UNIVERSIDADE FEDERAL DE SANTA CATARINA

RICARDO EMANUEL MUELLER

NÚMEROS DE LIOUVILLE

Blumenau

2018

Ricardo Emanuel Mueller

NÚMEROS DE LIOUVILLE

Trabalho de Conclusão de Curso submetido ao Curso de Licenciatura em Matemática da Universidade Federal de Santa Catarina para a obtenção do Grau de Licenciado em Matemática.

Orientador: Prof. Dr. Felipe Vieira

Blumenau

2018

Catalogação na fonte pela Biblioteca Universitária da Universidade Federal de Santa Catarina.

Arquivo compilado às 17:53h do dia 28 de novembro de 2018.

Ricardo Emanuel Mueller
Números de Liouville : / Ricardo Emanuel Mueller; Orientador, Prof. Dr. Felipe Vieira; , - Blumenau, 17:53, 28 de novembro de 2018.
67 p.

Trabalho de Conclusão de Curso - Universidade Federal de Santa Catarina, Departamento de Matemática (MAT), Centro de Blumenau, Curso de Licenciatura em Matemática.

Inclui referências

1. Aproximações Diofantinas. 2. Enumerabilidade. 3. Números Algébricos. 4. Números de Liouville. 5. Números Transcendentes. I. Prof. Dr. Felipe Vieira II. III. Curso de Licenciatura em Matemática IV. Números de Liouville

CDU 02:141:005.7

Ricardo Emanuel Mueller

NÚMEROS DE LIOUVILLE

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Licenciado em Matemática, e aprovado em sua forma final pelo Curso de Licenciatura em Matemática do Departamento de Matemática (MAT), Centro de Blumenau da Universidade Federal de Santa Catarina.

Blumenau, 28 de novembro de 2018.

Prof. Dr. André Vanderlinde da Silva
Coordenador do Curso de Licenciatura em Matemática

Banca Examinadora:

Prof. Dr. Felipe Vieira
Orientador
Universidade Federal de Santa Catarina – UFSC

Prof. Dr. Jorge Luiz Deolindo Silva
Universidade Federal de Santa Catarina – UFSC

Prof. Dr. Rafael Aleixo de Carvalho
Universidade Federal de Santa Catarina – UFSC

Este trabalho é dedicado a todos que um dia se interessaram pela natureza dos números.

AGRADECIMENTOS

Primeiramente, agradeço aos meus pais, Denise e Douglas, pelo imenso carinho e apoio. Seria impossível concluir esta etapa da minha vida sem vocês.

Agradeço aos meus demais familiares pela presença em momentos importantes e por sempre acreditarem em mim.

Agradeço também aos professores da UFSC, campus Blumenau. Em especial, meu orientador, o Prof. Dr. Felipe Vieira, por suas sugestões, bem como por acreditar neste projeto desde o início.

Fica aqui minha nota de agradecimento aos meus colegas de curso. Esta parte ficaria demasiadamente extensa caso citasse cada um de vocês. No entanto, gostaria de agradecer meu amigo Fábio, particularmente, por suas precisas observações.

"You work for a long period of time and the results don't really show, but at some point everything just comes together and you start to play better, or get more confidence."

Fabiano Caruana

RESUMO

Este trabalho apresenta uma introdução à teoria dos números transcendentes. O objetivo é abordar o tema de modo que seja compreensível para alunos que estão cursando uma graduação em matemática. Assim, inicialmente, são discutidos os conceitos de número algébrico, número transcendente, enumerabilidade e aproximações diofantinas. Isto forma a base necessária para a assimilação dos primeiros números transcendentes descobertos, os números de Liouville.

Palavras-chaves: Aproximações Diofantinas. Enumerabilidade. Números Algébricos. Números de Liouville. Números Transcendentes.

ABSTRACT

This monography presents an introduction to the transcendental number theory. The purpose is to approach the theme in such a way that it would be comprehesive for undergraduate students in mathematics. Therefore, initially, discuss the concepts of algebraic numbers, transcendental numbers, enumerability and diofantine approximations. These concepts compose the basis necessary to comprehend the first transcendental numbers discovered, namely the Liouville's numbers.

Keywords: Diophantine Approximations. Enumerability. Algebraic Numbers. Liouville's Numbers. Transcendental Numbers.

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais.
$\mathbb{N}_n$	Conjunto dos números naturais menores ou iguais à n.
$\mathbb{P}$	Conjunto dos números primos.
$\mathbb{Z}$	Conjunto dos números inteiros.
$\mathbb{Q}$	Conjunto dos números racionais.
$\mathbb{R}$	Conjunto dos números reais.
(a, b)	Intervalo aberto de a até b, isto é, para $a, b \in \mathbb{R}$ tem-se que $(a, b) = \{x \in \mathbb{R} : a < x < b\}$.
$[a, b]$	Intervalo fechado de a até b, isto é, para $a, b \in \mathbb{R}$ tem-se que $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$.
$\mathbb{C}$	Conjunto dos números complexos.
$\overline{\mathbb{Q}}$	Conjunto dos números algébricos.
$\overline{\Psi}$	Conjunto dos números transcendentes.
$\mathbb{L}$	Conjunto dos números de Liouville.
$\mathbb{Z}[x]$	Conjunto dos polinômios de variável x e com coeficientes inteiros.
A_+	Conjunto formado pelos elementos não negativos de A.
A^*	Conjunto formado pelos elementos não nulos de A.
$(A, +, \times)$	Conjunto A munido com as operações + e $\times$.
$X \times Y$	Conjunto formado pelo produto cartesiano entre X e Y, ou seja, $X \times Y = \{(x, y) : x \in X, y \in Y\}$.

$\mathrm{Im}(f)$	Imagem da função $f : A \longrightarrow B$. Define-se como $\mathrm{Im}(f) = \{y \in B : \exists x \in A, f(x) = y\}$.
$g \circ f$	Composição da função $f : A \longrightarrow B$ com a função $g : B \longrightarrow C$, ou seja, é o conjunto $$\{(x, z) \in A \times C : \exists y \in B, (x, y) \in f \wedge (y, z) \in g\}.$$
$f'(x)$	Derivada primeira da função f em relação a x.
$\det(A)$	Determinante da matriz A.
$\lvert a \rvert$	Valor absoluto de a. Se $a \geq 0$ tem-se que $\lvert a \rvert = a$. Caso $a < 0$, $\lvert a \rvert = -a$.
$\sum_{i=1}^{n} a_i$	Somatório. Soma dos a_i, onde i varia entre os números naturais, a partir de 1 até n, ou seja, tem-se que $\sum_{i=1}^{n} a_i = (a_1 + a_2 + \ldots + a_n)$.
$\prod_{i=1}^{n} a_i$	Produtório. Produto dos a_i, onde i varia entre os números naturais, a partir de 1 até n, ou seja, tem-se que $\prod_{i=1}^{n} a_i = (a_1 \cdot a_2 \cdot \ldots \cdot a_n)$.

SUMÁRIO

1 INTRODUÇÃO

Esta monografia é um estudo sobre números transcendentes. A partir de um ponto de vista, algo une os números transcendentes com números racionais, naturais, reais e complexos. Este elo é a constatação de que todos são conjuntos numéricos. Mas, por que um conjunto recebe a denominação tão especial de transcendente? Ora, esta nomeação é comumente atribuída a Leonhard Euler, um prolífico matemático que viveu no século XVIII. Acredita-se que tal nomenclatura venha da ideia de que tais números não podem ser zerados através de operações algébricas envolvendo números inteiros. Entretanto, Euler não conseguiu dar um exemplo e nem sequer mostrou que existem números transcendentes. Em 1851 é que foram dados os primeiros exemplos decimais, por Joseph Liouville. Estes primeiros números provados transcendentes foram chamados de números de Liouville.

No Capítulo 2 são apresentadas as definições de números algébricos e transcendentes. Na sequência, é exposto o conceito de enumerabilidade, desenvolvido por Georg Cantor para "contar" os elementos de um conjunto. Um dos resultados mais importantes dele foi a demonstração de que não é possível "contar" os elementos do conjunto dos números reais. Entretanto, mais surpreendente que isto é o fato do conjunto dos números transcendentes também não ser "contável", e este é um dos principais resultados do Capítulo 2. Além disso, como os números algébricos formam um corpo, é possível o estudo de algumas propriedades envolvendo números transcendentes, mesmo sem provar que determinado número é transcendente. Tais propriedades servem de fechamento deste capítulo. O Capítulo 2 foi escrito, em grande parte, com base em [6], [3] e [7].

O Capítulo 3 trata de aproximações diofantinas. Mais especificamente, apresenta modos de aproximar números irracionais por meio de números racionais. A justificativa da existência deste capítulo no trabalho é a possível dificuldade em entender a definição de número de Liouville, bem como as demonstrações envolvidas. Inclusive, historicamente sabe-se que os próprios números de Liouville surgiram após analisar o que seria um número "bem aproximado" por racionais. Para a construção do Capítulo 3, foram utilizadas, principalmente, as referências [9] e [8].

No Capítulo 4, [7] foi utilizado como principal referência. Este capítulo é o ápice do trabalho, uma vez que o leitor tem contato com a primeira prova de que alguns números são transcendentes, no caso fala-se sobre os números de Liouville. Novamente, no fechamento são apresentadas propriedades envolvendo tais números.

Por fim, para melhor aproveitamento da obra, recomenda-se que o leitor tenha domínio em fundamentos de aritmética, estruturas algébricas, teoria dos conjuntos, álgebra linear e análise real.

2 NÚMEROS ALGÉBRICOS E TRANSCENDENTES

No início deste capítulo serão apresentados os números algébricos e transcendentes. Na sequência, a intenção é apresentar algumas propriedades envolvendo os números transcendentes, assim como familiarizar o leitor com a álgebra destes números, uma vez que os números de Liouville surgiram da necessidade de mostrar como é a "forma" de um número transcendente.

2.1 UMA BREVE HISTÓRIA DOS NÚMEROS TRANSCENDENTES

Em 1768 Johann Heinrich Lambert havia conjecturado que os números reais e e π eram transcendentes, entretanto a transcendência destes números só foi demonstrada, respectivamente, em 1873 (Charles Hermite) e 1882 (Ferdinand Von Lindemann). Somente em 1844, Joseph Liouville provou a existência de números transcendentes, bem como em 1851 apresentou os primeiros exemplos numéricos.

2.2 DEFINIÇÕES PRELIMINARES

Definição 2.1. Chamamos de *número algébrico* qualquer $x \in \mathbb{C}$ tal que x é solução de uma equação polinomial com coeficientes inteiros, ou seja, x é raiz de um polinômio $P(x)$, não nulo, da forma

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

com $a_n, a_{n-1} \ldots, a_1, a_0 \in \mathbb{Z}$.

Usamos $\overline{\mathbb{Q}}$ para denotar o conjunto dos números algébricos.

Observação 1. Existe uma maneira diferente de enunciar esta definição. Para isto, considera-se $L|K$ uma extensão de corpos (veja com mais detalhes no Capítulo 4 de [7]). De modo mais geral, pode-se definir que um $\alpha \in L$ é um número algébrico sobre K, quando para algum $P \in K[x]$ tem-se que $P(\alpha) = 0$. Entretanto, para este trabalho, irá ser utilizada somente a primeira definição, uma vez que é o suficiente para a apresentação do conteúdo.

Definição 2.2. Um número é denominado *transcendente* quando ele pertencer a $\mathbb{C}$, mas não for algébrico. O conjunto cujos elementos são todos os números transcendentes será denotado por $\overline{\Psi}$.

Observação 2. Segundo esta definição, perceba que $\mathbb{C} = \overline{\Psi} \cup \overline{\mathbb{Q}}$, ou seja, $\mathbb{C} = \overline{\Psi} \cup \overline{\mathbb{Q}}$ é uma cisão de $\mathbb{C}$. Ademais, números transcendentes não são raízes de polinômios em $\mathbb{Z}[x]$.

2.2.1 Alguns exemplos

Exemplo 2.2.1. Dado $\alpha \in \mathbb{Z}$, considere a seguinte equação polinomial:

$$x - \alpha = 0.$$

Assim, temos que α é raiz do polinômio $P(x) = x - \alpha$. Portanto, segue que todo número inteiro é também algébrico.

Exemplo 2.2.2. Agora considere $\beta \in \mathbb{Q}$, então β pode ser reescrito como $\frac{p}{q}$ com $p, q \in \mathbb{Z}$ e $q \neq 0$. Assim, perceba que β é raiz do seguinte polinômio com coeficientes inteiros:

$$P(x) = qx - p.$$

Portanto, todo número racional é algébrico. Deste modo, todo número transcendente deve ser irracional.

Observação 3. De agora em diante, será assumido, sem perda de generalidade, que $\frac{p}{q} \in \mathbb{Q}$, com $p, q \in \mathbb{Z}$, terá sempre $q > 0$.

Exemplo 2.2.3. Seja $c \in \mathbb{C}$, com c da forma $\sqrt[n]{a}$, para $a \in \mathbb{Z}$ e $n \in \mathbb{N}$. Observe que $\sqrt[n]{a}$ é solução da seguinte equação:

$$x^n - a = 0.$$

Logo, nem todo irracional é transcendente.

Exemplo 2.2.4. O número de ouro $\phi = \frac{1+\sqrt{5}}{2}$ é algébrico, pois

$$\begin{aligned}\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1+\sqrt{5}}{2}\right) - 1 &= \frac{1+2\sqrt{5}+5}{4} - \left(\frac{2+2\sqrt{5}}{4}\right) - \frac{4}{4} \\ &= \frac{0}{4} \\ &= 0.\end{aligned}$$

Portanto, ϕ é raiz do polinômio $P(x) = x^2 - x - 1$.

Exemplo 2.2.5. Em [11] são expostos alguns exemplos de números transcendentes, como: e, π, e^{π}, $2^{\sqrt{2}}$, $\ln 2$, $sen(1)$.

Destaca-se aqui a facilidade de encontrar números algébricos. Por meio de poucos exemplos foi possível dizer que os números racionais e que o conjunto das raízes quadradas de naturais são formados somente por números algébricos. Entretanto, é relativamente mais complexo estabelecer um conjunto com infinitos elementos e todos transcendentes. Isto leva à próxima seção, onde será discutido como contar elementos de um conjunto, ou seja, quer-se saber a quantidade de números transcendentes.

2.3 EXISTÊNCIA DOS NÚMEROS TRANSCENDENTES

Inicialmente faz-se necessário apresentar como, matematicamente, se dá o processo da contagem de elementos em um conjunto.

2.3.1 Enumerabilidade de conjuntos

Definição 2.3. Dado $n \in \mathbb{N}$, considere o conjunto

$$\mathbb{N}_n = \{x \in \mathbb{N} : 0 \leq x \leq n\}.$$

Temos que um conjunto F é *finito* quando é vazio ou caso exista uma função bijetora φ tal que $\varphi : \mathbb{N}_n \longrightarrow F$, para algum $n \in \mathbb{N}$. Caso essa bijeção não exista, dizemos que o conjunto é *infinito* ou que, simplesmente, o conjunto não é *finito*.

Assim, a grosso modo, quando se contam os elementos de um conjunto, na verdade se está construindo uma bijeção entre parte dos números naturais e o conjunto em questão. A seguir, segue um exemplo de como isto é feito.

Exemplo 2.3.1. O conjunto $A = \{0, 2, 4, 6\}$ é finito, pois temos

$$\begin{aligned} f : \mathbb{N}_3 &\longrightarrow A \\ x &\mapsto 2x. \end{aligned}$$

Com efeito, f é injetora, uma vez que para quaisquer $a, b \in A$, obtemos que $f(a) = f(b) \implies 2a = 2b$ e, pela lei do cancelamento em $\mathbb{N}$, $a = b$. Além disso, f é sobrejetora, pois dado $y \in A$, temos que $\frac{y}{2} \in \mathbb{N}_3$ (porque todo elemento de A é par menor ou igual que 6) e $f(\frac{y}{2}) = 2 \cdot \frac{y}{2} = y$. Portanto, f é bijetora e, consequentemente, A é um conjunto finito.

Neste caso, o conjunto A possui 4 elementos. De modo similar, quando existir a bijeção $f : \mathbb{N}_n \longrightarrow A$, para qualquer A, segue que A terá $n + 1$ elementos.

Os próximos objetos matemáticos apresentados serão relevantes principalmente para categorizar os conjuntos infinitos.

Informalmente, pode-se dizer que "existem conjuntos infinitos que são maiores que outros". Georg Cantor, em 1891, foi quem conduziu esta ideia, após mostrar que é impossível estabelecer uma injeção do conjunto dos números reais para o conjunto dos números naturais. Logo, é possível pensar que um conjunto deve ser maior que o outro. Este estudo parte do conceito de enumerabilidade de um conjunto.

Definição 2.4. Um conjunto E é denominado *enumerável* se, e somente se, existe uma função injetora $\varphi : E \longrightarrow \mathbb{N}$.

Caso o enunciado acima não seja verdadeiro para determinado conjunto, simplesmente dizemos que este conjunto é *não enumerável*.

Teorema 2.1. *Todo conjunto finito é enumerável.*

Demonstração. Considere B um conjunto finito. Então existe uma função bijetora $\varphi : \mathbb{N}_n \longrightarrow B$, para algum $n \in \mathbb{N}$. Uma vez que a função é bijetora, existe uma função inversa $\varphi^{-1} : B \longrightarrow \mathbb{N}_n$ também bijetora. Seguindo, tome a seguinte função:

$$\begin{aligned} g : \mathbb{N}_n &\longrightarrow \mathbb{N} \\ x &\mapsto x. \end{aligned}$$

Sabemos que esta função é injetora, pois dados $a, b \in \mathbb{N}_n$, segue que $f(a) = f(b) \implies a = b$. Como a composição de funções injetoras é uma função injetora, temos que a função $(g \circ \varphi^{-1})$ é injetora. Portanto, B é enumerável. ■

A seguir, quer-se apresentar o primeiro exemplo de conjunto infinito e enumerável. Assim, foi escolhido inicialmente o conjunto dos números primos para tal exemplo, tanto pela facilidade em construir uma função injetora com os números naturais, quanto pela beleza da demonstração de sua infinitude.

Teorema 2.2. *Existem infinitos números primos.*

Demonstração. Suponha, por absurdo, $n \in \mathbb{N}$ e o conjunto de todos os primos $\mathbb{P}_n = \{p_0, p_1, p_2 \ldots, p_n\}$. Assim, tome o número

$$T_{p+1} = \prod_{i=0}^{n} p_i + 1.$$

Note que, para dado $p_j \in \mathbb{P}_n$, segue que p_j divide $\prod_{i=0}^{n} p_i$. Então, pelo algoritmo da divisão, existe $q \in \mathbb{Z}$ tal que

$$\prod_{i=0}^{n} p_i = qp_j.$$

Logo, segue que

$$T_{p+1} = qp_j + 1.$$

Isso indica que T_{p+1} e p_j, para todo $j = 0, 1, \ldots, n$, são primos entre si. Mas perceba que se T_{p+1} é um número composto, temos que existe um primo que divide ele, pois $T_{p+1} > 1$. Isso implica que

$T_{p+1} \notin \mathbb{P}_n$ e que T_{p+1} é primo. O absurdo provém de supor que o conjunto dos números primos é finito. Portanto, existem infinitos números primos. ■

Exemplo 2.3.2. O conjunto dos números primos é enumerável.

Considere $\mathbb{P} = \{x \in \mathbb{N} : x \text{ é primo}\}$. Tome a função

$$\begin{aligned} \varphi : \mathbb{P} &\longrightarrow \mathbb{N} \\ x &\mapsto x. \end{aligned}$$

Como φ é injetora, segue que $\mathbb{P}$ é um conjunto infinito, mas enumerável.

Exemplo 2.3.3. O conjunto dos números pares é enumerável.

Considere $P = \{x \in \mathbb{Z} : 2|x\}$ o conjunto dos números pares. Observe a função

$$\begin{aligned} \varphi :\ P &\longrightarrow \mathbb{N} \\ x &\mapsto \begin{cases} x & \text{se } x \geq 0; \\ -x+1 & \text{se } x < 0. \end{cases} \end{aligned}$$

Perceba que esta função está bem definida, pois P é a união dos pares maiores ou iguais à zero com os pares menores que zero. Além disto, todo par positivo está em $\mathbb{N}$, bem como quando $x \leq 0$ segue que $-x + 1 \in \mathbb{N}$. Na sequência, perceba que a primeira parte da regra já discutimos em exemplos anteriores, é simples de verificar a injetividade. Para a segunda parte tome $\varphi(a) = \varphi(b)$, com $a, b \in P$ e negativos. Assim, $-a + 1 = -b + 1 \implies a = b$. Portanto a segunda parte é injetora também. Além disso, a primeira parte da função leva números pares à números pares, enquanto a segunda parte leva números pares à números ímpares. Logo, a imagem gerada pela primeira parte da função é disjunta da imagem gerada pela segunda parte. Portanto, φ é injetora e P enumerável.

Entretanto, isto não é o suficiente para contar-se o número de elementos do conjunto dos números transcendentes. Para tal, terão que ser utilizados resultados mais "fortes", conforme os enunciados à seguir.

Teorema 2.3. *Qualquer subconjunto de um conjunto enumerável é enumerável.*

Demonstração. Sejam X e Y conjuntos tais que $Y \subset X$ e X enumerável. Então existe uma função $\varphi : X \longrightarrow \mathbb{N}$ injetora. Agora, tome $\varphi|Y : Y \longrightarrow \mathbb{N}$. Como $\varphi|Y$ é uma restrição de φ, segue que $\varphi|Y$ é injetora também. Portanto, todo subconjunto de um conjunto enumerável é enumerável. ■

Teorema 2.4. *A união de dois conjuntos enumeráveis é um conjunto enumerável.*

Demonstração. Considere os conjuntos enumeráveis X e Y. Assim, existem funções injetoras $\varphi_1 : X \longrightarrow \mathbb{N}$ e $\varphi_2 : Y \longrightarrow \mathbb{N}$. Podemos restringir o contradomínio de modo a termos somente a imagem da função como contradomínio, tornando as funções bijetoras sem alterar a lei de formação. Assim, tome

$$\begin{aligned} Im(\varphi_1) &= \{a \in \mathbb{N} : \exists x \in X,\, \varphi_1(x) = a\}; \\ Im(\varphi_2) &= \{b \in \mathbb{N} : \exists y \in Y,\, \varphi_2(y) = b\}. \end{aligned}$$

Logo, obtemos as bijeções

$$\begin{aligned} \varphi_1 &: X \longrightarrow Im(\varphi_1); \\ \varphi_2 &: Y \longrightarrow Im(\varphi_2). \end{aligned}$$

Assim, podemos definir as seguintes funções:

$$\begin{aligned} \Phi_1 : Im(\varphi_1) &\longrightarrow \mathbb{N} \\ x &\mapsto 2x; \end{aligned} \qquad \begin{aligned} \Phi_2 : Im(\varphi_2) &\longrightarrow \mathbb{N} \\ x &\mapsto 2x+1. \end{aligned}$$

Veja que Φ_1 e Φ_2 são funções injetoras, pois dados $a_1, a_2 \in Im(\varphi_1)$, temos que $\Phi_1(a_1) = \Phi_1(a_2) \implies 2a_1 = 2a_2 \implies a_1 = a_2$. Por outro lado, para quaisquer $b_1, b_2 \in Im(\varphi_2)$ dados, note que obtemos $\Phi_2(b_1) = \Phi_2(b_2) \implies 2b_1 + 1 = 2b_2 + 1 \implies b_1 = b_2$. Note também que na imagem de Φ_1 temos só naturais pares, enquanto na imagem de Φ_2 só constam ímpares. Agora, como $X \cup Y = X \cup (Y - X)$, podemos definir a seguinte função por partes:

$$\begin{aligned} \varphi : X \cup Y &\longrightarrow \mathbb{N} \\ x &\mapsto \begin{cases} (\Phi_1 \circ \varphi_1)(x), & \text{se } x \in X; \\ (\Phi_2 \circ \varphi_2)(x), & \text{se } x \in (Y - X). \end{cases} \end{aligned}$$

Como a composição de funções injetoras é uma função injetora e as imagens de Φ_1 e Φ_2 são disjuntas, segue que φ é injetora. Por fim, conclui-se que $X \cup Y$ é enumerável. ■

Teorema 2.5. *A união enumerável de conjuntos enumeráveis é um conjunto enumerável.*

Demonstração. Considere $\mathbb{E}$ um conjunto enumerável cujos elementos são conjuntos enumeráveis. Como $\mathbb{E}$ é enumerável, temos que existe φ_0 tal que $\varphi_0 : \mathbb{E} \longrightarrow \mathbb{N}$ é injetora. Portanto, restringindo o contradomínio, obtemos $\varphi_1 : \mathbb{E} \longrightarrow Im(\varphi_0)$ bijetora. Assim, podemos definir a seguinte função:

$$\begin{aligned} \varphi_2 : Im(\varphi_1) &\longrightarrow \mathbb{N} \\ x &\mapsto 2^{x+1}. \end{aligned}$$

Esta função é injetora, pois para $a, b \in \mathbb{N}$ dados, obtemos que vale $2^{a+1} = 2^{b+1} \iff a = b$. Fazendo a composição, conseguimos $(\varphi_2 \circ \varphi_1)$ injetora. Agora, para cada $A_n \in \mathbb{E}$ temos uma função $\lambda_n : A_n \longrightarrow \mathbb{N}$ injetora. Assim, tome

$$\begin{aligned} \varphi_3 : \bigcup_{n=0}^{\infty} Im(\lambda_n) &\longrightarrow \mathbb{N} \\ x &\mapsto (\varphi_2 \circ \varphi_1)(A_n) \cdot 3^{x+1}, \end{aligned}$$

dado $x \in \lambda_n(A_n)$. Perceba que φ_3 é injetora, pois dados $a, b, y, z \in \mathbb{N}$ temos que $2^a 3^{y+1} = 2^b 3^{z+1} \iff y = z$ e $a = b$, pois 2 e 3 são primos entre si. Seguindo, considere a função injetora $(\varphi_3 \circ \lambda_n)$. Note que dados $A_p, A_q \in \mathbb{E}$, temos

$$Im(\varphi_3 \circ \lambda_p) \cap Im(\varphi_3 \circ \lambda_q) = \emptyset,$$

pois cada conjunto A_n é associado à um único $2^{x+1} \in \mathbb{N}$ e cada elemento de A_n é associado à um $2^{x_1+1} \cdot 3^{x_2+1} \in \mathbb{N}$. Assim, seja U o conjunto formado pela união de todos os elementos de $\mathbb{E}$ e defina $\varphi_4 : U \longrightarrow \mathbb{N}$, por partes, com a seguinte lei de formação:

$$x \in A_n \implies \varphi_4(x) = (\varphi_3 \circ \lambda_n)(x).$$

Mas, perceba que φ_4 pode não ser função caso existam $A_p, A_q \in \mathbb{E}$ tais que $A_p \cap A_q \neq \emptyset$, uma vez que existiria também x tal que $\varphi_4(x)$ é igual à dois ou mais números naturais. Todavia, isto não é problema, pois basta selecionarmos somente um único valor para $\varphi_4(x)$. Assim, teríamos uma função $\varphi_5 : U \longrightarrow \mathbb{N}$ injetora. Portanto, a união enumerável de conjuntos enumeráveis é um conjunto enumerável. ■

Teorema 2.6. *O conjunto dos números reais é não enumerável.*

Demonstração. Suponha, por absurdo, que $\mathbb{R}$ é enumerável. Assim, existe $f : \mathbb{R} \longrightarrow \mathbb{N}$ injetora. Como $Im(f) \subset \mathbb{N}$, segue que podemos criar uma lista dos números reais conforme sua associação com os naturais. Note também que $Im(f) \neq \emptyset$, pois $\mathbb{R}$ é um conjunto infinito (todos os números primos estão em $\mathbb{R}$). Assim, pelo princípio da boa ordenação e sem perda de generalidade, tome i_0 como menor elemento de $Im(f)$ e $r_0 \in \mathbb{R}$ o elemento associado à i_0. Perceba que $Im(f) - \{i_0\}$ também possui um menor elemento, que iremos chamar de i_1, associado à $r_1 \in \mathbb{R}$. Assim, sucessivamente, sempre retirando o menor elemento, podemos listar todos os números reais conforme do seguinte modo:

$$\begin{gathered} i_0 \leftarrow r_0 \\ i_1 \leftarrow r_1 \\ i_2 \leftarrow r_2 \\ i_3 \leftarrow r_3 \\ i_4 \leftarrow r_4 \\ \vdots \end{gathered}$$

Continuando, seja $a \in \mathbb{R}$. Na forma decimal temos que

$$a = a_0, a_1 a_2 a_3 \ldots$$

onde $a_0 \in \mathbb{Z}$ é a parte inteira de a e a_n, para $n \in \mathbb{N}^*$, os seus dígitos. Agora, considere a_0 diferente da parte inteira de r_0, a_1 diferente do primeiro dígito após a vírgula de r_1, a_2 diferente do segundo dígito após a vírgula de r_2, a_n diferente do n-ésimo dígito após a vírgula de r_n. Logo a é diferente de qualquer r_n listado. Mas todos os reais estão listados e $a \in \mathbb{R}$ não está. O absurdo é obtido após assumirmos que $\mathbb{R}$ é enumerável. Portanto, $\mathbb{R}$ é não enumerável. ■

2.3.2 Enumerabilidade para os conjuntos dos números algébricos e transcendentes

Uma opção para provar que um conjunto é não vazio seria mostrar um exemplo numérico. Entretanto, matematicamente, existem ferramentas que permitem mostrar que um conjunto é não vazio mesmo sem saber exemplificar um número pertencente a este conjunto. Para este segundo trabalho, seguiu-se esta segunda opção, e a ferramenta escolhida foi a enumerabilidade.

Teorema 2.7. *O conjunto dos números algébricos é enumerável.*

Demonstração. Dado um polinômio com coeficientes inteiros

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

sua *altura* é definida como

$$|P| = |a_n| + \ldots + |a_1| + |a_0| + n\,.$$

Sabemos pelo Teorema Fundamental da Álgebra que $P(x) = 0$ possui precisamente n raízes complexas. Por combinatória sabemos que o número de polinômios com coeficientes inteiros de uma altura dada é finito. Assim, o conjunto das raízes dos polinômios com uma determinada altura também é finito. Portanto, o conjunto de todas as raízes de todos os polinômios de todas as alturas é um conjunto enumerável, pois é a união de um conjunto enumerável de conjuntos finitos (Teorema 2.5). ■

Teorema 2.8. *O conjunto dos números transcendentes $\overline{\Psi}$ é não enumerável.*

Demonstração. Como $\overline{\mathbb{Q}}$ é enumerável, temos que $\overline{\mathbb{Q}} \cap \mathbb{R}$ é enumerável. Segue que $(\overline{\Psi} \cap \mathbb{R}) \cup (\overline{\mathbb{Q}} \cap \mathbb{R}) = \mathbb{R}$, pela lei do terceiro excluído. Como a união de dois conjuntos enumeráveis é um conjunto enumerável e $\mathbb{R}$ não é enumerável, temos que $\overline{\Psi} \cap \mathbb{R}$ é infinito e não enumerável. Portanto, existem números transcendentes. ■

O Teorema 2.8 é surpreendente. Quer dizer que mesmo excluindo todos os números racionais e todas as raízes (com qualquer índice natural maior que 0) de primos, por exemplo, ainda tem-se "uma quantidade maior de números" no conjunto, se comparado com o que foi retirado.

2.4 ALGUMAS PROPRIEDADES DOS NÚMEROS ALGÉBRICOS E TRANSCENDENTES

Nesta seção será apresentado que o conjunto dos números algébricos forma um corpo. Este fato permite determinar várias propriedades sobre números algébricos e transcendentes. Entretanto, para tal demonstração serão enunciados vários outros resultados auxiliares. Alguns destes podem parecer desconexos do objetivo, entretanto são importantes. Além disso, recomenda-se a leitura do Capítulo 4 de [3], visto que serviu de grande inspiração nesta parte do trabalho.

2.4.1 Resultados auxiliares

Teorema 2.9. $(\mathbb{C}, +, \cdot)$ *é um corpo.*

Demonstração. Para mostrar esse resultado, necessitamos provar as propriedades de um corpo. Para isto, sejam $a+bi, c+di, e+fi \in \mathbb{C}$ e as seguintes operações:

$$+ : (a+bi) + (c+di) = (a+c) + (b+d)i;$$
$$\cdot : (a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i.$$

Vamos demonstrar as propriedades:

1. (Fechamento da adição):

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

Como $a, b, c, d \in \mathbb{R}$, temos que $a+c, b+d \in \mathbb{R}$. Portanto, $\mathbb{C}$ é fechado para a operação $+$.

2. (Associatividade da adição):

$$\begin{aligned}
&[(a+bi)+(c+di)]+(e+fi)= \\
&=[(a+c)+(b+d)i]+(e+fi) \\
&=[(a+c)+e]+[(b+d)+f]i \\
&=[a+(c+e)]+[b+(d+f)]i \\
&=(a+bi)+[(c+e)+(d+f)i] \\
&=(a+bi)+[(c+di)+(e+fi)].
\end{aligned}$$

3. (Comutatividade da adição):

$$\begin{aligned}
(a+bi)+(c+di)&=(a+c)+(b+d)i \\
&=(c+a)+(d+b)i \\
&=(c+di)+(a+bi).
\end{aligned}$$

4. (Identidade da adição):
Tome $0+0i \in \mathbb{C}$. Perceba que

$$(0+0i)+(a+bi)=(a+bi)+(0+0i)=(a+0)+(b+0)i=a+bi.$$

Portanto, $0+0i$ é a identidade para a operação $+$.

5. (Elemento inverso da adição):
Tome $-a+(-b)i \in \mathbb{C}$. Note que

$$\begin{aligned}
(-a+(-b)i)+(a+bi)&=(a+bi)+(-a+(-b)i) \\
&=(a+(-a))+(b+(-b))i \\
&=(a-a)+(b-b)i \\
&=0+0i.
\end{aligned}$$

Portanto, $\forall a+bi \in \mathbb{C}$ temos que $-a+(-b)i$ é seu inverso aditivo.

6. (Fechamento da multiplicação):

$$(a+bi)\cdot(c+di) = (ac-bd)+(ad+bc)i.$$

Como $a, b, c, d \in \mathbb{R}$, temos que $ac-bd, ad+bc \in \mathbb{R}$. Portanto, para operação $\cdot$, $\mathbb{C}$ é fechado.

7. (Associatividade da multiplicação):

$$\begin{aligned}
&[(a+bi)\cdot(c+di)]\cdot(e+fi) = \\
&= [(ac-bd)+(ad+bc)i]\cdot(e+fi) \\
&= [(ac-bd)e-(ad+bc)f]+[(ac-bd)f+(ad+bc)e]i \\
&= (ace-bde-adf-bcf)+(acf-bdf+ade+bce)i \\
&= [a(ce-df)-b(de+cf)]+[a(de+cf)+b(ce-df)]i \\
&= (a+bi)\cdot[(ce-df)+(de+cf)i] \\
&= (a+bi)\cdot[(c+di)\cdot(e+fi)].
\end{aligned}$$

8. (Comutatividade da multiplicação):

$$\begin{aligned}
(a+bi)\cdot(c+di) &= (ac-bd)+(ad+bc)i \\
&= (ca-db)+(cb+da)i \\
&= (c+di)\cdot(a+bi).
\end{aligned}$$

9. (Identidade da multiplicação):
Considere agora $1+0i \in \mathbb{C}$. Veja que

$$\begin{aligned}
(a+bi)\cdot(1+0i) &= (1+0i)\cdot(a+bi) \\
&= (1a-0b)+(1b+0a)i \\
&= a+bi.
\end{aligned}$$

10. (Elemento Inverso da multiplicação):
Tome $a+bi \in \mathbb{C}^*$. Note que $a^2+b^2 \neq 0$ e $\frac{a}{a^2+b^2}+\left(-\frac{b}{a^2+b^2}\right)i$

é um número complexo. Seguindo,

$$\begin{aligned}
&\left[\frac{a}{a^2+b^2}+\left(-\frac{b}{a^2+b^2}\right)i\right]\cdot(a+bi)= \\
&=(a+bi)\cdot\left[\frac{a}{a^2+b^2}+\left(-\frac{b}{a^2+b^2}\right)i\right] \\
&=\left(\frac{a^2}{a^2+b^2}+\frac{b^2}{a^2+b^2}\right)+\left(-\frac{ab}{a^2+b^2}+\frac{ba}{a^2+b^2}\right)i \\
&=1+0i.
\end{aligned}$$

Portanto, para todo $a+bi \in \mathbb{C}^*$, temos que $\frac{a}{a^2+b^2}+\left(-\frac{b}{a^2+b^2}\right)i$ é seu inverso multiplicativo.

11. (Distributividade pela esquerda e direita):
Como a multiplicação é comutativa, basta fazer apenas para um lado:

$$\begin{aligned}
&(a+bi)\cdot[(c+di)+(e+fi)]= \\
&=(a+bi)\cdot[(c+e)+(d+f)i] \\
&=[a(c+e)-b(d+f)]+[a(d+f)+b(c+e)]i \\
&=(ac+ae-bd-bf)+(ad+af+bc+be)i \\
&=[(ac-bd)+(ae-bf)]+[(ad+bc)+(af+be)]i \\
&=[(ac-bd)+(ad+bc)i]+[(ae-bf)+(af+be)i] \\
&=(a+bi)\cdot(c+di)+(a+bi)\cdot(e+fi).
\end{aligned}$$

Portanto, $(\mathbb{C},+,\cdot)$ é corpo. ■

Isto não é o suficiente para demonstrar que o conjunto dos números algébricos, munido com as operações usuais, é um corpo. É fato que, se excluirmos as propriedades 1 e 6, as demais valem. Entretanto, o que garante, por exemplo, que a soma de dois números algébricos também é um número algébrico? Não só isso, mas como saber se o inverso de um número algébrico também é um número algébrico? Deseja-se, então, ter um número algébrico após submeter quaisquer dois números algébricos a operações entre si. Diz-se neste caso que precisa-se provar o fechamento do conjunto dos algébricos para as operações usuais. Para isto, antes de iniciar a demonstração do fato, considere os dois próximos lemas.

Lema 2.10. *Se α é raiz de um polinômio com coeficientes inteiros de grau n, então α^j é combinação linear com coeficientes racionais de $\alpha^{n-1}, \alpha^{n-2}, \ldots, \alpha, 1$, para todo j natural tal que $j \geq n$.*

Demonstração. Seja α raiz de um polinômio com coeficientes inteiros de grau n. Então α satisfaz uma equação polinomial da forma

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

com $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}$. Dividindo ambos lados da equação pelo coeficiente do termo líder, obtemos

$$x^n + q_{n-1} x^{n-1} + \ldots + q_1 x + q_0 = 0,$$

onde $q_{n-1}, \ldots, q_1, q_0 \in \mathbb{Q}$. Assim, substituindo x por α, segue que

$$\alpha^n = -q_{n-1}\alpha^{n-1} - \ldots - q_1\alpha + q_0.$$

Desse modo, estamos escrevendo α^n como combinação linear com coeficientes racionais de $\alpha^{n-1}, \ldots, \alpha, 1$. Todavia, utilizando indução, suponha que α^{n+k} é combinação linear com coeficientes racionais de $\alpha^{n-1}, \ldots, \alpha, 1$, ou seja,

$$\alpha^{n+k} = q_{n-1}\alpha^{n-1} + \ldots + q_1\alpha + q_0,$$

com $q_{n-1}, \ldots, q_1, q_0 \in \mathbb{Q}$ e $k \in \mathbb{N}$. Então, segue que

$$\begin{aligned}
\alpha^{n+k+1} &= \alpha\alpha^{n+k} \\
&= \alpha(q_{n-1}\alpha^{n-1} + \ldots + q_1\alpha + q_0) \\
&= q_{n-1}\alpha^n + \ldots + q_1\alpha^2 + q_0\alpha \\
&= q_{n-1}(-a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha + a_0) + \ldots + q_1\alpha^2 + q_0\alpha.
\end{aligned}$$

Como a multiplicação e soma de racionais também resulta em números racionais, chegamos que α^{n+k+1} pode ser escrito como combinação linear com coeficientes racionais de $\alpha^{n-1}, \ldots, \alpha, 1$. Então α^j é combinação linear com coeficientes racionais de $\alpha^{n-1}, \ldots, \alpha, 1$, para $j \in \mathbb{N}$ tal que $j \geq n$. ■

Definição 2.5. Dizemos que X é uma *forma linear com coeficientes racionais* se pode expresso da forma

$$X = q_1x_1 + \ldots + q_nx_n,$$

com $q_1, \ldots, q_n \in \mathbb{Q}$. Chamamos também $x_1, \ldots, x_n$ de *indeterminadas.*

Definição 2.6. Dizemos que um conjunto de formas lineares com coeficientes racionais $S = \{X_1, X_2, \ldots, X_n\}$ é linearmente dependente sobre os racionais quando existem $r_1, r_2 \ldots, r_n \in \mathbb{Q}$, com ao menos um $r_i \neq 0$, tais que

$$r_1X_1 + r_2X_2 + \ldots + r_nX_n = 0.$$

Lema 2.11. *Sejam $n+1$ formas lineares com coeficientes racionais e com indeterminadas $x_1, \ldots x_n$. O conjunto formado pelas $n+1$ formas lineares é linearmente dependente sobre os racionais.*

Demonstração. Inicialmente, tome as seguintes $n+1$ formas lineares com n indeterminadas:

$$\begin{aligned} X_1 &= q_{11}x_1 + \ldots + q_{1n}x_n \\ X_2 &= q_{21}x_1 + \ldots + q_{2n}x_n \\ &\vdots \\ X_{n+1} &= q_{n+1,1}x_1 + \ldots + q_{n+1,n}x_n. \end{aligned}$$

Temos que mostrar que existem $r_1, \ldots, r_{n+1} \in \mathbb{Q}$ de modo que

$$r_1X_1 + r_2X_2 + \ldots + r_nX_n + r_{n+1}X_{n+1} = 0,$$

com ao menos um r_i diferente de zero. Assim, substituindo cada X_i por sua expressão dada no início da demonstração, queremos

$$\begin{aligned} & r_1(q_{11}x_1 + \ldots + q_{1n}x_n) + \ldots + r_{n+1}(q_{n+1,1}x_1 + \ldots \\ & \ldots + q_{n+1,n}x_n) = \\ & = (q_{11}r_1 + q_{21}r_2 + \ldots + q_{n+1,1}r_{n+1})x_1 + \ldots \\ & \ldots + (q_{1n}r_1 + q_{2n}r_2 + \ldots + q_{n+1,n}r_{n+1})x_n = \\ & = 0. \end{aligned}$$

Logo, podemos montar o seguinte sistema de equações lineares:

$$\begin{cases} q_{11}r_1 + q_{21}r_2 + \ldots + q_{n+1,1}r_{n+1} = 0 \\ \vdots \\ q_{1n}r_1 + q_{2n}r_2 + \ldots + q_{n+1,n}r_{n+1} = 0. \end{cases}$$

Caso a matriz dos coeficientes do sistema linear contenha uma matriz N de ordem n cujo determinante é diferente de zero, tome, sem perda de generalidade, $r_{n+1} = 1$ (ou um número racional qualquer diferente de zero ao invés de um), com r_{n+1} sendo a variável que não possui seus respectivos coeficientes presentes na matriz N. Obtemos então

$$\begin{cases} q_{11}r_1 + q_{21}r_2 + \ldots + q_{n1}r_n = -q_{n+1,1} \\ \vdots \\ q_{1n}r_1 + q_{2n}r_2 + \ldots + q_{nn}r_n = -q_{n+1,n}. \end{cases}$$

Continuando, nosso sistema poderia ser escrito como $Nr = b$, ou seja,

$$\begin{bmatrix} q_{11} & \ldots & q_{n1} \\ \vdots & & \vdots \\ q_{1n} & \ldots & q_{nn} \end{bmatrix} \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} -q_{n+1,1} \\ \vdots \\ -q_{n+1,n} \end{bmatrix}.$$

Como N é inversível, por ter determinante diferente de zero, temos solução única do sistema. Além disso, teremos somente números racionais como solução, uma vez que os números racionais são fechados para as operações utilizadas nos elementos das matrizes, quando as invertemos e multiplicamos. Caso a matriz dos coeficientes não contenha uma matriz de ordem n com determinante diferente de zero, tome a maior matriz M de ordem m tal que $m < n$ e $det(M) \neq 0$. Sem perda de generalidade, suponha

$$M = \begin{bmatrix} q_{11} & \ldots & q_{m1} \\ \vdots & & \vdots \\ q_{1m} & \ldots & q_{mm} \end{bmatrix},$$

bem como $r_{m+1} = 1$ e $r_{m+2} = r_{m+3} = \ldots = r_{n+1} = 0$. Encontramos a solução deste sistema de modo similar ao que fizemos anteriormente. Entretanto, temos que garantir que esta solução também satisfaça as equações

$$\begin{cases} q_{1,m+1}r_1 + \dots q_{m,m+1}r_m = -q_{m+1,m+1} \\ \vdots \\ q_{1n}r_1 + \dots + q_{mn}r_m = -q_{m+1,n}. \end{cases}$$

De fato, suponha, por contradição, que existe uma equação da forma $q_{1,j}r_1 + \dots + q_{m,j}r_m = -q_{m+1,j}$ que não é satisfeita para algum j, com $j \in \mathbb{N}$ tal que $m+1 \leq j \leq n$. Assim, utilizando propriedades de determinantes obtemos

$$\begin{vmatrix} q_{11} & \dots & q_{m1} & q_{m+1,1} \\ & \vdots & & \\ q_{1m} & \dots & q_{mm} & q_{m+1,m} \\ q_{1j} & \dots & q_{mj} & q_{m+1,j} \end{vmatrix} = \begin{vmatrix} q_{11} & \dots & q_{m1} & 0 \\ & \vdots & & \\ q_{1m} & \dots & q_{mm} & 0 \\ q_{1j} & \dots & q_{mj} & A \end{vmatrix} \neq 0,$$

com $A = q_{1j}r_1 + \dots + q_{mj}r_n + q_{m+1,j} \neq 0$. Isto contradiz a hipótese de que M é a maior matriz quadrada com determinante diferente de zero presente na matriz dos coeficientes. Logo, as soluções do sistema satisfazem todas as equações remanescentes. Portanto, pelo primeiro e segundo casos, $n+1$ formas lineares com n indeterminadas são linearmente dependentes sobre os racionais. ■

2.4.2 O corpo dos números algébricos e suas consequências

Nesta parte, volta-se a falar sobre números algébricos e transcendentes. É importante destacar também que a próxima demonstração utiliza o conceito de subcorpo. Para melhor compreensão sobre corpos e subcorpos, recomenda-se a leitura das duas primeiras seções do Capítulo 3 de [4].

Teorema 2.12. $(\overline{\mathbb{Q}}, +, \cdot)$ *é um subcorpo dos complexos.*

Demonstração. Para mostrarmos isso devemos provar os seguintes itens para quaisquer $\alpha, \beta \in \overline{\mathbb{Q}}$:

1. $\alpha + \beta \in \overline{\mathbb{Q}}$;

2. $\alpha\beta \in \overline{\mathbb{Q}}$;
3. $-\alpha \in \overline{\mathbb{Q}}$;
4. $\alpha^{-1} \in \overline{\mathbb{Q}}$, onde $\alpha \neq 0$.

Inicialmente, tomemos $\alpha, \beta \in \overline{\mathbb{Q}}$. Suponha que α satisfaça (I) e que β satisfaça (II), conforme a seguir:

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

$$b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0 = 0, \tag{II}$$

com $a_n, a_{n-1}, \ldots, a_1, a_0, b_m, b_{m-1} \ldots, b_1, b_0 \in \mathbb{Z}$.

No caso do item 1, tome os seguintes $mn + 1$ números:

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

Veja que, pelo Teorema do binômio de Newton, conseguimos reescrever todos estes números como combinação linear com coeficientes racionais de $\alpha^j\beta^k$, com $0 \leq j \leq mn$ e $0 \leq k \leq mn$. Porém, vamos considerar $0 \leq j \leq n-1$ e $0 \leq k \leq m-1$, uma vez que, após utilizar o Lema 2.10, basta trocar $\alpha^j\beta^k$ pela combinação linear com coeficientes racionais adequada quando $j \geq n$ ou $k \geq m$. Assim, por combinatória, temos nm configurações diferentes para $\alpha^j\beta^k$ e $mn+1$ números. Logo, pelo Lema 2.11, existem $r_0, r_1, \ldots r_{nm} \in \mathbb{Q}$ tais que

$$r_0 + r_1(\alpha + \beta) + \ldots + r_{nm}(\alpha + \beta)^{nm} = 0,$$

com ao menos um $r_i \neq 0$. Continuando, como os coeficientes de $1, (\alpha+\beta), \ldots, (\alpha+\beta)^{nm}$ são números racionais, podemos expressá-los em forma de fração de inteiros. Multiplicando ambos os lados desta igualdade pelo produtório de todos os denominadores desses racionais, obtemos que $\alpha + \beta$ satisfaz uma equação polinomial com coeficientes inteiros. Portanto, $\alpha + \beta$ é algébrico.

De modo similar, para o item 2, tome os $mn + 1$ números a seguir:

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

Novamente, podemos reescrever todos estes números como combinação linear com coeficientes racionais de $\alpha^j\beta^k$, com $0 \leq j \leq n-1$ e $0 \leq k \leq m-1$. Assim, pelo Lema 2.11, existem $r_0, r_1, \ldots r_n m \in \mathbb{Q}$ tais que

$$r_0 + r_1(\alpha\beta) + \ldots + r_{nm}(\alpha\beta)^{nm} = 0,$$

com ao menos um $r_i \neq 0$. De modo análogo ao caso anterior, conseguimos uma equação polinomial com coeficientes inteiros que é satisfeita por $\alpha\beta$. Portanto, temos que $\alpha\beta$ é algébrico.

Para o item 3, perceba que, como α satisfaz (I), temos que $-\alpha$ satisfaz a seguinte igualdade:

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

Verificando, obtemos que:

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

Portanto, $-\alpha \in \overline{\mathbb{Q}}$.

Para provar o item 4, tome α conforme as condições iniciais e $\alpha \neq 0$. Perceba que, como α satisfaz (I), temos que α^{-1} irá satisfazer a seguinte equação polinomial:

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

De fato, pois:

$$a_0(\alpha^{-1})^n + a_1(\alpha^{-1})^{n-1} + \ldots + a_{n-1}(\alpha^{-1}) + a_n = \\ \frac{a^n}{a^n}[a_0(\alpha^{-1})^n + a_1(\alpha^{-1})^{n-1} + \ldots + a_{n-1}(\alpha^{-1}) + a_n] = \\ \frac{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0}{a^n} = \frac{0}{a^n} = 0.$$

Portanto, $\alpha^{-1} \in \overline{\mathbb{Q}}$. ■

Agora já há o suficiente para se enunciar alguns resultados que envolvem números transcendentes e algébricos. Existem vários outros além dos apresentados aqui, todavia o foco é somente expor algumas formas de utilizar o Teorema 2.12.

Teorema 2.13. *Se $\alpha, \beta \in \overline{\Psi}$, então $(\alpha + \beta) \in \overline{\Psi}$ ou $(\alpha - \beta) \in \overline{\Psi}$.*

Demonstração. Sejam $\alpha, \beta \in \overline{\Psi}$. Agora suponha, por absurdo, que $(\alpha+\beta), (\alpha-\beta) \in \overline{\mathbb{Q}}$. Perceba que temos $(\alpha+\beta)+(\alpha-\beta) = 2\alpha \in \overline{\mathbb{Q}}$, pelo Teorema 2.12. Entretanto, $2\alpha 2^{-1} = \alpha \in \overline{\mathbb{Q}}$. Absurdo, pois contraria a hipótese. Portanto, $(\alpha + \beta) \in \overline{\Psi}$ ou $(\alpha - \beta) \in \overline{\Psi}$. ■

Teorema 2.14. *Se $\alpha \in \overline{\Psi}$ e $\frac{p}{q} \in \mathbb{Q}^*$, então $\frac{p\alpha}{q} \in \overline{\Psi}$.*

Demonstração. Sejam $\alpha \in \overline{\Psi}$ e $\frac{p}{q} \in \mathbb{Q}^*$. Suponha, por absurdo, que $\frac{p\alpha}{q} \in \overline{\mathbb{Q}}$. Então, $\frac{p\alpha}{q} \cdot \frac{q}{p} = \alpha \in \overline{\mathbb{Q}}$, pelo Teorema 2.12. Absurdo, porque contraria a hipótese. Portanto, $\frac{p\alpha}{q} \in \overline{\Psi}$. ■

Teorema 2.15. *Se $\alpha \in \overline{\mathbb{Q}}$ e $\frac{p}{q} \in \mathbb{Q}$, $q \in \mathbb{N}^*$, então $\alpha^{\frac{p}{q}} \in \overline{\mathbb{Q}}$.*

Demonstração. Sejam $\alpha \in \overline{\mathbb{Q}}$ e $\frac{p}{q} \in \mathbb{Q}$ (q natural não nulo). Perceba que, como α é algébrico, temos que α^p também é, pois $(\overline{\mathbb{Q}}, +, \cdot)$ é corpo. Assuma então $Q(x) \in \mathbb{Z}[x]$ tal que $Q(\alpha^p) = 0$, com grau m. Agora tome $R(x) \in \mathbb{Z}[x]$ com os mesmos coeficientes de $Q(x)$, só que com o grau de todos os x multiplicados por q. Então, note que

$$\begin{aligned} R(\sqrt[q]{\alpha^p}) &= r_0(\sqrt[q]{\alpha^p})^{qm} + r_1(\sqrt[q]{\alpha^p})^{q(m-1)} + \ldots + r_n^{q0} \\ &= r_0(\alpha^p)^m + r_1(\alpha^p)^{m-1} + \ldots + r_n \\ &= Q(\alpha^p) \\ &= 0. \end{aligned}$$

Assim, $\sqrt[q]{\alpha^p} = \alpha^{\frac{p}{q}}$ é raiz de $R(x)$ e, consequentemente, pertence à $\overline{\mathbb{Q}}$. ■

Teorema 2.16. *Se $\alpha, \beta \in \overline{\Psi}$, então $(\alpha + \beta) \in \overline{\Psi}$ ou $(\alpha \cdot \beta) \in \overline{\Psi}$.*

Demonstração. Suponha, por absurdo, que $(\alpha+\beta), (\alpha\beta) \in \overline{\mathbb{Q}}$. Assim, perceba que $(\alpha+\beta)^2, (-2\alpha\beta) \in \overline{\mathbb{Q}}$, pois $\overline{\mathbb{Q}}$ é fechado para a operação de multiplicação. Seguindo, temos que

$$(\alpha + \beta)^2 - 2\alpha\beta = \alpha^2 + \beta^2 \in \overline{\mathbb{Q}}.$$

Por outro lado, então obtemos que

$(\alpha-\beta)^2 = \alpha^2+\beta^2-2\alpha\beta \in \overline{\mathbb{Q}} \implies \alpha-\beta = (\alpha^2+\beta^2-2\alpha)^{\frac{1}{2}} \in \overline{\mathbb{Q}}.$

Logo, temos que $(\alpha+\beta), (\alpha-\beta) \in \overline{\mathbb{Q}}$. Absurdo, pois, pelo Teorema 2.13, dados $\alpha, \beta \in \overline{\Psi}$ mostramos que $(\alpha+\beta) \in \overline{\Psi}$ ou $(\alpha-\beta) \in \overline{\Psi}$. Portanto, $(\alpha+\beta) \in \overline{\Psi}$ ou $(\alpha\cdot\beta) \in \overline{\Psi}$. ■

Corolário 2.17. *Se $\alpha \in \overline{\Psi}$, então $\alpha^{-1} \in \overline{\Psi}$.*

Demonstração. Seja $\alpha \in \overline{\Psi}$. Suponha, por absurdo, que $\alpha^{-1} \in \overline{\mathbb{Q}}$. Como $\overline{\mathbb{Q}}$ é corpo, temos que $(\alpha^{-1})^{-1} \in \overline{\mathbb{Q}}$. Mas $(\alpha^{-1})^{-1} = \alpha$. Absurdo. Portanto, $\alpha^{-1} \in \overline{\Psi}$. ■

Teorema 2.18. *Se $\alpha \in \overline{\Psi}$, então $\alpha^\alpha \in \overline{\Psi}$ ou $\alpha^{\alpha+1} \in \overline{\Psi}$.*

Demonstração. Seja $\alpha \in \overline{\Psi}$. Tome, por absurdo, $\alpha^\alpha, \alpha^{\alpha+1} \in \overline{\mathbb{Q}}$. Pelo Teorema 2.12, segue que

$$\alpha^{\alpha+1}(\alpha^\alpha)^{-1} = \alpha \in \overline{\mathbb{Q}}.$$

Absurdo, pois isto contraria a hipótese. Portanto, temos que $\alpha^\alpha \in \overline{\Psi}$ ou $\alpha^{\alpha+1} \in \overline{\Psi}$. ■

São necessários métodos muitos mais duros para demonstrar a transcendentalidade de alguns números. Entretanto, perceba o que é possível provar assumindo a transcendentalidade de π.

Exemplo 2.4.1. $\pi + \frac{1}{\pi}$ é transcendente.

Demonstração. Seja π transcendente. Temos, pelo Teorema 2.16 que $\pi + \frac{1}{\pi} \in \overline{\Psi}$ ou $\pi \cdot \left(\frac{1}{\pi}\right) \in \overline{\Psi}$. Entretanto, $\pi \cdot \left(\frac{1}{\pi}\right) = 1 \in \overline{\mathbb{Q}}$. Logo, segue que $\pi + \frac{1}{\pi} \in \overline{\Psi}$. ■

Observação 4. Um problema em aberto na matemática é determinar se $\pi + e$ e $\pi - e$ são algébricos ou transcendentes. Entretanto, pelo Teorema 2.13, podemos afirmar com toda a certeza que um deles é transcendente. Outro problema em aberto é determinar a transcendência ou não de π^π e $\pi^{\pi+1}$. Mas o Teorema 2.18 nos garante que um destes números é transcendente.

3 APROXIMAÇÕES DIOFANTINAS

3.1 APROXIMAÇÕES DE IRRACIONAIS POR RACIONAIS

Um dos tópicos presentes no ramo das aproximações diofantinas é a aproximação de irracionais por racionais. Sabe-se também que os números transcendentes são também irracionais. Assim, nesta seção, obtém-se objetos matemáticos importantes para a compreensão dos números de Liouville, que são apresentados no Capítulo 4.

Teorema 3.1. *Para todo número irracional α, existe um inteiro m de modo que vale*

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

Demonstração. Sejam α um número irracional e m o número inteiro mais próximo de α. Inicialmente note que, como α é um número irracional temos que ele não é um número da forma $\frac{z}{2}$, com $z \in \mathbb{Z}$. Assim, a distância dele para o inteiro mais próximo na reta é menor que $\frac{1}{2}$. Logo, temos que

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

■

De modo simplificado, é possível substituir o enunciado deste resultado por "Qualquer número irracional está a uma distância menor que $\frac{1}{2}$ de algum número inteiro".

Exemplo 3.1.1. Vejamos o caso de $\log_2 9$. Inicialmente, precisamos saber se este número é irracional. Suponha então, por absurdo, que $\log_2 9 = \frac{a}{b}$ com $a, b \in \mathbb{Z}$, b não nulo, tais que $mdc(a, b) = 1$. Assim, segue que

$$\log_2 9 = \frac{a}{b} \iff 2^{\frac{a}{b}} = 9 \iff 2^a = (3 \cdot 3)^b = 3^b \cdot 3^b.$$

Visto que 2 não é divisor de 3, esta igualdade não se mantém. Portanto, $\log_2 9$ é irracional. Agora, com a intenção de construir a desigualdade, perceba que $81 < 128 \implies \sqrt{81} < \sqrt{128} \implies 9 < 2^{\frac{7}{2}}$, pois a função $f(x) = \sqrt{x}$ é crescente. Logo, como a função $\log_2 x$ também é crescente, segue que

$$\begin{aligned} \log_2 2^3 < \log_2 9 < \log_2 2^{\frac{7}{2}} &\implies \log_2 9 - \log_2 2^3 < \log_2 2^{\frac{7}{2}} - \log_2 2^3 \\ &\implies \log_2 9 - 3 < \frac{7}{2} - 3 = \frac{1}{2}. \end{aligned}$$

Portanto,

$$|\log_2 9 - 3| < \frac{1}{2}.$$

Observação 5. Em vez do Teorema 3.1, pode-se partir também do fato de existir um número racional entre quaisquer dois números reais distintos dados (diz-se que $\mathbb{Q}$ é denso em $\mathbb{R}$). Assim, dado um número irracional α e um $\varepsilon \in \mathbb{R}$ tal que $\varepsilon > 0$, tem-se que existe $\frac{p}{q} \in \mathbb{Q}$ de modo que vale

$$\left|\alpha - \frac{p}{q}\right| < \varepsilon.$$

Isso quer dizer que ao tomar um número irracional α e um número real β distintos, sempre existirá um número racional $\frac{p}{q}$ entre α e β. Em [8], o autor inicia o estudo sobre aproximações diofantinas partindo desta perspectiva.

3.2 APROXIMAÇÕES MELHORES

Os próximos resultados têm o objetivo de melhorarem a aproximação apresentada no Teorema 3.1. O porquê disso está relacionado ao modo que Joseph Liouville encontrou alguns números transcendentes, a partir de uma aproximação "especial".

Proposição 3.2. *Dados um número irracional α e um número natural não nulo n, existe um número racional m/n tal que*

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{2n}.$$

Demonstração. Sejam α um número irracional, n um número natural não nulo e m o número inteiro mais próximo de $n\alpha$ (note que $n\alpha$ é irracional também). Assim, pelo Teorema 3.1, decorre que

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

Portanto,

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{2n}.$$

■

Teorema 3.3. *Dados um número irracional α e um natural não nulo k, existe um número racional m/n, onde n não excede k, de modo que*

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{nk}.$$

Demonstração. Sejam um número irracional α e um natural não nulo k. Então $n\alpha$, com n variando entre os naturais de 1 até k, pode ser escrito como a soma de sua parte inteira x_n com sua decimal y_n, conforme vemos abaixo

$$n\alpha = x_n + y_n \implies n\alpha - x_n = y_n.$$

Perceba que $n\alpha - x_n$ pode assumir valores em $(0, 1)$ e é irracional. Logo, consideremos 2 casos:

Caso 1: Existe n tal que $0 < n\alpha - x_n < \frac{1}{k}$.

Podemos afirmar então que

$$-\frac{1}{k} < n\alpha - x_n < \frac{1}{k}.$$

Logo, basta dividir tudo por um $n \in \mathbb{N}^*$, que está entre 1 e k.

Caso 2: Todos os y_n respeitam $\frac{1}{k} < n\alpha - x_n < 1$.

Note que podemos separar o segmento de reta $[0, 1]$ em k intervalos $\left(0, \frac{1}{k}\right), \left(\frac{1}{k}, \frac{2}{k}\right), \ldots, \left(\frac{k-1}{k}, 1\right)$. Como $n\alpha - x_n$ não está em $\left(0, \frac{1}{k}\right)$, segue que temos $k-1$ intervalos onde ele possa estar. Pelo princípio da casa dos pombos (veja com mais detalhes na página 53 de [10]) segue que existe um intervalo que contém ao menos 2 números, uma vez que temos k números. Considere então y_r e y_j distintos no mesmo intervalo. Assim, segue que

$$-\frac{1}{k} < y_j - y_r < \frac{1}{k}.$$

Seguindo,

$$-\frac{1}{k} < (j\alpha - x_j) - (r\alpha - x_r) < \frac{1}{k}.$$

Então

$$-\frac{1}{k} < (j-r)\alpha - (x_j - x_r) < \frac{1}{k}.$$

Chamando $j-r$ de n e $(x_j - x_r)$ de m, temos

$$-\frac{1}{k} < n\alpha - m < \frac{1}{k}.$$

Dividindo por n

$$-\frac{1}{nk} < \alpha - \frac{m}{n} < \frac{1}{nk}.$$

■

Exemplo 3.2.1. Vamos aproximar $\sqrt{19}$ pelo método acima, com $k=3$. Inicialmente, veja que

$$\begin{aligned}\sqrt{19} &= 4,35889\ldots = 4 + 0,35889\ldots\\ 2\sqrt{19} &= 8,71779\ldots = 8 + 0,71779\ldots\\ 3\sqrt{19} &= 13,07669\ldots = 13 + 0,07669\ldots\end{aligned}$$

Como $0,07669\ldots < \frac{1}{3}$, caímos no caso 1 do Teorema 3.3. Portanto, segue que

$$-\frac{1}{3} < 3\sqrt{19} - 13 < \frac{1}{3} \implies -\frac{1}{3\cdot 3} < \sqrt{19} - \frac{13}{3} < \frac{1}{3\cdot 3}.$$

Logo,

$$\left|\sqrt{19} - \frac{13}{3}\right| < \frac{1}{3\cdot 3}.$$

Exemplo 3.2.2. Agora vejamos para $\alpha = \sqrt{11}$ e $k = 5$. Desta vez, temos que

$$\begin{aligned}
\sqrt{11} &= 3,31662\ldots = 3 + 0,31662\ldots \\
2\sqrt{11} &= 6,63324\ldots = 6 + 0,63324\ldots \\
3\sqrt{11} &= 9,94987\ldots = 9 + 0,94987\ldots \\
4\sqrt{11} &= 13,26649\ldots = 13 + 0,26649\ldots \\
5\sqrt{11} &= 16,58312\ldots = 16 + 0,58312\ldots
\end{aligned}$$

Perceba agora que nenhuma parte decimal é menor que $\frac{1}{5}$. Ainda assim, temos que $\frac{1}{5} < 0,31662\ldots < \frac{2}{5}$ e $\frac{1}{5} < 0,26649\ldots < \frac{2}{5}$. Logo, caímos no caso 2 do Teorema 3.3. Obtemos assim

$$-\frac{1}{5} < (\sqrt{11}-3)-(4\sqrt{11}-13) < \frac{1}{5} \implies -\frac{1}{3\cdot 5} < \sqrt{11}-\frac{10}{3} < \frac{1}{3\cdot 5}.$$

Portanto,

$$\left|\sqrt{11} - \frac{10}{3}\right| < \frac{1}{3\cdot 5}.$$

3.3 SEQUÊNCIAS E OUTRAS APROXIMAÇÕES

No Capítulo 4 serão apresentados os números de Liouville. Contudo, é necessário encontrar uma sequência de números racionais que obedece determinada regra para demonstrar que um número é de Liouville. Assim, nesta seção serão apresentados objetos matemáticos que permitirão uma melhor compreensão sobre a natureza de tais números.

Definição 3.1. Uma *sequência* é uma função $x : \mathbb{N} \longrightarrow A$, que associa cada número natural a um elemento do conjunto A.

Modificando o contradomínio para o conjunto dos números racionais, obtemos uma *sequência de racionais*, bem como se trocarmos A pelo conjunto dos números inteiros, obtemos uma *sequência de inteiros*.

Será utilizada a notação (x_n) para indicar a sequência x. O conjunto de todos os termos da sequência (x_n) será denotado por $x(\mathbb{N}) = \{x_0, x_1, x_2, \ldots, x_n, \ldots\}$.

Exemplo 3.3.1. Considere uma sequência (x_n), com a seguinte regra de formação:

$$x_n = \begin{cases} 2^n, \text{ se } n \text{ é par;} \\ 2^{n-1}, \text{ se } n \text{ é ímpar.} \end{cases}$$

Assim, a sequência que se obtém é $(1, 1, 4, 4, 16, 16, \ldots)$.

Exemplo 3.3.2. Tome a sequência (x_n), com a seguinte lei de formação:

$$x_n = \frac{1}{n+1}, \forall n \in \mathbb{N}.$$

Logo, a sequência obtida pela regra é $\left(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right)$.

Definição 3.2. Dizemos que uma sequência de números reais (x_n) é *limitada* quando existem $\alpha, \beta \in \mathbb{R}$ tais que $\alpha < x_n < \beta$, para todo $x_n \in x(\mathbb{N})$. Uma sequência de números reais é *ilimitada* quando não for *limitada.*

No Exemplo 3.3.1 temos uma sequência ilimitada, pois para qualquer $\beta \in \mathbb{R}_+^*$ tem-se que $n > \beta \implies x_n > \beta$. No entanto, o Exemplo 3.3.2 apresenta uma sequência limitada, uma vez que todos os termos estão entre 0 e 2.

Definição 3.3. Um número real α é denominado *aproximável na ordem t por racionais* se existirem uma constante real $c > 0$ e uma sequência (p_j/q_j), com $q_j > 0$, de racionais distintos e irredutíveis tais que

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{c}{{q_j}^t}, n \in \mathbb{N}^*.$$

Observação 6. Quando fala-se de racional irredutível, quer-se dizer que a fração de inteiros que representa aquele racional é irredutível, ou seja, não há divisores comuns (diferentes de 1 e -1) entre o numerador e o denominador.

Teorema 3.4. *Dado um número irracional α, existem infinitos números racionais m/n, na forma irredutível, que satisfazem*

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{n^2}.$$

Demonstração. Utilizando o Teorema 3.3, perceba que $k \geq n$ e, consequentemente, $\frac{1}{kn} \leq \frac{1}{n^2}$. Assim, segue que existe $\frac{m}{n} \in \mathbb{Q}$ tal que

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{n^2}.$$

Entretanto, queremos que $\frac{m}{n}$ seja irredutível. Assim, tome $\frac{r_m}{r_n}$ como forma irredutível de $\frac{m}{n}$. Como $\alpha - \frac{m}{n} = \alpha - \frac{r_m}{r_n}$ e $\frac{1}{n^2} \leq \frac{1}{r_n^2}$, segue que

$$\left|\alpha - \frac{r_m}{r_n}\right| < \frac{1}{r_n^2}.$$

Falta ainda mostrar que existem infinitos números racionais que satisfazem esta última desigualdade. Para isso, suponha, por absurdo, que existam $\frac{m_1}{n_1}, \frac{m_2}{n_2}, \ldots, \frac{m_i}{n_i} \in \mathbb{Q}$ que satisfaçam. Seguindo, tome $k \in \mathbb{Z}_+$ tal que $\frac{1}{k}$ seja menor que a distância entre α e $\frac{m_1}{n_1}, \frac{m_2}{n_2}, \ldots, \frac{m_i}{n_i}$. Assim, como temos k e α, pelo Teorema 3.3, segue que existe $\frac{m}{n} \in \mathbb{Q}$ tal que

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{nk}.$$

Ora, conforme explicado anteriormente, $\frac{1}{kn} \leq \frac{1}{n^2}$. Logo,

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{n^2}.$$

Então $\frac{m}{n}$ satisfaz as condições do Teorema 3.4, mas não está listado. Absurdo! Portanto, existem infinitos números racionais que satisfazem as condições do Teorema 3.4. ■

Em outras palavras, este último resultado diz que todo número irracional é aproximável na ordem 2 por racionais. Inclusive, o Teorema 3.4 pode ser considerado uma forma fraca do Teorema da Aproximação de Dirichlet.

Observação 7. O Teorema 3.4 não vale se substituirmos n^2 por n elevado à uma potência natural maior que 2, entretanto consegue-se melhorar o resultado multiplicando $\frac{1}{n^2}$ por um $c \in \mathbb{R}_+^*$ menor que 1. Inclusive, Adolf Hurwitz mostrou que o menor c possível é $\frac{1}{\sqrt{5}}$ (veja [8]).

4 NÚMEROS DE LIOUVILLE

Neste capítulo serão apresentados os números de Liouville e algumas de suas propriedades. Grande parte do conteúdo está presente em [7], entretanto a abordagem é ligeiramente diferente.

4.1 UMA PROPRIEDADE PARA TODOS OS NÚMEROS REAIS ALGÉBRICOS

A ideia de Liouville era construir uma propriedade válida para todos os números reais algébricos e, posteriormente, construir um número real que não satisfizesse esta propriedade.

Na demonstração de tal propriedade é utilizado o Teorema do Valor Médio. Segue abaixo seu enunciado.

Teorema 4.1. *Se f é uma função contínua no intervalo $[a, b]$ e diferenciável em (a, b), então existe $c \in (a, b)$ tal que*

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

Observação 8. A demonstração do Teorema 4.1 foge ao escopo desse trabalho e pode ser verificada na página 272 de [6].

A propriedade construída por Liouville é geralmente chamada de Teorema de Liouville. Perceba a seguir que esta propriedade vale para qualquer raiz real de um polinômio com coeficientes inteiros e de grau maior ou igual a 2. Entretanto, se um número real α é raiz de um polinômio $P(x)$ com coeficientes inteiros e de grau 1, podemos construir um polinômio de grau 2 com coeficientes inteiros efetuando o produto entre $P(x)$ e $(x + z)$, onde $z \in \mathbb{Z}$. Assim, a propriedade a seguir vale para qualquer número real algébrico.

Teorema 4.2. *Seja α uma raiz real de um polinômio com coeficientes inteiros e de grau $n \geq 2$. Então existe uma constante $c(\alpha) \in \mathbb{R}_+^*$ tal que*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^n}, \forall \frac{p}{q} \in \mathbb{Q}.$$

Demonstração. Nesta demonstração utilizaremos o Teorema do Valor Médio. Por isso, aparecerá $\frac{1}{1+max_{|t-\alpha|\leq 1}|P'(t)|q^n}$.

Seja $P(x) \in \mathbb{Z}[x]$, de grau $n \geq 2$ e com raiz α. Separemos em 2 casos:

Caso 1: $|\alpha - \frac{p}{q}| \geq 1$.

Temos que o teorema vale, pois $\left|\alpha - \frac{p}{q}\right| \geq 1 \geq \frac{1}{1+max_{|t-\alpha|\leq 1}|P'(t)|q^n}$.

Caso 2: $|\alpha - \frac{p}{q}| < 1$.

Aqui, caso $\frac{p}{q}$ for uma raiz de $P(x)$, tome $m < 1$ como a menor distância entre α e tais raízes. Logo, tem-se que

$$\left|\alpha - \frac{p}{q}\right| \geq m \implies \left|\alpha - \frac{p}{q}\right| \geq \frac{m}{q^n}.$$

Agora, se $P\left(\frac{p}{q}\right) \neq 0$, como $q^n P\left(\frac{p}{q}\right)$ é inteiro não nulo, temos que $\left|q^n P\left(\frac{p}{q}\right)\right| \geq 1$. Utilizando o Teorema do Valor Médio temos que existe $t_0 \in \mathbb{R}$, com t_0 entre α e $\frac{p}{q}$, tal que

$$|P'(t_0)| = \left|\frac{P(\alpha) - P\left(\frac{p}{q}\right)}{\alpha - \frac{p}{q}}\right| = \frac{\left|P(\alpha) - P\left(\frac{p}{q}\right)\right|}{\left|\alpha - \frac{p}{q}\right|}$$

$$\implies \left|\alpha - \frac{p}{q}\right| \cdot |P'(t_0)| = \left|P(\alpha) - P\left(\frac{p}{q}\right)\right| = \left|P\left(\frac{p}{q}\right)\right|.$$

Continuando,

$$q^n\left|P'(t_0)\right|\left|\alpha - \frac{p}{q}\right| = \left|q^n P\left(\frac{p}{q}\right)\right| \geq 1.$$

Portanto, chegamos que

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{q^n(1+|P'(t_0)|)} \geq \frac{1}{q^n(1+max_{|t-\alpha|\leq 1}|P'(t)|)}.$$

Por fim, basta tomar $c(\alpha) = min\left\{m, \frac{1}{1+max_{|t-\alpha|\leq 1}|P'(t)|}\right\}$ para o teorema valer. ■

4.2 OS PRIMEIROS TRANSCENDENTES

Em conformidade com o início deste capítulo, a seguir é definido um novo conjunto numérico.

Definição 4.1. O número real α é denominado *Número de Liouville* se existir uma sequência $(p_j/q_j)_{j\geq 1}, q_j > 1$, de racionais distintos e irredutíveis de tal modo que

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

A partir da Definição 3.3, pode-se dizer então que os números de Liouville são aproximáveis na ordem j por racionais.

Ainda assim, é necessário provar a existência de algum número que satisfaz tais condições. Para isto, considere o próximo exemplo.

Exemplo 4.2.1. O número $\sum_{i=1}^{\infty} 10^{-i!}$ é um número de Liouville.

Demonstração. Para provar este fato, tome a seguinte sequência (x_n) de números racionais distintos:

$$\begin{cases} x_1 = 10^{-1}; \\ x_{n+1} = x_n + 10^{-(n+1)!}. \end{cases}$$

Perceba que tal sequência converge para $\sum_{i=1}^{\infty} 10^{-i!}$. Note também que, se efetuarmos as somas de frações, o elemento x_n sempre será uma fração irredutível da forma $\frac{c}{10^{n!}}$, com $c \in \mathbb{N}$. Assim, para x_1 temos

$$\begin{aligned} \left|\sum_{i=1}^{\infty} 10^{-i!} - x_1\right| &= \left|\sum_{i=1}^{\infty} 10^{-i!} - \frac{1}{10^1}\right| \\ &= \sum_{i=2}^{\infty} 10^{-i!} \\ &< \frac{1}{(10^1)^1}. \end{aligned}$$

Agora, para x_n, tal que $n \geq 2$, segue que

$$\begin{aligned}\left|\sum_{i=1!}^{\infty} 10^{-i!} - x_n\right| &= \left|\sum_{i=1}^{\infty} 10^{-i!} - \frac{c}{10^{n!}}\right| \\ &= \sum_{i=n+1}^{\infty} 10^{-i!} \\ &< \frac{1}{(10^{n!})^n}.\end{aligned}$$

Portanto, $\sum\limits_{i=1}^{\infty} 10^{-i!}$ é um número de Liouville. ■

Observação 9. Todo número da forma $\sum_{k=1}^{\infty} \frac{a_k}{10^{k!}}$, onde a_k é um algarismo de 1 a 9, é um número de Liouville. Em especial, quando $a_k = 1$, temos a *constante de Liouville.*

Existe uma definição alternativa de Número de Liouville, especialmente útil para futuras demonstrações. Entretanto, como já foi definido Número de Liouville, agora será demonstrada a equivalência entre as definições.

Teorema 4.3. *L é um número de Liouville se, e somente se, para todo $j \in \mathbb{N}^*$, existe $\frac{p}{q} \in \mathbb{Q}$, de modo que*

$$\left|L - \frac{p}{q}\right| < \frac{1}{q^j}.$$

Demonstração. Seja L um Número de Liouville. Então existe uma sequência $(p_j/q_j)_{j \geq 1}$ tal que

$$\left|L - \frac{p_j}{q_j}\right| < \frac{1}{{q_j}^j}, \forall j \geq 1.$$

Considere $n > 0$. Então o elemento $\frac{p_n}{q_n}$ da sequência $(p_j/q_j)_{j \geq 1}$ satisfaz

$$\left|L - \frac{p_n}{q_n}\right| < \frac{1}{{q_n}^n}.$$

Por outro lado, suponha que para todo $j > 0$, existe ao menos um

$\frac{p}{q} \in \mathbb{Q}$ de modo que

$$\left|L - \frac{p}{q}\right| < \frac{1}{q^j}.$$

Assim, monte a sequência de racionais $(p_n/q_n)_{n\geq 1}$, onde $\frac{p_n}{q_n}$ é um racional, que satisfaz

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

Portanto, existe uma sequência de racionais $(p_n/q_n)_{n\geq 1}$, com $q_n > 1$, tal que

$$\left|L - \frac{p_n}{q_n}\right| < \frac{1}{q^n}, \forall n \geq 1.$$

■

Agora resta provar que os números de Liouville não satisfazem o Teorema 4.2. Para tal, é necessário mostrar dois resultados de antemão.

Teorema 4.4. *Dado um número de Liouville α, sua sequência de denominadores $(q_j)_{j\geq 1}$ associada é ilimitada.*

Demonstração. Seja α um Número Liouville. Isso implica que existe uma sequência $(p_j/q_j)_{j\geq 1}, q_j > 1$, de racionais distintos e irredutíveis que satisfazem

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

Suponha agora, por absurdo, que existe $\beta \in \mathbb{R}$ de tal modo que $0 < q_j < \beta$, para todo $j \in \mathbb{Z}$ tal que $j \geq 1$. Assim, perceba que, como $q_j \geq 1$, segue que $\left|\alpha - \frac{p_j}{q_j}\right| < 1 \implies |q_j\alpha - p_j| < q_j$. Entretanto, chega-se que $|p_j| - |q_j\alpha| < |q_j\alpha - p_j| < q_j$ (resultado obtido a partir da desigualdade triangular). Isso gera uma limitação para (p_j) também, visto que $|p_j| < q_j + |q_j\alpha| < |\beta(|\alpha| + 1)|$. Absurdo, pois como p_j e q_j seriam inteiros e limitados e não seria possível construir uma sequência (p_j/q_j) com infinitos números racionais distintos. Portanto, $(q_j)_{j\geq 1}$ é ilimitada. ■

Teorema 4.5. *Todos os números de Liouville são irracionais.*

Demonstração. Seja α um número de Liouville. Suponha, por absurdo, que α é racional, ou seja, $\alpha = \frac{p}{q}$, com $p, q \in \mathbb{Z}$. Assim, existe uma sequência $(p_j/q_j)_{j\geq 1}$ tal que

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

uma vez que $pq_j - p_jq$ é um número inteiro diferente de zero. Logo,

$$\frac{1}{q_j^j} > \frac{1}{|q|q_j} \implies |q| > q_j^{j-1}.$$

Absurdo, pois $(q_j)_{j\geq 1}$ é ilimitada. Portanto, todo número de Liouville é irracional. ■

Enfim, pode-se mostrar que os números de Liouville não satisfazem o Teorema 4.2 e, logo, não são reais algébricos. Assim, os números de Liouville só podem ser transcendentes.

Teorema 4.6. *Todo número de Liouville é transcendente.*

Demonstração. Perceba inicialmente que, uma vez que qualquer número de Liouville é irracional, nenhum deles será raiz de um polinômio de grau 1 com coeficientes inteiros. Assim, suponha, por absurdo, que α é um número de Liouville e algébrico, sendo raiz de um polinômio irredutível de grau $n \geq 2$. Então utilizando o Teorema 4.2, bem como a definição de número de Liouville, segue que existe $c(\alpha)$ e uma sequência de racionais $(p_j/q_j)_{j\geq 1}$ tais que

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

Logo,

$$q_j^{j-n} < \frac{1}{c(\alpha)}, \forall j \geq 1.$$

Absurdo, pois $(q_j)_{j\geq 1}$ é ilimitado. O absurdo provém de assumir que α é algébrico. Portanto, todo número de Liouville é transcendente. ■

4.3 ALGUMAS PROPRIEDADES DOS NÚMEROS DE LIOUVILLE

Após mostrar que todos os números de Liouville são transcendentes, pode-se partir para o estudo de propriedades envolvendo-os.

Teorema 4.7. *Sejam $\alpha \in \mathbb{Q}$ e L um número de Liouville. Então $\alpha + L$ é número de Liouville.*

Demonstração. Sejam $\alpha = \frac{r}{s}$ um número racional e L um número de Liouville. Logo, existe uma sequência $(p_j/q_j)_{j\geq 1}$ tal que

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

Considere agora a sequência $((p_j/q_j) + \alpha)_{j\geq 1}$, onde cada termo da sequência anterior é somado à α. Agora, como a sequência $(q_j)_{j\geq 1}$ é ilimitada, tome $k > 0$ e $j > k$, tais que $q_j > s^k$. Logo,

$$\begin{aligned} \left| (L+\alpha) - \left(\frac{p_j}{q_j} + \alpha \right) \right| &= \left| \left(L + \frac{r}{s} \right) - \left(\frac{p_j s + r q_j}{q_j s} \right) \right| \\ &= \left| L - \frac{p_j}{q_j} \right| \\ &< \frac{1}{q_j^j} \\ &\leq \frac{1}{q_j^{k+1}} \\ &< \frac{1}{q_j^k s^k} \\ &= \frac{1}{(q_j s)^k}. \end{aligned}$$

Logo, pelo Teorema 4.3, temos que $\alpha + L$ é um Número de Liouville. ∎

Teorema 4.8. *Sejam $\alpha \in \mathbb{Q}^*$ e L um número de Liouville. Então αL é número de Liouville.*

Demonstração. Seja $\alpha = \frac{r}{s}$ um número racional, não nulo, e L um número de Liouville. Logo, existe uma sequência $(p_j/q_j)_{j\geq 1}$ tal que

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

Considere agora a sequência $((p_j/q_j)\alpha)_{j\geq 1}$, onde cada termo da sequência é multiplicado por α. Agora, como a sequência $(q_j)_{j\geq 1}$ é ilimitada, tome k>0 e $j > k$, tal que $q_j > |r|s^{k-1}$. Logo,

$$\left|\left(L \cdot \frac{r}{s}\right) - \left(\frac{p_j r}{q_j s}\right)\right| < \frac{|r|}{q_j^j s} \leq \frac{|r|}{q_j^{k+1} s} < \frac{|r|}{q_j^k |r| s^{k-1} s} < \frac{1}{(q_j s)^k}.$$

Portanto, utilizando novamente o Teorema 4.3, temos que αL é um número de Liouville. ■

Teorema 4.9. *Seja $L \in \mathbb{R}$. Se existe uma constante $C \in \mathbb{Q}_+^*$ e uma sequência $(p_j/q_j)_{j\geq 1}$, sendo $q_j > 1$, de modo que*

$$\left|L - \frac{p_j}{q_j}\right| < \frac{C}{q_j^j}, \forall j \in \mathbb{N}^*,$$

então L é um número de Liouville.

Demonstração. Seja $L \in \mathbb{R}$, $C \in \mathbb{Q}_+^*$ e uma sequência $(p_j/q_j)_{j\geq 1}$ que satisfaz as hipóteses. Perceba que $\frac{L}{C}$ é número de Liouville, pois

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

Logo, $C \cdot \frac{L}{C} = L$ é número de Liouville. ■

A partir do Teorema 4.9, é possível utilizar uma ideia similar à presente na página 34 de [1] para demonstrar o próximo resultado.

Teorema 4.10. *Seja L um número de Liouville. Então L^a é, também, número de Liouville para $a \in \mathbb{Z}^*$.*

Demonstração. Seja L número de Liouville. Então, pelo Teorema 4.3, para todo $j \in \mathbb{N}^*$, existe $\frac{p}{q} \in \mathbb{Q}$ tal que

$$\left| L - \frac{p}{q} \right| < \frac{1}{q^j}.$$

Tome $j = ab$, com $a, b \in \mathbb{N}$, com $a \neq 0$. Perceba que, como L é irracional e $\frac{1}{q^{ab}} \leq 1$, temos que $\frac{p}{q} \in (L-1, L+1)$. Assim, como $\mathbb{R}$ é ilimitado, sabemos que existe um $A \in \mathbb{Q}_+^*$, tal que $A > 0$ e $(L-1, L+1) \subset [-A, A]$. Considere $C = aA^{a-1} > 0$ uma constante. Logo,

$$\begin{aligned} \left| L^a - \left(\frac{p}{q}\right)^a \right| &= \left| L - \frac{p}{q} \right| . \left| L^{a-1} + L^{a-2}\frac{p}{q} + \ldots + \left(\frac{p}{q}\right)^{a-1} \right| \\ &< \frac{1}{q^{ab}}(A^{a-1} + A^{a-2}A + \ldots + A^{a-1}) \\ &= \frac{1}{q^{ab}}(aA^{a-1}) \\ &= \frac{C}{(q^a)^b}. \end{aligned}$$

Pelo Teorema 4.9, segue que L^a é número de Liouville se $a \in \mathbb{N}^*$. Ainda falta mostrar que L^{-1} também é número de Liouville para demonstração do teorema estar completa. Neste sentido, perceba que $|pL| \geq |L| \implies \frac{1}{|pL|} \leq \frac{1}{|L|}$, para todo p inteiro não nulo. Veja que existe $\frac{r}{s} \in \mathbb{Q}^*$ tal que $\frac{1}{|L|} < \frac{1}{\left|\frac{r}{s}\right|} = D > 0$, pois $\mathbb{Q}$ é denso em $\mathbb{R}$. Uma vez que L é número de Liouville, sabe-se pelo Teorema 4.3 que existe $\frac{p}{q} \in \mathbb{Q}^*$ tal que $\left| L - \frac{p}{q} \right| < \frac{1}{q^{a+1}}$, para todo $a \in \mathbb{N}^*$. Seguindo, temos

$$\begin{aligned} \left| L^{-1} - \left(\frac{p}{q}\right)^{-1} \right| = \left| \frac{1}{L} - \frac{q}{p} \right| = \left| \frac{1p - Lq}{Lp} \right| & \\ &= \frac{q}{|Lp|} \left| L - \frac{p}{q} \right| \\ &< \frac{q}{|Lp| . |q^{a+1}|} \\ &< \frac{D}{q^a}. \end{aligned}$$

Como para todo $\alpha \in \mathbb{N}^*$ existe um $\frac{p}{q} \in \mathbb{Q}^*$ que satisfaz a desigualdade, é possível montar uma sequência desses $\frac{p}{q}$. Assim, L^{-1} é número de Liouville. Portanto, L^a é número de Liouville para $a \in \mathbb{Z}^*$. ■

Teorema 4.11. *Todo número racional não nulo pode ser representado como produto de dois números de Liouville.*

Demonstração. Seja L número de Liouville e n um número racional não nulo. Então tome $m = Ln$. Note que, pelo Teorema 4.8, m é número de Liouville. Temos também que L^{-1} é número de Liouville, segundo o Teorema 4.10. Portanto $n = L^{-1}m$, ou seja, n pode ser escrito como uma multiplicação de números de Liouville. ■

Teorema 4.12. *Dado um número de Liouville L, seu produto com um número irracional n (não de Liouville) resulta em um número irracional.*

Demonstração. Seja L número de Liouville e n um número irracional que não é de Liouville. Suponha, por absurdo, que $Ln = \alpha$, tal que $\alpha \in \mathbb{Q}$. Então $n = L^{-1}\alpha$, mas L^{-1} é número de Liouville e α é racional. Logo $L^{-1}\alpha$, pelo Teorema 4.10, é número de Liouville. Absurdo, pois isso contraria o fato de n não ser número de Liouville. Logo, Ln é irracional. ■

Teorema 4.13. *Qualquer número real pode ser escrito como a soma de dois números de Liouville.*

Demonstração. Inicialmente, tome $d \in \mathbb{Q}$ e L_1 número de Liouville. Perceba que $L_2 = d + L_1$ é número de Liouville, pelo Teorema 4.7. Assim, $d = L_2 - L_1$ é um racional escrito como soma de números de Liouville. Seguindo, seja $d \in \mathbb{R} - \mathbb{Q}$. Então podemos reescrever d como $\lfloor d \rfloor + \{d\}$, onde $\lfloor d \rfloor \in \mathbb{Z}$ é a parte inteira e $\{d\}$ é a parte fracionária de d. Note que $\{d\} \in (0, 1)$ e, assim, podemos reescrevê-lo em sua forma 2-ádica, ou seja, $d = \sum_{n \geq 1} a_n.2^{-n}$, com $a_n \in \{0, 1\}$.

Agora, suponha

$$\begin{aligned} L_1 &:= \sum_{n\geq 1} \alpha_n \cdot 2^{-n}; \\ L_2 &:= \sum_{n\geq 1} \beta_n \cdot 2^{-n}, \end{aligned}$$

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

$$\begin{aligned} \alpha_k = a_k \text{ e } \beta_k = 0 \text{ se } n \text{ for ímpar;} \\ \beta_k = a_k \text{ e } \alpha_k = 0 \text{ se } n \text{ for par.} \end{aligned}$$

Perceba que $L_1 + L_2 = d$. Entretanto, ainda falta provar que L_1 e L_2 são números de Liouville. Para L_1, dado $n \in \mathbb{N}^*$ qualquer, defina $q_n := 2^{(2n)!-1}$ e $p_n := q_n(\alpha_1 2^{-1} + \ldots + \alpha_{(2n)!-1} 2^{-(2n)!+1})$. Seguindo, obtemos que

$$L_1 - \frac{p_n}{q_n} = \sum_{i\geq 1} \alpha_i 2^{-i} - \sum_{i=1}^{(2n)!-1} \alpha_n 2^{-i} = \sum_{i\geq (2n)!} \alpha_i 2^{-i}.$$

Todavia, note que, como estamos trabalhando com L_1, temos que $\alpha_i = 0$ quando $(2n)! \leq i < (2n+1)!$. Logo, chegamos que

$$\begin{aligned} \left| L_1 - \frac{p_n}{q_n} \right| &= \sum_{i\geq (2n+1)!} \alpha_i 2^{-i} \\ &\leq \sum_{i\geq (2n+1)!} 2^{-i} \\ &= 2^{-(2n+1)!} \left(2^0 + 2^{-1} + 2^{-2} \ldots\right) \\ &= 2^{-(2n+1)!+1} \\ &< 2^{-n((2n)!-1)} \\ &= \frac{1}{q_n^n}. \end{aligned}$$

Por outro lado, para provar que L_2 é número de Liouville, dado $n \in \mathbb{N}^*$, tome $q_n = 2^{2n}$ e $p_n = q_n(\beta_1 2^{-1} + \ldots + \beta_{(2n)!} 2^{-(2n)!})$. Então temos que

$$L_2 - \frac{p_n}{q_n} = \sum_{i\geq 1} \beta_i 2^{-i} - \sum_{i=1}^{(2n)!} \beta_i 2^{-i} = \sum_{(2n)!+1} \beta_i 2^{-i}.$$

Agora, uma vez que estamos utilizando L_2, temos que $\beta_i = 0$ para $(2n+1)! \leq i < (2n+2)!$, bem como é possível reescrevermos a igualdade da seguinte forma:

$$\begin{aligned}
\left| L_2 - \frac{p_n}{q_n} \right| &= \sum_{i \geq (2n+2)!} \beta_i 2^{-i} \\
&\leq \sum_{i \geq (2n+2)} 2^{-i} \\
&= 2^{-(2n+2)!} \left(2^0 + 2^{-1} + 2^{-2} \dots \right) \\
&= 2^{-(2n+2)!+1} \\
&< 2^{-n(2n)!} \\
&= \frac{1}{q_n^n}.
\end{aligned}$$

■

Observação 10. Paul Erdös demonstrou também em 1962 que qualquer número real pode ser expresso como produto de dois números de Liouville. Tal fato pode ser verificado em [2].

Teorema 4.14. *O conjunto dos números de Liouville* $\mathbb{L}$ *é não enumerável.*

Demonstração. Suponha $\mathbb{L}$ enumerável. Então existe uma função injetora f com domínio $\mathbb{L}$ e contradomínio $\mathbb{N}$. Defina

$$\begin{aligned}
g : \mathbb{L} \times \mathbb{L} &\longrightarrow \mathbb{N} \\
(x, y) &\mapsto 2^{f(x)} 3^{f(y)}.
\end{aligned}$$

Perceba que g é injetora, uma vez que

$$g(x_1, y_1) = g(x_2, y_2) \iff 2^{f(x_1)} 3^{f(y_1)} = 2^{f(x_2)} 3^{f(y_2)}.$$

Mas, pelo Teorema Fundamental da Aritmética, isto só acontece quando $f(x_1) = f(x_2)$ e $f(y_1) = f(y_2)$. Assim, $(x_1, y_1) = (x_2, y_2)$, pois f é injetora. Logo, $\mathbb{L} \times \mathbb{L}$ é enumerável. Entretanto, pelo Teorema 4.13, é possível estabelecer uma injeção h com domínio $\mathbb{R}$ e contradomínio $\mathbb{L} \times \mathbb{L}$. Para tal, basta associar cada número real a um único par ordenado cuja soma das entradas do par é igual ao número real. Por fim, note que $(g \circ h) : \mathbb{R} \longrightarrow \mathbb{N}$ é injetora, por ser uma composição de funções injetoras. Assim, $\mathbb{R}$ é enumerável. Absurdo, pois isso contraria o Teorema 2.6. O absurdo provém de assumir que $\mathbb{L}$ é enumerável. Portanto, $\mathbb{L}$ é não enumerável. $\blacksquare$

5 CONSIDERAÇÕES FINAIS

Esta monografia possibilitou um estudo mais aprofundado sobre um assunto que, por vezes, não é discutido durante a graduação em matemática. Além disso, outro ponto positivo, foram as diversas demonstrações construídas durante a escrita. Isto deixou o trabalho com um "nível autoral" acima do esperado.

O autor não pretende parar o estudo sobre a "Teoria dos Números Transcendentes" por aqui. Os próximos passos incluem, por exemplo, aprender generalizações do Teorema 4.2 (de Liouville), entender o Teorema de Lindemann-Weierstrass e Gelfond-Schneider, com o intuito de construir um novo material. Além disso, por ser um amante da pesquisa, possui grande interesse em resolver problemas em aberto nesta área.

REFERÊNCIAS

[1] Matheus Manoel Dantas. “Descobrindo o universo transcendente com os números de Liouville”. Trabalho de Conclusão de Curso (Graduação em Matemática). Uberlândia: Universidade Federal de Uberlândia, 2017.

[2] Paul Erdös. “Representations of real numbers as sums and products of Liouville numbers”. Em: *Michigan Mathematical Journal* 9 (1962), pp. 59–60.

[3] Djairo Guedes de Figueiredo. *Números Irracionais e Transcendentes.* 3ª ed. Coleção de Iniciação Científica. Rio de Janeiro: SBM, 2011, p. 81.

[4] Adilson Gonçalves. *Introdução à álgebra.* 5ª ed. Projeto Euclides. Rio de Janeiro: IMPA, 2013, p. 194.

[5] Elon Lages Lima. *Álgebra Linear.* 9ª ed. Coleção Matemática Universitária. Rio de Janeiro: IMPA, 2016, p. 357.

[6] Elon Lages Lima. *Curso de análise v.1.* 14ª ed. Projeto Euclides. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2016, p. 432.

[7] Diego Marques. *Teoria dos Números Transcendentes.* 1ª ed. Coleção Textos Universitários. Rio de Janeiro: SBM, 2013, p. 223.

[8] Ivan Niven. *Diophantine Approximations.* 1ª ed. New York: Dover Publications, 2008, p. 76.

[9] Ivan Niven. *Números. Racionais e Irracionais.* Trad. por Renate Watanabe. 1ª ed. Coleção de Iniciação Científica. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012, p. 175.

[10] José Plínio de Oliveira Santos. *Introdução à Teoria dos Números.* 3ª ed. Coleção Matemática Universitária. Rio de Janeiro: IMPA, 2014, p. 198.

[11] Eric W. Weisstein. *CRC Concise Encyclopedia of Mathematics.* 2ª ed. CRC Press, 2002, p. 3252.