Universidade Federal da Bahia - UFBA
Instituto de Matemática e Estatística - IME
Sociedade Brasileira de Matemática - SBM
Mestrado Profissional em Matemática em Rede Nacional - PROFMAT
Dissertação de Mestrado

NÚMEROS TRANSCENDENTES E A CLASSIFICAÇÃO DE MAHLER COM ÊNFASE NOS *U-NÚMEROS*

Silvano Gomes Pio

Salvador-Bahia

Janeiro de 2019

NÚMEROS TRANSCENDENTES E A CLASSIFICAÇÃO DE MAHLER COM ÊNFASE NOS *U-NÚMEROS*

Silvano Gomes Pio

Dissertação de Mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UFBA como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Evandro Carlos Ferreira dos Santos.

Salvador-Bahia

Janeiro de 2019

Ficha catalográfica elaborada pelo Sistema Universitário de Bibliotecas (SIBI/UFBA),
com os dados fornecidos pelo(a) autor(a).

Gomes Pio, Silvano
Números Transcendentes e a Classificação de Mahler com ênfase nos U-Números / Silvano Gomes Pio. -- Salvador, 2019.
53 f.

Orientador: Evandro Carlos Ferreira dos Santos.
Dissertação (Mestrado - Mestrado profissional em Matemática em Rede Nacional - PROFMAT) -- Universidade Federal da Bahia, Instituto de Matemática e Estatística, 2019.

1. Números Algébricos. 2. Números Transcendentes . 3. Classificação de Mahler. 4. U-númerps. 5. Números de Liouville. I. Ferreira dos Santos, Evandro Carlos. II. Título.

Números transcendentes e a classificação de Mähler com ênfase nos U-números.

Silvano Gomes Pio

Dissertação de Mestrado apresentada à comissão Acadêmica Institucional do PROFMAT-UFBA como requisito parcial para obtenção do título de Mestre em Matemática, aprovada em 16/01/2019.

Banca Examinadora:

Prof. Dr. Evandro Carlos Ferreira dos Santos (orientador)
UFBA

Prof. Dr. Carlos Eduardo Nogueira Bahiano
UFBA

Prof^{a}. Dr^{a}. Mariana Pinheiro Gomes da Silva
UFRB

À minha família

Agradecimentos

Agradeço a todos os funcionários Universidade Federal da Bahia.

Aos professores que lecionaram a turma do PROFMAT 2016.

Aos colegas da turma PROFMAT 2016, pelo apoio nos momentos de fraqueza.

À CAPES pela bolsa de estudos que recebi durante o curso.

Ao professor Adriano Cattai pelo apoio.

Ao professor e orientador, Evandro Carlos Ferreira dos Santos, pela confiança e apoio.

Resumo

Neste trabalho, explanaremos sobre o conjunto dos números algébricos e transcendentes. Trataremos da classificação de Mahler dos números reais com ênfase na classe dos *U-números*. E por fim, será apresentado como proposta didática, o estudo do problema grego clássico da quadratura do círculo com o intuito de incentivar, não só a construção de figuras planas, mas também os estudos sobre números transcendentes no Ensino Médio.

Palavras chaves: Números Algébricos, Números Transcendentes, Números de Liouville, Classificação de Mahler dos Números Reais, Quadratura do Círculo.

Abstract

In this work, we will explain the set of algebraic and transcendent numbers. We will deal with Mahler's classification of real numbers with emphasis on *U-numbers* class. Finally, it will be presented as a didactic proposal, the study of the classical Greek problem of squaring the circle in order to encourage not only the construction of flat figures but also the studies on transcendent numbers in high school.

Keywords: Algebraic Numbers, Transcendent Numbers, Liouville Numbers, Mahler Classification of Real Numbers, Circle Square.

Sumário

Introdução

A ideia de número surgiu há mais de 30.000 anos e vem se desenvolvendo desde as antigas civilizações.

Com o passar do tempo surgiram as primeiras formas de contagem e medidas, pois a medida que se civilizava, o homem, passou a praticar, não somente a caça e a coleta de frutos, mas também o cultivo de plantas e a criação de animais.

Aos poucos, a humanidade apropriou-se e foi se aperfeiçoando de um modelo abstrato de contagem baseado na sucessão de números (Tal como no conjunto dos números inteiros).

Os Números Naturais vieram pela primitiva e simples necessidade de organização e contagem. As demais "espécies" de números surgiram da necessidade de resolver problemas do dia a dia e intrigaram matemáticos em diferentes épocas [11].

Com o desenvolvimento dos métodos de contagem e medidas, assim como os primeiros cálculos, eram notados o surgimento de números "estranhos", como por exemplo o número π.

Dado um número real qualquer, se esse número for raiz de alguma equação polinomial de coeficientes inteiros, ele seria algébrico, caso contrário esse número seria transcendente [11].

O número π é uma constante resultante da razão do comprimento pelo diâmetro de qualquer círculo. Seu valor aproximado com duas casas decimais é $3,14$. No capítulo 2 deste trabalho, veremos que o número π além de irracional é também um número transcendente [4].

O número e (Número de Euler) é um número irracional e transcendente (como π) [4]. Este é um número muito utilizado em funções logarítmicas como base do logaritmo natural e em funções exponenciais. O seu valor aproximado com duas casas decimais é $2,71$.

Em 1873, Charles Hermite provou que e é um número transcendente. Aproximadamente uma década depois, o alemão Ferdinand von Lindemann publicou uma demonstração de que π também era transcendente [4].

Como vimos, os números e e π são irracionais e transcendentes. Contudo, nem todos os números irracionais são transcendentes [11]. Diferente dos números irracionais, os números racionais são todos algébricos [11].

Questões envolvendo a natureza transcendental dos números fascinam os matemáticos desde meados do século $XVIII$, tornando-se uma área central da teoria dos números [4]. Contudo, o que tornou esse estudo intrigante e desafiador era a incapacidade de exibir exemplos ou algum tipo de classificação para os números transcendentes.

Grandes matemáticos deram suas contribuições a esta linha de pesquisa, como Cantor, Hilbert e Euler, mas o primeiro número a ter sua transcendência demonstrada foi dado em 1851 pelas mãos do francês Joseph Liouville (1809-1882) que passou a ser chamado de constante de Liouville em sua homenagem [**?** 11].

No capítulo 1, falaremos sobre o conjunto dos números algébricos, veremos exemplares desses números, trataremos da enumerabilidade desse conjunto e veremos também algumas propriedades válidas para o mesmo.

No capítulo 2, falaremos sobre o conjunto dos números transcendentes, trataremos da não enumerabilidade desse conjunto, abordaremos acerca dos números de Liouville inclusive da constante de Liouville (que foi primeiro número comprovadamente transcecndente), veremos também os números de Liouville são transcendentes, assim como os números e (Número de Euler) e π [**?** 11].

No capítulo 3, falaremos sobre a Classificação de Mahler dos números reais, veremos uma nova definição de números transcendentes e como a referida classificação de Mahler nos proporcionou uma nova compreenção dos mesmos. Veremos que o conjunto dos números de Liouville é uma subclasse dos números transcendentes, os quais, por sua vez, podem ser representados como três classes disjuntas de números, como por exemplo os *U-números* [8, 9, 10].

A classe dos *U-números* terá maior destaque neste trabalho, pois a mesma pode ser representada como subclasses, tal como os U_1-*números*, que é formados pelo conjunto dos números de Liouville. Ainda neste capítulo, veremos alguns exemplares de *U-números*. Diversos exempleres de *U-números* podem ser encontrados na literatura [8, 9, 10].

Por fim, trataremos das demais classes de números reais, segundo a classificação de Mahler (os A,T e *S-números*) e veremos também que os números e e π, apesar de serem transcendentes, não pertencem a classe dos *U-números* [8, 9, 10].

No capítulo 4, apresentaremos o problema clássico da quadratura do círculo como proposta didática para o Ensino Médio. O qual nos permitiria abordar também sobre a transcendencia do número π, assim como quadrar algumas figuras planas [13].

Capítulo 1

Conjuntos dos Números Algébricos

Um determinado número real (ou complexo), α, é dito *algébrico*, se existe algum

$$P(x) = a_0 + a_1 x + \ldots + a_n x^n,$$

em que $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, não todos nulos, tal que $P(\alpha) = 0$. Caso contrário, α é transcendente.

Neste trabalho, usaremos, também, a notação $P(x) \in \mathbb{Z}[x]$ para caracterizar $P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, em que a_0, a_1, a_2, $\ldots$, $a_n \in \mathbb{Z}$.

Neste capítulo falaremos do conjunto dos números algébricos. Neste trabalho o conjunto dos números algébricos será representado por $\overline{\mathbb{Q}}$.

1.1 Conjunto dos Números Algébricos

Definição 1. Sendo $\alpha \in \mathbb{R}$ (ou $\alpha \in \mathbb{C}$), dizemos que $\alpha \in \overline{\mathbb{Q}}$, se existe algum $P(x) \in \mathbb{Z}[x]$, tal que $P(\alpha) = 0$.

Exemplo 1. Todo número racional é algébrico.
De fato, sendo $x \in \mathbb{Q}$, então $x = \dfrac{p}{q}$, com $p, q \in \mathbb{Z}$ e $q \neq 0$. Como x é solução de equações do tipo $qx - p = 0$, logo x é um número algébrico.

Exemplo 2. Nem todo número algébrico é racional.

(a) O número $\sqrt{2}$ é irracional e algébrico. De fato, supondo que $\sqrt{2}$ seja um número racional e, como tal, podemos escrever

$$\sqrt{2} = \frac{p}{q}, \quad \text{onde } p, q \in \mathbb{Z} \text{ e } (p, q) = 1.$$

Multiplicando ambos os membros por q e elevando-os ao quadrado temos:

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

Portanto, p^2 é par, pois é o dobro do número inteiro q^2. Por outro lado, se $p = 2s+1$, com $s \in \mathbb{Z}$ (p ímpar), teríamos $p^2 = 2r+1$ com $r = 2s(s+1)$ o que é uma contradição, pois p^2 é par. Então escrevendo $p = 2s$, teríamos

$$(2s)^2 = 2q^2 \Longleftrightarrow 4s^2 = 2q^2 \Longleftrightarrow 2s^2 = q^2.$$

Assim, vemos que q^2 tem de ser par e, pelo mesmo raciocínio usado para p e p^2, q também terá de ser par. Mas se p e q são pares, então são ambos divisíveis por 2 e a fração $\dfrac{p}{q}$ pode ainda ser simplificada, mas como $(p, q) = 1$, temos uma contradição e, portanto, $\sqrt{2}$ não é um número racional (ou seja, $\sqrt{2}$ é irracional). Além disso, fazendo $x = \sqrt{2}$, teríamos: $x = \sqrt{2} \Longrightarrow x^2 = 2 \Longrightarrow x^2 - 2 = 0$, logo $\sqrt{2}$ é solução da equação $x^2 - 2 = 0$ e, portanto, é algébrico.

(b) O número $\sqrt[n]{p}$, onde $n \geq 2$ é inteiro e p primo, é irracional e algébrico. De fato, suponha que $\sqrt[n]{p}$, onde $n \geq 2$ é inteiro e p primo, é racional. Então fazendo $\sqrt[n]{p} = \dfrac{a}{b}$, com $(a, b) = 1$, teríamos

$$\sqrt[n]{p} = \frac{a^n}{b^n} \Longrightarrow b^n p = a^n \Longrightarrow p|a^n \Longrightarrow p|a.$$

Portanto, $a = kp$,com $k \in \mathbb{Z}^*$, daí segue que $b^n p = (kp)^n = k^n \cdot p^n$, logo, $b^n = k^n p^(n-1)$ implicando $p|b^n$ de onde $p|b$. Daí segue que $(p, q) = p \neq 1$, logo temos uma contradição e, portanto, $\sqrt[n]{p}$ não é um número racional (ou seja, $\sqrt[n]{p}$ é irracional). Agora, fazendo $x = \sqrt[n]{p}$, tem-se que:

$$x = \sqrt[n]{p} \Longrightarrow x^n = p \Longrightarrow x^n - p = 0.$$

Daí segue que $\sqrt[n]{p}$ é solução da equação $x^n - p = 0$ e, portanto, é algébrico.

(c) Sendo $i = \sqrt{-1}$, um número complexo, como

$$i = \sqrt{-1} \Rightarrow i^2 = -1 \Rightarrow i^2 + 1 = 0,$$

logo i é um número algébrico.

Definição 2. Um determinado número algébrico será *inteiro algébrico* (inteiro sobre $\mathbb{Z}$) se o coeficiente líder de sua equação polinômio for igual a 1.

Observação. Todo inteiro algébrico é um número algébrico mas, em geral, a recíproca não é válida.

Exemplo 3. O número $\sqrt{2+\sqrt{3}} \in \overline{\mathbb{Q}}$ é inteiro algébrico, pois, sendo $x = \sqrt{2+\sqrt{3}}$, temos:

$$x^2 = 2 + \sqrt{3} \Rightarrow x^2 - 2 = \sqrt{3} \Rightarrow x^4 - 4x^2 + 4 = 3 \Rightarrow x^4 - 4x^2 + 1 = 0.$$

Ou seja, $\sqrt{2+\sqrt{3}}$ é solução da equação $x^4 - 4x^2 + 1 = 0$.
Observe que o número $\frac{\sqrt[3]{3}}{2}$ é algébrico mas não é inteiro algébrico. De fato,

$$y = \frac{\sqrt[3]{3}}{2} \Rightarrow 2y = \sqrt[3]{3} \Rightarrow 8y^3 = 3 \Rightarrow 8y^3 - 3 = 0.$$

ou seja, então $\frac{\sqrt[3]{3}}{2}$ é solução da equação $8y^3 - 3 = 0$, contudo, o coeficiente do termo de maior grau não é 1.

Definição 3. Seja $\alpha \in \mathbb{R}$, dizemos que α é um *número algébrico de grau* n, se existe $P(x) \in \mathbb{Q}[x]$ mônico, de menor grau n, que satisfaz $P(\alpha) = 0$.

Observação. O grau do polinômio $P(x) \in \mathbb{Q}[x]$ é denotado por ∂P.

Exemplo 4.

(a) $\sqrt{2}$ é um número algébrico de grau 2, pois é soluo de $x^2 - 2 = 0$;

(b) $\sqrt{2+\sqrt{3}}$ é um número algébrico de grau 4, pois é solução da equação $x^4-4x^2+1 = 0$.

Teorema 1. Todo número inteiro algébrico (inteiro sobre $\mathbb{Z}$) real ou é um número inteiro ou é um número irracional.

Demonstração. Supondo que $x \in \mathbb{Q}$, onde $x = \dfrac{p}{q}$, tal que $p, q \in \mathbb{Z}$ e $q > 1$, com $(p, q) = 1$, é inteiro algébrico. Então o mesmo é raiz de uma equação polinomial do tipo:

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0,$$

ou seja,

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

Desenvolvendo as potências, tem-se

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

Multiplicando ambos os membros por q^n, temos:

$$p^n + a_{n-1} \cdot p^{n-1} \cdot q + \ldots + a_1 \cdot p \cdot q^{n-1} + a_0 \cdot q^n = 0.$$

Isolando p^n e evidenciando q, temos

$$p^n = q\left(-a_{n-1} \cdot p^{n-1} - \ldots - a_1 \cdot p \cdot q^{n-2} - a_0 \cdot q^{n-1}\right).$$

Fazendo $A = -a_{n-1} \cdot p^{n-1} - \ldots - a_1 \cdot p \cdot q^{n-2} - a_0 \cdot q^{n-1}$, onde $A \in \mathbb{Z}$, logo $p^n = q \cdot A$. Daí, podemos afirmar que q divide p^n, implicando que q divide p e, portanto $(p, q) = q > 1$, que é uma contradição. $\square$

Para melhor compreender a proposições a seguir é necessário uma boa noção de enumerabilidade. Ao leitor interessado em compreender melhor alguma propriedade sobre esse assunto, sugiro consultar o capítulo 4 de [4]. Contudo, um conjunto é chamado *enumerável* se tem a mesma cardinalidade de $\mathbb{N}$.

Proposição 1. O conjunto dos números algébricos é enumerável.

Demonstração. Dado $P(x) = a_0 + a_1x + \cdots + a_nx^n$, o conjunto das raízes de P é denotado por R_P. Note que R_P tem no máximo n elementos. Para todo $n \in \mathbb{N}$, existe apenas uma quantidade enumerável de polinômios, em $\mathbb{Z}[x]$, com grau n. De fato, considerando $X_n = \{Q \in \mathbb{Z}[x]; \partial Q = n\}$. Tomando $\psi : \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n \text{ cópias}} \times \mathbb{Z}^* \to X_n$ dado por

$$\psi(a_0, a_1, \ldots, a_n) = a_0 + a_1x + \ldots + a_nx^n.$$

Note facilmente que ψ é bijeção. Como $\mathbb{Z} \times \ldots \times \mathbb{Z} \times \mathbb{Z}^*$ é enumerável, segue-se que X_n também o é.

Definindo $A_n = \bigcup_{\partial P = n} R_P$. Pelos comentários feitos anteriormente e pelo fato de que a união enumerável de conjuntos finitos é enumerável, segue-se A_n é enumerável. Agora é só observar que

$$\overline{\mathbb{Q}} = \bigcup_{n \in \mathbb{N}} A_n.$$

Daí $\overline{\mathbb{Q}}$ é enumerável (pois é escrito como união enumerável de enumeráveis). □

No próximo teorema veremos algumas propriedades do conjunto dos números algébricos.

Teorema 2. Para o conjunto dos números algébricos valem as seguintes propriedades:

(i) O simétrico $-a$ de um número algébrico a, é algébrico.

(ii) O inverso a^{-1} de um número algébrico a, com a não nulo, é algébrico.

(iii) A soma de dois números algébricos é um número algébrico.

(iv) O produto de dois números algébricos é um número algébrico.

Demonstração. (i) Se a é algébrico, então ele é raiz de uma equação do tipo

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

portanto $-a$ é raiz da equação:

$$(-1)^na_nx^n + (-1)^{n-1}a_{n-1}x^{n-1} + \cdots + (-1)a_1x + a_0 = 0.$$

Isto demonstra a propriedade *(i).*

(ii) Se a, não nulo, satisfaz a equação

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

então a^{-1} satisfaz a equação:

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

Isto demonstra a propriedade *(ii)*.

(iii) Para ajudar a demonstrar a propriedade *(iii)* vamos precisar de alguns conhecimentos sobre formas lineares com coeficientes racionais.

Definição 4. Uma *forma linear com coeficientes racionais* é uma expressão da forma:

$$X = q_1 x_1 + \cdots + q_n x_n,$$

onde $q_1, \ldots, q_n$ são todos racionais. Os x_i's são chamados indeterminados.

Lema 1. Dadas $n+1$ formas lineares

$$\begin{array}{rcl} X_1 & = & q_{1,1}x_1 + \ldots + q_{n,1}x_n \\ & \vdots & \\ X_{n+1} & = & q_{1,n+1}x_1 + \ldots + q_{n,n+1}x_n \end{array}$$

elas são linearmente dependentes sobre os racionais, isto é, existem $r_1, \ldots, r_{n+1} \in \mathbb{Q}$, com pelo menos um r_i distinto de zero, tais que

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

Demonstração. (do Lema 1) Substituindo os X_i's por suas expressões dadas no enunciado do Lema, vemos que

$$r_1 X_1 + \cdots + r_{n+1}X_{n+1} = 0$$

estará satisfeita se os r_i's forem as soluções do sistema de equações lineares (n equações com $n+1$ incógnitas)

$$\begin{array}{rcl} q_{1,1}r_1 + \ldots + q_{1,n+1}r_{n+1} & = & 0 \\ & \vdots & \\ q_{n,1}r_1 + \cdots + q_{n,n+1}r_{n+1} & = & 0. \end{array}$$

Pode-se mostrar que o sistema acima tem soluções racionais $r_1, \ldots, r_{n+1}$ uma vez que os coeficientes do sistema são também racionais. □

Sejam a e b algébricos. Logo existem equações polinomiais:

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0 \tag{1.1}$$

$$x^n + b_{m-1}x^{n-1} + \ldots + b_1 x + b_0 = 0 \tag{1.2}$$

com coeficientes racionais (a equação da definição de números algébricos tem coeficientes inteiros, as equações acima são obtidas dividindo-se a equação original pelo coeficiente líder), tais que a seja raiz de (1.1) e b seja raiz de (1.2). De (1.1) obtemos:

$$a^n = -a_{n-1} \cdot a^{n-1} - \ldots - a_1 \cdot a - a_0, \tag{1.3}$$

isto é, a^n está expresso como uma combinação linear de $1, a, \ldots, a^{n-1}$, usando coeficientes racionais.

Multiplicando-se (1.3) por a e substituindo-se o a^n, obtido na expressão pelo seu valor dado em (1.3), obtemos a^{n+1} expresso como combinação linear dos mesmos $1, a, \ldots, a^{n-1}$ usando-se também coeficientes racionais. E assim, sucessivamente, todas as potências a^j, para $j \geq n$, são expressos como combinações lineares de $1, a, \ldots, a^{n-1}$ usando-se coeficientes racionais.

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

Nosso objetivo será mostrar que $a+b$ satisfaz uma equação polinomial de grau $m \cdot n$ com coeficientes racionais, implicando então que $a+b$ seja algébrico. Com isso em vista, considere os $m \cdot n + 1$ números

$$1, a+b, (a+b)^2, \ldots, (a+b)^{m \cdot n} \tag{1.4}$$

Desenvolvendo as várias potências, e usando-se o que se viu acima sobre a representação de potências a^j, $j \geq n$, e b^k, $k \geq m$, obtemos que os números em (1.4) podem ser expressos como combinações lineares de $m \cdot n$ números $a^j b^k$, $0 \leq j \leq n-1$, $0 \leq k \leq m-1$, usando-se coeficientes racionais. Agora, aplicamos o Lema 1 acima: os X_i's são os $m \cdot n + 1$ números de (1.4), os x_i's são os $m \cdot n$ números $a^j b^k$. Logo, existem racionais $r_0, r_1, \ldots, r_{m \cdot n}$ tais que

$$r_0 + r_1(a+b) + \ldots + r_{m \cdot n}(a+b)^{m \cdot n} = 0,$$

o que mostra que $a+b$ satisfaz uma equação polinomial com coeficientes racionais. Isto demonstra a propriedade (iii).

(iv) Segue as mesmas linhas da demonstração da propriedade (iii). Em (1.4), entretanto, consideramos as potências

$$1, ab, (ab)^2, \dots, (ab)^{m \cdot n}.$$

Isto demonstra a propriedade (iv).

Portanto, estão provadas todas as propriedades descritas neste teorema.

$\square$

Capítulo 2

Conjunto dos Números Transcendentes

No capítulo anterior falamos sobre o conjunto dos números algébricos. Neste capítulo falaremos do conjunto dos números transcendentes. Já vimos que um determinado número real que não seja algébrico, será transcendente.

Desde a antiguidade, o surgimento de números “estranhos” como, por exemplo, o número π, intrigavam os matemáticos da época que buscavam explicações para tais fatos e soluções de problemas [4].

Os estudos dos números transcendentes provêm de diversos problemas antigos como a clássica questão grega da **quadratura do círculo** [4], as pesquisas de *Liouville* e *Cantor* [4], as investigações de *Hermite* sobre a função exponencial [4], o sétimo problema da famosa lista dos 23 problemas de Hilbert [4] e as formas lineares em logaritmos devidas a Baker [4].

A palavra Transcendente foi usada pela primeira vez num contexto matemático por *Leibniz* em 1682 [4].

No século $XVIII$, Euler foi provavelmente a primeira pessoa a criar uma definição para números transcendentes [4].

Liouville, em 1844, provou a existência de números transcendentes e, em 1851, produziu os primeiros exemplares dos mesmos [4], como por exemplo, a Constante de Liouville.

Neste trabalho, o conjunto dos números transcendentes será representado por $\mathbb{T}$.

2.1 Conjunto dos Números Transcendentes

Definição 5. Sendo $\alpha \in \mathbb{R}$ (ou $\alpha \in \mathbb{C}$), dizemos que $\alpha \in \mathbb{T}$, se existe algum $P(x) \in \mathbb{Z}[x]$, tal que $P(\alpha) \neq 0$.

Diferente do conjunto dos números algébricos, o conjunto dos números transcendentes é não enumerável. E, de acordo com a Proposição 3 a seguir, veremos que quase todos os números reais são transcendentes [11]. Contudo, é muito difíciel identificá-los, pois a prova da transcendencia de um número é, geralemnte, bastante complicada.

A Proposição 2 a seguir trata da não enumerabilidade do conjunto dos números transcendentes.

Proposição 2. Os números transcendentes são não enumeráveis.

Demonstração. Dado $\alpha \in \mathbb{R}$ (ou $\alpha \in \overline{\mathbb{Q}}$, ou $\alpha \in \mathbb{T}$), como $\overline{\mathbb{Q}}$ é enumerável e a união de dois conjuntos enumeráveis é um conjunto enumerável, então basta mostrar que $\mathbb{R}$ é não enumerável para concluir que $\mathbb{T}$ também o é (não enumerável), caso contrário $\mathbb{R}$ teria que ser enumerável. O resultado recorre do teorema abaixo. $\square$

Teorema 3. O conjunto dos números reais $\mathbb{R}$, é não enumerável.

Demonstração. Tomando $[0,1) \subset \mathbb{R}$, se $[0,1)$ é não enumerável, então $\mathbb{R}$ também será não enumerável.

Supondo, por absurdo, que $[0,1)$ seja enumerável. Então existe $x \in [0,1)$ tal que $x = 0, a_{n,1}a_{n,2}a_{n,3}\ldots$, com $n \in \{1,2,3,\ldots\}$ e $a_{n,1}a_{n,2}a_{n,3}\ldots \in \{0,1,2,3,4,5,6,7,8,9\}$, logo x é um dos números da lista:

$$\begin{array}{l} 0, a_{1,1}a_{1,2}a_{1,3}\ldots \\ 0, a_{2,1}a_{2,2}a_{2,3}\ldots \\ 0, a_{3,1}a_{3,2}a_{3,3}\ldots \\ \vdots \end{array}$$

Note que podemos construir um número $0, b_11b_2b_3\ldots$ diferente de todos os outros acima. De fato, tome $0, b_1b_2b_3\ldots$ tal que

$$\begin{aligned} b_1 &= 9 - a_{1,1} \\ b_2 &= 9 - a_{2,2} \\ b_3 &= 9 - a_{3,3} \\ &\vdots \\ b_k &= 9 - a_{k,k},\ k \in \mathbb{N}. \end{aligned}$$

Observe que $b_i = \{0,1,2,3,4,5,6,7,8,9\}$, com $i \in \mathbb{N}$. Logo $0, b_1b_2b_3\ldots \in [0,1)$, mas como $b_1 \neq a_{1,1}$, $b_2 \neq a_{2,2}$, $b_3 \neq a_{3,3}$, $\ldots$, $b_k \neq a_{k,k}$ tem-se que $0, b_1b_2b_3\ldots \neq 0, a_{n,1}a_{n,2}a_{n,3}\ldots$ para todo $n \in \mathbb{N}$, o que é uma contradição. Portanto $[0,1)$ é não enumerável. Consequentemente $\mathbb{R}$ também o é. Isto prova o teorema. $\square$

Segue que a Proposição 2 também é verdadeira.

Um conjunto $A \subset \mathbb{R}^t$ tem *medida (de Lebesgue) nula* e, escrevemos $m(A) = 0$ se para todo $\varepsilon > 0$, existe uma quantidade enumerável de bolas abertas $(B_n)_n$ tais que

- $A \subseteq \bigcup_{n\in\mathbb{N}} B_n$;
- $\sum\limits_{n=1}^{\infty} \mathrm{Vol}(B_n) < \varepsilon$.

Claramente o volume (Vol) de um conjunto é o comprimento e a área deste conjunto, quando $t = 1$ e 2, respectivamente.

Dizemos que uma propriedade é satisfeita por *quase todos* os números complexos se, o subconjunto de $\mathbb{C}$ que não satisfaz tal propriedade, tem medida nula [11].

A Proposição 3 a seguir dá a natureza quantitativa dos números transcendentes.

Proposição 3. Quase todos os números são transcendentes.

Demonstração. Devemos provar que $m(\overline{\mathbb{Q}}) = 0$. De fato, dado $\varepsilon > 0$, como $\overline{\mathbb{Q}}$ é enumerável, então podemos considerar $\overline{\mathbb{Q}} = \{a_1, a_2, \ldots\}$. Defina então as bolas abertas

$$B_n = \{z \in \mathbb{C}; |z - a_n| < r_n\}, \text{ onde } r_n = \frac{1}{n}\sqrt{\frac{3\varepsilon}{\pi^3}}.$$

Claramente, $\overline{\mathbb{Q}} \subset \cup B_n$, além disso,

$$\text{Área}\left(\bigcup_{n\in\mathbb{N}} B_n\right) \leq \sum_{n=1}^{\infty} \text{Área}(B_n) = \sum_{n=1}^{\infty} \pi r_n^2 = \frac{3\pi\varepsilon}{\pi^3}\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{3\varepsilon}{\pi^2}\cdot\frac{\pi^2}{6} = \frac{\varepsilon}{2} < \varepsilon.$$

Segue-se então o resultado, onde usamos que $\zeta(2) = \sum\limits_{n=1}^{\infty} n^{-2} = \frac{\pi^2}{6}$. [6]. □

Neste caso, dizemos que o conjunto dos números transcendentes tem medida total em $\mathbb{C}$, isto é, $m(\mathbb{T}) = \infty$.

Nas próximas secções desse capítulo, veremos as demonstrações da transcendência dos números de Liouville, e (número de Euler) e π.

Os números transcendentes mais conhecidos são e e π [4].

Mesmo depois de 120 anos da prova da transcendência de e e π, até hoje a natureza aritmética de $e + \pi$ e $e\pi$ é desconhecida.

No entanto, um desses números (provavelmente ambos) é transcendente, pois e e π são raízes de $x^2 - (e + \pi)x + e\pi$ e $\overline{\mathbb{Q}}$ é algebricamente fechado. Portanto, conjectura-se que, sendo e e π algebricamente independentes, implicaria a transcendência dos números acima [6].

2.2 Os números de Liouville

Os primeiros exemplares de números transcendentes foram os **números de Liouville**. Sendo o primeiro número comprovadamente transcendente chamado de **Constante de Liouville**. A Constante de Liouville foi desenvolvida exclusivamente para ser um exemplar de número transcendente.

Joseph Liouville, por volta de 1844, desenvolveu uma propriedade que era satisfeita por todos os números algébricos e, portanto, se algum número não a satisfizesse, ele, seria transcendente [4]. Os números de Liouville são números ajustados a não satisfazer tal propriedade [4].

O conjunto dos números de Liouville será representado, neste trabalho, por $\mathbb{L}$. E sua transcendência estará devidamente demonstrada ainda nesta seção. Além disso, no capítulo 3 deste trabalho, veremos que o conjunto dos números de Liouville pode ser apresentado, segundo a Classificação de Mahler [8, 9, 10], como uma **subclasse** de números transcendentes.

O Teorema 4 a seguir trata da propriedade criada por *Liouville*, a qual nos referimos acima.

Teorema 4 (Liouville)**.** Seja α uma raiz irracional de um polinômio irredutível $P(x) \in \mathbb{Z}[x]$ com $n = \partial P(x) \geq 2$. Então existe uma constante $c(\alpha)$ tal que $\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n}$ para qualquer número racional $\frac{p}{q}$. Uma escolha conveniente para essa constante é

$$c(\alpha) = \frac{1}{1 + \max\limits_{|t-\alpha|\geq 1} |P'(t)|},$$

onde $P'(t)$ denota a derivada de $P(x)$ no ponto t e t é um número real entre α e $\frac{p}{q}$.

Demonstração. Separemos o problema em dois casos.

- Caso $\left|\alpha - \frac{p}{q}\right| > 1$. Como $q \in \mathbb{Z}^*$ então $q^n \geq 1$, além disso, $1 \geq c(\alpha)$ de modo que $1 \geq \frac{c(\alpha)}{q^n}$. Logo $\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n}$.

- Caso $\left|\alpha - \frac{p}{q}\right| \leq 1$. Primeiramente, sendo $P(x) \in \mathbb{Z}[x]$ um polinômio irredutível sobre $\mathbb{Z}$, de maior grau 1, então $P(x)$ é irredutível sobre $\mathbb{Q}$. De fato, supondo que $P(x) = G(x)H(x)$, $G(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \frac{a_2}{b_2}x^2 + \cdots + \frac{a_n}{b_n}x^n$ e $H(x) = \frac{c_0}{d_0} + \frac{c_1}{d_1}x + \frac{c_2}{d_2}x^2 + \cdots + \frac{c_m}{d_m}x^m$, onde $\partial G(x) \geq 1$ e $\partial H(x) \geq 1$. Seja $\alpha = mmc(b_0, b_1, b_2, ..., b_n)$ e $\beta = mmc(d_0, d_1, d_2, \ldots, d_m)$. Portanto $\alpha G(x)$ é primitivo e $\beta H(x)$ também, de modo que $\alpha G(x)\beta H(x) = \alpha\beta P(x)$ é primitivo pelo Lema de Gauss. Ora, sendo assim devemos ter $\alpha = \pm 1$ e $\beta = \pm 1$ de modo que $G(x) \in \mathbb{Z}[x]$ e $H(x) \in \mathbb{Z}[x]$ e portanto $P(x) \in \mathbb{Z}[x]$, mas, por hipótese $P(x)$ é irredutível sobre $\mathbb{Z}$, assim chegamos em um absurdo. Portanto $P(x)$ é irredutível sobre $\mathbb{Q}$. Dessa maneira, $P\left(\frac{p}{q}\right) \neq 0$ pois $\frac{p}{q} \in \mathbb{Q}$. Além disso $q^n \cdot P\left(\frac{p}{q}\right)$ é certamente um número inteiro pois $n = \partial P(x)$, portanto $\left|q^n \cdot P\left(\frac{p}{q}\right)\right| \geq 1$. Agora, o Teorema do Valor Médio nos garante a existência, de pelo menos um $t \in \mathbb{R}$, que esteja entre α e $\frac{p}{q}$ tal que:

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

já que α é raiz do polinômio $P(x)$.

Multiplicando a equação acima por $|q^n|$ concluímos que $|q^n| \cdot \left|\alpha - \frac{p}{q}\right| \cdot |P'(t)| \geq 1$. Lembre também que estamos admitindo $\left|\alpha - \frac{p}{q}\right| \leq 1$ e assim $|t - \alpha| \leq 1$. Portanto temos:

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

Portanto, o teorema está provado.

$\square$

Definição 6 (Números de Liouville)**.** Um número α é chamado de *número de Liouville* se existir uma sequência de racionais $\left(\frac{p_j}{q_j}\right)_{j\in\mathbb{N}}$ distintos, com $q_j > 1$ $\forall j \in \mathbb{N}$, tal que

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j} \quad \forall j \in \mathbb{N}.$$

Agora veremos alguns exemplos de Números de Liouville, inclusive a Constante de Liouville.

Exemplo 5 (Constante de Liouville)**.** O número $\alpha = \sum\limits_{k=1}^{\infty} \frac{1}{10^{k!}}$ é um número de Liouville e é conhecido como a constante de Liouville. O valor dessa constante é de aproximadamente $0,110001000000000000000001000$0.

A seguir veremos a demonstração de que a constante de Liouville é um número de Liouville.

Perceba primeiramente que a série acima converge pelo teste da razão:

$$\lim_{k\to\infty}\frac{10^{k!}}{10^{(k+1)!}}=\lim_{k\to\infty}\frac{1}{10^{k+1}}=0$$

Sabendo que $\alpha=\sum_{k=1}^{\infty}\frac{1}{10^{k!}}$, defina $p_j=\sum_{k=1}^{j}10^{j!-k!}$ e $q_j=10^{j!}$. Assim

$$\begin{aligned}\left|\alpha-\frac{p_j}{q_j}\right| &= \sum_{k=1}^{\infty}\frac{1}{10^{k!}}-\sum_{k=1}^{j}\frac{1}{10^{k!}}\\ &= \sum_{k=j+1}^{\infty}\frac{1}{10^{k!}}=\frac{1}{10^{(j+1)!}}\left(1+\frac{1}{10^{(j+2)!-(j+1)!}}+\frac{1}{10^{(j+3)!-(j+1)!}}+\cdots\right)\end{aligned}$$

Agora veja que

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

Como

$$\left(1+\frac{1}{10}+\frac{1}{10^2}+\frac{1}{10^3}+\cdots\right)=\left(1+\frac{1}{9}\right)=\frac{10}{9}$$

temos que

$$\left|\alpha-\frac{p_j}{q_j}\right|<\frac{1}{10^{(j+1)!}}\frac{10}{9}=\frac{10}{9\cdot 10^{j!}\left(10^{j!}\right)^j}<\frac{1}{\left(10^{j!}\right)^j}<\frac{1}{\left(q_j\right)^j}$$

o que garante-nos que α é um número de Liouville.

Exemplo 6. Generalizando o exemplo anterior, se $b\geq 2$ é um inteiro, então $\alpha=\sum_{n=0}^{\infty}a_nb^{-n!}$ é número de Liouville, para toda escolha de $a_n\in\{1,...,b-1\}$. De fato escolha $q_j=b^{j!}$ e $p_j=\sum_{n=1}^{j}a_nb^{j!-n!}$. Então

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

Os números de Liouville são números reais que podem ser bem aproximados por racionais. Vide Teorema 5.

Teorema 5. α é um número de Liouville, se e somente se, para todo $n\geq 1$ existe um racional $\frac{p}{q}$, com $q>1$, tal que:

$$0<\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^n}.$$

Demonstração.

($\Rightarrow$) Se α é um número de Liouville, existe uma sequência de racionais $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ tal que $0 < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^n}$. Basta agora tomar, para cada n, $p = p_n$ e $q = q_n$.

($\Leftarrow$) Sabemos que para cada n existe $\frac{p_n}{q_n}$, dependendo de n, tal que a desigualdade do enunciado é válida o $q_n > 1$. Defina portanto, $A = \bigcup_{n\in\mathbb{N}} \left\{\frac{p_n}{q_n}\right\}$. Perceba agora que A não pode ser finito, pois se fosse, existiria $\frac{P}{Q} \in A$ tal que $\left|\alpha - \frac{P}{Q}\right| < \frac{1}{Q^n}$ para todo $n \in N^{\#} \subset \mathbb{N}$, onde $N^{\#}$ é infinito. Ora, dessa maneira teríamos obrigatoriamente a igualdade $\frac{P}{Q} = \alpha$. Um absurdo, pois $0 < \left|\alpha - \frac{P}{Q}\right|$. Assim, A é infinito e o resultado segue.

□

Os próximos teoremas e a proposição servirão para demonstrar a transcendência dos números de Liouville.

Teorema 6 (O Grande Lema)**.** A sequência $(q_j)_{j\in\mathbb{N}}$, da definição 6, é ilimitada.

Demonstração. Suponha, por absurdo, que não seja assim. Portanto $\exists M > 0$ tal que $q_j \leq M$ par a todo $j \in \mathbb{N}$. Como $\left|\alpha - \frac{p_j}{q_j}\right| \leq \frac{1}{q_j^j} < 1$ temos $q_j\left|\alpha - \frac{p_j}{q_j}\right| = |q_j\alpha - p_j| < q_j$.

Além disso, como $|p_j| - |q_j\alpha| < |q_j\alpha - p_j|$ segue que $|p_j| < |q_j\alpha| + q_j < M(|\alpha| + 1)$. Logo $(p_j)_{j\in\mathbb{N}}$ é limitada.

Portanto $(q_j)_{j\in\mathbb{N}}$ e $(p_j)_{j\in\mathbb{N}}$ são sequências de números inteiros limitadas e portanto com apenas finitos termos distintos. Desse modo, $\left(\frac{p_j}{q_j}\right)_{j\in\mathbb{N}}$ é uma sequência de números racionais com finitos termos distintos, o que contraria o fato de tal sequência possuir os termos distintos. □

Proposição 4. Todo Número de Liouville é irracional.

Demonstração. Suponha $\alpha \in \mathbb{L}$, tal que $\alpha = \frac{p}{q} \in \mathbb{Q}$. Por hipótese, existe uma sequência $\left(\frac{p_j}{q_j}\right)_{j\in\mathbb{N}}$ de racionais distintos tais que $\left|\frac{p}{q} - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j}$, ou seja, $\left|\frac{pq_j - p_jq}{qq_j}\right| < \frac{1}{q_j^j}$. Além disso, como pq_j e p_jq são números inteiros distintos, a sua diferença em módulo é maior ou igual a 1 e assim obtemos:

$$|pq_j - p_jq| \geq 1 \Rightarrow \frac{1}{|qq_j|} \leq \left|\frac{pq_j - p_jq}{qq_j}\right| < \frac{1}{q_j^j}$$

Isso nos diz que $|q|q_j > q_j^j$ e portanto $|q| > q_j^{j-1}$, um absurdo pois pelo Grande Lema a sequência $(q_j)_{j\in\mathbb{N}}$ é ilimitada. Logo todo número de Liouville é irracional. $\square$

Por fim, o teorema que contém a prova da transcendência dos números de Liouville.

Teorema 7. Todo Número de Liouville é transcendente.

Demonstração. Pela Proposição 4, se α for um número do Liouville então α é irracional. Suponha agora que α é algébrico e é raiz de $P(x)$ onde $\partial P(x) = n \geq 2$, então pelo teorema de Liouville (Teorema 4) temos que vale a seguinte desigualdade para qualquer racional $\frac{p}{q}$

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

Em especial essa desigualdade é valida para os números da sequência $\left(\frac{p_j}{q_j}\right)_{j\in\mathbb{N}}$ da definição de número de Liouville. Dessa forma temos que:

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

Da desigualdade acima segue que $q_j^{j-n} < \frac{1}{c(\alpha)}$, o que contradiz novamente o Grande Lema, pois assim teríamos a limitação de $(q_j)_{j\in\mathbb{N}}$. Portanto todo número de Liouville é transcendente. $\square$

Como consequência desse teorema podemos afirmar que, assim como todo número de Liouville, a Constante de Liouville é um número transcendente.

2.3 O número e é transcendente

O número e, chamado de *número de Euler*, é a base do logaritmo natural, vale aproximadamente $2,718281828459$, e pode ser apresentado como:

- $e = \lim_{n\to\infty}\left(1 + \frac{1}{n}\right)^n$, e
- $e = \sum_{n=0}^{\infty} \frac{1}{n!}$.

O número e é um número irracional e transcendente. A irracionalidade de e foi demonstrada por **Lambert** em 1761 e mais tarde por Euler [4]. A Prova da transcendência de e foi estabelecida pelo Matemático francês **Charles Hermite** em 1873, a qual sofreu sucessivas simplificações ao longo do tempo [4].

A demonstração a seguir, Teorema 8, é uma variação conferida a **Adolf Hurwitz**, da prova de **David Hilbert** da transcendência de e [4].

Teorema 8. O número e é transcendente.

Demonstração. Suponha que e é algébrico. Logo $a_m e^m + \cdots + a_1 e + a_o = 0$, para certos $a_i \in \mathbb{Q}$, $i = 0, \ldots, m$ e $a_0 \neq 0$. Podemos supor, sem perda de generalidade, que os a_i são inteiros para todo i.

O polinômio $f(x) = \dfrac{x^{p-1}(x-1)^p(x-2)^p \cdots (x-m)^p}{(p-1)!}$, onde p é um número primo, é de grau $mp + p - 1$, o que implica que $f^{(mp+p)}(x) = 0$.

Seja $F(x) = f(x) + f'(x) + \cdots + f^{(mp+p-1)}(x)$. Temos

$$\frac{d}{dx}\{e^{-x}F(x)\} = e^{-x}\{F'(x) - F(x)\} = -e^{-x}f(x) \tag{2.1}$$

logo, para todo j,

$$a_j \int_0^j e^{-x} f(x)dx = a_j \left[-e^{-x}F(x)\right]_0^j = a_j F(0) - a_j e^{-j} F(j).$$

Multiplicando ambos os lados por e^j, somando para $j = 0, 1, \ldots, m$, e considerando que $a_m e^m + \ldots + a_0 = 0$, obtemos:

$$\begin{aligned} \sum_{j=0}^{m} \left(a_j e^j \int_0^j e^{-x} f(x)dx \right) &= F(0) \sum_{j=0}^{m} a_j e^j - \sum_{j=0}^{m} a_j F(j) \qquad (2.2) \\ &= -\sum_{j=0}^{m} \sum_{i=0}^{mp+p-1} a_j f^{(i)}(j). \end{aligned}$$

Lema 2. Para todo i e j, $f^{(i)}(j)$ é inteiro divisível por p exceto se $j = 0$ e $i = p - 1$, e então $f^{(p-1)}(0) = (-1)^p \cdots (-m)^p$.

Demonstração. (do Lema) Usando a regra de Leibniz, se $j \neq 0$, então o único termo não nulo vem do fator $(x - j)^p$ derivando p vezes. Desde que $\dfrac{p!}{(p-1)!} = p$, esses termos são inteiros divisíveis por p.

Se $j = 0$, o único termo não divisível por p é obtido para $i = p - 1$ e então

$$f^{(p-1)}(0) = (-1)^p \cdot \ldots \cdot (-m)^p.$$

□

Segue-se que a expressão (2.2) é da forma $Kp - a_0(-1)^p \cdots (-m)^p$, com $K \in \mathbb{Z}$.

Se $p > \sup(m, |a_0|)$, o inteiro $a_0(-1)^p \cdot \ldots \cdot (-m)^p$ não é divisível por p. Logo para um número primo p suficientemente grande, o lado esquerdo de (2.2) é um inteiro que não é divisível por p e portanto $Kp - a_0(-1)^p \cdot \ldots \cdot (-m)^p$ é não nulo.

Vamos dar uma cota superior para a integral. Se $0 \leq x \leq m$, então

$$|f(x)| \leq \frac{m^{mp+p-1}}{(p-1)!}.$$

o que implica

$$\begin{aligned}\left|\sum_{j=0}^{m}\left(a_j e^j \int_0^j e^{-x} f(x) dx\right)\right| &\leq \sum_{j=0}^{m} |a_j| e^j \int_0^j \frac{m^{mp+p-1}}{(p-1)!} dx \\ &\leq \left(\sum_{j=0}^{m} |a_j| e^j\right) \frac{m^{mp+p}}{(p-1)!}\end{aligned}$$

que tende a 0 quando p tende a infinito.

Logo obtivemos uma condição o qual prova que e é transcendente. □

2.4 O número π é transcendente

O número π representa o valor da razão entre a circunferência de qualquer círculo e seu diâmetro. É a mais antiga constante matemática que se conhece. É um número irracional, com infinitas casas decimais e não periódico. π vale aproximadamente $3,141592653589$.

Lindermann, em 1882, estendeu a demonstração de que e é transcendente e mostrou que π também o é [4].

Teorema 9. π é transcendente.

Demonstração. Suponha que π é algébrico sobre $\mathbb{Q}$. Então, π é algébrico sobre $\mathbb{Z}$. Como o produto de números algébricos é também um número algébrico, então πi é algébrico sobre $\mathbb{Z}$ e, portanto, existe um polinômio

$$\theta_1(x) \in \mathbb{Z}[x] \tag{2.3}$$

com raízes $\alpha_1 = \pi i, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$. Como $e^{\pi i} + 1 = 0$, então

$$(e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \cdots (e^{\alpha_n} + 1) = 0. \tag{2.4}$$

Observe que ao expandir o produto na equação (2.4) os expoentes de e tornam-se somas de $\alpha_1, a_2, \ldots, \alpha_n$ tomados 2 a 2, 3 a 3, n a n. Desejamos construir um polinômio cujas raízes são essas somas.

Primeiro, considero as somas de $\alpha_1, \alpha_2, \ldots, \alpha_n$ tomados 2 a 2, isto é,

$$\alpha_1 + \alpha_2, \alpha_1 + \alpha_3, \ldots, \alpha_{n-1} + a_n. \tag{2.5}$$

Por (2.3), todos os polinômios simétricos elementares de $\alpha_1, \alpha_2, \ldots, \alpha_n$ são racionais e, portanto, todos os polinômios simétricos elementares das somas (2.5) são também racionais. Daí, segue que existe um polinômio

$$\theta_2(x) \in \mathbb{Z}[x], \tag{2.6}$$

cujas raízes são as somas (2.5). Analogamente, existem polinômios

$$\theta_3(x), \ldots, \theta_n(x) \in \mathbb{Z}[x], \tag{2.7}$$

cujas raízes são as somas de $\alpha_1, a_2, \ldots, \alpha_n$ tomadas 3 a 3, ..., n a n, respectivamente.

Por construção, o polinômio em $\mathbb{Z}[x]$ dado por

$$\theta_1(x)\theta_2(x) \cdot \ldots \cdot \theta_n(x), \tag{2.8}$$

tem como raízes exatamente as somas que aparecem como expoentes do e na expansão do produto na equação (2.4).

Sejam $\beta_1, \beta_2, \ldots, \beta_r$ as raízes não nulas do polinômio (2.8). Então, o polinômio

$$\theta(x) = cx^r + c_1x^{r-1} + c_2x^{r-2} + \ldots + c_r. \tag{2.9}$$

cujas raízes são $\beta_1, \beta_2, \ldots, \beta_r$ tem coeficientes inteiros, ou seja, $\theta(x) \in \mathbb{Z}[x]$. Além disso, podemos escrever a equação (2.4) da seguinte maneira:

$$e^{\beta_1} + e^{\beta_2} + \ldots + e^{\beta_r} + e^0 + \ldots + e^0 = 0,$$

ou seja,

$$e^{\beta_1} + e^{\beta_2} + \ldots + e^{\beta_r} + k = 0, \tag{2.10}$$

onde k é um inteiro positivo.

Agora dado p um número primo, defina

$$f(x) = c^s x^{p-1} \frac{[\theta(x)]^p}{(p-1)!}, \tag{2.11}$$

onde $s = rp - 1$ e observe que $f(x)$ é um polinômio de grau $s + p$.

Defina também

$$F(x) = f(x) + f^{(1)}(x) + f^{(2)}(x) + \ldots + f^{(s+p)}(x) \tag{2.12}$$

e observe que

$$\frac{d}{dx}[e^{-x}F(x)] = -e^{-x}f(x). \tag{2.13}$$

Daí, pelo Teorema Fundamental do Cálculo segue que

$$e^{-x}F(x) - e^0F(0) = \int_0^x -e^{-y}f(y)dy, \tag{2.14}$$

e, portanto, fazendo a mudança de variável $y = \tau x$ na integral obtemos que

$$F(x) - e^xF(0) = -x\int_0^1 e^{(1-\tau)x}f(\tau x)d\tau, \tag{2.15}$$

Agora, tomando $x = \beta_1, \beta_2, \ldots, \beta_r$ em (2.15), somando as equações obtidas e usando (2.10) obtemos que

$$\sum_{j=1}^r F(\beta_j) + kF(0) = -\sum_{j=1}^r \beta_j \int_0^1 e^{(1-\tau)\beta_j}f(\tau\beta_j)d\tau. \tag{2.16}$$

Afirmamos que existe um número primo p_1 tal que o lado esquerdo da equação (2.16) é um número inteiro não nulo para todo $p \geq p_1$.

Para ver isso, primeiro observe que β_j é uma raiz de multiplicidade p de $f(x)$, para todo $j = 1, \ldots, r$. Daí, segue que

$$\sum_{j=1}^r f^{(t)}(\beta_j) = 0, \quad 1 \leq t \leq p. \tag{2.17}$$

Por outro lado, observe que

$$\begin{aligned} g(x) &= (p-1)!f(x) = c^s x^{p-1}[\theta(x)]^p \\ &= c^s x^{p-1}[cx^r + c_1x^{r-1} + c_2x^{r-2} + \ldots + c_r] \\ &= c^s h(x), \end{aligned}$$

onde $h(x) \in \mathbb{Z}[x]$ é um polinômio com grau $r+p-1$. Além disso, ao derivar $t \geq p$ vezes o polinômio $g(x)$, obtemos um polinômio cujos coeficientes contém o produto de pelo menos p números inteiros consecutivos cuja origem são os expoentes do x em $h(x)$. Daí, como $p!$ divide o produto de p números inteiros consecutivos, segue que

$$g^{(t)}(x) = c^s p! h_t(x), \quad t \geq p, \tag{2.18}$$

onde $h_t(x) \in \mathbb{Z}[x]$ e, portanto,

$$f^{(t)}(x) = c^s p h_t(x), \quad t \geq p. \tag{2.19}$$

Mais ainda, como $\deg(f(x)) = s + p$, então para $t \geq p$ temos $\deg(f^{(t)}(x)) \leq s$. Portanto, para $t \geq p$ a soma $\sum\limits_{j=1}^r f^{(t)}(\beta_j)$ é um polinômio simétrico em $\beta_1, \beta_2, \ldots, \beta_r$ com coeficientes inteiros divisíveis por $c^s p$ e, portanto, por (2.9) e pelo Teorema Fundamental das Funções Simétricas segue que

$$\sum_{j=1}^r f^{(t)}(\beta_j) = pa_t, \quad t \geq p, \tag{2.20}$$

onde $a_t \in \mathbb{Z}$. Daí, de (2.17) e (2.20) segue que

$$\sum_{j=1}^{r} F(\beta_j) = \sum_{j=1}^{r}\left(\sum_{j=0}^{s+p} f^{(t)}(\beta_j)\right) = p\sum_{j=0}^{p+s} a_t = pA, \tag{2.21}$$

onde $A \in \mathbb{Z}$. Por outro lado, observe que

$$\begin{aligned} f^{(t)}(0) &= 0, \qquad 0 \leq t \leq p-2, \\ f^{(p-1)}(0) &= c^s c_r^p, \\ f^{(t)}(0) &= pb_t, \quad b_t \in \mathbb{Z}, \quad t \geq p, \end{aligned}$$

e portanto,

$$kF(0) = k\sum_{i=0}^{s+p} f^{(t)}(0) = kc^s c_r^p + kpB, \tag{2.22}$$

onde $B \in \mathbb{Z}$.

Seja p_1 um número primo maior que $\max\{|c|, |c_r|, |k|\}$. Então, p_1 não divide $kc^s c_r^{p_1}$, portanto, p_1 não divide o inteiro

$$\sum_{j=1}^{r} F(\beta_j) + kF(0) = kc^s c_r^{p_1} + p_1(A + kB), \tag{2.23}$$

ou seja, esse inteiro é não nulo. Logo,

$$p \geq p_1 \quad \Rightarrow \quad \left|\sum_{j=1}^{r} F(\beta_j) + kF(0)\right| \geq 1. \tag{2.24}$$

Agora, afirmamos que o lado direito da equação (2.16) converge para 0 quando $p \to +\infty$ (dentre números primos).

Para ver isso, observe que por (2.9) e (2.11) com $0 \leq \tau \leq 1$ temos as seguintes estimativas:

$$|\theta(\tau\beta_j)| \leq M_j, \quad M_j > 0, \quad j = 1, \ldots, r, \tag{2.25}$$

e

$$\left|e^{(1-\tau)\beta_j} f(\tau\beta_j)\right| \leq \frac{e^{\beta_j}}{|c\beta_j|}\frac{|c^r\beta_j M_j|^p}{(p-1)!}, \quad j = 1, \ldots, r. \tag{2.26}$$

Daí, podemos estimar o lado direito da equação (2.16) da seguinte maneira:

$$\begin{aligned} \left|\sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-\tau)\beta_j} f(\tau\beta_j) d\tau\right| &\leq \sum_{j=1}^{r} |\beta_j| \int_0^1 \left|e^{(1-\tau)\beta_j} f(\tau\beta_j)\right| d\tau \\ &\leq \sum_{j=1}^{r} |\beta_j| \int_0^1 \frac{e^{\beta_j}}{|c\beta_j|}\frac{|c^r\beta_j M_j|^p}{(p-1)!} d\tau \\ &\leq \sum_{j=1}^{r} \frac{e^{\beta_j}}{|c|}\frac{|c^r\beta_j M_j|^p}{(p-1)!}. \end{aligned}$$

Mas, essa última soma converge para 0 quando $p \to +\infty$ e, portanto, o lado direito da equação (2.16) também converge para 0. Em particular, existe um número primo p_2 tal que

$$p \geq p_2 \quad \Rightarrow \quad \left| \sum_{j=1}^{r} \beta_j \int_0^1 e^{(1-\tau)\beta_j} f(\tau\beta_j) d\tau \right| \geq 1. \tag{2.27}$$

Seja $p_0 = \max\{p_1, p_2\}$. Então, para $p \geq p_0$, por um lado temos de (2.24) que o lado esquerdo de (2.16) é maior ou igual que 1 e, por outro lado, temos de (2.27) que o lado direito de (2.16) é menor que 1, ou seja, uma contradição.

Logo π não é algébrico sobre $\mathbb{Q}$, ou seja, π é transcendental sobre $\mathbb{Q}$. $\square$

Capítulo 3

Classificação de Mahler

Neste capítulo, explanaremos sobre a classificação de Marler (dos números transcendentes), veremos que existem subclasses nessa classificação, além de algumas propriedades e consequências importantes.

Como vimos, o conjunto dos números reais (ou complexos) pode ser dividido entre números algébricos e transcendentes. Ou seja, um número real ou é algébrico ou transcendente. Contudo, no início do século XX, foram criadas várias classificações para os números transcendentes, no entanto, elas não foram consideradas relevantes. A primeira classificação interessante foi criada por Kurt Mahler em 1932, a qual nos levou a uma nova compreensão dos números transcendentes.

3.1 Classificação de Mahler

Vejamos algumas considerações preliminares importantes:

Definição 7. Dois números ξ e ζ são ditos *algebricamente dependentes* se existe um polinômio, não nulo, de duas variáveis $P(x,y) \in \mathbb{Z}[x,y]$ tal que $P(\xi,\zeta) = 0$.

Definição 8. Seja $P(x) \in \mathbb{Z}[x]$ com $P(x) = a_0 + a_1 x + \ldots + a_n x^n$. A *altura* de P é dada por $\mathcal{H}(P) := \max\{|a_0|, \ldots, |a_n|\}$.

Definição 9. A altura e o grau de um número algébrico α, denotados respectivamente por $\mathcal{H}(\alpha)$ e $\partial(\alpha)$, são iguais à altura e o grau do seu polinômio minimal.

Vejamos agora generalizações dos teoremas de Liouville e Dirichlet, os quais são fundamentais para a construção da classificação de Mahler.

Teorema 10 (Liouville)**.** Seja α um número algébrico de grau d e N um inteiro positivo. Então existe uma constante positiva $c = c(\alpha, N)$ tal que para todo polinômio $P(z) \in \mathbb{Z}[z]$, satisfazendo $\partial P \leq N$ e $P(\alpha) \neq 0$, vale

$$|P(\alpha)| \geq \frac{c}{\mathcal{H}(P)^{d-1}},$$

em que $\mathcal{H}(P)$ é a altura do polinômio P.

Demonstração. Seja $f(z) = a_d z^d + \ldots + a_1 z + a_0$ o polinômio minimal de α sobre $\mathbb{Z}$, com $a_d > 0$. Denotando os conjugados de α por $\alpha_1, \alpha_2, \ldots, \alpha_d$, com $\alpha_1 = \alpha$, temos

$$f(z) = a_d(z - \alpha_1)\ldots(z - \alpha_d).$$

Agora, se $P(z) \in \mathbb{Z}[z]$ é tal que $P(z) = b_k z^k + \ldots + b_1 z + b_0$, $P(\alpha) \neq 0$ e $k \leq N$, então podemos fatorar $P(z)$ como

$$P(z) = b_k(z - \beta_1)\ldots(z - \beta_k).$$

Note que $\alpha_m \neq \beta_i$ para todo par de índices m e i. Com efeito, se tivéssemos $\alpha_m = \beta_i$ para um par m e i, então $P(\alpha_m) = 0$. Mas como $f(z)$ é o polinômio minimal de α_m, devemos ter que $f(z)|P(z)$ e logo $P(\alpha) = 0$, o que contradiz a nossa escolha. Feita esta observação, concluímos que $|\alpha_m - \beta_i| > 0$ para todo par de índices m e i, e podemos então calcular o duplo produtório

$$\prod_{m=1}^{d}\prod_{i=1}^{k}|\alpha_m - \beta_i|.$$

Por um lado, temos a igualdade

$$\prod_{m=1}^{d}\left(\prod_{i=1}^{k}|\alpha_m - \beta_i|\right) = \prod_{m=1}^{d}\frac{1}{|b_k|}|P(\alpha_m)|.$$

Por outro lado,

$$\prod_{i=1}^{k}\left(\prod_{m=1}^{d}|\beta_i - \alpha_m|\right) = \prod_{m=1}^{k}\frac{1}{|b_k|}|f(\beta_i)|.$$

Logo,

$$\frac{1}{|b_k|^d}\prod_{m=1}^{d}|P(\alpha_m)| = \frac{1}{a_d^k}\prod_{i=1}^{k}|f(\beta_i)|.$$

E assim,

$$|P(\alpha)| = \frac{|b_k|^d \prod\limits_{i=1}^{k}|f(\beta_i)|}{a_d^k \prod\limits_{m=2}^{d}|P(\alpha_m)|}.$$

Afirmamos que $|b_k|^d \prod_{i=1}^{k} |f(\beta_i)|$ é um inteiro positivo. De fato, considere o seguinte polinômio simétrico $F(x_1, \ldots, x_k) = f(x_1) \ldots f(x_k)$ com coeficientes inteiros. Pelo Teorema Fundamental das Funções Simétricas, existe um polinômio com coeficientes inteiros $G(y_1, \ldots, y_k)$, tal que

$$F(x_1, \ldots, x_k) = f(x_1) \ldots f(x_k) = G(\sigma_1(x_1, \ldots, x_k), \ldots, \sigma_k(x_1, \ldots, x_k)).$$

Pela definição de $F(x_1, \ldots, x_k)$, temos

$$\begin{aligned} F(x_1, \ldots, x_k) &= (a_d x_1^d + \ldots + a_1 x_1 + a_0) \ldots (a_d x_k^d + \ldots + a_1 x_k + a_0) \\ &= a_d^k (x_1, \ldots, x_k)^d + \ldots + a_0^k = a_d^k (\sigma_k(x_1, \ldots, x_k))^d + \ldots + a_0^k \\ &= G(\sigma_1(x_1, \ldots, x_k), \ldots, \sigma_k(x_1, \ldots, x_k)). \end{aligned}$$

Assim, $\partial G \geq d$.
Supondo que $\partial G > d$, então deve existir um monômio de $G(\sigma_1(x_1, \ldots, x_k), \ldots, \sigma_k(x_1, \ldots, x_k))$, digamos

$$(\sigma_{i_1}(x_1, \ldots, x_k))^{c_1} \ldots (\sigma_{i_n}(x_1, \ldots, x_k))^{c_n},$$

de grau maior do que d, isto é, $c_1 + \ldots + c_n > d$. Observando as potências das funções simétricas, temos

$$(\sigma_{i_t}(x_1, \ldots, x_k))^{c_t} = (x_1, \ldots, x_{i_t} + A_t(x_1, \ldots, x_k))^{c_t} = (x_1, \ldots, x_{i_t})^{c_t} + B_t(x_1, \ldots, x_k),$$

para todo $t \in \{1, \ldots, n\}$, em que A_t e B_t são polinômios em k variáveis com coeficientes inteiros. Logo, o possível monômio é

$$\begin{aligned} \prod_{t=1}^{n} \sigma_{i_t}(x_1, \ldots, x_k)^{c_t} &= \prod_{t=1}^{n} ((x_1, \ldots, x_k)^{c_t} + B_t(x_1, \ldots, x_k)) \\ &= x_1^{c_1 + \ldots + c_n} \cdot D(x_2, \ldots, x_k) + E(x_1, \ldots, x_k), \end{aligned}$$

com $D(x_2, \ldots, x_k)$ e $E(x_1, \ldots, x_k)$ polinômios não constantes com coeficientes inteiros. Mas isso é um absurdo, pois a potência de x_1 é maior do que d. Portanto ocorre a igualdade $\partial G = d$. Como $P(z) = b_k(z - \beta_1) \ldots (z - \beta_k)$, temos também as seguintes igualdades

$$\begin{aligned} \sigma_1 &:= \sigma_1(\beta_1, \ldots, \sigma_k) = \beta_1 + \ldots + \beta_k = -\frac{b_{k-1}}{b_k} \\ \sigma_2 &:= \sigma_2(\beta_1, \ldots, \sigma_k) = \beta_1\beta_2 + \ldots + \beta_{k-1}\beta_k = -\frac{b_{k-2}}{b_k} \\ &\vdots \\ \sigma_k &:= \sigma_k(\beta_1, \ldots, \sigma_k) = \beta_1 \cdot \ldots \cdot \beta_k = (-1)^k \frac{b_0}{b_k}. \end{aligned}$$

Assim $G(\sigma_1, \ldots, \sigma_k)$ é um número racional cujo denominador é igual a b_k^d e podemos finalmente concluir que

$$b_k^d \prod_{i=1}^{k} f(\beta_i) = b_k^d F(\beta_1, \ldots, \beta_k) = b_k^d G(\sigma_1, \ldots, \sigma_k) \in \mathbb{Z}.$$

Portanto $|b_k|^d \prod_{i=1}^{k} |f(\beta_i)|$ é um inteiro positivo. Utilizando este fato, obtemos

$$|P(\alpha)| = \frac{|b_k|^d \prod_{i=1}^{k} |f(\beta_i)|}{a_d^k \prod_{m=2}^{k} |P(\alpha_m)|} \geq \frac{1}{a_d^k \prod_{m=2}^{k} |P(\alpha_m)|}.$$

Majorando as quantidades $|P(\alpha_i)|$, para $i \in \{2, \ldots, d\}$, obtemos

$$\begin{aligned} |P(\alpha_i)| &= |b_k\alpha_i^k + \ldots + b_1\alpha_i + b_0| \leq |b_k||\alpha_i|^k + \ldots + |b_1||\alpha_i| + |b_0| \\ &\leq \mathcal{H}(P)(|\alpha_i|^k + \ldots + |\alpha_i| + 1). \end{aligned} \tag{3.1}$$

Denotando $A = \max\{|\alpha_2|, \ldots, |\alpha_d|\}$, como $k \leq N$, de acordo com (3.1), para $i \in \{2, \ldots, d\}$ teremos

$$|P(\alpha)| = \mathcal{H}(P)(A^k + \ldots + A + 1) \leq \mathcal{H}(P) \underbrace{(A^k + \ldots + A + 1)}_{C_1(\alpha,N)}.$$

Finalmente,

$$|P(\alpha)| \geq \frac{1}{a_d^k} \cdot \frac{1}{\prod_{i=2}^{d} \mathcal{H}(P)C_1(\alpha, N)} \geq \frac{C}{\mathcal{H}(P)^{d-1}},$$

em que $C = \dfrac{1}{a_d^k C_1(\alpha, N)^{d-1}}$. □

O teorema de **Dirichlet** afirma que se $\xi \in \mathbb{R}$ é um número irracional, então existem infinitos racionais $\frac{p}{q}$, com $q \geq 1$, tais que

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

Ou seja, $|P(\xi)| < \frac{1}{q}$, onde $P(x) = qx - p$. Note também que $\mathcal{H}(P) \geq q$.

Nosso próximo objetivo é estender o teorema de **Dirichlet**. Vejamos a seguir.

Teorema 11 (Dirichlet)**.** Sejam ξ um número complexo e N um inteiro positivo, de modo que ξ ou é transcendente ou é um algébrico de grau maior do que N. Então existe uma constante $C = C(\xi, N) > 0$ tal que para todo inteiro positivo H, existe um polinômio não nulo $P(z) \in \mathbb{Z}[z]$, com $\partial P \leq N$ e $\mathcal{H}(P) \leq H$ satisfazendo

$$|P(\xi)| < \frac{C}{H^{\frac{N-1}{2}}}.$$

Demonstração. Quando $N = 1$, então podemos escolher $C = C(\xi, 1) = 2|\xi| + 1$ e considerar o polinômio $P(z) = z$. Neste caso, $\mathcal{H}(P) = 1 \leq H$ para todo H inteiro positivo e, temos que

$$|P(\xi)| = |\xi| < 2|\xi| + 1 = C(\xi, 1) = \frac{C}{H^0}.$$

Assim, o teorema é válido no caso $N = 1$. Para o caso mais interessante, $N \geq 2$, vamos recorrer ao Princípio das Gavetas (de Dirichlet). Primeiro, para inteiros positivos N e H, denote por $\mathcal{Q}_{N,H}$ o conjunto de polinômios

$$\mathcal{Q}_{N,H} = \left\{ P(z) \in \mathbb{Z}[z]; P(z) = \sum_{n=0}^{N} a_n z^n \ \text{ e } \ 0 \leq a_n \leq H, \quad n = 0, \ldots, N \right\}.$$

Note que $\#\mathcal{Q}_{N,H} = (H+1)^{N+1}$. De fato, já que tais polinômios são totalmente determinados pela escolha dos seus $N+1$ coeficientes e para cada um destes temos $H+1$ possibilidades, pelo Princípio Fundamental da Contagem temos um total de $(H+1)^{N+1}$ escolhas possíveis para tais coeficientes, ou seja $(H+1)^{N+1}$ polinômios distintos em $\mathcal{Q}_{N,H}$. Também, temos que o conjunto dos valores $\mathcal{Q} = \{P(\xi);\ P(z) \in \mathcal{Q}_{N,H}\}$ tem a mesma cardinalidade de $\mathcal{Q}_{N,H}$. Com efeito, é claro que $\#Q \leq \#Q_{N,H}$. Se tivéssemos $\#Q < \#\mathcal{Q}_{N,H}$, então pelo menos dois polinômios distintos $P_1^*(z) = P_2^*(z)$ em $\mathcal{Q}_{N,H}$ são tais que $P_1^*(\xi) = P_2^*(\xi)$. Mas isto implicaria a existência de um polinômio $P^*(z) = P_1^*(z) - P_2^*(z)$ de grau menor ou igual a N, do qual ξ é raiz, o que contradiz o fato de que o grau de ξ é maior do que N. Concluímos então que $\#\mathcal{Q} = \#\mathcal{Q}_{N,H} = (H+1)^{N+1}$. Usando a desigualdade triangular, obtemos

$$|P(\xi)| \leq a_n|\xi|^n + \ldots + a_1|\xi| + a_0 \leq (|\xi|^n + \ldots + |\xi| + 1)\, H =: B,$$

para todo $P(z) \in \mathcal{Q}_{N,H}$. Como $|P(\xi)| \leq B$, implica $\max\{|Re(P(\xi))|, |Im(P(\xi))|\} \leq B$, temos que $P(\xi) \in [-B, B]^2$ para todo $P(z) \in \mathcal{Q}_{N,H}$. Dividimos $[-B, B]^2$ em s^2 quadrados menores, estes terão lado igual a $\frac{2B}{s}$. Para aplicarmos o Princípio das Gavetas, queremos que a quantidade de valores em $\mathcal{Q}$ exceda o número de quadrados nenores, ou seja,

$$s^2 < (H+1)^{N+1}.$$

Se tomarmos $s = \left\lfloor (H+1)^{\frac{N+1}{2}} \right\rfloor - 1$, então

$$s^2 < \left((H+1)^{\frac{N+1}{2}} \right)^2 = (H+1)^{N+1},$$

como desejado. Além disso, como $N \geq 2$ e $H \geq 1$, então $s \geq \lfloor \sqrt{2^3} \rfloor - 1 = 1$ e nossa escolha está bem definida. Logo, pelo Princípio das Gavetas, existem polinômios $P_1(z)$ e $P_2(z)$ em $\mathcal{Q}_{N,H}$ tais que $P_1(\xi)$ e $P_2(\xi)$ estão no mesmo quadrado de lado $2B/s$. Portanto,

$$|P_1(\xi) - P_2(\xi)| \leq \frac{2B\sqrt{2}}{s} \text{ (diagonal do quadrado).}$$

Tomando $P(z) = P_1(z) - P_2(z)$, então como $\max\{\partial P_1, \partial P_2\} \leq N$, obviamente $\partial P \leq N$. Por outro lado, escrevemos $P_1(z) = \sum_{n=0}^{N} a_n z^n$ e $P_2(z) = \sum_{n=0}^{N} b_n z^n$, então $P(z) = \sum_{n=0}^{N} c_n z^n$ onde $c_n = a_n - b_n$. Como $0 \leq a_n \leq H$ e $0 \leq b_n \leq H$, então $|c_n| \leq H$, para todo $n = 0, 1, \ldots, N$ e portanto $\mathcal{H}(P) \leq H$. Além disso, temos a desigualdade

$$|P(\xi)| \leq 2\sqrt{2}(1 + |\xi| + \ldots + |\xi|^N)\frac{H}{\left\lfloor (H+1)^{\frac{N+1}{2}} \right\rfloor - 1}. \tag{3.2}$$

Afirmamos que $\left\lfloor (H+1)^{\frac{N+1}{2}} \right\rfloor - 1 \geq \left\lfloor H^{\frac{N+1}{2}} \right\rfloor$. De fato, se N é ímpar, digamos $N = 2k+1$, então

$$s = \left\lfloor (H+1)^{\frac{2k+2}{2}} \right\rfloor - 1 = (H+1)^{k+1} + 1 - 1 \geq H^{k+1} + 1 = \left\lfloor H^{\frac{N+1}{2}} \right\rfloor.$$

Quando $N = 2K$, então

$$s = \left\lfloor (H+1)^k (H+1)^{\frac{1}{2}} \right\rfloor - 1 \geq \left\lfloor H^{\frac{2k+1}{2}} + H^{\frac{1}{2}} \right\rfloor - 1 \geq \left\lfloor H^{\frac{2k+1}{2}} + 1 \right\rfloor - 1 = \left\lfloor H^{\frac{N+1}{2}} \right\rfloor.$$

Provada tal afirmação, podemos reescrever (3.2) como

$$|P(\xi)| \leq 2\sqrt{2}(1 + |\xi| + \ldots + |\xi|^N)\frac{H}{\left\lfloor H^{\frac{N+1}{2}} \right\rfloor}.$$

Mas $3\lfloor x \rfloor > 2x$ para todo $x \geq 1$, então

$$|P(\xi)| < \frac{3\sqrt{2}(1 + |\xi| + \ldots + |\xi|^N)}{H^{\frac{N-1}{2}}} = \frac{C}{H^{\frac{N-1}{2}}},$$

onde $C = C(\xi, N) := 3\sqrt{2}(1 + |\xi| + \ldots + |\xi|^N)$. □

Para facilitar, chamaremos os dois resultados anteriores de Teorema Geral de Liouville e Dirichlet, respectivamente.

Como consequência das generalizações dos teoremas de Dirichlet e Liouville, conseguimos uma nova definição para números transcendentes.

Agora, sendo ξ um número real (ou complexo) e $P(z) \in \mathbb{Z}[z]$, vamos analisar os casos em que $|P(\xi)|$, dependendo do grau e da altura de P, se aproxima muito de zero, mas sempre com $P(\xi) \neq 0$.

Teorema 12. Dado um número complexo ξ e inteiros positivos H e N, sejam

$$\begin{aligned}\mathcal{P}_{N,H} &= \{P(z) \in \mathbb{Z}[z],\ \partial P \leq N \text{ e } \mathcal{H}(P) \leq H\} \\ \Omega(\xi, N, H) &= \min\{|P(\xi)|; P(z) \in \mathcal{P}_{N,H} \text{ e } P(\xi) \neq 0\}.\end{aligned}$$

Defina $\omega(\xi, N, H)$ como

$$\Omega(\xi, N, H) = H^{-\omega(\xi,N,H)\cdot N},$$

$\omega(\xi, N) := \lim_{H\to\infty} \sup \omega(\xi, N, H)$ e $\omega(\xi) := \lim_{N\to\infty} \sup \omega(\xi, N)$. Então ξ é transcendente se, somente se, $\omega(\xi) \neq 0$.

Demonstração. Vamos agora examinar o quão próximo de zero $|P(\xi)|$ pode se tornar quando variamos $P(z)$ sobre todos os polinômios em $\mathbb{Z}[x]$, com grau e altura menores ou iguais a N e H, respectivamente e tais que $P(\xi) \neq 0$. Para isto, definimos

$$\begin{aligned} \mathcal{P}_{N,H} &= \{P(z) \in \mathbb{Z}[z]; \partial P \leq H\}, \\ \Omega(\xi, N, H) &= \min\{|P(\xi)|; P(z) \in \mathcal{P}_{N,H} \text{ e } P(\xi) \neq 0\}. \end{aligned}$$

Para podermos comparar bem $\Omega(\xi, N, H)$ ao expoente de H no Teorema Geral de Dirichlet, gostaríamos de expressar $\Omega(\xi, N, H)$ como $H^{-\Theta N}$ para uma escolha conveniente de Θ. Esta observação nos leva a definir o expoente $\omega(\xi, N, H)$ satisfazendo a equação

$$\Omega(\xi, N, H) = H^{-\omega(\xi,N,H)N}.$$

Assim, determinar qual o menor valor de $\Omega(\xi, N, H)$ para infinitos H e N é equivalente a determinar qual o maior valor possível para $\Omega(\xi, N, H)$ quando variamos os valores de H e N. Se ξ é transcendente, podemos usar o Teorema Geral de Direchlet e garantir que, para todo H e N fixados, existem uma constante positiva $C = C(\xi, N)$ e um polinômio $P(z) \in P_{N,H}$ tais que

$$\Omega(\xi, N, H) \leq |P(\xi)| < \frac{C}{H^{\frac{N-1}{2}}} \Rightarrow H^{-\omega(\xi,N,H)N} < \frac{C}{H^{\frac{N-1}{2}}}.$$

Aplicando a função logaritmo na última desigualdade anterior, obtemos

$$-\omega(\xi, N, H) \cdot N \log(H) < \log(C) - \frac{N-1}{2} \log(H).$$

E assim,

$$\frac{N-1}{2} < \frac{\log(C)}{\log(H)} + \omega(\xi, N, H) \cdot N. \tag{3.3}$$

Primeiramente, vamos observar qual o crescimento de $\omega(\xi, N, H)$ para os infinitos valores de H. Não sabemos se o $\lim\limits_{H\to\infty} \omega(\xi, N, H)$ existe, mas como estamos interessados no maior ponto de acumulação de $\omega(\xi, N, H)$, para N fixo e $H \to \infty$, basta verificarmos o $\limsup\limits_{H\to\infty} \omega(\xi, N, H)$ (limite superior), que sempre existe. Assim, definimos

$$\omega(\xi, N) = \limsup_{H\to\infty} \omega(\xi, N, H).$$

Aplicando $\limsup\limits_{H\to\infty}$ em ambos os lados da desigualdade (3.3), temos

$$\limsup_{H\to\infty} \frac{N-1}{2} \leq \underbrace{\limsup_{H\to\infty} \frac{\log(C)}{\log(H)}}_{\to 0} + \omega(\xi, N) \cdot N.$$

ou seja,

$$\frac{N-1}{2} \leq \omega(\xi, N) \cdot N \Rightarrow \omega(\xi, N) \geq \frac{N-1}{2N}.$$

Denotando $\omega(\xi)$ com o maior ponto de acumulação da função $\omega(\xi, N)$ quando $N \to \infty$, ou seja

$$\omega(\xi) := \limsup_{N\to\infty} \omega(\xi, N) \geq \limsup_{N\to\infty} \frac{N-1}{2N} = \frac{1}{2}.$$

Concluímos que se ξ é transcendente, então $\omega(\xi)$ é diferente de zero (mais precisamente, deve ser pelo menos $1/2$).

Nosso próximo objetivo é estimar $\omega(\xi)$ no caso em que ξ é algébrico de grau d. Seja $P(z) \in \mathcal{P}_{N,H}$ o polinômio que satisfaz

$$|P(\xi)| = \Omega(\xi, N, H) = H^{-\omega(\xi,N,H)N}.$$

Aplicando o Teorema Geral de Liouville, temos

$$\frac{c(\xi, N)}{H^{d-1}} \leq \frac{c(\xi, N)}{\mathcal{H}(P)^{d-1}} \leq |P(\xi)| = H^{-\omega(\xi,N,H)N},$$

O que implica (aplicando a função log)

$$\omega(\xi, N, H) \leq \frac{d-1}{N} - \frac{\log(c(\xi, N))}{N\log(H)}.$$

Logo,

$$\omega(\xi, N) = \limsup_{H\to\infty} \omega(\xi, N, H) \leq \frac{d-1}{N} - \underbrace{\limsup_{H\to\infty} \frac{\log(c(\xi, N)}{N\log(H)}}_{\to 0}$$

e assim

$$\omega(\xi) = \limsup_{N\to\infty} \omega(\xi, N) \leq \limsup_{N\to\infty} \frac{d-1}{N} = 0 \Rightarrow \omega(\xi) \leq 0.$$

Por outro lado, como a sequência $(\Omega(\xi, N, H))_{N\geq 1}$ é não crescente, então $\Omega(\xi, N, H) \leq \Omega(\xi, 1, H) \leq 1$, para todo $H \geq |\xi| + 1$. Daí,

$$\omega(\xi, N, H) = -\frac{\log(\Omega(\xi, N, H))}{N\log(H)} \geq 0,$$

quando $H \geq |\xi| + 1$. Assim $\omega(\xi) \geq 0$ (na verdade esse argumento vale também se ξ é transcendente) e concluímos que se α é algébrico, então $\omega(\alpha) = 0$. Com isso, acabamos de provar um critério para transcendência. $\square$

Portanto, a classificação dos números reais ficaria da seguinte forma:

Para todo ξ real (ou complexo), tem-se:

- $\omega(\xi) = 0$, equivale a ξ algébrico;
- $\omega(\xi) \neq 0$, equivale a ξ transcendente.

Contudo, como $\omega(\xi) \geq 0$ pode-se considerar o seguinte:

- $\omega(\xi) = 0$ (ξ algébrico);
- $0 < \omega(\xi) < \infty$ (ξ transcendente);
- $\omega(\xi) = \infty$ (ξ transcendente).

Observe que se $\omega(\xi, N_0) = \infty$ para algum $N_0 \in \mathbb{N}$, então

$$\omega(\xi) = \limsup_{N\to\infty} \omega(\xi, N) \geq \omega(\xi, N_0) = \infty \to \omega(\xi) = \infty.$$

Portanto, existem duas maneiras de se obter $\omega(\xi) = \infty$:

(i) $\omega(\xi, N_0) = \infty$; para algum N_0,

(ii) $\omega(\xi, 1), \omega(\xi, 2), \ldots$ não possui ponto de acumulação.

Dessa forma, temos uma classificação mais refinada dos números reais (ou complexos):

- $\omega(\xi) = 0$ (ξ algébrico);
- $0 < \omega(\xi) < \infty$ (ξ transcendente);
- $\omega(\xi) = \infty$ e existe um N_0 tal que $\omega(\xi, N_0) = \infty$ (ξ transcendente);
- $\omega(\xi) = \infty$ e para todo N, $\omega(\xi, N) \neq \infty$ (ξ transcendente).

Para analisar melhor os casos em que ξ é transcendente, vamos definir $\nu(\xi)$ como sendo o maior inteiro positivo N tal que $\omega(\xi, N) = \infty$. Logo, caso $\omega(\xi, N) < \infty$ para todo N, então $\nu(\xi) = \infty$. Agora, se $\omega(\xi) = \infty$, então $\nu(\xi)$ pode ser finito ou infinito. Deste modo, temos quatro possibilidades para $\omega(\xi)$ e $\nu(\xi)$ que correspondem às quatro classes acima e dão origem à seguinte *classificação devida a Mahler* para número real (ou complexo) ξ:

- A-números, se $\omega(\xi) = 0$ e (logo) $\nu(\xi) = \infty$;
- S-números, se $0 < \omega(\xi) < \infty$ e (logo) $\nu(\xi) = \infty$;
- U-números, se $\omega(\xi) = \infty$ e $\nu(\xi) < \infty$;
- T-números, se $\omega(\xi) = \infty$ e $\nu(\xi) = \infty$.

A notação "*A-números*" foi propositalmente escolhida para denotar os números algébricos. O significado das letras S, T e U não parece tão evidente. Acredita-se que Mahler escolheu a letra S em homenagem ao seu orientador C. L. Siegel e as letras T e U sem nenhum significado especial devem ter sido escolhidas por serem as duas seguintes do alfabeto.

Os A-números são os números algébricos, pois $\omega(\xi) = 0$. Os demais, S, U e T-números, são classes disjuntas de números transcendentes.

3.2 A Classe dos U-números

A classe dos U-números é uma classe da classificação de Mahler em que $\omega(\xi) = \infty$ e $\nu(\xi) < \infty$, para todo real (ou complexo) ξ.

Os possíveis valores de $\nu(\xi)$ (menor que infinito) nos permite definir subclasses dentro da classe dos U-números. Vejamos:

Definição 10. Sejam ξ um número real (ou complexo) e m um inteiro positivo. Então ξ é dito um *U-Número de tipo m* se $\omega(\xi) = \infty$ e $\nu(\xi) = m$. Os U-números de tipo m também são conhecidos como *U_m-números*.

Exemplo 7. Os números de Liouville são U-números.

Mais precisamente, o Conjunto dos Números de Liouville equivale à classe dos U-números do tipo 1. Ou seja, $\mathbb{L}$ equivale a subclasse U_1-números.

Proposição 5. Os números de Liouville são exatamente os U_1-números.

Demonstração. Seja ξ um número de Liouville e $\left(\dfrac{p_n}{q_n}\right)_n \in \mathbb{Q}$, com $q_n > 1$ e tal que

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n^n},$$

para todo $n \geq 1$. Logo $|P_n(\xi)| < q_n^{1-n}$, para todo $n \geq 1$, onde $P_n(z) = q_n z - p_n$. Denotando $H_n = \mathcal{H}(P_n) = \max\{|p_n|, q_n\}$. Assim,

$$H_n^{-\omega(\xi,1,H_n)} = \Omega(\xi, 1, H_n) \leq |P_n(\xi)| < q_n^{1-n}.$$

Observe que se pode supor, sem perda de generalidade, que H_n é q_n ou $|p_n|$, para todo n. Isso pode ser feito após uma reordenação de índices. Supondo que $H_n = q_n$, deduza que $\omega(\xi, 1, H_n) \geq n - 1$ e portanto

$$\omega(\xi, 1) \geq \limsup_{n\to\infty} \omega(\xi, 1, H_n) = \infty.$$

Logo ξ é U-número.

No caso em que $H_n = |p_n|$, como $\dfrac{p_n}{q_n}$ é convergente (tem limite ξ), então existe uma constante $K > 0$, tal que $|p_n| \leq Kq_n$. Daí $H_n^{-\omega(\xi,1,H_n)} \leq K^{n-1}H_n^{n-1}$ implicando

$$\omega(\xi, 1, H_n) \geq n - 1 - (n-1)\frac{\log(K)}{\log(H_n)}.$$

Sugere-se que $\omega(\xi, 1) = \infty$ e ξ é U-Número. Observe que, em ambos os casos, foi mostrado que $\nu(\xi) = 1$. Portanto, a proposição é verdadeira. $\square$

Paul Erdös, em 1962, mostrou que todo número real pode ser escrito como a soma de dois números de Liouville.

Como vimos, o conjunto dos número de Liouville equivale à subclasse U_1-*números.* Portanto, podemos afirmar que todo número real pode ser escrito como a soma de dois U_1-*números.*

Teorema 13 (Erdös)**.** Todo número real pode ser escrito como soma de dois números de Liouville.

Demonstração. Se $t \in \mathbb{Q}$ e ξ é um número de Liouville, então $\omega = t - \xi$ também é número de Liouville e $t = \xi + \omega$. Para o caso em que $t \notin \mathbb{Q}$, podemos escrever $t = \lfloor t \rfloor + \{t\}$, onde $\lfloor t \rfloor \in \mathbb{Z}$ é a parte fracionária e $\{t\}$ é irracional. Claramente, $t \in \mathbb{L}$ se, e somente se, $\{t\} \in \mathbb{L}$. Assim basta-nos mostrar que todo t entre 0 e 1 pode ser escrito na forma desejada. Como $t \in (0,1)$, podemos escrever sua expansão 2-ádica como $t = \sum_{n \geq 1} a_n \cdot 2^{-n}$, onde $a_n \in \{0,1\}$. Defina

$$\xi := \sum_{n \geq 1} \alpha_n \cdot 2^{-n} \quad \text{e} \quad \omega := \sum_{n \geq 1} \beta_n \cdot 2^{-n}$$

onde para $n! \leq k < (n+1)!$, temos

$$\begin{aligned} \alpha_k = a_k \text{ e } \beta_k = 0 \quad \text{se} \quad n = 1, 3, 5, \ldots \\ \beta_k = a_k \text{ e } \alpha_k = 0 \quad \text{se} \quad n = 2, 4, 6, \ldots \end{aligned}$$

Agora, resta-nos mostrar que ξ e ω são números de Liouville. Faremos a demonstração apenas para ξ (o caso ω é análogo). Dado $n \geq 1$, seja $q_n := 2^{(2n)!-1}$ e $p_n := q_n(\alpha_1 2^{-1} + \ldots + \alpha_{(2n)!-1} 2^{-(2n)!+1})$. Assim

$$\xi - \frac{p_n}{q_n} = \sum_{m \geq 1} \alpha_m 2^{-m} - \sum_{m=1}^{(2n)!-1} \alpha_m 2^{-m} = \sum_{m \geq (2n)!} \alpha_m 2^{-m} \tag{3.4}$$

Como $\alpha_m = 0$ para $(2n)! \leq m < (2n+1)!$, podemos reescrever a igualdade em (3.4) como

$$\left| \xi - \frac{p_n}{q_n} \right| = \sum_{m \geq (2n+1)!} \alpha_m 2^{-m} \leq \sum_{m \geq (2n+1)!} 2^{-m} = 2^{-(2n+1)!+1} < 2^{-n[(2n)!-1]} = \frac{1}{q_n^n}.$$

Portanto ξ é número de Liouville. □

Exemplo 8. Em 1953, LeVeque [7] provou que, para todo $m \geq 1$ e $\ell = \sum_{n=1}^{\infty} 10^{-n!}$ (ℓ é a constante de Liouville), tem-se que $\sqrt[m]{\dfrac{3+\ell}{4}}$ é um U_m-*número.*

Observação. Denotamos por ω_n^* como o supremo do número real ω^* para o qual existem infinitos números algébricos reais α de grau n satisfazendo

$$0 < |\xi - \alpha| < \mathcal{H}()^{-\omega^*-1},$$

onde $\mathcal{H}()$ (a chamada altura de α) é o máximo de valores absolutos de coeficientes do polinômio mínimo de α. O número ξ é dito ser U_m^*-número (de acordo com LeVeque [7]) se ${}_m^*(\xi) = \infty$ e ${}_n^*(\xi) = \infty$ para $1 \leq n < m$ (m é chamado de tipo do U-número). Nós apontamos que nós realmente definimos um koksma U_m^*-número ao invés de um Mahler U_m-número. No entanto, é bem conhecido que eles são os mesmos [12].

Exemplo 9. Usando o método de Gütting [5] podemos encontrar U_m-números explícitos de uma maneira mais natural: Pelo produto de algum número algébrico de grau m pela constante de Liouville. Além disso, obtemos um limite superior para ω_n^*, com $1 \leq n < m$. Vejamos:

Teorema 14. *Seja α um número algébrico de grau m. Suponha que o polinômio minimal P de α tem coeficiente líder da forma $2^a \cdot 5^b > 1$ e $p \nmid P(0)$, para $p = 2, 5$, e sendo ℓ a constante de Liouville. Então $\alpha\ell$ é um U_m-número, com*

$$\omega_n^*(\alpha\ell) \leq 2m^2n + m - 1, \quad \text{para } n = 1, \ldots, m-1. \tag{3.5}$$

Por exemplo, $\sqrt[m]{\dfrac{3}{2}} \cdot \ell$ é um U_m-número para todo $m \geq 1$.

Antes da demonstração deste teorema, dois resultados técnicos são necessários.

Lema 3. *Dado $P(x) \in \mathbb{Z}[x]$ com grau m e $\dfrac{a}{b} \in \mathbb{Q}^*$. Se $Q(x) = a^m P\left(\dfrac{bx}{a}\right)$, então*

$$\mathcal{H}(Q) \leq \max\{|a|, |b|\}^m \mathcal{H}(P),$$

onde, $\mathcal{H}(P)$ á a altura de P.

Demonstração. Se $P(x) = \sum_{j=0}^{m} a_j x^j$, então $Q(x) = \sum_{j=0}^{m} a_j b^j a^{m-j} x^j$. Supondo, sem perda de generalização, que $|a| \geq |b|$, temos $|a|^m |a_j| \geq |a|^{m-j} |a_j| |b|^j$ para $0 \leq j \leq m$. Portanto o lema está provado. $\square$

Além deste lema, usamos o fato de que números algébricos não são bem aproximados por números algébricos.

Lema 4 (Cf Corolário A.2 de [2])**.** *Sejam α e β dois números algébricos, não nulos, distintos de graus n e m, respectivamente. Então nós temos*

$$|\alpha - \beta| \geq (n+1)^{-\frac{m}{2}} (m+1)^{-\frac{n}{2}} \max\left\{ \frac{(n+1)^{-\frac{m-1}{2}}}{2^{-n}}, \frac{(m+1)^{-\frac{n-1}{2}}}{2^{-m}} \right\} \times H(\alpha)^{-m} H(\beta)^{-n}.$$

Demonstração. Um esboço da prova pode ser encontrado no apêndice a do [2]. □

Demonstração. (do Teorema 14) Para $k \geq 1$, defina

$$p_k = 10^{k!}\sum_{j=1}^{k} 10^{-j}, \quad q_k = 10^{k!} \text{ e } \alpha_k = \frac{p_k}{q_k} = \sum_{j=1}^{k} 10^{-j}.$$

Observamos que $\mathcal{H}(\alpha_{k-1}) < \mathcal{H}(\alpha_k) = 10^{k!} = \mathcal{H}(\alpha_{k-1})^k$ e

$$|\ell - \alpha_k| < \frac{10}{9}\mathcal{H}(\alpha_k)^{-k-1}. \tag{3.6}$$

Assim, definindo $y_k = \alpha\alpha_k$, obtemos de (3.6)

$$|\alpha\ell - y_k| \leq c\mathcal{H}(\alpha_k)^{-k-1}. \tag{3.7}$$

onde $c = \dfrac{10|\alpha|}{9}$. Segue-se Lema 3 que $\mathcal{H}(\alpha_k)^m \geq \mathcal{H}(\alpha)^{-1}\mathcal{H}(y_k)$ e assim concluímos que

$$|\alpha\ell - y_k| \leq c\mathcal{H}(\alpha_k)^{\frac{k+1}{m}}\mathcal{H}(y_k)^{-\frac{k+1}{m}} \tag{3.8}$$

Consequentemente, $\alpha\ell$ é um U-número do tipo no máximo m (desde y_k tem grau m).

Nós reivindicamos que $\mathcal{H}(\alpha_k) \leq \mathcal{H}(y_k)$, para todo $k \geq 1$. De fato, seja $P(x) = \sum_{j=0}^{m} a_j x^j$ o polinômio minimal de α. Em particular, $P(\alpha) = 0$ e um cálculo simples dá $Q(y_k) = 0$, onde $Q(x) = \sum_{j=1}^{m} a_j p_k^{m-j} q_k^j x^j \in \mathbb{Z}[x]$. Note que $\partial\mathcal{Q} = m$ e y_k é um número algébrico de grau m. Assim, para provar que Q é o polinômio mínimo de y_k, precisamos provar que Q é primitivo. Em outras palavras, devemos provar que

$$\partial(a_0 p_k^m, a_1 p_k^{m-1} q_k, \ldots, a_m q_k^m) = 1.$$

Isto segue imediatamente dos fatos que $\partial(a_0, \ldots, a_m) = 1$ e as hipóteses em a_0 em a_m (rendendo $\partial(a_0, q_k) = \partial(a_m, p_k) = 1$), nós deixamos os detalhes para o leitor. Assim, em particular, devemos provar que

$$\mathcal{H}(y_k) \geq \max\{|a_0||p_k|^n, |a_n||q_k|^n\} \geq \max\{|p_k|, |q_k|\} = \mathcal{H}(\alpha_k)$$

como desejado.

Agora usamos isso junto com o Lema 3 para obter

$$\mathcal{H}(y_{k+1}) \leq \mathcal{H}(\alpha)\mathcal{H}(\alpha_{k+1})^m = \mathcal{H}(\alpha)\mathcal{H}(\alpha_k)^{(k+1)m} \leq \mathcal{H}(\alpha)\mathcal{H}(y_k)^{(k+1)m}. \tag{3.9}$$

Agora, seja y um número algébrico real de grau n, com $n < m$ e $\mathcal{H}(y) \geq \mathcal{H}(y_1)$. Assim, existe um k suficientemente grande tal que

$$\mathcal{H}(y_k) < \mathcal{H}(y)^{2m^2} < \mathcal{H}(y_{k+1}) \leq \mathcal{H}(\alpha)\mathcal{H}(y_k)^{(k+1)m} \tag{3.10}$$

Por outro lado, o Lema 4 produz

$$|y_k - y| \geq f(m,n)\mathcal{H}(y)^{-m}\mathcal{H}(y_k)^{-n} \tag{3.11}$$

Onde $f(m,n)$ é um número positivo que não depende de k e y (veja o Lema 4). Portanto, pela cadeia de desigualdades na (3.10)

$$|y_k - y| \geq f(m,n)\mathcal{H}(\alpha)^{-\frac{1}{2m}}\mathcal{H}(y_k)^{-\frac{k+1}{2-n}} \tag{3.12}$$

Tomando $\mathcal{H}(y)$ grande o suficiente, o índice k satisfaz

$$\mathcal{H}(y_k)^{\frac{k+1}{2-n}} \geq 2cf(m,n)^{-1}\mathcal{H}(\alpha)^{\frac{k+1}{2m}} \tag{3.13}$$

Assim (3.8), (3.12) e (3.13) produzem $|y_k - y| \geq 2|\alpha\ell - y_k|$. Portanto, exceto para muitos números algébricos y, de grau n estritamente menor do que m, temos

$$\begin{aligned} |\alpha\ell - y| \geq |y_k - y| - |\alpha\ell - y_k| \quad &\geq \quad \frac{1}{2}|y_k - y| \geq \frac{f(m,n)}{2}\mathcal{H}(y)^{-m}\mathcal{H}(y_k)^{-n} \\ &> \quad \frac{f(m,n)}{2}\mathcal{H}(y)^{-2m^2n-m}, \end{aligned}$$

onde usamos o lado esquerdo de (3.10). Em conclusão, $\alpha\ell$ é um U_m-número com $\omega_n^*(\alpha\ell) \leq 2m^2n + m - 1$. Isso finaliza essa demonstração. □

3.3 As Classes dos A, S e T-Números

A classe dos *A-números* corresponde ao conjunto dos números algébricos. Portanto, todo número algébrico é um *A-número.*

Em 1929, Popkent [15] provou que para $n \in \mathbb{N}$ existe uma constante positiva $C = C(n)$, tal que

$$|P(e)| \geq H^{-n-C(\log(\log(H)))}$$

para todo $P(z) \in \mathbb{Z}[z]$ de grau n e altura H suficiente grande. Segue que e é *S-números.*

No mesmo artigo em que apresentou sua classificação, Mahler [8] refinou o resultado de Popken, mostrando que a constante C (que depende de n) pode ser tomada como $C = cn^2\log(n)$, onde $c > 0$ é uma constante absoluta (isto é, não depende de nenhum parâmetro). Nesse mesmo artigo, foi provado que e^α é S-número para todo $\alpha \in \overline{\mathbb{Q}}^*$. Mahler [9] ainda provou que π e $\log(\alpha)$ não são *U-número*, para $\alpha \in \overline{\mathbb{Q}}^*$.

Em 1970, W. Shmidt [16] provou a existência dos *T-números*, mas sem explicar nenhum exemplo. Até hoje não existe nenhuma amostra dessa classe de números.

Uma das consequências mais fortes da classificação de Mahler é que dois números algebricamente dependentes devem pertencer a mesma classe. Em outras palavras:

Sejam ξ e ζ números transcendentes que pertencem à classes diferentes (na classificação de Mahler) e $F(x, y) \in \overline{\mathbb{Q}}[x, y]$ um polinômio não constante. Então $F(\xi, \zeta)$ é transcendente.

Na verdade, satisfazer essa propriedade é um pré-requisito para que uma classificação dos números transcendentes seja considerada "interessante".

Em poucas palavras, a ideia para a demonstração desse fato, é supor que ξ e ζ são algebricamente dependentes, logo existe um polinômio não nulo $\mathcal{Q}(x, y) \in \mathbb{Z}[x, y]$ satisfazendo $\mathcal{Q}(\xi, \zeta) = 0$. Com isso, deve-se mostrar que ξ e ζ possuem as mesmas propriedades em relação a aproximação diofantina.

Capítulo 4

Quadratura do Círculo: Uma Proposta Didática Para o Ensino Médio

Uma proposta didática para o ensino médio seria estudar o problema da quadratura do círculo em meio aos conteúdos de geometria plana no currículo de matemática. Nesse contexto, ainda seria possível abordar noções básicas de números transcendentes, além de quadrar algumas figural planas.

4.1 Quadratura do Círculo

A quadratura do círculo é um problema proposto pelos antigos matemáticos gregos consistindo em construir um quadrado com a mesma área de um dado círculo servindo-se somente de uma régua e compasso em um número finito de etapas.

Como vimos, *Ferdinand Lindemann*, em 1882, provou que π é um número transcendente, isto é, não existe um polinômio com coeficientes inteiros ou racionais não todos nulos dos quais π seja raiz.

A transcendência de π estabelece a impossibilidade de se resolver o problema da quadratura do círculo, ou seja, é impossível construir, somente com régua e compasso, um quadrado cuja área seja rigorosamente igual à área de um determinado círculo.

A ação de quadrar (transformar uma figura em um quadrado de mesma área) é bem antiga, pois os gregos já sabiam quadrar vários polígonos.

A seguir veremos dois bons exemplos sobre a ação de quadrar: A quadratura do retângulo e a do triângulo. Contudo, para demonstrar que é possível quadrar qualquer polígono, basta mostrar que um polígono de n lados pode ser transformado em um polígono equivalente de $n-1$ lados. No entanto, não é possível quadrar a mais simples das figuras curvilíneas, o círculo, como pensavam os antigos matemáticos gregos. [13].

Exemplo 10. Para realizar a quadratura de um determinado retângulo, pode ser feito o seguinte procedimento:

1. Seja ABCD o retângulo dado. Faça uma circunferência com centro em D e raio CD.
2. Prolongue o seguimento AD interceptando a circunferência em um ponto N.
3. Determine o ponto médio M do seguimento AN.
4. Faça uma circunferência com centro M e raio AM.
5. Trace a perpendicular a AM por D e marque o ponto E na intersecção com a circunferência maior.
6. Construa um quadrado sobre o seguimento DE. Este quadrado terá a mesma área do retângulo ABCD.

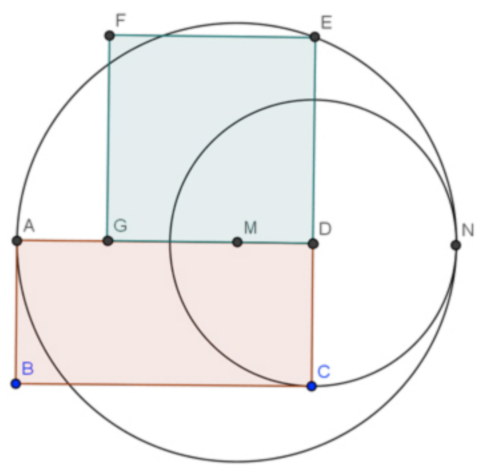

Figura 4.1: Quadratura de um Retângulo

Vejamos: a área do retângulo é dada por:

$$A_{\text{retângulo}} = AD \cdot DC = AD \cdot DN.$$

Da figura, temos:

$$\begin{aligned} AD &= AM + MD \\ DN &= MN - MD = AM - MD \end{aligned}$$

Assim:

$$A_{\text{retângulo}} = AD \cdot DN = (AM + MD) \cdot (AM - MD) = (AM)^2 - (MD)^2.$$

Do triângulo retângulo MDE, temos que:

$$(ME)^2 = (MD)^2 + (DE)^2$$

Mas $ME = AM$, logo:

$$A_{\text{retângulo}} = (AM)^2 - (MD)^2 = (MD)^2 + (DE)^2 - (MD)^2 = (DE)^2 = A_{\text{quadrado}}.$$

Como a área do quadrado $DEFG$ é dada por $(DE)^2$, temos que

$$A_{\text{retângulo}} = A_{\text{quadrado}}.$$

Exemplo 11. Para a quadratura de um triângulo, primeiro o transformamos em um retângulo e depois procedemos como na construção acima.

1. 1. Seja ABC o triângulo dado. Trace sua altura CK e encontre o ponto médio M desde segmento, como na Figura 4.2.

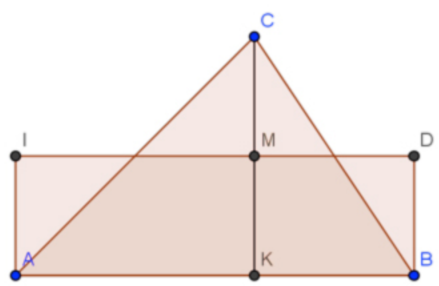

Figura 4.2: Quadratura de um Triângulo - Parte 1

2. Construa o retângulo $ABDI$ com base AB passando por M. Este retângulo $ABDI$ possui mesma área que o triângulo ABC. De fato,

$$A_{\text{triângulo}} = \frac{b \cdot h}{2} = \frac{AB \cdot CK}{2} = AB \cdot MK = A_{\text{retângulo}}.$$

A partir do retângulo, $ABDI$, gerado, podemos construir um quadrado com a mesma área desse retângulo (como vimos no exemplo anterior) e que, consequente, tem a mesma área do triângulo ABC dado.

Agora, análogo à quadratura do retângulo, fazemos:

$$A_{\text{retângulo}} = AB \cdot MK = ID \cdot DN.$$

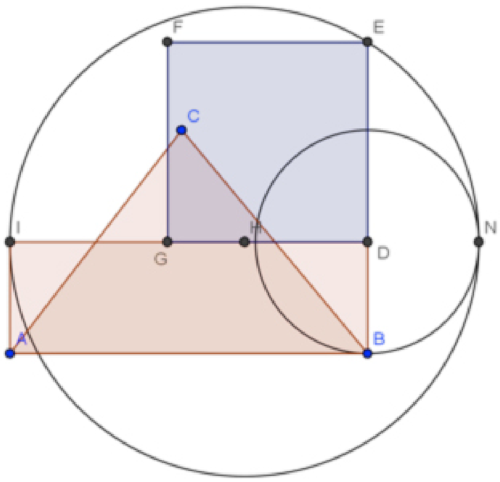

Figura 4.3: Quadratura de um Triângulo - Parte 2

Da Figura 4.3, temos:

$$\begin{aligned} ID &= IH + HD \\ DN &= HN - HD = IH - HD. \end{aligned}$$

Assim:

$$A_{\text{retângulo}} = ID \cdot DB = ID \cdot DN = (IH + HD) \cdot (IH - HD) = (IH)^2 - (HD)^2. \tag{4.1}$$

Do triângulo retângulo HDE, temos que:

$$(HE)^2 = (HD)^2 + (DE)^2.$$

Mas $HE = IH$, (raio) logo:

$$(IH)^2 = (HD)^2 + (DE)^2$$

De (4.1),

$$A_{\text{retângulo}} = (IH)^2 - (HD)^2 = (HD)^2 + (DE)^2 - (HD)^2 = (DE)^2 = A_{\text{quadrado}}.$$

Como a área do quadrado $DEFG$ é dada por $(DE)^2$, temos que

$$A_{\text{retângulo}} = A_{\text{quadrado}}.$$

Assim,

$$A_{\text{triângulo}} = A_{\text{retângulo}} = A_{\text{quadrado}}$$

Portanto, por transitividade,

$$A_{\text{triângulo}} = A_{\text{quadrado}}.$$

Referências Bibliográficas

[1] BUGEAUD, Y. *Approximation by algebraic Numbers, Cambridge Tracts in Mathematics*, Vol 160, Cambridge University Press, New York (2004).

[2] ENDLER, O. *Teoria dos números algébricos*, Vol. 15. Instituto de Matemática Pura e Aplicada, CNPq (1986). 4, 3.2

[3] ERDÖ S, P. *Representations of real number as sums and products of Liouville numbers*, Michigan Math. J. 9, 59-60 (1962).

[4] FIGUEIREDO, Djairo Guedes de. *Números Irracionais e Transcendentes*, Rio de Janeiro: Publicação da Sociedade Brasileira de Matemática (SBM). Coleção Iniciação Científica 3^a Ed. (2011). (document), 1.1, 2, 2.1, 2.2, 2.3, 2.4

[5] GÜTTING, R. *Zur Berechnung der Mahlerschen Funktionen* $_n$, J. Reine Angew. Math. 232, 122-135 (1968). 9

[6] HAVIL, J. *Gama: Explorando a Constante de Euler.* Princeton, New Jersey: Princeton University Press. pp. 37-42 (Capítulo 4). ISBN 0-691-09983-9, (2003). 2.1

[7] LEVEQUE, W. J. *On Mahler's U-números*, J. of the London Math. Soc28 (1953) 220-229. 8, 3.2

[8] MAHLER, K. *Zur Aproximathion der Exponentialfunktionen und des Logarithmus*, I, II. J. reine angew. Math., 166, (1932) 118-150. (document), 2.2, 3.3

[9] MAHLER, k. *On the Aproximation of* π. Proc. Akad. Wenyensch. Ser. A. 56 (1953), 30-42. (document), 2.2, 3.3

[10] MAHLER, K. *On the Aproximation of logarithms of algebraic numbers.* Philos. Trans. Roy. Soc. London. Ser. A, 245 (1953) 371-398. (document), 2.2

[11] MARQUES, D. *Teoria dos números transcendentes.* SBM (2013). (document), 2.1, 2.1

[12] MARQUES, D. e SONDOW, J. *Schanuel conjecture and the algebraic powrs z^w and w^z with z and w transcendental.* East-West Journal Mathematics, 12 (2010) 75-84. 3.2

[13] MEES, Jociane. *Duplicação, trissecação e quadratura.* Trabalho de conclusão de curso. Santa Catarina, 1999. Disponível em `http://repositorio.ufsc.br/xmlui/handle/123456789/97040` (document), 4.1

[14] OTTO ENDLER, Teoria dos Números Algébricos. Imos Gráficos e Editora.

[15] POPKENT, J. *Zur Transzendenz von e*. Math. Z., 29 (1929) 525-541. 3.3

[16] SCHMIDT, W. *T-numbers do exist*, Symposia Math. 6 (1970) 3-26. [16] RIBENBOIM, P. (2000) My Number, My Frieds: Popular Lectures on Number Theory. Springer-Verlag. 3.3

[17] RIBENBOIM, P. *My Number, My Frieds: Popular Lectures on Number Theory.* Springer-Verlag. (2000).