos que $\mathrm{P'(z)}$ teria 4 raízes distintas.

De fato, obteríamos as igualdades:

$$P'\left(z_1 + \lambda(z_2 - z_1)\right) = P'\left(z_2 + \mu(z_3 - z_2)\right) = P'\left(z_3 + \varphi(z_4 - z_3)\right) = P'\left(z_4 + \gamma(z_1 - z_4)\right) = 0$$

onde $\lambda, \mu, \varphi, \gamma$ são números reais pertencentes ao intervalo aberto $(0,1)$. Vejamos que os valores onde P' está aplicado acima são 2 a 2 distintos. Sem perda de generalidade, suponhamos que ocorresse a igualdade:

$$\left(z_1 + \lambda(z_2 - z_1)\right) = \left(z_2 + \mu(z_3 - z_2)\right)$$

Logo, teríamos

$$(\lambda - 1).(z_2 - z_1) = \varphi(z_3 - z_2) \Rightarrow\ (\lambda - 1).(-2i) = \varphi(-2 + 2i) \Rightarrow$$
$$\Rightarrow 2\varphi + i(-2\varphi - 2\lambda + 2) = 0 \Rightarrow\ 2\varphi = 0$$

e $-2\varphi - 2\lambda + 2 = 0 \Rightarrow\ \varphi = 0$ e $-2\lambda + 2 = 0\ \Rightarrow\ \lambda = 1$.

Absurdo, pois $0 < \lambda < 1$.

Analogamente, vemos que as outras possíveis igualdades também não ocorrem. Como $\mathrm{P(z)}$ é um polinômio de grau 4, temos $\mathrm{P'(z)}$ um polinômio de grau 3. Porém, isso contraria o teorema fundamental de álgebra que diz que um polinômio de grau 3, no caso $\mathrm{P'(z)}$, tem exatamente 3 raízes complexas.

Portanto, temos de abrir mão da igualdade no Teorema do Valor Médio. Em seu lugar, mostraremos um resultado que chamamos de "Desigualdade do Valor Médio".

Teorema 1) Seja $\mathrm{f}: \mathbb{C} \to \mathbb{C}$ uma função analítica e sejam $\mathrm{z}_1, \mathrm{z}_2 \in \mathbb{C}$. Então,

(9.6) $|f(z_2) - f(z_1)| \leq 2\,|z_2 - z_1|\, sup\{\,|f'(z_1 + \lambda\,(z_2 - z_1))|\,; 0 \leq \lambda \leq 1\}$,

onde |z| representa o módulo do complexo $z = x + iy$, isto é, $|z| = \sqrt{x^2 + y^2}$.

Demonstração: Demonstraremos primeiramente que

(9.7) $|f(z_0) - f(0)| \leq 2\,|z_0| \sup\{|f'(\lambda z_0)|\ ;\ 0 \leq \lambda \leq 1\}$.

Isso feito, (9.6) segue-se facilmente pela aplicação de (9.7) à função $g(z) = f(z + z_1)$ e ao ponto $z_0 = z_2 - z_1$. De fato, $g(z) = f(z + z_1)$ é uma função analítica e $g'(z) = f'(z + z_1)$ pela regra da cadeia. Logo temos

$$|g(z_0) - g(0)| \leq 2|z_0|\, sup\{|g'(\lambda z_0)|; 0 \leq \lambda \leq 1\} \Rightarrow$$

$$|f(z_2) - f(z_1)| \leq 2|z_2 - z_1|\, sup\{|f'(\lambda z_0 + z_1)|; 0 \leq \lambda \leq 1\} \Rightarrow$$

$$|f(z_2) - f(z_1)| \leq 2|z_2 - z_1|\, sup\{|f'(z_1 + \lambda(z_2 - z_1))|; 0 \leq \lambda \leq 1\}.$$

Sejam u e v as partes real e imaginária de $f(z)$. Dado $z_0 = x_0 + iy_0$, defina as funções $\Phi : \mathbb{R} \to \mathbb{R}$ e $\Psi : \mathbb{R} \to \mathbb{R}$ pelas expressões

$$\Phi(\lambda) = u(\lambda x_0, \lambda y_0),$$

$$\Psi(\lambda) = v(\lambda x_0, \lambda y_0).$$

Aplicando o Teorema do Valor Médio às funções reais Φ e Ψ obtemos

(9.8) $\Phi(1) - \Phi(0) = \Phi'(\lambda_1),\ 0 < \lambda_1 < 1,$

(9.8') $\Psi(1) - \Psi(0) = \Psi'(\lambda_2),\ 0 < \lambda_2 < 1,$

Para calcular as derivadas de Φ e Ψ, usamos o Teorema de Derivação das Funções Compostas. Assim, de (9.8) e (9.8'), obtemos

$$u(x_0, y_0) - u(0,0) = u_x(\lambda_1 x_0, \lambda_1 y_0)x_0 + u_y(\lambda_1 x_0, \lambda_1 y_0)y_0,$$

$$v(x_0, y_0) - v(0,0) = v_x(\lambda_2 x_0, \lambda_2 y_0)x_0 + v_y(\lambda_2 x_0, \lambda_2 y_0)y_0,$$

e daí

$$f(z_0) - f(0) = u_x(\lambda_1 x_0, \lambda_1 y_0)x_0 + u_y(\lambda_1 x_0, \lambda_1 y_0)y_0$$

(9.9) $+ i\,\{\, v_x(\lambda_2 x_0, \lambda_2 y_0)x_0 + v_y(\lambda_2 x_0, \lambda_2 y_0)y_0\}\,.$

Agora usaremos a desigualdade

$$|z| \leq |x| + |y|.$$

Ou seja, o módulo de um número complexo $z = x + iy$ é menor ou igual que a soma dos valores absolutos de sua parte real e imaginária, bem como a desigualdade de *Cauchy-Schwarz*

$$|a_1 b_1 + a_2 b_2| \leq \sqrt{{a_1}^2 + {a_2}^2}\,.\sqrt{{b_1}^2 + {b_2}^2}$$

onde a_1, a_2, b_1, b_2 são números reais quaisquer. O leitor poderá reconhecer na desigualdade de *Chauchy-Schwarz* um fato que ele conhece: "dados dois vetores $(a_1, a_2), (b_1, b_2)$ do plano, o valor absoluto do produto escalar desses dois vetores é menor ou igual que o produto de seus módulos". Utilizando essas duas desigualdades em (9.9) obtemos

$$|f(z_0) - f(0)| \leq$$

(9.10)

$$\leq \sqrt{u_x^2(\lambda_1 x_0, \lambda_1 y_0) + u_y^2(\lambda_1 x_0, \lambda_1 y_0)} \cdot \sqrt{{x_0}^2 + {y_0}^2}$$

$$+ \sqrt{v_x^2(\lambda_2 x_0, \lambda_2 y_0) + v_y^2(\lambda_2 x_0, \lambda_2 y_0)} \cdot \sqrt{{x_0}^2 + {y_0}^2}$$

.

Observe que, em virtude de (9.3), (9.4) e das equações *Chauchy-Riemann*, os radicais em (10), envolvendo u e v são precisamente o módulo de $f'(z)$ calculado nos pontos $\lambda_1 z_0$ e $\lambda_2 z_0$, isto é,

$$|f(z_0) - f(0)| \leq |f'(\lambda_1 z_0)|\,|z_0| + |f'(\lambda_2 z_0)|\,|z_0| .$$

Como

$$0 < \lambda_1, \lambda_2 < 1 \Rightarrow |f'(\lambda_1 . z_0)| \leq \sup\{|f'(\lambda . z_0)|;\ 0 \leq \lambda \leq 1\}$$

e

$$|f'(\lambda_2 . z_0)| \leq \sup\{|f'(\lambda . z_0)|;\ 0 \leq \lambda \leq 1\}$$

.

Portanto, $|f(z_0) - f(0)| \leq 2|z_0| \sup\{|f'(\lambda z_0)|\ ;\ 0 \leq \lambda \leq 1\}$.

Mostrando a desigualdade (9.7) acima. Com isso, o Teorema 1 fica demonstrado.■

Demonstração da transcendência de π.

Suponhamos, por contradição, que π seja um número algébrico. Logo, $i\pi$, onde $i = \sqrt{-1}$, seria também algébrico como um produto de dois números algébricos, conforme Capítulo 5. Então, $i\pi$ seria raiz de uma equação polinomial de grau $n \geq 2$ com coeficientes inteiros, digamos:

(9.11) $P_1(x) = 0$

Representemos as raízes de (9.11) por $\alpha_1 = i\pi, \alpha_2, \dots, \alpha_n$. Como $e^{i\pi} = -1$, segue-se que:

(9.12)

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

pois $1 + e^{\alpha_1} = 0$

Se desenvolvermos o produto indicado em (9.12), obteremos uma expressão da forma: 1 + somatório de exponenciais cujos exponentes são:

(9.13.1) $\alpha_1, \alpha_2, \dots, \alpha_n$

(9.13.2) $\alpha_i + \alpha_j,\ para\ todos\ i < j$

(9.13.3) $\alpha_i + \alpha_j + \alpha_k,\ para\ todos\ i < j < k$

⋮ ⋮

(9.13.*n*) $\alpha_1 + \cdots + \alpha_n$

Observe que o número de termos em (13.1) é $\binom{n}{1} = n$, em (9.13.2) é $\binom{n}{2}$, em (9.13.3) é $\binom{n}{3}$, ..., em (9.13.*n*) é $\binom{n}{n} = 1$, onde $\binom{n}{m}$ são os coeficientes binomiais, isto é, $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ para $0 \leq m \leq n$.

Agora, do fato de que $\alpha_1, \ldots, \alpha_n$ satisfazem uma equação polinomial de grau n com coeficientes inteiros, juntamente com os resultados do Capítulo 8, segue-se as citações a partir do item b abaixo. Assim, obtemos que:

a) Os números em (9.13.1) satisfazem, obviamente, uma equação polinomial de grau $\binom{n}{1} = n$ com coeficientes inteiros, dada em (9.11), que reenumeramos

(9.14.1) $P_1(x) = 0$;

b) Os números em (9.13.2) satisfazem uma equação polinomial de grau com $\binom{n}{2}$ coeficientes inteiros

(9.14.2) $P_2(x) = 0$;

c) Os números em (9.13.3) satisfazem uma equação polinomial de grau $\binom{n}{3}$ com coeficientes inteiros

(9.14.3) $P_3(x) = 0,$

e assim sucessivamente. Em resumo, os números em (9.13.1), (9.13.2), ..., (9.13.*n*) satisfazem a equação polinomial

(9.15) $P_1(x) \ldots P_n(x) = 0$

com coeficientes inteiros cujo grau é $n + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n - 1$. Como alguns dos números em (9.13.1), ..., (9.13.*n*) podem se anular, podemos supor que m deles sejam diferentes de zero e representemo-los por $\beta_1, \ldots, \beta_m$. Logo, simplificando de (9.15) os fatores da forma x^q, para $q > 0$, caso haja, (e os haverá se $2^n - 1 > m$), obtemos que $\beta_1, \ldots, \beta_m$ são raízes de uma equação

(9.16) $R(x) \equiv cx^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0 = 0$,

com coeficientes inteiros, onde $c = c_m$ é o coeficiente líder de $R(x)$.

A seguir, efetuamos o produto de (9.12) e obtemos

(9.17) $\quad k + e^{\beta_1} + \cdots + e^{\beta_m} = 0 \quad$ onde $k = 2^n - m$.

De fato, temos a igualdade

$$\prod_{j=1}^{n}(1 + e^{a_j}) = 0 \Rightarrow (1 + e^{\alpha_1})(1 + e^{\alpha_2}) \ldots (1 + e^{\alpha_n}) = 0$$

$$\Rightarrow 1 + (e^{\alpha_1} + e^{\alpha_2} + e^{\alpha_3} + \cdots + e^{\alpha_n})$$

$$+ (e^{\alpha_1+\alpha_2} + \cdots + e^{\alpha_1+\alpha_n} + e^{\alpha_2+\alpha_3} + \cdots) + \cdots + e^{\alpha_1+\alpha_2+\cdots+\alpha_n}) = 0$$

.

Temos ao todo 2^n termos, dos quais m desses expoentes são diferentes de zero e o restante $(2^n - 1) - m$ são expoentes nulos, isto é, a exponencial deles é igual a 1. Logo, encontramos a equação (9.17) abaixo

$$\prod_{j=1}^{n}(1 + e^{a_j}) = 1 + e^{\beta_1} + \cdots + e^{\beta_m} + 1 + 1 + \cdots + 1$$

$$= 1 + e^{\beta_1} + \cdots + e^{\beta_m} + (2^n - 1) - m = k + e^{\beta_1} + \cdots + e^{\beta_m} = 0$$

onde $k = 2^n - m$.

Considere o polinômio

(9.18) $P(x) = \frac{c^s}{(p-1)!}\, x^{p-1}(R(x))^p \quad ,$

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

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

Segue-se do Exercício 1 (Capítulo 7) que

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

Aplicando o Teorema 1 à função analítica $f(z) = e^{-z}F(z)$, nos valores $\beta_j, 0 \in \mathbb{C}$ temos

(9.21)

$$\left|f(\beta_j) - f(0)\right| = \left|e^{-\beta_j}F(\beta_j) - F(0)\right| \leq 2\left|\beta_j\right| \sup\{\left|e^{-\lambda\beta_j}P(\lambda\beta_j)\right|; 0 \leq \lambda \leq 1\}$$

para $j = 1, \ldots, m$ (j fixo).

De fato, $f'\left(0 + \lambda.(\beta_j - 0)\right) = f'(\lambda.\beta_j) = -e^{-\lambda.\beta_j}.P(\lambda.\beta_j)$
para $j = 1, \ldots, m$ (j fixo). Fazendo

(9.22) $\varepsilon_j = 2\left|\beta_j\right| \sup\{\left|e^{(1-\lambda)\beta_j}\,P(\lambda\beta_j)\,\right|; 0 \leq \lambda \leq 1\}$

obtemos de (9.21) que

(9.23) $\left|F(\beta_j) - e^{\beta_j}\,F(0)\right| \leq \varepsilon_j$.

De fato,

$$\begin{aligned}\left|F(\beta_j) - e^{\beta_j}\,F(0)\right| &= \left|e^{\beta_j}\right|\left|e^{-\beta_j}F(\beta_j) - F(0)\right| \\ &\leq \left|e^{\beta_j}\right|2\left|\beta_j\right| \sup\{\left|e^{-\lambda\beta_j}P(\lambda\beta_j)\right|; 0 \leq \lambda \leq 1\} \\ &= 2\left|\beta_j\right| \sup\{\left|e^{(1-\lambda)\beta_j}\,P(\lambda\beta_j)\,\right|; 0 \leq \lambda \leq 1\} = \varepsilon_j\end{aligned}$$

Usando (9.17) e as expressões (9.23) para $j = 1, \ldots, m$ obtemos

(9.24)

$$|kF(0) + \sum_{j=1}^{m} F(\beta_j)| \ \leq \ \sum_{j=1}^{m} \varepsilon_j$$

.

De fato,

$$\left| kF(0) + \sum_{j=1}^{m} F(\beta_j) \right| =$$

$$= \ |kF(0) + \sum_{j=1}^{m} e^{\beta_j} F(0) + \sum_{j=1}^{m} F(\beta_j) - \sum_{j=1}^{m} e^{\beta_j} F(0)| \ =$$

$$= \left| F(0)[k + \ e^{\beta_1} + \cdots + \ e^{\beta_m}] + \sum_{j=1}^{m} [F(\beta_j) - e^{\beta_j} F(0)] \right| =$$

$$= \sum_{j=1}^{m} [F(\beta_j) - e^{\beta_j} F(0)] \ \leq \ \sum_{j=1}^{m} \varepsilon_j$$

.

O objetivo a partir deste momento é mostrar que o lado esquerdo de (9.24) é um número inteiro não nulo, e que o lado direito, para p conveniente, é menor que 1.

Devemos, pois, calcular várias derivadas de $P(x)$ nos pontos $0, \beta_1, \ldots, \beta_m$. Para as derivadas de ordem $i < p$, procedemos como no Exercício 5 (Capítulo 7). O polinômio $P(x)$ definido em (9.18) é da forma

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

onde

$$r = mp - 1 + p = s + p > p$$

Logo, temos

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

Por outro lado, segue-se diretamente de (9.18) a relação

(9.26) $P^{(i)}(\beta_j) = 0,\ i < p\ ,\ j = 1, \dots, m$

uma vez que nas derivadas $P^{(i)}(x)$, para $i < p$, a expressão $R(x)$ é fator comum, e $R(\beta_j) = 0$ para $j = 1, \dots, m$.

Para derivadas de ordem $i \geq p$, usamos, primeiramente, o Exercício 4 (Capítulo 7) para concluir que os coeficientes de $P^{(i)}(x)$ são inteiros divisíveis por p. Como, obviamente, esses coeficientes são divisíveis por c^s (veja (9.18)), concluímos que

(9.27) os coeficientes de $P^{(i)}(x)$ são inteiros divisíveis por pc^s , sempre que $i \geq p$.

Para ver isso, considere $Q(x) = c_0^p x^{p-1} + b_p x^p + \cdots + b_r x^r \in \mathbb{Z}[x]$, que é um polinômio de grau $r = mp + p - 1 = s + p > p$. Logo, $Q(x)$ satisfaz o Exercício 4 (Capítulo 7) e $P(x) = \frac{c^s}{(p-1)!}\, Q(x)$. Assim, $P^{(i)}(x) = c^s\, \frac{1}{(p-1)!}\, Q^{(i)}(x)$. Mas, para $i \geq p$, $\frac{1}{(p-1)!}\, Q^{(i)}(x)$ é um polinômio com coeficientes inteiros divisíveis por p. Portanto, $P^{(i)}(x)$ é um polinômio com coeficientes inteiros divisíveis por pc^s.

Logo, de (9.25) e (9.27) obtemos

$$F(0) = \sum_{i=0}^{r} P^{(i)}(0) = 0 + \cdots + 0 + P^{(p-1)}(0) + Restante(Múltiplo\ de\ \ pc^s)$$

valendo então

(9.28) $F(0) = c^s c_0^p + pc^s k_0$,

onde k_0 é um inteiro, cujo valor não importa para os nossos propósitos. Para os demais $F(\beta_j)$ observamos que

(9.29)

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

.

Agora observe a expressão

(9.30)

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

para cada i fixado, com $p < i < s + p = r$. Por (9.27) o polinômio $P^{(i)}$ tem coeficientes inteiros divisíveis por $p.c^s$. Além disso, como P tem grau $s + p = r$, segue-se que $P^{(i)}$ tem grau $s + p - i \leq s$, pois $p \leq i$. Logo, a expressão (9.30) pode ser escrita como

(9.31)

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

onde $Q(\beta_1, \dots, \beta_m)$ é um polinômio nos $\beta_i{'s}$ de grau menor ou igual a s, com coeficientes inteiros. É imediato que $Q(\beta_1, \dots, \beta_m)$ é um polinômio simétrico no $\beta_i{'s}$ com coeficientes inteiros. Logo, pelo Teorema 1 do Capítulo 8, existe um polinômio $G(\sigma_1, \dots, \sigma_m)$ de grau menor ou igual a s com coeficientes inteiros e onde $\sigma_1, \dots, \sigma_m$ são os polinômios simétricos elementares em $\beta_1, \dots, \beta_m$, (confira as expressões (8.3.1), ..., (8.3.n) do Capítulo 8), tal que

(9.32) $Q(\beta_1, \dots, \beta_m) = G(\sigma_1, \dots, \sigma_m)$.

Por outro lado, observe que

(9.33) $\sigma_1 = c^{-1}c_{m-1}$, $\sigma_2 = c^{-1}c_{m-2}, \dots,$ $\sigma_m = c^{-1}c_0$.

Logo, de (9.31), (9.32) e (9.33) segue-se que a expressão (9.30) é um inteiro divisível por p. Para ver isso, observemos que

$$\sum_{j=1}^{m} P^{(i)}(\beta_j) = pc^s\, Q(\beta_1, \dots, \beta_m) = pc^s G(\sigma_1, \dots, \sigma_m) = pc^s \sum a_{k_1 \dots k_n} {\sigma_1}^{k_1} \dots {\sigma_n}^{k_n}$$

onde $a_{k_1 \dots k_n} \in \mathbb{Z}$ e $k_1 + \cdots + k_n \leq s$. Daí, temos

$$\sum_{j=1}^{m} P^{(i)}(\beta_j) = p \sum a_{k_1 \dots k_n} c^s\, (c^{-1} c_{m-1})^{k_1} \dots (c^{-1} c_0)^{k_n}$$

$$= p \sum a_{k_1 \dots k_n} c^{s-(k_1+\cdots+k_n)}\, (c_{m-1})^{k_1} \dots (c_0)^{k_n} = p d_j$$

onde $d_j \in \mathbb{Z}$, pois $a_{k_1 \dots k_n}, c^{s-(k_1+\cdots+k_n)}, (c_{m-1})^{k_1}, \dots, (c_0)^{k_n}$ são todos números inteiros.

Voltando a (9.29) concluímos que

(9.34)

$$\sum_{j=1}^{m} F(\beta_j) = pk_1 \quad ,$$

onde k_1 é um inteiro cujo valor é irrelevante para nossos propósitos. A seguir, usando (9.28) e (9.34) obtemos que o lado esquerdo de (9.24) é um inteiro da forma

(9.35) $|kc^s {c_0}^p + pT|$

onde $T = c^s k_0 + k_1$.

De fato,

$$|kF(0) + \sum_{j=1}^{m} F(\beta_j)| = \left|kc^s c_0^p + kpc^s k_0 + pk_1\right| = \left|kc^s c_0^p + pT\right|$$

onde $T = kc^s k_0 + k_1$. Agora *escolhemos* o número primo p de modo que ele seja maior que k, c e c_o. Portanto, o inteiro (9.35) não é divisível por p, e, consequentemente, é um inteiro não nulo. Realmente, se p dividisse $kc^s {c_0}^p + pT$, como p divide pT, então p dividiria $kc^s {c_0}^p$, implicando que p divide k ou p divide c ou p divide c_0. Porém, a escolha de p torna isso impossível.

Para concluir a demonstração, necessitamos fazer a estimativa do termo no lado direito de (9.24). Seja

$$M = \max\{|\beta_1|, \dots, |\beta_m|\}$$

Logo,

(9.36)

$$\varepsilon_j \leq 2\, Me^M \frac{|c|^s}{(p-1)!} \sup\{\, |\lambda\beta_j|^{p-1} R(\lambda\beta_j)|^p;\ 0 \leq \lambda \leq 1\}$$

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

$$N = \max\{|R(z)|\,; |z| < M\}$$
$$Obs: |R(z)| \text{é } limitado, se\ |z| \leq M$$

a qual usada em (9.36) fornece

(9.37)

$$\varepsilon_j \leq 2\, Me^M \frac{|c|^s}{(p-1)!} M^{p-1} N^p$$

Como o fatorial domina qualquer exponencial, isto é,

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

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

(9.38)

$$\sum_{j=1}^{m} \varepsilon_j \leq \frac{m}{m+1} < 1$$

A expressão (9.38) juntamente com o fato que o lado esquerdo de (9.24) é inteiro não nulo resulta em um absurdo. Logo, π é transcendente.■

A demonstração de que π é transcendente e alguns fatos sobre a construção de segmentos com régua e compasso, os quais citaremos abaixo, dará solução ao problema da quadratura do círculo. As demonstrações das afirmações feitas nas linhas posteriores podem ser vistas no de L. H. Jacy Monteiro, "A Teoria de Galois".

Dado um segmento unitário, podemos construir a partir dele, usando apenas régua e compasso, segmentos de comprimento igual a qualquer número racional. Além disso, podemos construir $\sqrt{a}$, onde a é qualquer inteiro positivo. Assim, segmentos cujo comprimento seja $p + q\sqrt{a}$ onde $p, q \in \mathbb{Q}$ e $a \in \mathbb{N}$, podem ser construídos. Os números da forma $p + q\sqrt{a}$ onde $p, q \in \mathbb{Q}$ e $a \in \mathbb{N}$ são conhecidos como "surdos". Finalmente, pode-se provar que os únicos segmentos passíveis de serem construídos com régua e compasso são aqueles cujo comprimento seja um número surdo, ou um número da forma $p + q\sqrt{b}$ onde $p, q \in \mathbb{Q}$ e b é um número surdo, ou finitas combinações sucessivas dessa forma. Assim, todos os segmentos passíveis de serem construídos com régua e compasso têm comprimento igual a um número algébrico. Em verdade, nem todo número algébrico pode ser o comprimento de um determinado segmento.

Agora, voltando ao problema da quadratura do círculo, se fosse possível construir com régua e compasso o lado do quadrado cuja área é igual à área do círculo unitário de raio 1, então, tal quadrado teria área igual a π. Logo, o lado do quadrado seria um segmento de comprimento $\sqrt{\pi}$. Ou seja, $\sqrt{\pi}$ seria um segmento passível de ser construído com régua e compasso. Desta forma, $\sqrt{\pi}$ seria um número algébrico. Portanto, como $\pi = \left(\sqrt{\pi}\right)^2$, obteríamos que π seria um número algébrico. Absurdo, pois π é transcendente.

10 O 7º PROBLEMA DE HILBERT

O Segundo Congresso Internacional de Matemática, realizado em Paris no ano de 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. Não é exagero dizer que, de fato, o desenvolvimento da Matemática no século XX foi moldado pelo programa delineado por Hilbert naquela reunião.

Hilbert foi produto de uma época de grande brilhantismo da Matemática alemã. Dotado de uma inteligência fina e enorme capacidade de trabalho, fez contribuições marcantes nas áreas de Álgebra, Geometria, Análise e Fundamentos da Matemática. Portanto, quando expôs em Paris seus 23 problemas, nas mais diversas áreas, ele o fazia com a autoridade respeitada e incontestada de um dos mais capazes matemáticos da época.

Após enaltecer o esforço e dedicação necessários à pesquisa em Matemática, Hilbert enunciou apenas 10 dos 23 problemas. A relação de todos eles estavam no manuscrito que ele preparara com antecedência.

O 7º problema, o quarto apresentado oralmente, consistia em estabelecer se certos números eram transcendentes. Assim, por exemplo, não se sabia na época se $2^{\sqrt{2}}$ era transcendente ou algébrico. A inclusão desse problema na lista dos 23 revela bem a importância que Hilbert a ele atribuía. Ele sentia que o ataque a esse problema pelos matemáticos do século XX contribuiria para um desenvolvimento salutar da Matemática.

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

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

O Teorema de *Gelfond-Schneider* encerrou a questão sobre a natureza aritmética da potenciação de dois algébricos, visto que se $\alpha \in \{0,1\}$ ou se $\beta \in \mathbb{Q}$, então α^{β} é algébrico. No entanto, não é conhecido um resultado similar para o caso α^{β}, onde α e β são transcendentes. Em vista do Teorema de *Gelfond-Schneider*, somos levados a crer que o resultado dessa potenciação deveria ser um transcendente, porém e e $\log 2$ são transcendentes, mas $e^{\log 2}(= 2)$ é algébrico. Agora o caso $\alpha = \beta$, parece ser mais intrigante: o número α^{α} pode ser algébrico, para algum α transcendente? Uma resposta negativa para essa questão implicaria, de imediato, a transcendência de e^{e} e π^{π}. No entanto, a resposta é "Sim" e é decorrente do Teorema 2 que citaremos mais a frente.

Exemplo 1) Os números $2^{\sqrt{2}}$, 2^{i}, i^{i}, $i^{\sqrt{2}}$, $\left(\sqrt{2}\right)^{i}$ e $2^{\sqrt{-2}} = 2^{i\sqrt{2}}$ satisfazem as hipóteses do Teorema 1 e, portanto, são transcendentes.

Corolário 1) O número e^{π} é transcendente.

Demonstração: Como $e^{\pi i} = Cos(\pi) + i.Sen(\pi) = -1$ (relação de Euler), então $\left(e^{\pi i}\right)^{-i} = (-1)^{-i}$. Logo $e^{\pi} = \left(e^{\pi i}\right)^{-i} = (-1)^{-i}$ é transcendente, pelo Teorema de *Gelfond-Schneider*.

O número e^{π} é chamado de *constante de Gelfond*. Quanto aos números π^{e}, e^{e} e π^{π} ainda não é sabido se são transcendentes.

Teorema 2) O conjunto dos números algébricos da forma t^t, com t transcendente, é denso no intervalo $\left[e^{\frac{-1}{e}}, +\infty\right[$.

Aproveitamos a ocasião para lembrar que, mesmo depois de mais de 120 anos da prova da transcendência de e e π, até hoje a natureza aritmética (isto é, se é racional, irracional, algébrico ou transcendente) de $e\pi$ e $e+\pi$ permanece desconhecida. No entanto, pelo menos um desses números (provavelmente ambos) é transcendente, pois e e π são raízes do polinômio $x^2-(e+\pi)x+e\pi$ e $\overline{\mathbb{Q}}$ é algebricamente fechado. Realmente, se $e\pi$ e $e+\pi$ fossem algébricos, então as raízes do polinômio $x^2-(e+\pi)x+e\pi$ (no caso, e e π) também seriam números algébricos. Na verdade, de maneira mais geral, através de um raciocínio análogo, temos o seguinte resultado: se α e β são números transcendentes, então, pelo menos um dos números $\alpha+\beta$ ou $\alpha\beta$ também é transcendente.

11 CONCLUSÃO

O estudo dos números irracionais e transcendentes mostra a existência de uma área da Matemática ainda com muitas questões em aberto, sendo algumas delas bem antigas. Apesar de serem investigados há um bom tempo, os problemas dessa natureza vêm desafiando matemáticos por gerações. A natureza de números como $e\pi, e+\pi, e^e$ e π^π continua ainda sem resposta no que diz respeito a ser um número algébrico ou transcendente.

No decorrer dessa monografia, temos consciência da grande quantidade de cálculos envolvidos nas demonstrações dos principais resultados. Muitas vezes, lemos e relemos, parece não ter fim, só nos resta perseverar. Porém, para aqueles que vivenciam a Matemática no seu dia a dia, em suas pesquisas ou na sala de aula, sabem da satisfação em galgar degrau a degrau para ao final sentir o sabor de sua realização.

Neste trabalho, usamos algumas propriedades aritméticas e com muita frequência ferramentas do cálculo diferencial e integral. Provavelmente, muitos problemas em aberto necessitem de técnicas mais elaboradas como Teoria de Galois e Teoria das Funções de Variáveis Complexas. Talvez, novos ramos da Matemática devam surgir para que possamos ver as soluções de tais questões; ou velhos ramos devam se reinventar. Seja como for, provavelmente, técnicas mais elaboradas farão parte, cada vez mais, da resolução desses problemas.

REFERÊNCIAS

FIGUEIREDO, Djairo Guedes de. **Números Irracionais e Transcendentes**. 3ª edição. Rio de Janeiro: SBM (Coleção de Iniciação Científica; nº 1), 2011.

HEFEZ, Abramo. **Aritmética**. 1ª edição. Rio de Janeiro: SBM (Coleção PROFMAT), 2013.

HEFEZ, Abramo; FERNANDEZ, Cecília S. **Introdução à Álgebra Linear**. 1ª edição. Rio de Janeiro: SBM (Coleção PROFMAT), 2012.

HEFEZ, Abramo; VILLELA, Maria Lúcia Torres. **Polinômios e Equações Polinomiais**. 1ª edição. Rio de Janeiro: SBM (Coleção PROFMAT), 2012.

MARQUES, Diego. **Teoria dos Números Transcendentes**. 1ª edição. Rio de Janeiro: SBM (Coleção Textos Universitários), 2013.

MORITZ, R. **Annal of Mathematics**-Vol. 2 (pag. 57-59), 1901.

MUNIZ NETO, Antônio Caminha. **Fundamentos de Cálculo**. 1ª edição. Rio de Janeiro: SBM (Coleção PROFMAT), 2015.

NIVEN, Ivan. **Irrational Numbers**. Rahway, NIJ: The Mathematical Association of America, 1956.

THOMAS, George B. **Cálculo**.11ª edição. São Paulo: Pearson Education of Brasil Ltda, 2008.