UNIVERSIDADE FEDERAL DE SERGIPE

Centro de Ciências Exatas e Tecnologia

Departamento de Matemática

Potências Transcendentes: Uma Jornada pelo Teorema de Gelfond-Schneider

Monografia apresentada ao Departamento de Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do título de Licenciatura em Matemática.

por

Mirelly Larissa Ferreira Santos

Licenciatura em Matemática – São Cristóvão - SE

Orientador: Prof. Dr. Fábio dos Santos

Setembro de 2025

Mirelly Larissa Ferreira Santos

Potências Transcendentes: Uma Jornada pelo Teorema de Gelfond-Schneider

Monografia apresentada ao Departamento de Matemática da Universidade Federal de Sergipe, como requisito parcial para obtenção do título de Licenciatura em Matemática.

Orientador: Prof. Dr. Fábio dos Santos

São Cristóvão
Setembro de 2025

"Não atentando nós nas coisas que se veem, mas nas que se não veem; porque as que se veem são temporais, e as que se não veem são eternas."
(BÍBLIA. N. T. 2 Coríntios. 4:18)

AGRADECIMENTOS

Primeiro de tudo, agradeço a Deus pelo fôlego de vida, por ter me guiado e me sustentado durante toda minha trajetória, sem Ele tenho certeza que não estaria aqui, não estaria na matemática e muito menos teria forças suficientes para continuar a graduação.

Agradeço imensamente a minha família que sempre investiu no meu futuro, me dando todas as condições para que eu trilhasse o caminho que escolhi. Agradeço a minha mãe Icleildes de Jesus Santos, que sempre me apoiou, e a minha avó Terezinha de Jesus Santos que sempre dizia para eu levantar a cabeça e prosseguir apesar de tudo. A toda minha família eu sou extremamente grata.

Ao professor Fábio dos Santos, que carinhosamente apelidei de Pai acadêmico, agradeço por toda paciência, ensino, conselhos e todas as condições que tive de fazer essa monografia e de estabelecer metas futuras a respeito da minha vida acadêmica. Nunca vou esquecer de toda gentileza do professor Fábio que dizia que a orientação era um "trabalho em equipe", ele sempre esteve presente em cada linha escrita nesta monografia, me sinto honrada de ter sido aluna de um professor tão querido por todos. Agradeço também a todos os professores e funcionários do departamento de matemática da UFS que sempre me fizeram sentir acolhida, me sinto muito feliz de ter conhecido um departamento com tantos professores que tem paixão pelo ensino da matemática.

Por último, mas não menos importante, gostaria de citar algumas pessoas que foram muito importantes durante a minha trajetória acadêmica, meus companheiros de departamento que estavam sempre ali presentes, Bruno Sant'Anna que foi meu primeiro amigo desde que entrei na ufs e continua sendo até hoje, Jacineide Santos que foi uma verdadeira mãezona pra mim, Talita Dantas e Camille Aimée minhas amigas queridas, Carlos Ismael meu companheiro de estágio e de sofrimento que me auxiliou durante meus estudos e se tornou um dos meus grande amigos e Rafael Fagundes, meu namorado, que tive o prazer de conhecer nos meus últimos períodos de graduação e se tornou uma das pessoas mais importantes pra mim, agradeço por ser meu apoio nos momentos difíceis e o motivo das minhas risadas nos momentos bons.

Mirelly Larissa Ferreira Santos

"Um matemático que não é também um pouco poeta nunca será um matemático completo."

Karl Weierstrass

RESUMO

Esta monografia tem como foco o estudo do Teorema de Gelfond-Schneider, um dos resultados mais marcantes da teoria dos números transcendentais, cuja demonstração solucionou o sétimo problema de Hilbert. O texto conduz o leitor por uma jornada gradual de conceitos fundamentais, abordando desde as noções de números algébricos e transcendentais até resultados clássicos, como o Teorema de Liouville, a transcendência de constantes notáveis (como e e π) e o Teorema de Hermite-Lindemann. Em seguida, apresenta os métodos e resultados auxiliares que sustentam a demonstração de Gelfond e Schneider, explorando também consequências e aplicações do teorema, como a caracterização da transcendência de diversas potências algébricas. Dessa forma, o trabalho busca não apenas expor a prova desse resultado, mas também contextualizar sua importância para a consolidação da teoria da transcendência e para a resolução de problemas abertos da matemática moderna.

Palavras-chave: Teorema de Gelfond-Schneider, números transcendentais, teoria dos números, sétimo problema de Hilbert.

ABSTRACT

This monograph focuses on the study of the Gelfond-Schneider Theorem, one of the most remarkable results in the theory of transcendental numbers, whose proof solved Hilbert's seventh problem. The text guides the reader through a gradual journey of fundamental concepts, ranging from the notions of algebraic and transcendental numbers to classical results, such as Liouville's Theorem, the transcendence of notable constants (such as e and π), and the Hermite-Lindemann Theorem. Then, it presents the methods and auxiliary results that underpin the proof by Gelfond and Schneider, also exploring consequences and applications of the theorem, such as the characterization of the transcendence of various algebraic powers. Thus, this work aims not only to present the proof of this result but also to contextualize its importance for the consolidation of transcendence theory and for solving open problems in modern mathematics.

Keywords: Gelfond-Schneider Theorem, transcendental numbers, number theory, Hilbert's seventh problem.

LISTA DE SÍMBOLOS

$\mathbb{R}$	Conjunto dos números reais
$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{C}$	Conjunto dos números complexos
$\overline{\mathbb{Q}}$	Conjunto dos números algébricos
$\mathbb{T}$	Conjunto dos números transcendentes
$\mathbb{L}$	Conjunto dos números de Liouville
K^*	Elementos não nulos de K
K^+	Conjunto dos elementos positivos de K
$\overline{K}$	Fecho algébrico de K
$\operatorname{int} K$	Interior de K: maior subconjunto aberto de K
$\max K$	Maior elemento de K
$\min K$	Menor elemento de K
$K[x_1, \ldots, x_n]$	Polinômios em n variáveis com coeficientes em K
$K \times K$	Produto cartesiano de K por $K : \{(a, b) : a, b \in K\}$
K^n	Produto cartesiano de n-cópias de K
$\#K$	Quantidade de elementos (cardinalidade) de K
$B(a, r)$	Bola aberta em $\mathbb{R}^n$ de centro a e raio $r : \{x \in \mathbb{R}^n : \lvert x - a\rvert < r\}$
$a \mid b$	"a divide b"
$a \nmid b$	"a não divide b"
$n!$	Fatorial de $n : n(n-1)\ldots 2 \cdot 1$
$\operatorname{mdc}(a, b)$	Máximo divisor comum entre a e b
$\binom{m}{k}$	Coeficiente binomial de m, k a $k : \frac{m!}{k!(m-k)!}$
$\log x$	Logaritmo natural de x
f'	Derivada da função f
$f^{(n)}$	n-ésima derivada da função f
∂P	Grau do polinômio
$\mathcal{H}(P)$	Altura de $P(x) = \sum_{k=0}^{n} a_k x^k : \max\{\lvert a_0\rvert, \ldots, \lvert a_n\rvert\}$
$\operatorname{Re} z$	Parte real de um número complexo: $\frac{z+\overline{z}}{2}$
$\operatorname{Im} z$	Parte imaginária de um número complexo: $\frac{z-\overline{z}}{2i}$
$\ker f$	Seja $f : X \to Y$, temos que $\ker(f) = \{x \in X \mid f(x) = 0_Y\}$
$\forall$	Para todo

Sumário

Introdução

O estudo dos números transcendentes constitui um dos ramos mais fascinantes e desafiadores da teoria dos números, pois rompe com a intuição e amplia os horizontes do conhecimento matemático desde o século XIX. Um número transcendente é aquele que não é raiz de nenhum polinômio não nulo com coeficientes inteiros, diferenciando-se dos números algébricos, que são precisamente as soluções dessas equações. A investigação acerca desses números começou a ganhar solidez com Joseph Liouville, que forneceu os primeiros exemplos explícitos de transcendentais. Posteriormente, avanços decisivos foram alcançados por Charles Hermite e Ferdinand von Lindemann, ao demonstrarem a transcendência das constantes fundamentais e e π, respectivamente.

Nesse cenário, surge o Teorema de Gelfond-Schneider, que solucionou uma das célebres questões propostas por David Hilbert em sua lista de 1900: o sétimo problema, relativo à natureza da expressão a^b, quando a e b são números algébricos, com a $\neq 0, 1$ e b irracional. O resultado, provado independentemente por Gelfond e Schneider na década de 1930, estabelece que, sob tais condições, a^b é sempre transcendente. Esse teorema não apenas generaliza descobertas anteriores — como a transcendência de e^π —, mas também abriu caminho para métodos mais robustos na teoria da transcendência.

Para alcançar a compreensão desse resultado, esta monografia percorre um caminho progressivo. O Capítulo 1 apresenta conceitos preliminares, como extensões de corpos, o Lema de Gauss e medidas de irracionalidade, essenciais para a fundamentação teórica. O Capítulo 2 explora em detalhe os números algébricos e transcendentes, abordando o Teorema de Liouville, a transcendência de e e π, e culminando no Teorema de Hermite-Lindemann, um marco na área. Por fim, o Capítulo 3 dedica-se ao Teorema de Gelfond-Schneider, expondo os resultados auxiliares, sua demonstração e algumas de suas consequências, incluindo exemplos notáveis de potências transcendentais.

Assim, o presente trabalho busca não apenas apresentar a prova desse teorema, mas também contextualizar sua relevância histórica e matemática, evidenciando sua contribuição para a consolidação da teoria da transcendência como um campo central da matemática moderna.

Capítulo 1

Resultados Preliminares

Neste captítulo iremos tratar de conceitos de estruturas algébricas que são fundamentais para a teoria dos números transcendentes e para a demonstração do Teorema de Gelfond-Schneider. Alguns destes conceitos podem ser encontrados nas referências [20] , [10] e [8].

1.1 Extensão de corpos

Definição 1.1.1. Dados dois corpos L e K, dizemos que L é uma extensão de K, quando K for um subcorpo de L. Neste caso, consideramos L como um K-espaço vetorial L.

Definição 1.1.2. Dizemos que $\alpha \in L$ é algébrico sobre K se existe $P(x) \in K[x] - \{0\}$ tal que $P(\alpha) = 0$. Caso contrário α é dito transcendente sobre K.

Se $\alpha \in K$, claramente, α é algébrico sobre K, pois é raíz de $P(x) = x - \alpha$, com $P(x) \in K[x]$. Se para todo $\alpha \in L|K$, α é algébrico sobre K então $L|K$ é dito ser uma extensão algébrica.

Definição 1.1.3. Seja $\alpha \in L|K$, com α algébrico sobre K e seja $P(x)$ um polinômio mônico, de menor grau tal que $P(\alpha) = 0$. Pela minimalidade do grau segue de maneira clara que $P(x)$ é o único polinômio mônico irredutível em $K[x]$ tal que $P(\alpha) = 0$, o qual denotaremos por $P_{\alpha,K}$.

Definição 1.1.4. Se $\alpha \in L|K$ definimos $K[\alpha] = \{P(\alpha) : P(x) \in K[x]\}$.

Exemplo 1.1.1. Se $\alpha = \sqrt{2} \in L = \mathbb{R} \supset \mathbb{Q} = K$. Vamos mostrar que $K[\alpha] = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. De fato, pela definição 1.1.4 temos $\mathbb{Q}[\sqrt{2}] = \{P(\sqrt{2}) : P(x) \in \mathbb{Q}[x]\}$. Como $P(x) \in \mathbb{Q}[x]$ segue pelo algoritmo da divisão que existe $R(x), T(x) \in \mathbb{Q}(x)$ tais que $P(x) = T(x)(x^2 - 2) + R(x)$, onde $R(x) = a + bx$ com $a, b \in \mathbb{Q}$, e daí, vem que $P(\sqrt{2}) = R(\sqrt{2}) = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$.

Observação 1.1.1. Seja $L|K$ extensão e $\alpha \in L$. Definimos:

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], \quad g(\alpha) \neq 0 \right\},$$

como sendo o corpo gerado por α sobre K. Daí, temos que:

- Se α é **algébrico** sobre K: $K[\alpha] = K(\alpha)$
- Se α é **transcendente** sobre K: $K[\alpha] \subsetneq K(\alpha)$,
  onde $K[\alpha] \cong K[x]$ e $K(\alpha) \cong K(x)$

Logo, $K[\alpha] = K(\alpha) \Leftrightarrow \alpha$ é algébrico sobre K.

Teorema 1.1.1. Se $\alpha \in L|K$ e se $\psi : K[x] \to L$ é definida por $\psi(f(x)) = f(\alpha)$, então ψ é um homomorfismo tal que:

(i) $Im\psi = K[\alpha]$, $K \subset K[\alpha] \subset L$;

(ii) α é transcendente sobre $K \Leftrightarrow \ker(\psi) = \{0\}$;

(iii) Se α é algébrico sobre K e seu polinômio minimal $P_{\alpha,K}$ então $\ker(\psi) = K[x] \cdot P_{\alpha,K}$ é um ideal maximal de $K[x]$;

(iv) $K[x]/\ker(\psi) \simeq K[\alpha]$.

Demonstração. (i) Suponha $\beta \in \operatorname{Im}\psi$, por definição isso nos diz que:

$$\beta = \psi(f(x))$$

Para algum $f(x) \in K[x]$, mas isso implica que $\beta = f(\alpha)$, ou seja, $\beta \in K[\alpha]$;

(ii) Iremos demonstrar a primeira parte do item (ii) usando a contrapositiva, se $\ker(\psi) \neq \{0\}$, então α é algébrico.

Se $\ker(\psi) \neq 0$, então existe $f(x) \in K[x] - \{0\}$ tal que $\psi(f(x)) = 0$ e por definição, $f(\alpha) = 0$. Logo, α é algébrico.

Agora para a segunda parte do item (ii): Se α é algébrico, então $\ker(\psi) \neq \{0\}$.

Se α é algébrico, então $f(\alpha) = 0$, com $f(x) \in K[x] - \{0\}$. Assim, $\psi(f(x)) = 0 \Rightarrow f(x) \in \ker(\psi)$, logo $\ker(\psi) \neq \{0\}$;

(iii) Primeiro mostraremos que $\ker(\psi) = K[x] \cdot P_{\alpha,K}$, ou seja, $\ker(\psi)$ é um de ideal principal gerado por $P_{\alpha,K}$

- $\ker(\psi) \subset K[x] \cdot P_{\alpha,K}$
  Tome $f(x) \in \ker(\psi)$ e $f(\alpha) = 0$, como $P_{\alpha,K}$ é o polinômio minimal mônico e irredutível, temos que $P_{\alpha,K}$ divide todo polinômio em $K[x]$ tal que α é raiz, então pelo algoritmo da divisão euclidiana

  $$f(x) = P_{\alpha,K} \cdot q(x)$$

  Com $q(x) \in K[x]$ e assim temos que $f(x) \in K[x] \cdot P_{\alpha,K}$

- $K[x] \cdot P_{\alpha,K} \subset \ker(\psi)$
  Tome $g(x) \in K[x] \cdot P_{\alpha,K}$, então $g(x) = q_1(x) \cdot P_{\alpha,K}$ com $q_1(x) \in K[x]$. Fazendo $x = \alpha$ temos

  $$g(\alpha) = q_1(\alpha).P_{\alpha,K}(\alpha)$$

  Como α é algébrico isso nos diz que $g(\alpha) = 0$. Assim, $g(x) \in \ker(\psi)$. Portanto, $\ker(\psi) = K[x] \cdot P_{\alpha,K}$ por inclusão de conjuntos.

Considere J um ideal de $K[x]$ tal que $J \supsetneq K[x] \cdot P_{\alpha,K}$, tome $f(x) \in J$, tal que $f(x)$ não esteja no ideal gerado por $P_{\alpha,K}$ de α. Como $P_{\alpha,K}$ é irredutível, tem-se que $\text{mdc}(P_{\alpha,K}, f(x)) = 1$. Pelo teorema de Bézout [1] existem $h(x), g(x) \in K[x]$, tais que

$$h(x) \cdot P_{\alpha,K} + g(x) \cdot f(x) = 1,$$

mas isso implica que qualquer polinômio de $K[x]$ pode ser escrito como $s(x) = s(x)h(x) \cdot P_{\alpha,K} + s(x)g(x) \cdot f(x)$, donde $s(x) \in J$, pois $P_{\alpha,K}$ e $f(x)$ pertencem a J. Logo, o único ideal de $K[x]$ que contém $K[x] \cdot P_{\alpha,K} = \ker(\psi)$, mas não é igual a ele, é o próprio $K[x]$;

(iv) Pelo primeiro teorema dos isomorfismos temos que:

$$K[x]/\ker(\psi) \simeq \text{Im}\,\psi.$$

E pelo item **(i)** $K[x]/\ker(\psi) \simeq K[\alpha]$.

□

Corolário 1.1.2. Se $\alpha, \beta \in L|K$ são raízes de um mesmo polinômio irredutível sobre K, então $K(\alpha)$ e $K(\beta)$ são corpos isomorfos.

Demonstração. Por hipótese segue que $P_{\alpha,K} = P_{\beta,K}$ e pelos itens (iii) e (iv) do teorema

[1] Seja K um corpo e sejam $f(x), g(x) \in K[x]$ polinômios não ambos nulos. Se $d(x) = \text{mdc}(f(x), g(x))$, então existem polinômios $q(x), h(x) \in K[x]$ tais que: $q(x)f(x) + h(x)g(x) = d(x)$

1.1.1 temos que:

$$K[x]\cdot P_{\alpha,K} = \ker(\psi) = K[x]\cdot P_{\beta,K}$$

além disso, $K(\alpha)\simeq K[x]/\ker(\psi)\simeq K(\beta)$,. □

Proposição 1.1.3. Seja $L|K$ extensão, e $\alpha\in L$ algébrico sobre K. Se o grau do polinômio $P_{\alpha,K}$ é n, então: **a)** para todo $f(x)\in K[x]$, $f(\alpha)$ pode ser expresso de modo único na forma $f(\alpha)=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$, onde $a_i\in K$. **b)** Se $K=\mathbb{Z}_p=\{\overline{0},\overline{1},\ldots,\overline{p-1}\}$ então $K(\alpha)$ é um corpo contendo exatamente p^n elementos.

Demonstração. **a)** Seja $P_{\alpha,K}(x)$ o polinômio minimal de α sobre K, com $\deg P_{\alpha,K}=n$. Dado $f(x)\in K[x]$, pelo algoritmo da divisão existem $q(x),r(x)\in K[x]$ tais que:

$$f(x)=q(x)P_{\alpha,K}(x)+r(x),\quad \text{com } r(x)=0 \text{ ou } \deg r(x)<n.$$

Avaliando em α e usando $P_{\alpha,K}(\alpha)=0$, obtemos $f(\alpha)=r(\alpha)$. Como $\partial r(x)<n$, podemos escrever:

$$r(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}\Rightarrow f(\alpha)=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}.$$

Para a unicidade, suponha que

$$f(\alpha)=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}=b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1}.$$

Definindo $q(x)=(a_0-b_0)+(a_1-b_1)x+\cdots+(a_{n-1}-b_{n-1})x^{n-1}$, temos $q(\alpha)=0$ e $\deg q(x)<n$. Como $P_{\alpha,K}$ é o polinômio minimal de grau n, segue que $q(x)\equiv 0$, logo $a_i=b_i$ para todo i.

b) Pelo item (a), todo elemento de $K(\alpha)$ se escreve de forma única como

$$a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1},\quad a_i\in\mathbb{Z}_p.$$

Como cada a_i pode assumir p valores e há n coeficientes, há exatamente p^n elementos em $K(\alpha)$. Além disso, como $P_{\alpha,K}$ é irredutível (por ser minimal), o ideal $(P_{\alpha,K})$ é maximal em $K[x]$, logo $K(\alpha)\cong K[x]/(P_{\alpha,K})$ é um corpo.

□

Definição 1.1.5. O grau da extensão $L|K$, denotada por $[L:K]$, é igual à dimensão de L como K-espaço vetorial. Dizemos que $\mathcal{B}$ é uma base da extensão $L|K$, quando $\mathcal{B}$ é base do K-espaço vetorial L.

Proposição 1.1.4 (Multiplicidade do grau)**.** Sejam K,L e M corpos tais que $K\subseteq L\subseteq M$. Então $[M:K]=[M:L].[L:K]$, onde cada extensão possui grau finito.

Demonstração. Seja $v_1, \ldots, v_r$ uma base de M sobre L (onde $r = [M : L]$) e seja $u_1, \ldots, u_s$ uma base de L sobre K (onde $s = [L : K]$). Vamos provar que:

$$\beta = \left\{ v_i \cdot u_j : \begin{array}{l} i = 1, \ldots, r \\ j = 1, \ldots, s \end{array} \right\},$$

é uma base de M com rs elementos, sobre K e isto demonstra a proposição. Primeiramente vamos provar que β é um conjunto L.I. em M sobre K. Se $\alpha_{ij} \in K, 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s$ e $\sum_{i,j} \alpha_{ij} v_i u_j = 0$. Podemos escrever essa equação do seguinte modo:

$$(\alpha_{11}u_1 + \alpha_{12}u_2 + \cdots + \alpha_{1s}u_s)v_1 + \cdots + (\alpha_{r1}u_1 + \alpha_{r2}u_2 + \cdots + \alpha_{rs}u_s)v_r = 0.$$

Ora como os u_j's estão em L segue, pela independência linear dos v_i's em M sobre L, que:

$$\begin{cases} \alpha_{11}u_1 + \alpha_{12}u_2 + \cdots + \alpha_{1s}u_s = 0 \\ \vdots \\ \alpha_{r1}u_1 + \alpha_{r2}u_2 + \cdots + \alpha_{rs}u_s = 0. \end{cases}$$

Agora como os α_{ij}'s estão em K segue pela independência linear dos u_j's em L sobre K que cada $\alpha_{ij} = 0$ onde $1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s$. Assim β é um conjunto L.I. de M sobre K. Agora vamos provar que β é um conjunto gerador de M sobre K. De fato, seja $y \in M$. Sendo $v_1, \ldots, v_r$ uma base de M sobre L existem $\lambda_1, \ldots, \lambda_r \in L$ tais que,

$$y = \lambda_1 v_1 + \cdots + \lambda_r v_r.$$

Sendo cada $\lambda_i \in L$ e $u_1, \ldots, u_s$ uma base de L sobre K existe $\alpha_{ij} \in K$, $1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s$ tais que,

$$\lambda_i = \alpha_{i1}u_1 + \alpha_{i2}u_2 + \cdots + \alpha_{is}u_s.$$

Daí segue imediatamente que,

$$y = \sum_{i,j} \alpha_{ij} v_i u_j.$$

Portanto, β é uma base de M sobre K com $rs = [M : L] \cdot [L : K]$ elementos, logo $[M : K] = [M : L] \cdot [L : K]$. □

Teorema 1.1.5. Sejam $L|K$ uma extensão e $\alpha \in L$ algébrico sobre K de grau n. Então $[K(\alpha) : K] = n$ e $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base $L|K$.

Demonstração. Seja $\alpha \in L|K$ um elemento algébrico sobre K tal que o grau de $\partial P_{\alpha,K} = n$. Vimos pela proposição 1.1.3 que todo elemento $K(\alpha)$ pode ser escrito de modo único como combinação linear sobre K de $1, \alpha, \ldots, \alpha^{n-1}$. Assim, $1, \alpha, \ldots, \alpha^{n-1}$ é uma base de $K[\alpha]$ sobre K e isto nos diz que $[K(\alpha) : K] = n$. □

Teorema 1.1.6. Sejam $L|K$ uma extensão e $\alpha \in L$. Então α é algébrico sobre K se e só se $[K(\alpha) : K] < \infty$.

Demonstração. Suponha α é algébrico sobre K. Pelo teorema 1.1.5 temos

$$[K(\alpha) : K] = \partial P_{\alpha,K} \leqslant n < \infty.$$

Suponha $[K(\alpha) : K] = n$. Pelo teorema 1.1.5, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é base da extensão $K(\alpha)|K$. Em particular, é um conjunto linearmente independente maximal sobre K. Assim, existem $a_0, \ldots, a_{n-1}, a_n \in K$, não todos nulos, tais que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0,$$

mostrando que α é algébrico sobre K. □

Assim, se K é um corpo de números algébricos (isto é, uma extensão finita de $\mathbb{Q}$) e θ um elemento de K. Então todo elemento $\beta \in \mathbb{Q}(\theta)$ pode ser unicamente representado como um polinômio em θ coeficientes em $\mathbb{Q}$, isto é,

$$\beta = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}, \quad a_i \in \mathbb{Q},$$

onde $n = [\mathbb{Q}(\theta) : \mathbb{Q}]$.

Além disso, podemos facilmente generalizar esse fato da seguinte maneira: sejam K um corpo de números algébricos e $\theta_1, \ldots, \theta_s$ elementos de K. Então para todo elemento $\beta \in \mathbb{Q}(\theta_1, \ldots, \theta_s)$, temos

$$\beta = f(\theta_1, \ldots, \theta_s), \quad \text{onde} \quad f(x_1, \ldots, x_s) \in \mathbb{Q}[x_1, \ldots, x_s].$$

O conjunto dos números algébricos é denotado por $\overline{\mathbb{Q}}$ e, para simplificar em alguns momentos, $\mathbb{T}$ denotará o conjunto dos números transcendentes. Mostraremos a seguir que o conjunto dos números algébricos forma um corpo.

Proposição 1.1.7. Dados a e $b \in \overline{\mathbb{Q}}$, temos:

(i) $a \pm b \in \overline{\mathbb{Q}}$;

(ii) $a \cdot b \in \overline{\mathbb{Q}}$;

(iii) Se $a \neq 0$, então $a^{-1} \in \overline{\mathbb{Q}}$.

Demonstração. (i) Como a e b são algébricos, então $[\mathbb{Q}(a, b) : \mathbb{Q}] < \infty$, mas $\mathbb{Q}(a \pm b) \subset \mathbb{Q}(a, b)$, logo $[\mathbb{Q}(a \pm b) : \mathbb{Q}] < \infty$ e portanto $a \pm b \in \overline{\mathbb{Q}}$;

(ii) Note que $\mathbb{Q}(a\cdot b)\subset\mathbb{Q}(a,b)$. Daí, $[\mathbb{Q}(a\cdot b):\mathbb{Q}]<\infty$ e então $a\cdot b\in\overline{\mathbb{Q}}$;

(iii) É só observar que $\mathbb{Q}(a)=\mathbb{Q}(a^{-1})$, portanto $[\mathbb{Q}(a^{-1}):\mathbb{Q}]=[\mathbb{Q}(a):\mathbb{Q}]$. Daí $a^{-1}\in\overline{\mathbb{Q}}$.

□

O fato de $\mathbb{Q}$ ser denso em $\mathbb{R}$ garante também a densidade de $\overline{\mathbb{Q}}$ em $\mathbb{R}$. Se denotarmos $\overline{\mathbb{Q}}_m$ como o conjunto dos algébricos de grau m, temos em particular que $\overline{\mathbb{Q}}_1=\mathbb{Q}$. Assim, o próximo resultado fornece uma informação mais forte.

Proposição 1.1.8. Para todo $m\geqslant 1$, o conjunto $\overline{\mathbb{Q}}_m$ é denso em $\mathbb{R}$.

Demonstração. Defina o conjunto $\mathcal{P}_m:=\{Q(1+\sqrt[m]{2}):Q\in\mathbb{Q}\}$. Note que tal conjunto é denso em $\mathbb{R}$, pois se $(a,b)\subseteq\mathbb{R}$, então existe um $Q\in\mathbb{Q}$ no intervalo $(\frac{a}{1+\sqrt[m]{2}},\frac{b}{1+\sqrt[m]{2}})$. Portanto $\mathcal{P}_m\cap(a,b)\neq\varnothing$. Agora, o resultado segue pois $1+\sqrt[m]{p}$ é raiz de $P(x)=(x-1)^m-p$ que é irredutível sobre $\mathbb{Q}$, visto que $P(x+1)$ é irredutível pelo critério de Eisenstein [2]. □

A seguir forneceremos algumas definições e resultados mais técnicos sobre extensões algébricas.

Definição 1.1.6. Um polinômio $P(x_1,\ldots,x_n)\in\mathbb{A}[x_1,\ldots,x_n]$, onde $\mathbb{A}$ é um anel, é chamado simétrico ou função simétrica em $x_1,\ldots,x_n$ se

$$P(x_1,\ldots,x_n)=P(x_{\alpha(1)},\ldots,x_{\alpha(n)}),$$

para toda permutação $\alpha\in S_n$, onde S_n é o conjunto das permutações do conjunto $\{1,\ldots,n\}$. Para cada, $1\leqslant k\leqslant n$, o polinômio

$$\sigma_k(x_1,\ldots,x_n)=\sum_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n}x_{i_1}x_{i_2}\ldots x_{i_k},$$

é simétrico em $x_1,\ldots,x_n$ e é chamado de k-ésima função simétrica elementar.

Exemplo 1.1.2. A função $P(x,y)=x^2+y^2$ é simétrica e além disso pode ser escrita da seguinte forma:

- $\sigma_1=x+y$
- $\sigma_2=xy$

[2] Seja $P(x)=a_nx^n+\cdots+a_0$ um polinômio com coeficientes inteiros. Se existe p primo, tal que: (i) $p\mid a_0,a_1,\ldots,a_{n-1}$; (ii) $p\nmid a_n$; (iii) $p^2\nmid a_0$.

e note que

$$(x+y)^2 = x^2 + 2xy + y^2.$$

Portanto,

$$P(x,y) = x^2 + y^2 = (x+y)^2 - 2xy = \sigma_1^2 - 2\sigma_2.$$

Teorema 1.1.9 (Teorema Fundamental das Funções Simétricas)**.** Seja P uma função simétrica em n variáveis com coeficientes em $\mathbb{A}$. Então existe $\varphi \in \mathbb{A}[x_1,\ldots,x_n]$ tal que

$$P(x_1,\ldots,x_n) = \varphi(\sigma_1(x_1,\ldots,x_n),\ldots,\sigma_n(x_1,\ldots,x_n)),$$

onde $\sigma_1(x_1,\ldots,x_n),\ldots,\sigma_n(x_1,\ldots,x_n)$ estão definidos 1.1.6.

Demonstração. Vamos proceder por indução no número de variáveis e no grau do polinômio.

Caso base: Para $n = 1$, as únicas funções simétricas são os polinômios em x_1, e $\sigma_1 = x_1$, então o resultado é trivial com $\varphi = P$.

Passo indutivo: Suponha o teorema válido para $n-1$ variáveis.

Seja $P(x_1,\ldots,x_n)$ um polinômio simétrico. Considere P como polinômio em x_n com coeficientes em $A[x_1,\ldots,x_{n-1}]$:

$$P(x_1,\ldots,x_n) = \sum_{k=0}^{m} Q_k(x_1,\ldots,x_{n-1})x_n^k.$$

Como P é simétrico, cada Q_k também é simétrico nas variáveis $x_1,\ldots,x_{n-1}$ (pois a simetria é preservada quando fixamos uma variável).

Pela hipótese de indução, existem polinômios ψ_k tais que:

$$Q_k(x_1,\ldots,x_{n-1}) = \psi_k(\sigma_1(x_1,\ldots,x_{n-1}),\ldots,\sigma_{n-1}(x_1,\ldots,x_{n-1})).$$

Agora, note que as funções simétricas elementares em $n-1$ variáveis podem ser expressas em termos das funções simétricas em n variáveis:

$$\sigma_i(x_1,\ldots,x_{n-1}) = \sigma_i(x_1,\ldots,x_n) - x_n\sigma_{i-1}(x_1,\ldots,x_{n-1}) \quad \text{para } i = 1,\ldots,n-1.$$

Substituindo, obtemos:

$$P(x_1,\ldots,x_n) = \sum_{k=0}^{m} \psi_k(\sigma_1 - x_n, \sigma_2 - x_n\sigma_1,\ldots,\sigma_{n-1} - x_n\sigma_{n-2})x_n^k,$$

onde $\sigma_i = \sigma_i(x_1,\ldots,x_n)$.

Esta expressão pode ser vista como um polinômio em x_n com coeficientes que são polinômios nas funções simétricas elementares. Como x_n é raiz do polinômio:

$$t^n - \sigma_1 t^{n-1} + \sigma_2 t^{n-2} - \cdots + (-1)^n \sigma_n = 0,$$

podemos reduzir qualquer potência x_n^k com $k \geqslant n$ usando esta relação, expressando x_n^k como combinação polinomial de 1, x_n, $x_n^2, \ldots, x_n^{n-1}$ com coeficientes que são polinômios em $\sigma_1, \ldots, \sigma_n$.

Assim, após esta redução, obtemos:

$$P(x_1, \ldots, x_n) = \sum_{j=0}^{n-1} R_j(\sigma_1, \ldots, \sigma_n) x_n^j,$$

onde cada R_j é um polinômio com coeficientes em A.

Agora, como P é simétrico, ele deve ser invariante por permutações das variáveis. Em particular, se trocarmos x_n por qualquer outra variável x_i, a expressão deve permanecer a mesma. Isso força que todos os coeficientes R_j para $j \geqslant 1$ devem ser identicamente nulos, pois caso contrário a expressão não seria simétrica.

Portanto, temos:

$$P(x_1, \ldots, x_n) = R_0(\sigma_1, \ldots, \sigma_n).$$

Tomando $\varphi = R_0$, obtemos o resultado desejado:

$$P(x_1, \ldots, x_n) = \varphi(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)).$$

Assim, concluímos a demonstração. □

Proposição 1.1.10. Sejam $\beta_1, \ldots, \beta_n$ raízes de um polinômio

$$f(x) = bx^n + c_1 x^{n-1} + \cdots + c_n,$$

com coeficientes inteiros. Se $P(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ é simétrico, então $P(\beta_1, \ldots, \beta_n) \in \mathbb{Q}$. Além disso, se $P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ e $\partial P = t$ então $b^t P(\beta_1, \ldots, \beta_n) \in \mathbb{Z}$.

Demonstração. (1ª parte) Pelo Teorema Fundamental das Funções Simétricas, existe $\varphi(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ tal que

$$P(x_1, \ldots, x_n) = \varphi(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)),$$

logo

$$P(\beta_1, \ldots, \beta_n) = \varphi(\sigma_1(\beta_1, \ldots, \beta_n), \ldots, \sigma_n(\beta_1, \ldots, \beta_n)).$$

Por outro lado, como $\beta_1, \ldots, \beta_n$ raízes de $f(x) = bx^n + c_1x^{n-1} + \cdots + c_n$, então $\sigma_i(\beta_1, \ldots, \beta_n) = (-1)^i \frac{c_i}{b} \in \mathbb{Q}$ (as chamadas relações de Girard). Daí $P(\beta_1, \ldots, \beta_n) \in \mathbb{Q}$.
(2ª parte) Se $P(x_1, \ldots, x_n)$ é um polinômio simétrico com coeficientes inteiros, então pelo Teorema 1.1.9,

$$P(x_1, \ldots, x_n) = \varphi(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)), \tag{1.1.1}$$

onde $\varphi(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, assim

$$\varphi(x_1, \ldots, x_n) = \sum_{(i)} a_{(i)} x_1^{i_1} \ldots x_n^{i_n},$$

onde $a_{(i)} \in \mathbb{Z}$. Por 1.1.1, o grau de φ é t, isto é, $\max_{(i)}\{i_1 + \cdots + i_n | a_{(i)} \neq 0\} = t$. Por outro lado, $\sigma_i(\beta_1, \ldots, \beta_n) = (-1)^i \frac{c_i}{b}$. Aplicando a igualdade 1.1.1 para $\beta_1, \ldots, \beta_n$, obtemos:

$$\begin{aligned} P(\beta_1, \ldots, \beta_n) &= \varphi(\sigma_1(\beta_1, \ldots, \beta_n), \ldots, \sigma_n(\beta_1, \ldots, \beta_n)) \\ &= \sum_{(i)} a_{(i)} \sigma_1(\beta_1, \ldots, \beta_n)^{i_1} \ldots \sigma_n(\beta_1, \ldots, \beta_n)^{i_n} \\ &= \sum_{(i)} a_{(i)} (-1)^{i_1} \left(\frac{c_1}{b}\right)^{i_1} \ldots (-1)^{ni_n} \left(\frac{c_n}{b}\right)^{i_n} \\ &= \sum_{(i)} (-1)^m \frac{a_{(i)}}{b^{i_1 + \cdots + i_n}} c_1^{i_1} \ldots c_n^{i_n}, \end{aligned}$$

onde $m = i_1 + 2i_2 + \cdots + ni_n$. Portanto,

$$b^t P(\beta_1, \ldots, \beta_n) = \sum_{(i)} (-1)^m b^{t-(i_1 + \cdots + i_n)} a_{(i)} c_1^{i_1} \ldots c_n^{i_n}.$$

Como $t \geqslant i_1 + \cdots + i_n$, para todo multi-índice (i), então

$$b^t P(\beta_1, \ldots, \beta_n) \in \mathbb{Z}.$$

Assim, concluímos a demonstração. □

Teorema 1.1.11 (Teorema do Elemento Primitivo)**.** Se α_1, $\alpha_2, \ldots, \alpha_s$ são algébricos sobre $\mathbb{Q}$, então existe γ algébrico sobre $\mathbb{Q}$, tal que

$$\mathbb{Q}[\gamma] = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_s).$$

Demonstração. Vamos proceder por indução no número de elementos. O caso $s = 1$ é trivial (tomamos $\gamma = \alpha_1$).

Suponhamos o resultado válido para $s - 1$ elementos. Então existe β algébrico

sobre $\mathbb{Q}$ tal que:

$$\mathbb{Q}(\beta) = \mathbb{Q}(\alpha_1, \ldots, \alpha_{s-1})$$

Agora precisamos mostrar que existe γ algébrico sobre $\mathbb{Q}$ tal que:

$$\mathbb{Q}(\gamma) = \mathbb{Q}(\beta, \alpha_s).$$

Sejam $f(x)$ e $g(x)$ os polinômios mínimos de β e α_s sobre $\mathbb{Q}$, respectivamente. Sejam $\beta = \beta_1, \beta_2, \ldots, \beta_m$ as raízes de $f(x)$ e $\alpha_s = \alpha_{s1}, \alpha_{s2}, \ldots, \alpha_{sn}$ as raízes de $g(x)$.

Como $\mathbb{Q}$ é infinito, existe $c \in \mathbb{Q}$ tal que:

$$c \neq \frac{\beta_i - \beta}{\alpha_s - \alpha_{sj}} \quad \text{para todo } i = 1, \ldots, m \text{ e } j = 2, \ldots, n.$$

Definimos:

$$\gamma = \beta + c\alpha_s.$$

Claramente, $\gamma \in \mathbb{Q}(\beta, \alpha_s)$, logo $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\beta, \alpha_s)$.

Agora vamos mostrar que $\alpha_s \in \mathbb{Q}(\gamma)$. Considere os polinômios:

$$h(x) = f(\gamma - cx) \in \mathbb{Q}(\gamma)[x].$$

Note que:

$$h(\alpha_s) = f(\gamma - c\alpha_s) = f(\beta) = 0.$$

Mas $h(\alpha_{sj}) = f(\gamma - c\alpha_{sj})$ para $j \neq 1$. Pela escolha de c, temos que $\gamma - c\alpha_{sj} \neq \beta_i$ para todo i, pois:

$$\gamma - c\alpha_{sj} = \beta + c\alpha_s - c\alpha_{sj} = \beta + c(\alpha_s - \alpha_{sj}).$$

Se $\beta + c(\alpha_s - \alpha_{sj}) = \beta_i$ para algum i, então $c = \frac{\beta_i - \beta}{\alpha_s - \alpha_{sj}}$, o que contradiz a escolha de c.

Portanto, $h(\alpha_{sj}) \neq 0$ para $j \neq 1$, e assim α_s é a única raiz comum de $g(x)$ e $h(x)$. O máximo divisor comum de $g(x)$ e $h(x)$ em $\mathbb{Q}(\gamma)[x]$ é então $(x - \alpha_s)$, logo $x - \alpha_s \in \mathbb{Q}(\gamma)[x]$, o que implica que $\alpha_s \in \mathbb{Q}(\gamma)$.

Como $\beta = \gamma - c\alpha_s$ e ambos γ e α_s estão em $\mathbb{Q}(\gamma)$, segue que $\beta \in \mathbb{Q}(\gamma)$. Portanto:

$$\mathbb{Q}(\beta, \alpha_s) \subseteq \mathbb{Q}(\gamma).$$

Concluímos que $\mathbb{Q}(\gamma) = \mathbb{Q}(\beta, \alpha_s) = \mathbb{Q}(\alpha_1, \ldots, \alpha_s)$, e γ é algébrico sobre $\mathbb{Q}$ pois é

elemento de uma extensão algébrica. □

Definição 1.1.7. Uma extensão algébrica $\mathbb{Q}(\theta)|\mathbb{Q}$ é chamada normal se todo polinômio em $\mathbb{Q}[x]$ que tem pelo menos uma raiz em $\mathbb{Q}(\theta)$, tiver todas as raízes em $\mathbb{Q}(\theta)$.

Por exemplo, a extensão $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ é normal, mas a extensão $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ não é, já que $\sqrt[3]{2}(1+i\sqrt{3})/2$ é raiz de x^3-2, mas não pertence a $\mathbb{Q}(\sqrt[3]{2})$.

Proposição 1.1.12. Sejam $\alpha_1,,\ldots,\alpha_s$ números algébricos, então existe θ algébrico tal que

$$\mathbb{Q}(\theta) \supset \mathbb{Q}(\alpha_1,\ldots,\alpha_s)$$

e $\mathbb{Q}(\theta)|\mathbb{Q}$ é normal.

Demonstração. Pela proposição 1.1.7, existe γ algébrico sobre $\mathbb{Q}$ tal que

$$\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha_1,\ldots,\alpha_s).$$

Considere $P_{\gamma,\mathbb{Q}}$ o polinômio minimal de γ. Sejam $\gamma=\gamma_1,\ldots,\gamma_m$ as m raízes de $P_{\gamma,\mathbb{Q}}$. Aplicando novamente a proposição 1.1.7, temos que existe θ algébrico tal que

$$\mathbb{Q}(\theta) = \mathbb{Q}(\gamma_1,\ldots,\gamma_s) \supset \mathbb{Q}(\gamma) = \mathbb{Q}(\alpha_1,\ldots,\alpha_s).$$

Resta-nos provar que $\mathbb{Q}(\theta)|\mathbb{Q}$ é normal. De fato, considere $g(x)\in\mathbb{Q}[x]$ irredutível e mônico, com uma raiz $\alpha\in\mathbb{Q}(\theta)$, ou seja $g=P_{\alpha,\mathbb{Q}(\theta)}$. Queremos mostrar que toda raiz de $g(x)$ pertence a $\mathbb{Q}(\theta)$. Como $\alpha\in\mathbb{Q}(\theta)=\mathbb{Q}(\gamma_1,\ldots,\gamma_m)$, então existe um polinômio $f(x_1,\ldots,x_m)\in\mathbb{Q}[x_1,\ldots,x_m]$ tal que $\alpha=f(\gamma_1,\ldots,\gamma_m)$. Defina então o seguinte polinômio:

$$G(x) = \prod_{\sigma\in S_m} \left(x - f(\gamma_{\sigma(1)},\ldots,\gamma_{\sigma(m)})\right), \tag{1.1.2}$$

onde $\sigma\in S_m$. Portanto, $\partial G = m!$ e os coeficientes de $G(x)$ são funções simétricas em $\{f(\gamma_{\sigma(1)},\ldots,\gamma_{\sigma(m)})\}_{\sigma\in S_m}$. Por outro lado, quando permutamos $\{\gamma_1,\ldots,\gamma_m\}$ temos que $\{f(\gamma_{\sigma(1)},\ldots,\gamma_{\sigma(m)})\}_{\sigma\in S_m}$ fica invariante. Logo os coeficientes de $G(x)$ são funções simétricas em $\gamma_1,\ldots,\gamma_m$ e pela Proposição 1.1.10 são racionais, daí $G(x)\in\mathbb{Q}[x]$ e $G(\alpha)=0$. Segue-se então que $g(x)\mid G(x)$, isto é, $G(x)=g(x)h(x)$ para algum $h(x)\in\mathbb{Q}[x]$. Sejam $\alpha=a_1,\ldots,a_l$ as raízes de $g(x)$ então

$$G(a_j) = g(a_j)\,h(a_j) = 0, \quad \forall j\in\{1,\ldots,l\}.$$

Daí a_j é raiz de $G(x)$ para todo $j\in\{1,\ldots,l\}$. Olhando para 1.1.2, observe que, para todo

$j \in \{1,\ldots,m\}$, existe $\tilde{\sigma} \in S_m$ tal que

$$a_j = f\left(\gamma_{\tilde{\sigma}(1)},\ldots,\gamma_{\tilde{\sigma}(m)}\right) \in \mathbb{Q}(\theta).$$

Portanto, $\mathbb{Q}(\theta)|\mathbb{Q}$ é normal. □

Lembremos que os conjugados sobre $\mathbb{Q}$, de um número algébrico γ são as raízes do polinômio minimal de γ sobre $\mathbb{Q}$. Comumente nos referimos aos conjugados sobre $\mathbb{Q}$ apenas por conjugados. Agora definiremos um novo tipo de conjugação.

Definição 1.1.8. Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ uma extensão algébrica. Dado $\gamma \in \mathbb{Q}(\theta)$ temos que $\gamma = h(\theta)$ onde $h(x) \in \mathbb{Q}[x]$ e $\partial h \leqslant n-1$. Sejam $\theta = \theta^{(1)},\theta^{(2)},\ldots,\theta^{(n)}$ as n raízes do polinômio minimal de θ sobre $\mathbb{Q}$ então $\gamma = \gamma^{(1)},\gamma^{(2)},\ldots,\gamma^{(n)}$ são chamados conjugados de γ sobre $\mathbb{Q}(\theta)$ ou $\mathbb{Q}(\theta)$-conjugados de γ, onde

$$\gamma^{(i)} = h(\theta^{(i)}), \quad 1 \leqslant i \leqslant n.$$

Não é difícil provar que o grau da extensão $\mathbb{Q}(\sqrt{2}+\sqrt{3})|\mathbb{Q}$ é 4 e assim $1, \sqrt{2}+\sqrt{3}, (\sqrt{2}+\sqrt{3})^2, (\sqrt{2}+\sqrt{3})^3$ é base dessa extensão. Como $\pm(\sqrt{2}+\sqrt{3}), \pm(\sqrt{2}-\sqrt{3})$ são os conjugados de $\sqrt{2}+\sqrt{3}$, então

$$-\frac{9}{2}(\sqrt{2}\pm\sqrt{3}) + \frac{1}{2}(\sqrt{2}\pm\sqrt{3})^3 = \sqrt{2}$$
$$-\frac{9}{2}[(\sqrt{2}\pm\sqrt{3})] + \frac{1}{2}[-(\sqrt{2}\pm\sqrt{3})]^3 = \sqrt{2}$$

Uma explicação mais geral para esse fato será apresentada na proposição 1.2.2. A seguir mostraremos mais resultados sobre extensões algébricas.

1.2 Mais resultados sobre extensões algébricas

Os pré-requisitos necessários para esta seção incluem resultados sobre a teoria de Galois, cuja definição formal pode ser encontrada em [20]. Assumiremos familiaridade do leitor com esses tópicos.

Proposição 1.2.1. Sejam α e β números algébricos em um corpo K de grau n sobre os racionais. Se os conjugados de α sobre K são $\alpha = \alpha^{(1)},\alpha^{(2)},...,\alpha^{(n)}$ e os de β são $\beta = \beta^{(1)},\beta^{(2)},...,\beta^{(n)}$. Então os conjugados de $\alpha+\beta$ e $\alpha.\beta$ são da forma $\alpha^{(k)}+\beta^{(k)}$ e $\alpha^{(k)}.\beta^{(k)}$, para $1 \leqslant k \leqslant n$, respectivamente.

Demonstração. Como $[K:\mathbb{Q}] = n$, então existe $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$, logo $\alpha = h(\theta)$ e

$\beta = g(\theta)$ onde $h(x) = \sum_{j=0}^{n-1} a_j x^j, g(x) = \sum_{j=0}^{n-1} b_j x^j$ com $a_j, b_j \in \mathbb{Q}$. Portanto,

$$\alpha + \beta = \sum_{j=0}^{n-1} (a_j + b_j)\theta^j = F(x), \text{onde} \quad F(x) = \sum_{j=0}^{n-1} (a_j + b_j)x^j.$$

Daí, para $i \in \{1, \ldots, n\}$

$$(\alpha + \beta)^{(i)} = F(\theta^{(i)}) = \sum_{j=0}^{n-1} (a_j + b_j)(\theta^{(i)})^j = h(\theta^{(i)}) + g(\theta^{(i)}) = \alpha^{(i)} + \beta^{(i)}.$$

O caso $\alpha \cdot \beta$ é análogo. □

Note que γ tem n conjugados sobre $\mathbb{Q}(\theta)$ e m conjugados sobre $\mathbb{Q}$, onde $m \mid n$. A relação entre os dois conceitos de conjugação é estabelecido na próxima proposição.

Proposição 1.2.2. (i) Os conjugados de γ sobre $\mathbb{Q}(\theta)$ são os conjugados sobre $\mathbb{Q}$ todos repetidos $\frac{n}{m}$ vezes;

(ii) $\gamma \in \mathbb{Q}$ se e só se todos seus conjugados sobre $\mathbb{Q}(\theta)$ são iguais;

(iii) $\mathbb{Q}(\gamma) = \mathbb{Q}(\theta)$ se e só se todos os conjugados de γ sobre $\mathbb{Q}(\theta)$ são distintos.

Demonstração. (i) Seja $f(x)$ o polinômio mínimo de γ sobre $\mathbb{Q}$, que tem grau $d = [\mathbb{Q}(\gamma) : \mathbb{Q}]$. Seus conjugados sobre $\mathbb{Q}$ são as d raízes distintas de $f(x)$.

Por 1.1.4, temos:

$$n = [\mathbb{Q}(\theta) : \mathbb{Q}] = [\mathbb{Q}(\theta) : \mathbb{Q}(\gamma)] \cdot [\mathbb{Q}(\gamma) : \mathbb{Q}] = m \cdot d,$$

logo, $d = n/m$.

Considere a ação do grupo de Galois $G = \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ sobre γ. O estabilizador de γ é isomorfo a $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\gamma))$, que tem ordem m. Pelo Teorema da Órbita-Estabilizador [3], a órbita de γ sob a ação de G tem tamanho $|G|/|\mathrm{Est}(\gamma)| = n/m = d$. Isso significa que existem exatamente d valores distintos no conjunto $\{\sigma(\gamma) \mid \sigma \in G\}$, e cada um desses valores é atingido exatamente m vezes (pois $|G| = n = d \cdot m$). Estes valores são, por definição, os conjugados de γ sobre $\mathbb{Q}$;

(ii) Se $\gamma \in \mathbb{Q}$, então γ é fixo por todo automorfismo $\sigma \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$. Portanto, $\sigma(\gamma) = \gamma$ para todo σ.

Se $\sigma(\gamma) = \gamma$ para todo $\sigma \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$, então γ pertence ao corpo fixo de G. Como $\mathbb{Q}(\theta)/\mathbb{Q}$ é uma extensão de Galois, o corpo fixo é exatamente $\mathbb{Q}$. Logo, $\gamma \in \mathbb{Q}$;

[3] Seja G um grupo finito agindo em um conjunto X. Para qualquer $x \in X$, temos: $|G| = |G \cdot x| \cdot |G_x|$

(iii) Se $\mathbb{Q}(\gamma) = \mathbb{Q}(\theta)$, então $[\mathbb{Q}(\gamma) : \mathbb{Q}] = n$. Portanto, o polinômio mínimo de γ sobre $\mathbb{Q}$ tem grau n, o que significa que γ tem n conjugados distintos sobre $\mathbb{Q}$.

Se γ tem n conjugados distintos sobre $\mathbb{Q}$, então $[\mathbb{Q}(\gamma) : \mathbb{Q}] = n$. Como $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\theta)$ e $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$, segue que $\mathbb{Q}(\gamma) = \mathbb{Q}(\theta)$.

□

Definição 1.2.1. Sejam $K|\mathbb{Q}$ uma extensão. Um número $\alpha \in K$ é dito inteiro algébrico se for raiz de um polinômio mônico com coeficientes inteiros.

Definição 1.2.2. Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ uma extensão algébrica de grau n, então $N(\alpha)$ (a norma de α) é definida como o produto dos conjugados de α sobre $\mathbb{Q}(\theta)$.

Proposição 1.2.3. Sejam $\alpha, \beta \in \mathbb{Q}(\theta)$, então:

(i) $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$;

(ii) $N(\alpha) = 0$ se e só se $\alpha = 0$;

(iii) Se α é inteiro algébrico, então $N(\alpha) \in \mathbb{Z}$;

(iv) Se α é racional, então $N(\alpha) = \alpha^n$.

Demonstração. (i) Pela proposição 1.2.1, temos que

$$\begin{aligned} N(\alpha\beta) &= (\alpha\beta)^{(1)}(\alpha\beta)^{(2)} \dots (\alpha\beta)^{(n)} = (\alpha^{(1)}\beta^{(1)})(\alpha^{(2)}\beta^{(2)}) \dots (\alpha^{(n)}\beta^{(n)}) \\ &= \alpha^{(1)}\alpha^{(2)} \dots \alpha^{(n)} \cdot \beta^{(1)}\beta^{(2)} \dots \beta^{(n)} = N(\alpha) \cdot N(\beta); \end{aligned}$$

(ii) Se $\alpha = 0$ claramente $N(\alpha) = 0$. Suponha que $N(\alpha) = 0$, como $N(\alpha) = \alpha^{(1)}\alpha^{(2)} \dots \alpha^{(n)}$ então $\alpha^{(i)} = 0$ para algum $i \in \{1, \dots, n\}$, mas

$$\alpha^{(i)} = \sum_{j=0}^{n-1} a_j (\theta^{(i)})^j.$$

Logo, $a_1 = a_2 = \cdots = a_n = 0$ e portanto $\alpha = \sum_{j=0}^{n-1} a_j \theta^j = 0$;

(iii) Sendo α inteiro algébrico, o polinômio minimal de α tem coeficientes inteiros. Seja P tal polinômio,

$$P(x) = x^n + a_1 x^n + \cdots + a_{n-1} x + a_n, \quad \text{com} \quad a_i \in \mathbb{Z}.$$

Temos,

$$\begin{aligned} P(x) &= (x-\alpha)(x-\alpha^{(2)})\dots(x-\alpha^{(n)}) \\ &= x^n - \sigma_1(\alpha,\alpha^{(2)},\dots,\alpha^{(n)})x^{n-1} + \dots \\ &+ (-1)^n\sigma_n(\alpha,\alpha^{(2)},\dots,\alpha^{(n)}). \end{aligned}$$

Daí, $a_i = (-1)^i\sigma_i(\alpha,\alpha^{(2)},\dots,\alpha^{(n)})$ O resultado então segue-se pois

$$N(\alpha) = \sigma_n(\alpha,\alpha^{(2)},\dots,\alpha^{(n)}) = (-1)^n a_n \in \mathbb{Z};$$

(iv) Se $\alpha \in \mathbb{Q}$ então $\alpha = h(\theta)$ onde $h(x) = \alpha$. Daí, $\alpha^{(i)} = h(\theta^{(i)}) = \alpha$, para $1 \leqslant i \leqslant n$. Portanto, $N(\alpha) = \alpha^{(1)}\alpha^{(2)}\dots\alpha^{(n)} = \alpha^{(n)}$.

□

É fácil ver que $(i), (ii)$ e (iii) são válidos para a definição de norma, como o produto dos conjugados α.

Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ extensão algébrica. Um conjunto de inteiros algébricos $\{\alpha_1,\dots,\alpha_n\}$ é chamado base integral de $\mathbb{Q}(\theta)$, se todo $\alpha \in \mathbb{Q}(\theta)$, inteiro algébrico, pode ser escrito de forma única como

$$\alpha = b_1\alpha_1 + \dots + b_n\alpha_n, \quad b_i \in \mathbb{Z}.$$

O discriminante de uma base $\{\alpha_1,\dots,\alpha_n\}$ de $\mathbb{Q}(\theta)|\mathbb{Q}$ é definido por

$$\Delta[\alpha_1,\dots,\alpha_n] = \left[\det\begin{pmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} & \dots & \alpha_n^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \dots & \alpha_n^{(n)} \end{pmatrix}\right]^2,$$

onde $\alpha_j^{(i)}$ é o i-ésimo conjugado de α_j, para $1 \leqslant i \leqslant n$.

Proposição 1.2.4. Se α é um número algébrico, então existe $r \in \mathbb{Z}^+$ tal que $r\alpha$ é inteiro algébrico.

Demonstração. Seja α um número algébrico. Então existe um polinômio minimal mônico sobre $\mathbb{Q}$:

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \quad \in \mathbb{Q}[x].$$

Multiplicando pelo mínimo múltiplo comum (MMC) dos denominadores dos coeficientes

a_i, obtemos um polinômio primitivo em $\mathbb{Z}[x]$:

$$g(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \quad \in \mathbb{Z}[x],$$

onde $c_n \neq 0$ e $\gcd(c_n, \ldots, c_0) = 1$. Agora, considere $r = c_n$ (o coeficiente líder de g). Vamos mostrar que $r\alpha$ é inteiro algébrico.
Substitua x por $\dfrac{y}{r}$ no polinômio $g(x)$ e multiplique ambos os lados por r^n.

$$\begin{aligned} g\left(\frac{y}{r}\right) = c_n\left(\frac{y}{r}\right)^n + c_{n-1}\left(\frac{y}{r}\right)^{n-1} + \cdots + c_1\left(\frac{y}{r}\right) + c_0 = 0 \\ c_n y^n + (c_{n-1})r y^{n-1} + \cdots + c_1 r^{n-1} y + c_0 r^n = 0. \end{aligned}$$

Fazendo $\beta = r\alpha = c_n\alpha$, temos que β satisfaz:

$$\beta^n + (c_{n-1}/c_n)r\beta^{n-1} + \cdots + (c_1/c_n)r^{n-1}\beta + (c_0/c_n)r^n = 0.$$

Como todos os c_i são inteiros e $r = c_n$, os coeficientes tornam-se inteiros:

$$\beta^n + c_{n-1}\beta^{n-1} + c_{n-2}c_n\beta^{n-2} + \cdots + c_1 c_n^{n-2}\beta + c_0 c_n^{n-1} = 0.$$

Portanto, $\beta = r\alpha$ é raiz de um polinômio mônico com coeficientes inteiros, ou seja, é um inteiro algébrico. □

Definição 1.2.3. Se K é uma extensão finita de $\mathbb{Q}$, seu anel de inteiros $\mathcal{O}_K$ é definido como:

$$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ é inteiro algébrico sobre } \mathbb{Z}\}$$

A seguir vamos enunciar alguns resultados clássicos e úteis sobre base integral.

Proposição 1.2.5. Toda base integral é base.

Demonstração. Seja K um corpo de números com anel de inteiros $\mathcal{O}_K$, e seja $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ uma base integral de $\mathcal{O}_K$.

Geração de K sobre $\mathbb{Q}$: Como $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$, todo $\beta \in K$ é da forma $\beta = \frac{a}{b}$ com $a \in \mathcal{O}_K$, $b \in \mathbb{Z}\backslash\{0\}$. Então:

$$a = c_1\alpha_1 + \cdots + c_n\alpha_n \quad (c_i \in \mathbb{Z}) \quad \Rightarrow \quad \beta = \frac{c_1}{b}\alpha_1 + \cdots + \frac{c_n}{b}\alpha_n \quad ,$$

logo $\{\alpha_1, \ldots, \alpha_n\}$ gera K sobre $\mathbb{Q}$.

Independência linear sobre $\mathbb{Q}$: Suponha $q_1\alpha_1 + \cdots + q_n\alpha_n = 0$ com $q_i \in \mathbb{Q}$. Multiplicando por $d \in \mathbb{Z}$ tal que $dq_i \in \mathbb{Z}$:

$$(dq_1)\alpha_1 + \cdots + (dq_n)\alpha_n = 0.$$

Como a base é linearmente independente sobre $\mathbb{Z}$, temos $dq_i = 0$ e assim $q_i = 0$. Logo, é linearmente independente sobre $\mathbb{Q}$. Portanto, $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de K sobre $\mathbb{Q}$ □

Proposição 1.2.6. Todo corpo de números algébricos tem pelo menos uma base integral

Demonstração. Seja K um corpo de números algébricos de grau $n = [K : \mathbb{Q}]$, e seja $\mathcal{O}_K$ seu anel de inteiros.

Afirmação: $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto n [4].

Como K é uma extensão finita de $\mathbb{Q}$, existe uma base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ de K sobre $\mathbb{Q}$. Multiplicando por um inteiro adequado, podemos assumir que $\alpha_i \in \mathcal{O}_K$ para todo i. Além disso, $\mathcal{O}_K$ é um submódulo do $\mathbb{Z}$-módulo livre gerado por $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Como $\mathbb{Z}$ é um anel principal, todo submódulo de um $\mathbb{Z}$-módulo livre é livre. Portanto, $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto $m \leqslant n$. Mas $\mathcal{O}_K$ gera K sobre $\mathbb{Q}$ (pois todo elemento de K é da forma α/d para algum $\alpha \in \mathcal{O}_K$ e $d \in \mathbb{Z}$), logo $m = n$. Assim, $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto n. Agora mostraremos a existência da base integral. Seja $\{\omega_1, \omega_2, \ldots, \omega_n\}$ uma base de $\mathcal{O}_K$ como $\mathbb{Z}$-módulo. Então:

- Geração: Para todo $\alpha \in \mathcal{O}_K$, existem $c_1, c_2, \ldots, c_n \in \mathbb{Z}$ tais que

$$\alpha = c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n.$$

- Independência linear: Se

$$c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n = 0 \quad \text{com } c_i \in \mathbb{Z},$$

então $c_1 = c_2 = \cdots = c_n = 0$.

Portanto, $\{\omega_1, \omega_2, \ldots, \omega_n\}$ é uma base integral de K. Assim, todo corpo de números algébricos K possui um anel de inteiros $\mathcal{O}_K$ que é um $\mathbb{Z}$-módulo livre de posto $n = [K : \mathbb{Q}]$. Assim, existe uma base $\{\omega_1, \omega_2, \ldots, \omega_n\}$ de $\mathcal{O}_K$ sobre $\mathbb{Z}$, que é por definição uma base integral de K. □

1.3 Lema de Gauss

Lema 1.3.1 (Lema de Gauss)**.** Seja $f(x) \in \mathbb{Z}[x]$ tal que $f(x)$ é irredutível sobre $\mathbb{Z}$ então $f(x)$ é irredutível sobre $\mathbb{Q}$.

[4] Um $\mathbb{Z}$-módulo é essencialmente um grupo abeliano com uma multiplicação por escalar definida sobre o conjunto dos inteiros. As definições de $\mathbb{Z}$-módulo livre e posto são derivadas das definições base e dimensão de espaços vetoriais sobre os inteiros.

Demonstração. Suponhamos que $f(x)$ seja irredutível sobre $\mathbb{Z}$ mas $f(x) = g(x) \cdot h(x)$, onde $g(x), h(x) \in \mathbb{Q}[x]$ e $1 \leqslant \partial g(x), \partial h(x) < \partial f$.
Claramente existe inteiro positivo m tal que $m \cdot f(x) = g_1(x) \cdot h_1(x)$, onde $g_1(x), h_1(x) \in \mathbb{Z}[x]$. Assim temos,

$$g_1(x) = a_0 + a_1 x + \cdots + a_r x^r, a_i \in \mathbb{Z}$$

$$h_1(x) = b_0 + b_1 x + \cdots + b_s x^s, b_j \in \mathbb{Z}$$

Suponhamos agora que $p \mid m$, p primo. Vamos provar que $p \mid a_i$ para todo $i \in \{1, \ldots, r\}$ ou $p \mid b_j$ para todo $j \in \{1, \ldots, s\}$. De fato, se existem $i \in \{1, \ldots, r\}$ e $j \in \{1, \ldots, s\}$ tais que $p \nmid a_i$ e $p \nmid b_j$, consideremos i e j menores possíveis com esta propriedade. Ora, como $p \mid m$ temos que p divide o coeficiente de x^{i+j} do polinômio $mf(x) = g_1(x) \cdot h_1(x)$, isto é,

$$p \mid (b_0 \cdot a_{i+j} + b_1 \cdot a_{i+j-1} + \ldots + b_j \cdot a_i + \ldots + b_{i+j-1} \cdot a_1 + b_{i+j} \cdot a_0).$$

Pela nossa escolha de i e j temos que p divide cada parcela, exceto $b_j \cdot a_i$, do coeficiente de x^{i+j} de $g_1(x) \cdot h_1(x)$.
Como p divide toda a expressão, segue também que $p \mid b_j \cdot a_i$ e como p é um número primo temos que $p \mid b_j$ ou $p \mid a_i$, que é uma contradição. Assim, se p primo, $p \mid m$ então $p \mid a_i$ para todo $i \in \{1, \ldots, r\}$ ou $p \mid b_j$ para todo $j \in \{1, \ldots, s\}$. Sem perda de generalidade, suponhamos que $p \mid a_i$ para todo $i \in \{1, 2, \ldots, r\}$. Assim, $g_1(x) = p \cdot g_2(x)$ onde $g_2(x) \in \mathbb{Z}[x]$, e se $m = p \cdot m_1$ temos

$$p \cdot m_1 f(x) = p \cdot g_2(x) \cdot h_1(x)$$

$$m_1 f(x) = g_2(x) \cdot h_1(x).$$

Como o número de fatores primos de m é finito, prosseguindo no argumento acima (ou por indução sobre o número de fatores primos de m) chegaremos a:

$$f(x) = g^*(x) \cdot h^*(x) \quad \text{onde,}$$

$$g^*(x), h^*(x) \in \mathbb{Z}[x]$$

e $g^*(x)$ e $h^*(x)$ são múltiplos racionais de $g(x)$ e $h(x)$, respectivamente, contradizendo a irredutibilidade de $f(x)$ sobre $\mathbb{Z}$. □

1.4 Uma medida de irracionalidade

A demonstração da irracionalidade de um certo número é apenas a "ponta do iceberg" de vários outros problemas relacionados. Um deles é saber quão esse número é irracional. Mais precisamente, a medida de irracionalidade para um número irracional α

é uma função positiva e estritamente decrescente $f(x)$, para $x \geqslant 1$, e tal que

$$\left|\alpha - \frac{p}{q}\right| > f(q),$$

para todo número racional $\frac{p}{q}$, com $q \geqslant 1$. Ou seja, essa função mede o comportamento da distância entre α e qualquer racional.

Para exemplificarmos, encontraremos uma medida de irracionalidade para $\sqrt{2}$. Definimos $g(x) = x^2 - 2$ e $I = [\sqrt{2}-1, \sqrt{2}+1]$. Seja $\frac{p}{q} \in \mathbb{Q}$, com $q \geqslant 1$. Se $\frac{p}{q} \notin I$, então $|\sqrt{2} - \frac{p}{q}| > 1 \geqslant \frac{1}{q^2}$. Para o caso $\frac{p}{q} \in I$, usamos o Teorema do Valor Médio[5] para o intervalo fechado com extremos $\sqrt{2}$ e $\frac{p}{q}$. Assim, existe ζ no interior desse intervalo, tal que

$$g(\sqrt{2}) - g\left(\frac{p}{q}\right) = g'(\zeta)\left(\sqrt{2} - \frac{p}{q}\right),$$

onde, como usual, g' denota a derivada da função g. Portanto

$$\left|\sqrt{2} - \frac{p}{q}\right| = \left|\frac{g(\frac{p}{q})}{2\zeta}\right|.$$

Agora é suficiente notar que $|g(\frac{p}{q})| > \frac{1}{q^2}$ e que $\zeta < \sqrt{2}+1$, para obtermos

$$\left|\sqrt{2} - \frac{p}{q}\right| > \frac{1}{2(\sqrt{2}+1)q^2}.$$

Daí, a desigualdade acima é válida para todo $\dfrac{p}{q} \in \mathbb{Q}$ e, desse modo, a função $f(x) = \frac{1}{2(\sqrt{2}+1)x^2}$ é uma medida de irracionalidade para $\sqrt{2}$.

[5] Se a função $f : [a,b] \to \mathbb{R}$ é contínua em $[a,b]$ e derivável em (a,b), então existe $\xi \in (a,b)$ tal que $f(b) - f(a) = f'(\xi)(b-a)$.

Capítulo 2

Números Algébricos e Transcendentes

Neste captítulo iremos estudar propriedades aritméticas, algébricas e analíticas dos números algébricos e transcendentes.

2.1 Números Algébricos e Transcendentes

Definição 2.1.1. Seja $L|K$ uma extensão de corpos. Dizemos que α é algébrico sobre K se $\exists f(x) \in K[x] - \{0\}$ tal que $f(\alpha) = 0$. Caso contrário α é dito transcendente sobre K. Mais geralmente, os números $\alpha_1, \ldots, \alpha_n \in L$ são ditos algebricamente dependentes sobre K, se existe $f(x) \in K[x_1, \ldots, x_n]$, não nulo, tal que $f(\alpha_1, \ldots, \alpha_n) = 0$. Caso contrário, $\alpha_1, \ldots, \alpha_n$ são chamados algebricamente independentes sobre K.

Dizemos simplesmente que um número complexo é algébrico, quando for algébrico sobre $\mathbb{Q}$. Números não algébricos são chamados transcendentes.

Exemplo 2.1.1. $i, \sqrt{2}+\sqrt{3}$ e $\cos\frac{\pi}{1006} + i\,\mathrm{sen}\,\frac{\pi}{1006}$ são algébricos, pois são raízes, respectivamente, de x^2+1, x^4-10x^2+1 e $x^{2012}-1$.

O conjunto dos números algébricos é denotado $\overline{\mathbb{Q}}$ e, para simplificar em alguns momentos, $\mathbb{T}$ denotará o conjunto dos números transcendentes. Relembramos que um conjunto é chamado enumerável se tem a mesma cardinalidade de $\mathbb{N}$.

Proposição 2.1.1. O conjunto dos números algébricos é enumerável.

Demonstração. Dado $P(x) = a_0 + a_1 x + \cdots + a_n x^n$, o conjunto das raízes de P é denotado por $\mathcal{R}_P$. Note que $\mathcal{R}_P$ tem no máximo n elementos. Para todo $n \in \mathbb{N}$, existe apenas

uma quantidade enumerável de polinômios, em $\mathbb{Q}[x]$, com grau n. De fato, considere $\mathbb{X}_n = \{Q \in \mathbb{Q}[x] : \partial Q = n\}$. Tome $\psi : \underbrace{\mathbb{Q} \times \cdots \times \mathbb{Q}^*}_{n+1 \text{ cópias}} \longrightarrow \mathbb{X}_n$ dada por:

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

note que ψ é bijeção. Como $\mathbb{Q} \times \cdots \times \mathbb{Q}^*$ é enumerável, segue-se que $\mathbb{X}_n$ também o é. Definimos $\mathcal{A}_n = \bigcup_{\partial P = n} \mathcal{R}_P$. Pelos comentários feitos anteriormente e pelo fato de que a união enumerável de conjuntos finitos é enumerável, segue-se que $\mathcal{A}_n$ é enumerável. Agora é só observar que

$$\overline{\mathbb{Q}} = \bigcup_{n \in \mathbb{N}} \mathcal{A}_n.$$

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

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

$$A \subseteq \bigcup_{n \in \mathbb{N}} B_n \quad \text{e} \quad \sum_{n=1}^{\infty} v(B_n) < \epsilon$$

onde, v é o volume do conjunto. Note que o volume é o comprimento e a área deste conjunto, quando $t = 1, 2$, 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.
A proposição a seguir dá a natureza quantitativa dos números transcendentes.

Proposição 2.1.2. Quase todos os números são transcendentes.

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

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

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

$$\begin{aligned} \text{Área}\left(\bigcup_{n \in \mathbb{N}} B_n\right) &\leqslant \sum_{n=1}^{\infty} \text{Área}(B_n) = \sum_{n=1}^{\infty} \pi r_n^2 = \frac{3\epsilon}{\pi^2} \sum_{n=1}^{\infty} \frac{1}{n^2} \\ &= \frac{3\epsilon}{\pi^2}\left(\frac{\pi^2}{6}\right) = \frac{\epsilon}{2} < \epsilon. \end{aligned}$$

Segue-se então o resultado, onde usamos $\zeta(2) = \sum_{n=1}^{\infty} n^{-2} = \frac{\pi^2}{6}$. Nesse caso, dizemos que o conjunto dos números transcendentes tem medida total em $\mathbb{C}$, isto é, $m(\mathbb{T}) = \infty$. □

2.2 Teorema de Liouville

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

Teorema 2.2.1 (Liouville)**.** Seja α uma raiz real de um polinômio irredutível $P(x) \in \mathbb{Z}[x]$ de grau $n \geqslant 2$. Então existe uma constante positiva c_α tal que

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{c_\alpha}{q^n} \tag{2.2.1}$$

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

$$c_\alpha := \frac{1}{1 + \max_{|t-\alpha|\leqslant 1} |P'(t)|} \tag{2.2.2}$$

Demonstração. Com a escolha de c_α em 2.2.2, se tivermos $|\alpha - \frac{p}{q}| \geqslant 1$, o teorema é válido pois $1 \geqslant \frac{c_\alpha}{q^n}$. Para o caso $|\alpha - \frac{p}{q}| < 1$, observe que, como $P(x)$ é irredutível sobre $\mathbb{Z}$, ele será irredutível sobre $\mathbb{Q}$ pelo lema de Gauss 1.3.1 e assim $P(\frac{p}{q}) \neq 0$, o que implica $|q^n P(\frac{p}{q})| \geqslant 1$, visto que $q^n P(\frac{p}{q})$ é inteiro não nulo. Pelo teorema do valor médio, existe $t \in \mathbb{R}$ entre α e $\frac{p}{q}$, tal que

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

Portanto,

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{1}{q^n.(1 + |P'(t)|)} \geqslant \frac{1}{q^n(1 + \max_{|t-\alpha|\leqslant 1} |P'(t)|)} = \frac{c_\alpha}{q^n},$$

onde usamos que $|t - \alpha| \leqslant |\frac{p}{q} - \alpha| \leqslant 1$.
Observe que, por 2.2.1, a função $f(x) = \frac{c_\alpha}{x^n}$ é uma medida de irracionalidade para α. □

Exemplo 2.2.1. Alguns valores particulares de c_α são:

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

2.2.1 Números de Liouville

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

Definição 2.2.1. Um número real α é aproximável na ordem n por racionais, se existirem uma constante $C > 0$ e uma sequência $(\frac{p_j}{q_j})_{j\geqslant 1}$ de racionais distintos, com $q_j > 1$ e $(p_j, q_j) =$

1 tais que

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{C}{q_j^n}, \tag{2.2.3}$$

para todo $j \geqslant 1$.

Exemplo 2.2.2. Seja o número

$$\alpha = \sum_{k=1}^{\infty} 10^{-k!} = 0.11000100000000000000000010000\ldots \tag{2.2.4}$$

consideremos a sucessão de racionais definida por:

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

Temos, pois

$$\left|\alpha - \frac{v_j}{u_j}\right| = \sum_{k=j+1}^{\infty} \frac{1}{10^{k!}} = \frac{1}{10^{(j+1)!}}\left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + \ldots\right). \tag{2.2.5}$$

A expressão em parênteses é majorada por

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

Logo, o último membro de 2.2.5 é majorada por

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

e portanto

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

e como $u_j = 10^{j!}$, segue-se que α definido em 2.2.4 é um número de Liouville.

Podemos dizer que um número real é bem aproximado por racionais se é aproximável na ordem n por racionais, este resultado é conhecido como Teorema da aproximação de Dirichlet, que pode ser encontrado em [3]. Se $\alpha \in \mathbb{R}$ é um número irracional, então existem infinitos racionais $\frac{p}{q}$, com $q \geqslant 1$, tais que

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

Este é um dos resultados fundamentais em aproximação diofantina, em um certo sentido, o Teorema de Liouville diz que um número algébrico irracional não pode ser bem aproximado

por racionais. Portanto, Liouville construiu uma classe de números que são muito bem aproximados por racionais.

Definição 2.2.2. Um número real α é chamado de número de Liouville se existir uma sequência de racionais $(\frac{p_j}{q_j})_{j\geqslant 1}$, com $q_j > 1$, tal que

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

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

Proposição 2.2.2. A sequência $(q_j)_{j\geqslant 1}$ é ilimitada.

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

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

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

Corolário 2.2.3. Todo número de Liouville é irracional.

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

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

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

Teorema 2.2.4. Todo número de Liouville é transcendente.

Demonstração. Pelo corolário 2.2.3, um número de Liouville α não pode ser racional. Daí suponha que α é algébrico de grau $n > 1$. Então pelo Teorema 2.2.1 segue-se que a relação 2.2.1 será válida para todo número racional. Em particular, para os $\frac{p_j}{q_j}$ da Definição 2.2.2. assim, teríamos

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

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

2.3 Transcendência de e

Antes da demonstração propriamente dita, vamos abordar dois pequenos lemas que serão úteis no decorrer do processo.

Lema 2.3.1. Seja $f(x)$ um polinômio com coeficientes inteiros e seja p um número inteiro positivo menor que o grau de $f(x)$. Então, para $i \geqslant p$

$$\frac{d^i}{dx^i}\left(\frac{f(x)}{(p-1)!}\right),$$

é um polinômio com coeficientes inteiros e divisíveis por p.

Demonstração. Uma vez que a derivada é um operador linear é suficiente mostrarmos que

$$\frac{d^i}{dx^i}\left(\frac{x^j}{(p-1)!}\right),$$

tem coeficiente inteiro e divisível por p. Se tivermos $i > j$ esta derivada será nula e não há nada a mostrar, por isso vamos considerar apenas o caso $i \leqslant j$. Lembrando que $\frac{d}{dx}x^n = nx^{n-1}$ podemos estabelecer, de maneira recursiva, o seguinte resultado:

$$\frac{d^i}{dx^i}\left(\frac{x^j}{(p-1)!}\right) = \frac{j!}{(j-i)!(p-1)!}x^{j-i}.$$

Vamos mostrar que $\frac{j!}{(j-i)!(p-1)!}$ é um número inteiro e divisível por p. Com efeito, temos:

$$\frac{j!}{(j-i)!(p-1)!} = \frac{j!i!}{(j-i)!i!(p-1)!}.$$

Mas $\frac{j!}{(j-i)!i!} = \binom{j}{i}$ é um dos coeficientes do desenvolvimento de $(a+b)^j$ sendo portanto um número inteiro, digamos k. Agora, lembrando que $i \geqslant p$ podemos escrever:

$$\frac{j!}{(j-i)!(p-1)!} = \frac{k\cdot i\cdot(i-1)(i-2)(i-3)\cdots p(p-1)!}{(p-1)!} = k\cdot i(i-1)(i-2)\cdots p.$$

Logo,

$$\frac{d^i}{dx^i}\left(\frac{f(x)}{(p-1)!}\right),$$

é um polinômio com coeficientes inteiros e divisíveis por p. □

Lema 2.3.2. Considere a sequência $\{a_p\}$ definida por:

$$a_p = \frac{e^n n^p (M)^p}{(p-1)!},$$

onde M é uma constante e n é um inteiro positivo. Então

$$\lim_{p\to\infty} a_p = 0.$$

Demonstração. Para provar esse Lema vamos usar o seguinte fato: Se $\sum_{n=1}^{\infty} b_n$ é convergente então $\lim_{n\to\infty} b_n = 0$. Com isso é suficiente mostrarmos que $\sum_{p=1}^{\infty} a_p$ converge. Para isto temos que,

$$\sum_{p=1}^{\infty} \frac{e^n n^p (M)^p}{(p-1)!} = \sum_{p=1}^{\infty} \frac{e^n (n\cdot M)^p}{(p-1)!} = e^n \sum_{p=0}^{\infty} \frac{(M\cdot n)^{p+1}}{p!} = e^n \sum_{p=0}^{\infty} c_p.$$

Pelo teste da razão é suficiente mostrarmos que $\lim_{p\to\infty} \left|\frac{c_{p+1}}{c_p}\right| < 1$. Calculemos este limite:

$$\lim_{p\to\infty} \left|\frac{c_{p+1}}{c_p}\right| = \lim_{p\to\infty} \left[\frac{(nM)^{p+2}}{(p+1)!} \cdot \frac{p!}{(nM)^{p+1}}\right] = \lim_{p\to\infty} \frac{nM}{p+1} = 0 < 1.$$

Assim a série converge e temos que $\lim_{p\to\infty} a_p = 0$. □

Observação 2.3.1. Considere $f(x)$ um polinômio de grau r com coeficientes reais. Seja

$$F(x) = f(x) + f^{(1)}(x) + f^{(2)}(x) + f^{(3)}(x) + \cdots + f^{(r)}(x), \tag{2.3.1}$$

onde $f^{(i)}(x)$ representa a i-ésima derivada de $f(x)$ em relação a x. Daí, temos que,

$$\frac{d}{dx}\left(e^{-x}F(x)\right) = e^{-x}f^{(1)}(x) - e^{-x}f(x) + e^{-x}f^{(2)}(x) - e^{-x}f^{(1)}(x) + \cdots +$$

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

Efetuando todos os cancelamentos e lembrando que $f^{(r+1)}(x) = 0$ teremos a seguinte relação:

$$\frac{d}{dx}\left(e^{-x}F(x)\right) = -e^{-x}f(x). \tag{2.3.2}$$

Uma vez que $F(x)$ é um polinômio e a função exponencial é infinitamente derivável podemos afirmar que $e^{-x}F(x)$ também é infinitamente derivável e portanto vale o Teorema do Valor Médio em qualquer intervalo da reta. Em particular, se tomarmos o intervalo

$[0,k]$, $k>0$, teremos:

$$e^{-k}F(k)-F(0)=-ke^{-k\theta_k}f(k\theta_k),$$

onde θ_k é um número real que depende de k e está entre 0 e 1. Multiplicando esta última igualdade por e^k, obtemos:

$$F(k)-e^kF(0)=-ke^{k(1-\theta_k)}f(k\theta_k) \tag{2.3.3}$$

Defina agora

$$\epsilon_k=F(k)-e^kF(0)=-ke^{k(1-\theta_k)}f(k\theta_k). \tag{2.3.4}$$

Com isso, vamos agora expor a demonstração da transcendência do número de Euler.

Teorema 2.3.3. O número de Euler é transcendente.

Demonstração. Vamos supor por absurdo, que e seja um número algébrico. Então existem constantes inteiras c_0, c_1, c_2, $c_3,\cdots,c_n$ tais que,

$$c_ne^n+c_{n-1}e^{n-1}+c_{n-2}e^{n-2}+\cdots+c_1e+c_0=0. \tag{2.3.5}$$

Podemos supor sem perda de generalidade que $c_0>0$. Observe agora que dado polinômio F citado na observação 2.3.1:

$$c_1\epsilon_1=c_1F(1)-c_1eF(0);$$

$$c_2\epsilon_2=c_2F(2)-c_2e^2F(0);$$

$$c_3\epsilon_3=c_3F(3)-c_3e^3F(0);$$

$$\vdots$$

$$c_n\epsilon_n=c_nF(n)-c_ne^nF(0).$$

Somando todas essas igualdades teremos:

$$c_1\epsilon_1+c_2\epsilon_2+c_3\epsilon_3+\cdots+c_n\epsilon_n=c_1F(1)+c_2F(2)+\cdots+c_nF(n)-\beta,$$

onde $\beta=F(0)(c_1e+c_2e^2+c_3e^3+\cdots c_ne^n)$. Mas, por 2.3.5, podemos concluir que $\beta=-c_0F(0)$ e portanto ficamos somente com:

$$c_1\epsilon_1+c_2\epsilon_2+c_3\epsilon_3+\cdots+c_n\epsilon_n=c_0F(0)+c_1F(1)+c_2F(2)+\cdots+c_nF(n). \tag{2.3.6}$$

Uma vez que $f(x)$ é um polinômio qualquer, vamos continuar nossa argumentação

fazendo

$$f(x) = \frac{1}{(p-1)!}x^{p-1}\left[(1-x)(2-x)\cdots(n-x)\right]^p,$$

onde p é um número primo tal que $p > n$ e $p > c_0$. Note que

$$(1-x)(2-x)(3-x)\cdots(n-x) = n! + \sum_{j=1}^{n} d_j x^j, \quad \text{com} \quad d_j \in \mathbb{Z}.$$

E portanto

$$f(x) = \frac{(n!)^p x^{p-1}}{(p-1)!} + \sum_{j=p}^{p(n+1)-1} \frac{b_j x^j}{(p-1)!} \quad \text{com} \quad b_j \in \mathbb{Z} \tag{2.3.7}$$

Observe que $x = 1, 2, 3, 4, \cdots, n$ é raiz de multiplicidade p do polinômio $f(x)$. Daí teremos que:

$$f(x) = f^{(1)}(x) = f^{(2)}(x) = \cdots = f^{(p-1)}(x) = 0, \quad \text{para} \quad x = 1, 2, 3, \cdots, n. \tag{2.3.8}$$

Aplicando o resultado do Lema 2.3.1 ao polinômio $f(x)$ podemos concluir que, para $x = 1, 2, 3, \cdots, n$, $f^{(p)}(x), f^{(p+1)}(x), \cdots, f^{(n(p+1)-1)}(x)$ assume somente valores múltiplos de p. Podemos afirmar que $F(x)$ é múltiplo de p para $x = 1, 2, 3, \cdots, n$ e portanto

$$c_1F(1) + c_2F(2) + c_3F(3) + \cdots + c_nF(n), \tag{2.3.9}$$

é múltiplo de p. Olhemos agora para $F(0)$, observe inicialmente que $x = 0$ é uma raiz de multiplicidade $p-1$ do polinômio $f(x)$. Deste fato segue que

$$f(0) = f^{(1)}(0) = \cdots = f^{(p-2)}(0) = 0. \tag{2.3.10}$$

Para $i \geqslant p$, $f^{(i)}(0)$ é um múltiplo de p, pelo Lema 2.3.1. Porém, da relação 2.3.7, temos que $f^{(p-1)}(0) = (n!)^p$. Uma vez que $p > n$ e p é primo, podemos concluir que p não divide $(n!)^p$ e portanto $f^{(p-1)}(0)$ é um número não divisível por p. Agora note que $F(0)$ é uma soma de inteiros, onde todos eles, exceto um são divisíveis por p. Logo p não divide $F(0)$ e, uma vez que $p > c_0$, p não divide $c_0F(0)$ e podemos finalmente afirmar que

$$c_0F(0) + c_1F(1) + c_2F(2) + \cdots + c_nF(n), \tag{2.3.11}$$

é um número inteiro não divisível por p.

Guardemos esta informação e trabalharemos agora o lado esquerdo da equação

2.3.6. Recordemos a definição abaixo dada por:

$$\epsilon_k = -ke^{k(1-\theta_k)} f(k\theta_k);$$
$$\epsilon_k = -ke^{k(1-\theta_k)} \frac{1}{(p-1)!} (k\theta_k)^{p-1} \left[|1-k\theta_k|\,|2-k\theta_k|\cdots|n-k\theta_k|\right]^p.$$

Em virtude da definição de $f(x)$ teremos então:

$$|\epsilon_k| = \frac{e^{k(1-\theta_k)}}{(p-1)!} k^p \theta_k^{p-1} \left[|1-k\theta_k|\,|2-k\theta_k|\cdots|n-k\theta_k|\right]^p.$$

Agora observe que, como $0 < k \leqslant n$ e $0 < \theta_k < 1$, para todo $i \in \mathbb{Z}$ tal que $0 < i \leqslant n$ vale a seguinte relação:

$$|i - k\theta_k| \leqslant |i| + |k\theta_k| \leqslant 2n.$$

E desta última desigualdade segue que

$$|1-k\theta_k|\,|2-k\theta_k|\cdots|n-k\theta_k|\right]^p \leqslant (2^n n^n)^p = (M)^p, \tag{2.3.12}$$

onde $M = 2^n n^n$ é uma constante. Como $k \leqslant n$ e $0 < \theta_k < 1$ teremos:

(i) $k(1-\theta_k) \leqslant n(1-\theta_k) \leqslant n \quad \Rightarrow \quad e^{k(1-\theta_k)} \leqslant e^n$;

(ii) $k^p \leqslant n^p$;

(iii) $\theta_k^{p-1} \leqslant 1$.

Destas três desigualdades e da desigualdade 2.3.12 nos permite escrever

$$|\epsilon_k| \leqslant \frac{e^n n^p (M)^p}{(p-1)!} \quad \text{para} \quad k \leqslant n.$$

Sabendo que o conjunto dos números primos é infinito e em virtude do Lema 2.3.2 podemos fazer com que os termos ϵ's sejam tão próximos de zero quanto se queira. Portanto podemos afirmar que:

$$|c_1\epsilon_1 + c_2\epsilon_2 + c_3\epsilon_3 + \cdots + c_n\epsilon_n| < 1, \tag{2.3.13}$$

para p suficientemente grande.

Em virtude da igualdade 2.3.6 e de 2.3.11, a parcela da esquerda na última desigualdade deve ser um número inteiro. Como ela é menor do que 1 devemos ter $c_1\epsilon_1 + c_2\epsilon_2 + c_3\epsilon_3 + \cdots + c_n\epsilon_n = 0$. Portanto, concluímos que

$$c_0F(0) + c_1F(1) + c_2F(2) + \cdots + c_nF(n) = 0.$$

O que implica que p divide

$$[c_0F(0) + c_1F(1) + c_2F(2) + \cdots + c_nF(n)].$$

Mas isso é um absurdo, pois vai contra o resultado 2.3.11. O absurdo se dá pelo fato de termos considerado o número e como sendo algébrico. Logo, o número e é transcendente. □

2.4 Transcendência de π

Teorema 2.4.1. O número π é transcendente.

Demonstração. Suponhamos por absurdo, que π seja algébrico. Então, $i\pi$ também será algébrico, por ser o produto de dois algébricos. Daí temos que $i\pi$ é raiz de um polinômio com coeficientes inteiros. Sejam $\alpha_1 = i\pi$, α_2, $\alpha_3, \cdots, \alpha_n$, as raízes deste polinômio. Da igualdade de Euler $e^{i\pi} + 1 = 0$, segue que:

$$0 = \prod_{j=1}^{n}(e^{\alpha_j} + 1) = K + \sum_{j=1}^{m} e^{\beta_j},$$

onde $K \in \mathbb{N}$ e $\beta_1,\beta_2,\beta_3, \cdots, \beta_n$ são números não nulos expressos por:

$$\alpha_i, \quad 1 \leqslant i \leqslant n \tag{2.4.1}$$

$$\alpha_i + \alpha_j, \quad 1 \leqslant i < j \leqslant n \tag{2.4.2}$$

$$\vdots$$

$$\alpha_1 + \alpha_2 + \cdots + \alpha_n, \tag{2.4.3}$$

e $k \in \mathbb{N}$ é obtido agrupando a soma dos termos cujos expoentes são nulos.

Os números $\beta_1,\beta_2,\beta_3, \cdots, \beta_m$ dados anteriormente são as raízes de um polinômio $R(x) = cx^m + c_{m-1}x^{m-1} + \cdots + c_1x + c_0$ de coeficientes inteiros. Tomando um primo p genérico e $s = m(p-1)$, definamos:

$$f(x) = \frac{c^s}{(p-1)!}x^{p-1}(R(x))^p. \tag{2.4.4}$$

O grau de f é $s+p$. Definamos também:

$$F(x) = f(x) + f^{'}(x) + f^{''}(x) + \cdots + f^{(s+p)}(x), \tag{2.4.5}$$

que assim como 2.3.2, satisfaz:

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

donde:

$$e^{-x}F(x) - F(0) = -\int_0^x e^{-t}f(t)dt.$$

Usando uma mudança de variável $t = \lambda x$ (onde λ é variável e x é fixo):

$$F(x) - e^{x}F(0) = -x\int_0^1 e^{(1-\lambda)x}f(\lambda x)d\lambda.$$

Somando as igualdades para $x = \beta_1, \beta_2, \beta_3, \cdots, \beta_m$, obtemos:

$$\sum_{j=1}^{m} F(\beta_j) + kF(0) = -\sum_{j=1}^{m}\beta_j\int_0^1 e^{(1-\lambda)\beta_j}f(\lambda\beta_j)d\lambda. \tag{2.4.6}$$

Observando que em 2.4.4 β_j é raiz de $f(x)$ de multiplicidade p, chegamos à conclusão que:

$$0 \leqslant t < p \quad \Rightarrow \quad \sum_{j=1}^{m} f^{(t)}(\beta_j) = 0.$$

Se $t \geqslant p$, apenas a p-ésima derivada de $R(x)$ no ponto $x = \beta_j$ é não nula. Derivando p vezes o polinômio $R(x)$ neste ponto, teremos um coeficiente $p!$ que cancelará o denominador $(p-1)!$ de $f(x)$, deixando p vezes um polinômio com coeficientes inteiros calculado em β_j. O que implica que $\frac{1}{c^s}f^{(t)}(\beta_j)$ é um polinômio em β_j com coeficientes inteiros divisíveis por p. Além disso, $\sum_{j=1}^{m} f^{(t)}(\beta_j)$ é simétrico nos β_j de grau menor ou igual a s. Daí, devido ao coeficiente c^s, este polinômio é de coeficientes inteiros e grau menor ou igual a s. Portanto:

$$p \leqslant t \quad \Rightarrow \quad \sum_{j=1}^{m} f^{(t)}(\beta_j) = pk_t \quad \text{com} \quad k_t \in \mathbb{Z}.$$

Examinaremos agora $F(0)$. Notamos que $f^{(t)}(0) = 0$ se $t \leqslant p-2$, $f^{(p-1)}(0) = c^s c_0^p$ e $f^{(t)}(0)$ é um inteiro divisível por p se $p \leqslant t$.

Portanto, o termo em 2.4.6 é da forma $Kp + kc^s c_0^p$ com K inteiro, e tal expressão é inteira. Tomando $p > \max\{k, |c|, |c_0|\}$, conseguimos em 2.4.6 um termo não divisível por p, (pois, $kc^s c_0^p$ não pode ser divisível), e, logo, não nulo. De 2.4.4, obtemos:

$$|f(\lambda\beta_j)| \leqslant \frac{|c|^s m_j^p}{(p-1)!} |\beta_j|^{p-1},$$

que segue se tomarmos $m_j = \max_{0\leqslant\lambda\leqslant 1} |R(\lambda\beta_j)|$. Portanto:

$$\left| -\sum_{j=1}^{m} \beta_j \int_0^1 e^{(1-\lambda)\beta_j} f(\lambda\beta_j) d\lambda \right| \leqslant \sum_{j=1}^{m} \frac{|\beta_j|^p |c|^s |m_j|^p B}{(p-1)!}, \tag{2.4.7}$$

onde $B = \sup_j \int_0^1 \left|e^{(1-\lambda)\beta_j}\right| d\lambda$.

Ora, o lado esquerdo da equação 2.4.7 é positivo e o lado direito tende a zero quando $p \to \infty$, o que é um absurdo. Como supomos que π era algébrico, chegamos numa contradição. Logo, π é transcendente. □

2.5 Teorema de Hermite-Lindemann

Os primeiros números transcendentes foram exibidos por Liouville, no entanto tais exemplos eram um tanto "artificiais". Porém, com a demonstração de Cantor de que quase todos os números são transcendentes, parecia razoável mostrar de maneira mais "concreta" exemplos de números conhecidos que são transcendentes. Em 1873, Hermite provou que e é transcendente, e, em 1882, Lindemann estendeu o método para provar que π também é transcendente, além disso, mostrou que a transcendência de e e π são casos especiais de um teorema bem mais geral. Esse teorema é conhecido como Teorema de Hermite-Lindemann.

Teorema 2.5.1 (Hermite-Lindemann)**.** Se $\alpha_1, \ldots, \alpha_m$ são números algébricos distintos, então $e^{\alpha_1}, \ldots, e^{\alpha_m}$ são linearmente independentes sobre o corpo dos números algébricos.

Exemplo 2.5.1. Suponha $\alpha_1 = 1$ e $\alpha_2 = \sqrt{2}$ (ambos algébricos e distintos). então, e^1 e $e^{\sqrt{2}}$ são linearmente independentes sobre $\overline{\mathbb{Q}}$. Isso significa que não existe $c_1, c_2 \in \overline{\mathbb{Q}}$ não nulos tais que:

$$c_1 e + c_2 e^{\sqrt{2}} = 0.$$

Se tal relação existisse, poderíamos escrever $e = -\dfrac{c_2}{c_1} e^{\sqrt{2}}$.

Quando $m = 2$, $\alpha_1 = 0$ e $\alpha_2 = \alpha \in \overline{\mathbb{Q}}$, não nulo, então obtemos o seguinte caso particular.

Corolário 2.5.2. Se α é algébrico não nulo, então e^α é transcendente.

Proposição 2.5.3. Os seguintes números são transcendentes:

(a) e;

(b) $\operatorname{sen}\alpha$, $\cos\alpha$, $\tan\alpha$, $\operatorname{senh}\alpha$, $\cosh\alpha$, $\tanh\alpha$ para todo $\alpha \in \overline{\mathbb{Q}}^*$;

(c) π;

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

Demonstração. (a) Para provar basta fazer $\alpha = 1$ no corolário 2.5.2;

(b) Utilizando a fórmula de Euler $e^{ix} = \cos x + i \operatorname{sen} x$, para $x \in \mathbb{R}$. Note que,

$$\begin{aligned}
2i(\operatorname{sen}\alpha)e^0 + (-1)e^{i\alpha} + e^{-i\alpha} &= 0 \\
2(\cos\alpha)e^0 + (-1)e^{i\alpha} + (-1)e^{-i\alpha} &= 0 \\
(i\tan\alpha - 1)e^{i\alpha} + (i\tan\alpha + 1)e^{-i\alpha} &= 0 \\
2(\operatorname{senh}\alpha)e^0 + (-1)e^{\alpha} + e^{-\alpha} &= 0 \\
2(\cosh\alpha)e^0 + (-1)e^{\alpha} + (-1)e^{-\alpha} &= 0 \\
(\tan\alpha - 1)e^{\alpha} + (\tan\alpha + 1) &= 0
\end{aligned}$$

Supondo $\alpha \neq 0$ então $i\alpha \neq 0$. Portanto, pelo Teorema 2.5.1,

$$\operatorname{sen}\alpha,\ \cos\alpha,\ \tan\alpha,\ \operatorname{senh}\alpha,\ \cosh\alpha,\ \tanh\alpha$$

são números transcendentes;

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

(d) Suponha que $\log\alpha \in \overline{\mathbb{Q}}^*$. Do segundo item temos que $e^{\log\alpha}$ é transcendente, mas $e^{\log\alpha} = \alpha \in \overline{\mathbb{Q}}$, essa contradição mostra que $\log\alpha \in \mathbb{T}$. Agora, por contradição, suponha $\theta = \operatorname{arcsen}\alpha$ é algébrico. Então pela definição $\alpha = \operatorname{sen}(\theta)$ podemos escrever

$$\alpha = \frac{e^{i\theta} - e^{-i\theta}}{2i},$$

multiplicando ambos os lados por $2i$, rearranjando e depois multiplicando por $e^{i\theta}$

$$\begin{aligned}
2i\alpha &= e^{i\theta} - e^{-i\theta}; \\
e^{i\theta} - e^{-i\theta} - 2i\theta &= 0;
\end{aligned}$$

$$e^{2i\theta} - 1 - 2i\alpha e^{i\theta} = 0. \tag{2.5.1}$$

Esta é uma equação polinomial em $e^{i\theta}$ com coeficientes algébricos. Aplicando o Teorema 2.5.1 na equação 2.5.1 temos uma relação polinomial não trivial satisfeita por $e^{i\theta}$, o que implicaria que $e^{i\theta}$ é algébrico, porém, isso contradiz o corolário 2.5.2, pois supomos que θ é algébrico. De modo análogo, podemos mostrar que as funções inversas de 2. são transcendentes.

□

O teorema de Hermite-Lindemann visto acima é uma versão "forte" de outro teorema também conhecido como Teorema de Lindemann-Weierstrass.

Teorema 2.5.4 (Hermite-Weierstrass)**.** Se $\alpha_1, \ldots, \alpha_m$ são números algébricos distintos, então $e^{\alpha_1}, \ldots, e^{\alpha_m}$ são linearmente independentes sobre $\mathbb{Q}$.

Recordando que um subconjunto $E \subseteq \mathbb{C}$ é denso, se todo subconjunto aberto de $\mathbb{C}$ intersepta E. Em outras palavras, o conjunto E é em certo sentido "onipresente" no plano complexo. O conjunto dos pontos algébricos (isto é, pares ordenados com coordenadas algébricas reais, ou equivalentemente $\overline{\mathbb{Q}}$) é denso em $\mathbb{C}$ (isomorfo à $\mathbb{R}^2$. No entanto, pelo teorema de Lindemann, o conjunto $G := \{(x, e^x) : x > 0\}$ não tem pontos algébricos. Em outros termos, os pontos de G escorregam por entre o conjunto denso $\overline{\mathbb{Q}}$ sem "tocá-lo".

Capítulo 3

Teorema de Gelfond-Schneider

Neste capítulo abordaremos o teorema demonstrado por Alexander Gelfond (1934) e, independentemente, por Theodor Schneider (1935). Além disso, apresentaremos consequências e resultados relacionados a potências transcendentes.

3.1 Resultados auxiliares

Em 1900, durante o Congresso Internacional de Matemática realizado em Paris, David Hilbert apresentou uma célebre lista com 23 problemas (ver Apêndice B). À época, todos eram questões em aberto, muitas das quais exerceram profunda influência sobre o desenvolvimento da matemática no século XX. O sétimo problema de Hilbert trata da natureza transcendente de potências algébricas. Antes, porém, de expor e demonstrar o teorema de Gelfond-Schneider, é necessário apresentar alguns resultados preliminares que servirão de base para a demonstração.

Proposição 3.1.1. Considere a matriz

$$V = \begin{bmatrix} 1 & p_1 & p_1^2 & \dots & p_1^{t-1} \\ 1 & p_2 & p_2^2 & \dots & p_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & p_t & p_t^2 & \dots & p_t^{t-1} \end{bmatrix}$$

com entradas p_j^a na j-ésima linha e $(1+a)$-ésima coluna, com $j = 1, 2, ..., t$ e $a = 0, 1, ..., t-1$. Essa matriz conhecida como matriz de Vandermonde tem o determinante dado por:

$$\det(V) = \prod_{1 \leqslant j < k \leqslant t} (p_k - p_j).$$

Demonstração. Vamos mostrar por indução que o determinante da matriz de Vandermonde é dado por:

$$\det(V) = \prod_{1 \leqslant j < k \leqslant t} (p_k - p_j).$$

Caso base: $n = 2$

$$V = \begin{bmatrix} 1 & p_1 \\ 1 & p_2 \end{bmatrix}, \quad \det(V) = p_2 - p_1 = \prod_{1 \leqslant i < j \leqslant 2} (p_j - p_i).$$

Passo indutivo: Suponha válido para $n-1$, ou seja:

$$\det \begin{bmatrix} 1 & p_1 & \dots & p_1^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & p_{n-1} & \dots & p_{n-1}^{n-2} \end{bmatrix} = \prod_{1 \leqslant i < j \leqslant n-1} (p_j - p_i).$$

Considere o polinômio:

$$P(x) = \det \begin{bmatrix} 1 & p_1 & p_1^2 & \dots & p_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & p_{n-1} & p_{n-1}^2 & \dots & p_{n-1}^{n-1} \\ 1 & p & p^2 & \dots & x^{n-1} \end{bmatrix}.$$

Temos que, $P(x)$ é polinômio de grau $\leqslant n-1$ em x, e o coeficiente de x^{n-1} é $\det(V_{n-1}) = \prod_{1 \leqslant i < j \leqslant n-1}(x_j - x_i)$. Logo,

$$P(x) = \left(\prod_{1 \leqslant i < j \leqslant n-1} (x_j - x_i) \right) \cdot \prod_{k=1}^{n-1} (x - x_k).$$

Avaliando em $x = x_n$:

$$\det(V) = P(x_n) = \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i).$$

Assim, concluímos a demonstração. □

Corolário 3.1.2. A matriz de Vandermonde tem determinante nulo se e somente se existe $j \neq k$ com $p_j = p_k$.

Demonstração. Se $\det(V) = 0$, então pelo menos um dos fatores $(p_k - p_j)$ deve ser zero. Isso implica que existe pelo menos um par (j, k) com $j \neq k$ tal que $p_k = p_j$.

Agora, nos resta mostrar que: Se existem $j \neq k$ com $p_j = p_k$, então $\det(V) = 0$. Se $p_j = p_k$ para $j \neq k$, então a matriz V tem duas linhas idênticas (a linha j e a linha k).

Sabemos que, se uma matriz tem duas linhas iguais, seu determinante é zero. Portanto, $\det(V) = 0$. □

Lema 3.1.3. Considere as m equações em n incógnitas

$$a_{k1}x_1 + a_{k2}x_2 + ... + a_{kn}x_n = 0, \quad k = 1, ..., m, \tag{3.1.1}$$

onde $a_{ij} \in \mathbb{Z}$ e $0 < m < n$. Seja A um inteiro positivo tal que $A \geqslant |a_{ij}|$ para todo i e j. Então existe uma solução não trivial $x_1, x_2, ..., x_n$ de 3.1.1 ($x_i \in \mathbb{Z}, 1 \leqslant i \leqslant n$) tal que

$$|x_j| < 1 + (nA)^{\frac{m}{n-m}}, \quad j = 1, 2, ..., n.$$

Demonstração. Denote y_k por $a_{k1}x_1 + a_{k2}x_2 + ... + a_{kn}x_n$, então todo ponto $x = (x_1, x_2, \ldots, x_n)$ corresponde a um ponto $y = (y_1, y_2, \ldots, y_m)$. Um ponto x é dito reticulado se suas coordenadas x_j são números inteiros. Observe que se x é reticulado, então seu correspondente y também o é. Seja q um inteiro positivo, especificado posteriormente. Considere o cubo n-dimensional C definido por $|x_j| \leqslant q, \quad j = 1, \ldots, n$. Note que existem $(2q+1)^n$ pontos reticulados em C. Para os correspondentes y, temos:

$$|y_k| = \left| \sum_{j=1}^{n} a_{kj}x_j \right| \leqslant \sum_{j=1}^{n} |a_{kj}||x_j| \leqslant \sum_{j=1}^{n} Aq = nAq.$$

Portanto, existem no máximo $2nAq + 1$ possibilidades para y_k. Como $k = 1, \ldots, m$ então temos $(2nAq+1)^m$ pontos reticulados dentro do cubo m-dimensional D, que têm todas as suas coordenadas em módulo $\leqslant nAq$. Mostraremos que existem mais pontos reticulados em C do que correspondentes em D, daí existem pontos reticulados em D que têm dois correspondentes distintos em C. De fato, basta-nos mostrar que

$$(2q+1)^n > (2nAq+1)^m. \tag{3.1.2}$$

Considere o intervalo $I = \left[(nA)^{\frac{m}{n-m}} - 1, (nA)^{\frac{m}{n-m}} + 1\right)$ com comprimento 2, logo existe um número par em I. Seja q o único inteiro positivo tal que

$$(nA)^{\frac{m}{n-m}} - 1 \leqslant 2q < (nA)^{\frac{m}{n-m}} + 1. \tag{3.1.3}$$

A primeira parte da desigualdade implica

$$(nA)^m \leqslant (2q+1)^{n-m}.$$

Temos então,

$$(2nAq+1)^m = (nA)^m\left(2q+\frac{1}{nA}\right)^m < (nA)^m(2q+1)^m$$
$$\leqslant (2q+1)^{n-m}(2q+1)^m = (2q+1)^n.$$

Segue-se que existe um ponto reticulado $y \in D$ imagem dos pontos $x' = (x'_1, \ldots, x'_n)$ e $x'' = (x''_1, \ldots, x''_n)$. Defina $x = x' - x''$; isto é, $x = (x_1, \ldots, x_n)$ onde $x_i = x'_i - x''_i$, $1 \leqslant i \leqslant n$. Como $x' \neq x''$ então $x \neq 0$ e

$$\begin{aligned} a_{k1}x_1 + \ldots + a_{kn}x_n &= a_{k1}(x'_1 - x''_1) + \ldots + a_{kn}(x'_n - x''_n) \\ &= (a_{k1}x'_1 + \ldots + a_{kn}x'_n) - (a_{k1}x''_1 + \ldots + a_{kn}x''_n) \\ &= y - y = 0, \quad \text{para} \quad k = 1, \ldots, m. \end{aligned}$$

Além disso, por 3.1.3

$$|x_j| = |x'_j - x''_j| \leqslant |x'_j| + |x''_j| \leqslant 2q < 1 + (nA)^{\frac{m}{n-m}}$$

□

Observação 3.1.1. Seja $\alpha \in K$ um número algébrico. A altura de α, denotada por $||\alpha||$, é o máximo entre os valores absolutos dos conjugados de α. Pela proposição 1.2.1, temos que

$$||\alpha + \beta|| \leqslant ||\alpha|| + ||\beta||$$
$$||\alpha.\beta|| \leqslant ||\alpha|| \cdot ||\beta||$$

Lema 3.1.4. Considere as p equações em q incógnitas

$$\alpha_{k1}\zeta_1 + \alpha_{k2}\zeta_2 + \ldots + \alpha_{kq}\zeta_q = 0, \quad k = 1, \ldots, p, \tag{3.1.4}$$

onde os coeficientes $\alpha_{ij} \in K$ são inteiros algébricos e $[K : \mathbb{Q}] = n$. Assuma que $0 < p < q$ e $A \geqslant 1$ tal que $A \geqslant ||\alpha_{ij}||$ para todos i, j. Então existe uma constante positiva c dependendo de K, mas independente de α_{ij}, p, q tal que o sistema 3.1.4 tem uma solução não trivial $\zeta_1, \zeta_2, \ldots, \zeta_q$ em inteiros sobre K, satisfazendo

$$||\zeta_k|| < c + c(cqA)^{\frac{p}{q-p}}, \quad k = 1, \ldots, q$$

Demonstração. Seja $\beta_1, \ldots, \beta_n$ uma base integral de $K|\mathbb{Q}$. Se α é inteiro sobre K então existem $g_1, \ldots, g_n \in \mathbb{Z}$ tal que α é escrito de forma única como

$$\alpha = g_1\beta_1 + \cdots + g_n\beta_n. \tag{3.1.5}$$

Denote os conjugados de α (sobre K) por $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ e de β_j por $\beta_j = \beta_j^{(1)}, \beta_j^{(2)}, \ldots, \beta_j^{(n)}$ para $j = 1, \ldots, n$. Passando o i-ésimo conjugado na igualdade 3.1.5, obtemos pela proposição 1.2.1:

$$\alpha^{(i)} = g_1\beta_1^{(i)} + \cdots + g_n\beta_n^{(i)}, \quad i = 1, \ldots, n. \tag{3.1.6}$$

Considere

$$A = \begin{pmatrix} \alpha^{(1)} \\ \vdots \\ \alpha^{(n)} \end{pmatrix}, \; B = \begin{pmatrix} \beta_1^{(1)} & \ldots & \beta_n^{(1)} \\ \vdots & \ddots & \vdots \\ \beta_1^{(n)} & \ldots & \beta_n^{(n)} \end{pmatrix}, \; G = \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix}$$

As igualdades em 3.1.6 têm a seguinte forma matricial:

$$BG = A. \tag{3.1.7}$$

Por outro lado, como $\{\beta_1, \ldots, \beta_n\}$ é base integral, então $(\det B)^2 = \Delta[\beta_1, \ldots, \beta_n] \neq 0$. Daí $\det B \neq 0$ e portanto existe B^{-1} (matriz inversa de B) que denotaremos por

$$B^{-1} = \begin{pmatrix} \beta_{11} & \beta_{12} & \ldots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \ldots & \beta_{2n} \\ \vdots & \vdots & \ddots & \ldots \\ \beta_{n1} & \beta_{n2} & \ldots & \beta_{nn} \end{pmatrix},$$

onde os β_{ij} só dependem das entradas de B. Multiplicando a igualdade 3.1.7 à esquerda por B^{-1}, obtemos:

$$G = B^{-1}A, \quad \text{isto é,} \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} = \begin{pmatrix} \beta_{11} & \beta_{12} & \ldots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \ldots & \beta_{2n} \\ \vdots & \vdots & \ddots & \ldots \\ \beta_{n1} & \beta_{n2} & \ldots & \beta_{nn} \end{pmatrix} \begin{pmatrix} \alpha^{(1)} \\ \vdots \\ \alpha^{(n)} \end{pmatrix}.$$

Portanto,

$$g_j = \beta_{j1}\alpha^{(1)} + \beta_{j2}\alpha^{(2)} + \cdots + \beta_{jn}\alpha^{(n)}, \quad j = 1, \ldots, n,$$

e então

$$|g_j| \leqslant |\beta_{j1}||\alpha^{(1)}| + \cdots + |\beta_{jn}||\alpha^{(n)}| \leqslant (|\beta_{j1}| + \cdots + |\beta_{jn}|)||\alpha|| < c_1||\alpha||$$
$$\text{onde,} \quad c_1 = \max_{1 \leqslant j \leqslant n} \{|b_{j1}| + \cdots + |b_{jn}|\} + 1.$$

Observe que c_1 depende de K mas independe de α. Portanto,

$$|g_j| < c_1||\alpha|| \quad (j = 1, \ldots, n). \tag{3.1.8}$$

Sendo ζ_i, para $i = 1, 2, \ldots, q$ inteiros algébricos satisfazendo 3.1.4, podemos escrevê-los em termos da base integral,

$$\zeta_i = \sum_{j=1}^{n} x_{ij}\beta_j, \quad i = 1, \ldots, q.$$

O problema então é determinar o comportamento dos números inteiros x_{ij}. Por 3.1.4 temos

$$0 = \sum_{i=1}^{q} \alpha_{ki}\zeta_i = \sum_{i=1}^{q}\sum_{j=1}^{n} x_{ij}\alpha_{ki}\beta_j. \tag{3.1.9}$$

Usando que o produto de inteiros algébricos resulta em um inteiro algébrico, então $\alpha_{ki}\beta_j$ é inteiro algébrico. Portanto,

$$\alpha_{ki}\beta_j = \sum_{r=1}^{n} m_{kijr}\beta_r, \quad k = 1, \ldots, p; \quad i = 1, \ldots, q; \quad j = 1, \ldots, n, \tag{3.1.10}$$

voltando à 3.1.9, obtemos

$$0 = \sum_{r=1}^{n} \left(\sum_{i=1}^{q}\sum_{j=1}^{n} x_{ij}m_{kijr} \right) \beta_r.$$

Como $\{\beta_1, \ldots, \beta_r\}$ é linearmente independente sobre $\mathbb{Q}$, temos

$$0 = \sum_{i=1}^{q}\sum_{j=1}^{n} x_{ij}m_{kijr}, \quad k = 1, \ldots, p; \quad r = 1, \ldots, n, \tag{3.1.11}$$

ou seja, temos um sistema de pn equações com qn incógnitas. Para aplicar o lema 3.1.3, basta-nos então majorar os números m_{kijr}. Por 3.1.10 e pelo mesmo argumento empregado para concluir a desigualdade em 3.1.8, deduzimos que

$$|m_{kijr}| < c_1||\alpha_{ki}\beta_j|| \leqslant c_1||\alpha_{ki}||||\beta_j|| \leqslant c_1 A||\beta_j|| \leqslant c_2 A,$$

onde c_2 é uma constante positiva que satisfaz:

$$c_2 \geqslant c_1||\beta_j|| \quad \text{e} \quad c_2 A \in \mathbb{Z}.$$

Podemos então aplicar o lema 3.1.3 ao sistema 3.1.11. Portanto, existe uma solução não

trivial x_{ij} em inteiros algébricos sobre K tais que

$$|x_{ij}| < 1 + (qnc_2A)^{\frac{ph}{qh-ph}} = 1 + (nc_2qA)^{\frac{p}{q-p}}.$$

Por outro lado, $\zeta_i = \sum_{j=1}^{n} x_{ij}\beta_j$. Daí,

$$||\zeta_i|| < n.\max_j ||\beta_j||(1 + (nc_2qA)^{\frac{p}{q-p}}). \tag{3.1.12}$$

Considere c uma constante positiva tal que $c \geqslant n||\beta_j|| \quad (j = 1, \ldots, n)$ e $c \geqslant nc_2$. Portanto, c só depende de K, e, voltando à 3.1.12, concluímos que

$$||\zeta_i|| < n \cdot \max_j ||\beta_j|| + n \cdot \max_j ||\beta_j||(nc_2qA)^{\frac{p}{q-p}} \leqslant c + c(cqA)^{\frac{p}{q-p}}.$$

Como $\{x_{ij} : i = 1, \ldots, q; j = 1, \ldots, n\} \neq \{0\}$ então um dos $\zeta_i \neq 0$. Segue-se então o resultado. □

3.2 O teorema e algumas consequências

Por fim, temos todas as ferramentas necessárias para provar o teorema de Gelfond-Schneider.

Teorema 3.2.1 (Gelfond-Schneider)**.** Seja $\alpha \in \overline{\mathbb{Q}} - \{0, 1\}$ e $\beta \in \overline{\mathbb{Q}} - \mathbb{Q}$. Então α^β é transcendente.

Demonstração. A demonstração seguirá por absurdo supondo que α^β é um número algébrico. Suponha por absurdo que α^β é algébrico. Escreva $\gamma = \alpha^\beta = e^{\beta \log \alpha}$ e portanto $K := \mathbb{Q}(\alpha, \beta, \gamma)$ é uma extensão finita de $\mathbb{Q}$. Definimos $h, m \in \mathbb{N}$ tais que h é o grau da extensão finita K sobre $\mathbb{Q}$ e $m = 2h + 3$. Note que h (e portanto m) está fixo a partir de agora, pois α, β e γ são dados. A seguir, introduziremos parâmetros auxiliares q, n, t que dependerão de m, mas onde q pode ser escolhido arbitrariamente grande. Defina os números $q, n, t \in \mathbb{N}$ tais que

$$q > 4m^2, \quad n = q^2/2m \quad \text{e} \quad t = q^2 = 2mn, \quad n > q. \tag{3.2.1}$$

Isso será crucial mais adiante, pois a contradição surgirá ao tomar q suficientemente grande (e, consequentemente, n e t grandes). Definamos também $\rho_1, \rho_2, \ldots, \rho_t$ como

$$(r + k\beta) \log \alpha, \quad \text{para} \quad r = 1, 2, \ldots, q; \quad k = 1, 2, \ldots, q, \tag{3.2.2}$$

em alguma ordem. Não precisamos especificar exatamente os ρ_i's. Considere a função

abaixo

$$F(z) = \sum_{j=1}^{t} \eta_j e^{z\rho_j}, \tag{3.2.3}$$

onde η_1, $\eta_2, \ldots, \eta_t$ são inteiros algébricos sobre K que serão especificados a posteriori. Note que $F(z)$ é uma função holomorfa (isto é, tem derivada em todo o plano complexo). O que queremos agora é mostrar que $F(z)$ está bem definida e estabelecer condições para que possamos aplicar o lema 3.1.4 à função. Queremos escolher os η_j não todos nulos, de modo que $F(z)$ tenha zeros de ordem pelo menos n em cada ponto inteiro $b = 1, \ldots, m$. Isso corresponde a impor as condições:

$$F^{(a)}(b) = 0, \qquad b = 1, \ldots, m, \quad a = 0, 1, \ldots, n-1.$$

Cada par (b, a) fornece uma equação linear homogênea nas incógnitas $\eta_1, \ldots, \eta_t$. Temos m valores de b e n valores de a, totalizando mn equações. Como $t = 2mn$ (pois $t = q^2 = 2mn$), o número de incógnitas é maior que o número de equações. Portanto, o sistema admite uma solução não trivial $(\eta_1, \ldots, \eta_t) \in K^t$, a qual pode ser escolhida com coeficientes de altura controlada pelo lema 3.1.4. Fazendo a a-ésima derivada de $F(z)$ e igualando a zero temos:

$$F^{(a)}(z) = \sum_{j=1}^{t} \eta_j \rho_j^a e^{z\rho_j} = 0,$$

aplicando a função em $z = b$ temos

$$F^{(a)}(b) = \sum_{j=1}^{t} \eta_j \rho_j^a e^{b\rho_j} = 0. \tag{3.2.4}$$

Por 3.2.2 temos que os coeficientes

$$\begin{aligned} \rho_j^a e^{\rho_j b} &= (r + k\beta)^a (\log \alpha)^a \cdot e^{b(r+k\beta)\log\alpha} \\ &= (r + k\beta)^a (\log \alpha)^a \cdot \alpha^{br} \alpha^{k\beta b} \\ &= (r + k\beta)^a (\log \alpha)^a \cdot \alpha^{br} (\alpha^{\beta})^{kb} \\ &= (r + k\beta)^a (\log \alpha)^a \cdot \alpha^{br} \gamma^{kb}. \end{aligned} \tag{3.2.5}$$

Note que $(\log \alpha)$ é transcendente (Teorema de Hermite-Lindemann). Porém, como queremos utilizar o lema 3.1.4 que exige coeficientes inteiros algébricos iremos "limpar" os coeficientes, primeiro eliminando o fator $(\log \alpha)^a$. Multiplicando 3.2.5 por $(\log \alpha)^{-a}$ temos

$$(r + k\beta)^a \cdot \alpha^{br} \gamma^{kb}. \tag{3.2.6}$$

Precisamos agora converter os coeficientes algébricos em inteiros algébricos. Para isso

usaremos a proposição 1.2.4 para obter um inteiro racional $c_1 > 0$ tal que $c_1\alpha$, $c_1\beta$ e $c_1\gamma$ sejam inteiros algébricos. Daí, precisamos de uma potência de c_1 suficientemente grande para "limpar" todos os possíveis denominadores que aparecem quando elevamos α, β e γ a várias potências e os multiplicamos. Vamos analisar cada potência de 3.2.6

- Em α^{br}.
  O expoente máximo de α é br e como $r \leqslant q$ e $b \leqslant m$, temos que $br \leqslant mq$. Portanto para "limpar" α^{br} precisamos de pelo menos mq fatores de α para cobrir todos os α^{br}.

- Em γ^{bk}.
  O expoente máximo de γ é bk e como $b \leqslant m$ e $k \leqslant q$, temos que $bk \leqslant mq$, ou seja, precisamos de pelo menos mq fatores de γ.

- Em $(r + k\beta)^a$.
  Expandindo temos
  $$(r + k\beta)^a = \sum_{i=0}^{a} \binom{a}{i} r^{a-i}(k\beta)^i,$$
  o termo com maior potência de β é quando $i = a : (k\beta)^a = k^a\beta^a$, o expoente máximo de β é "a", como $a = 0, \ldots, n-1$ temos que para "limpar" β^a precisamos de pelo menos n fatores.

Portanto, temos

$$mq + mq + n = 2mq + n.$$

Multiplicando 3.2.6 por c_1^{2mq+n} temos que

$$c_1^{2mq+n}(r + k\beta)^a \cdot \alpha^{br}\gamma^{kb}, \tag{3.2.7}$$

é um inteiro algébrico. Agora precisamos encontrar um limitante para os conjugados de 3.2.7 sobre K. Usando a observação 3.1.1 note que

$$\begin{aligned} ||r + k\beta|| &\leqslant ||r|| + ||k|| \cdot ||\beta|| \\ &\leqslant q + q||\beta|| = q(1 + ||\beta||). \end{aligned}$$

Defina $c_2 = \max\{||\alpha||, ||\gamma||, 1 + ||\beta||\}$. Assim, c_2 independe de n, q, t e note que como

$$\begin{aligned} q(1 + ||\beta||) &\leqslant qc_2 \\ ||\alpha^{rb}|| &\leqslant c_2^{rb} \\ ||\gamma^{kb}|| &\leqslant c_2^{kb}, \end{aligned}$$

temos que

$$\begin{aligned}||c_1^{2mq+n}(r+k\beta)^a\cdot\alpha^{br}\gamma^{kb}|| &\leqslant c_1^{2mq+n}c_2^{rb}c_2^{kb}(qc_2)^a\\ &\leqslant c_1^{2mq+n}c_2^{qm}c_2^{qm}(qc_2)^n = c_1^{2mq+n}c_2^{2mq}(qc_2)^n\\ &= (c_1c_2)^n(c_1c_2)^{2mq}q^n.\end{aligned}$$

Como $q^2 = 2mn$, então $q = \sqrt{2mn}$ e assim

$$\begin{aligned}q^n = (\sqrt{2mn})^n &= (\sqrt{2m})^n\cdot(\sqrt{n})^n\\ &= (\sqrt{2m})^n\cdot n^{n/2}.\end{aligned}$$

Logo,

$$(c_1c_2)^n[(c_1c_2)^{2m}]^q(\sqrt{2m})^n\cdot n^{n/2}. \tag{3.2.8}$$

Defina $c_3 = (c_1c_2)^{2m+1}\sqrt{2m}$ para fazermos a seguinte limitação

$$||c_1^{2mq+n}(r+k\beta)^a\cdot\alpha^{br}\gamma^{kb}|| \leqslant c_3^n n^{n/2} \quad (n>q),$$

onde c_3 independe de n. Finalmente pelo lema 3.1.4 concluímos que o sistema com mn equações e $2mn$ incógnitas

$$c_1^{2mq+n}(\log\alpha)^{-a}F^{(a)}(b) = 0,$$

com $a = 0,\ldots,n-1$ e $b = 1,\ldots,m$ tem solução não trivial η_j em inteiros algébricos com

$$\begin{aligned}||\eta_j|| < c + c(c2mnc_3^n n^{n/2})^{\frac{mn}{(2mn-mn)}} &= c + c(c2mnc_3^n n^{n/2})\\ &= c + 2c^2mnc_3^n n^{n/2}\\ &< 3c^2mnc_3^n n^{n/2},\end{aligned}$$

onde c depende de K mas independe de n. Como $2^n > n > q > m$, então $q \leqslant n-1$, logo $q^2 \leqslant (n-1)^2$, note que $4^n > (n-1)^2 \geqslant q^2$. Portanto, $4^n > mn$, daí

$$\begin{aligned}||\eta_j|| < 3c^2 4^n c_3^n n^{n/2} &= 3c^2(4c_3)^n n^{n/2}\\ &< c_4^n n^{n/2},\end{aligned} \tag{3.2.9}$$

onde $c_4 = 12c^2c_3$ (usamos que $3c^2 < (3c^2)^n$, pois c pode ser tomado maior que 1). Agora $F(z)$ está completamente definida. Considere agora o seguinte lema

Lema 3.2.2. Existem $p \geqslant n$ e $1 \leqslant B \leqslant m$ tais que $F^{(a)}(b) = 0$, para $a = 0,\ldots,p-1$, $b = 1,\ldots,m$ e $F^{(p)}(B) \neq 0$.

Demonstração. Se tal inteiro p existe, então da construção que fizemos anteriormente em 3.2.4 temos que para encontrarmos uma ordem em que a derivada é diferente de zero, nos pontos de B, essa ordem tem que ser maior que n. Logo é suficiente provar que existe $a = 0, \ldots, t-1$ com $t > n$ tal que $F^{(a)}(1) \neq 0$. Vamos supor por contradição que $F^{(a)}(1) = 0$ para todo $a = 0, \ldots, t-1$ daí,

$$\sum_{j=1}^{t} \eta_j \rho_j^a e^{\rho_j} = 0.$$

Como η_j's não são todos nulos, temos que

$$0 = \det(\rho_j^a e^{\rho_j}) = \det(\rho_j^a) \cdot \prod_{j=1}^{t} e^{\rho_j},$$

como $e^{\rho_j} \neq 0$ para qualquer ρ_j então temos que $\det(\rho_j^a) = 0$ que é exatamente o determinante de Vandermonde e pelo corolário 3.1.2 temos que $\rho_s = \rho_l$ para algum $s \neq l$, logo

$$(r_s + k_s\beta)\log\alpha = (r_l + k_l\beta)\log\alpha,$$

como $\log\alpha \neq 0$ temos que:

$$r_s + k_s\beta = r_l + k_l\beta \Rightarrow (k_s - k_l)\beta = r_s - r_l,$$

logo,

$$\beta = \frac{r_s - r_l}{k_s - k_l},$$

e β seria racional, o que é uma contradição. Portanto, existe algum $a = 0, \ldots, t-1$ com $t > n$ tal que $F^{(a)}(1) \neq 0$. □

Usando o lema anterior definimos o seguinte número não nulo

$$\begin{aligned} \zeta &= (\log\alpha)^{-p} F^{(p)}(B) \\ &= \sum_{j=1}^{t} \eta_j (r + k\beta)^p \alpha^{Br} \gamma^{Bk}. \end{aligned} \tag{3.2.10}$$

Agora usaremos a definição 1.2.2 para o seguinte lema

Lema 3.2.3. Existe uma constante positiva $\widetilde{C}$, independente de n e p tal que

$$|N(\zeta)| \geqslant \widetilde{C}^{-p},$$

onde $N(\zeta)$ é a norma de ζ no corpo de números $K = \mathbb{Q}(\alpha, \beta, \gamma)$.

Demonstração. Note que, semelhante ao que fizemos anteriormente, temos que $c_1^{p+2mq}\zeta$

é um inteiro algébrico, pois $(r+k\beta)^p\alpha^{Br}\gamma^{Bk}$ é um polinômio sobre α, β e γ com grau $p+Br+Bk \leqslant p+2mq$, já que $B \leqslant m$ e $r,k \leqslant q$. Como $q < n \leqslant p$ então

$$c_1^{p+2mq} < c_1^{p+2mp} = (c_1^{1+2m})^p = c_5^p \quad (\text{onde} \quad c_5 = c_1^{1+2m}).$$

Como $p > q$ então $p = q+s$, para algum $s \in \mathbb{N}$ e assim,

$$c_5^p\zeta = c_1^{p+2mp}\zeta = c_1^{p+2m(q+s)}\zeta = c_1^{p+2mq+2ms}\zeta = c_1^{2ms}(c_1^{p+2mq}\zeta).$$

Portanto, $c_5^p\zeta$ também é inteiro algébrico. Por (ii) e (iii) na proposição 1.2.3, $N(c_5^p\zeta) \in \mathbb{Z}^*$. Segue-se dos outros itens da proposição que

$$1 \leqslant |N(c_5^p\zeta)| = |N(c_5^p)\cdot N(\zeta)| = |N(c_5^p)|\cdot|N(\zeta)| = c_5^{ph}|N(\zeta)|.$$

Daí,

$$|N(\zeta)| \geqslant \widetilde{C}^{-p},$$

onde $\widetilde{C} = c_5^h$. Observe que $\widetilde{C}$ independe de n e p. □

Agora provaremos um lema que será crucial para a demonstração do teorema

Lema 3.2.4. Existe uma constante positiva $\tilde{c}$, independente de n e p, tal que

$$||\zeta|| \leqslant \tilde{c}^p p^p.$$

Demonstração. Por 3.2.10, temos

$$||\zeta|| \leqslant t\cdot\max_j\{||\eta_j||\cdot||r+k\beta||^p\cdot||\alpha||^{Br}\cdot||\gamma||^{Bk}\}.$$

Agora, $q < n \leqslant p$ e $t = 2mn < 2n^2 < 2^n$ para n suficientemente grande. Usando 3.2.9 e substituindo r, k, β, $||\alpha||$, $||\gamma||$ e $1+||\beta||$ pelos seus máximos q, q, m, c_2, c_2 e c_2, respectivamente, obtemos:

$$\begin{aligned} ||\zeta|| &\leqslant 2^n c_4^n n^{n/2} q^p c_2^p c_2^{mq} c_2^{mq} \\ &\leqslant 2^p c_4^p n^{n/2} q^p c_2^p c_2^{2mp} = (2c_4c_2^{1+2m})^p n^{n/2} q^p. \end{aligned} \tag{3.2.11}$$

Por outro lado, $q^2 = 2mn$ então

$$q^p = (\sqrt{2m})^p n^{p/2} \leqslant (\sqrt{2m})^p p^{p/2} \quad \text{e} \quad n^{n/2} \leqslant p^{p/2},$$

aplicando essa desigualdade em 3.2.11,

$$\begin{aligned} ||\zeta|| &\leqslant (2c_4c_2^{1+2m})^p n^{n/2} q^p \\ &\leqslant (2c_4c_2^{1+2m})^p p^{p/2} (\sqrt{2m})^p p^{p/2} = \tilde{c}^p p^p, \end{aligned}$$

onde $\tilde{c} = 2\sqrt{2m}c_4c_2^{1+2m}$. □

Pelo lema 3.2.2, a função inteira $F(z)$ tem zeros, de ordem pelo menos p nos pontos $z = 1, \ldots, m$. Portanto $S(z)$ definida a seguir também é função inteira.

$$S(z) = p!F(z)\prod_{b=1}^{m}(z-b)^{-p}\prod_{\substack{b=1\\ b\neq B}}^{m}(B-b)^p. \tag{3.2.12}$$

Podemos expandir $F(z)$ em série de Taylor em torno de $z = B$ [1],

$$F(z) = \frac{F^{(p)}(B)(z-B)^p}{p!} + \sum_{k=1}^{\infty}\frac{F^{(p+k)}(B)(z-B)^{p+k}}{(p+k)!}. \tag{3.2.13}$$

Pois, como $F(z)$ tem zeros de ordem pelo menos p, então $F(B) = F'(B) = F''(B) = \cdots = F^{(p-1)}(B) = 0$. Substituindo em 3.2.12, obtemos:

$$S(z) = p!\left(\frac{F^{(p)}(B)(z-B)^p}{p!} + \sum_{k=1}^{\infty}\frac{F^{(p+k)}(B)(z-B)^{p+k}}{(p+k)!}\right)\cdot\prod_{\substack{b=1\\ b\neq B}}^{m}(B-b)^p\prod_{b=1}^{m}(z-b)^{-p},$$

substituindo $\prod_{b=1}^{m}(z-b)^{-p} = \dfrac{1}{(z-B)^p}\cdot\dfrac{1}{\prod_{b\neq B}(z-b)^p}$ temos:

$$= \left(F^{(p)}(B)(z-B)^p + p!\sum_{k=1}^{\infty}\frac{F^{(p+k)}(B)(z-B)^{p+k}}{(p+k)!}\right)\cdot\frac{\prod_{b\neq B}^{m}(B-b)^p}{(z-B)^p\prod_{b\neq B}(z-b)^p}.$$

Daí,

$$= F^{(p)}(B)\frac{\prod_{b\neq B}^{m}(B-b)^p}{\prod_{b\neq B}(z-b)^p} + p!\sum_{k=1}^{\infty}\frac{F^{(p+k)}(B)(z-B)^k}{(p+k)!}\frac{\prod_{b\neq B}^{m}(B-b)^p}{\prod_{b\neq B}(z-b)^p}.$$

Fazendo $z = B$ em $S(z)$ temos que $S(B) = F^{(p)}(B)$. Daí, como $\zeta = (\log\alpha)^{-p}F^{(p)}(B)$, então

$$\zeta = (\log\alpha)^{-p}S(B).$$

[1] $F(z) = F(B) + F'(B)(z-B) + \dfrac{F''(B)}{2!}(z-B)^2 + \cdots + \dfrac{F^{(n)}(B)}{n!}(z-B)^n + \ldots$

Pela fórmula Integral de Cauchy (ver [4], p.84), temos:

$$S(B) = \frac{1}{2\pi i}\int_C \frac{S(z)}{z-B}dz,$$

onde C é uma curva simples fechada [2] em torno de $z = B$.

Vamos considerar C o círculo $|z| = \frac{p}{q}$. Note que,

$$\frac{p}{q} \geqslant \frac{n}{q} = \frac{q}{2m} > \frac{4m^2}{2m} = 2m > m \geqslant B.$$

Segue-se que $z = B$ está no interior do disco cujo bordo é C (isto é, $|z| \leqslant \frac{p}{q}$). Sabemos que se $u \in \mathbb{C}$, então $|e^u| \leqslant e^{|u|}$ [3], portanto, para todo z no círculo $|z| = \frac{p}{q}$,

$$\begin{aligned}|e^{z\rho_j}| \leqslant e^{|z\rho_j|} \leqslant e^{\frac{p}{q}(q+q|\beta|)|\log\alpha|} &= e^{p(1+|\beta|)|\log\alpha|} \\ &= (e^{(1+|\beta|)|\log\alpha|})^p = c_6^p,\end{aligned}$$

onde $c_6 = e^{(1+|\beta|)|\log\alpha|}$.

Observe que c_6 independe de n e p. Por 3.2.3 e 3.2.9, temos

$$\begin{aligned}|F(z)| = \left|\sum_{j=1}^{t}\eta_j e^{z\rho_j}\right| \leqslant \sum_{j=1}^{t}|\eta_j||e^{z\rho_j}| &\leqslant tc_4^n n^{\frac{n}{2}}c_6^p \\ &< 2^p c_4^p n^{\frac{n}{2}}c_6^p \quad (t < 2^n) \\ &= (2c_4c_6)^p p^{\frac{p}{2}}, \qquad (3.2.14)\end{aligned}$$

onde $c_7 = 2c_4c_6$. Também, para $b = 1, 2, \ldots, m$,

$$|z-b| \geqslant |z| - |b| \geqslant \frac{p}{q} - m \geqslant \frac{p}{2q}.$$

Daí,

$$|z-b|^{-p} \leqslant \left(\frac{2q}{p}\right)^p. \qquad (3.2.15)$$

[2] A curva $\alpha : [a,b] \to \mathbb{C}$ é dita fechada, se $\alpha(a) = \alpha(b)$. Se a função α for injetiva (executando a possibilidade de a curva ser fechada), a curva é chamada de simples.

[3] $|e^u| = |e^x||e^{iy}|$, onde e^{iy} tem módulo 1 e $e^x > 0$, logo $|e^u| = e^x$. Como $e^{|u|} = e^{\sqrt{x^2+y^2}}$. Assim, $e^x \leqslant e^{\sqrt{x^2+y^2}}$, pois $x \leqslant \sqrt{x^2+y^2}$

Aplicando 3.2.12, 3.2.14 à 3.2.15, obtemos

$$\begin{aligned}
|S(z)| &= |p!F(z)|\left|\prod_{b=1}^{m}(z-b)^{-p}\right|\left|\prod_{\substack{b=1\\ b\neq B}}^{m}(B-b)^{p}\right| \\
&< p!c_7^p p^{\frac{p}{2}}\prod_{b=1}^{m}\left(\frac{2q}{p}\right)^{p}\prod_{\substack{b=1\\ b\neq B}}^{m}|B-b|^{p} \\
&= p!c_7^p p^{\frac{p}{2}}\left(\frac{2q}{p}\right)^{mp}\prod_{\substack{b=1\\ b\neq B}}^{m}|B-b|^{p} \\
&= \left(c_7 2^m (2m)^{\frac{m}{2}}\prod_{\substack{b=1\\ b\neq B}}^{m}|B-b|\right)^{p} p!p^{\frac{p}{2}}\left(\frac{\sqrt{n}}{p}\right)^{mp} \\
&= c_8 p!p^{\frac{p}{2}}\left(\frac{\sqrt{n}}{p}\right)^{mp},
\end{aligned}$$

onde $c_8 = \left(c_7 2^m (2m)^{\frac{m}{2}}\prod_{\substack{b=1\\ b\neq B}}^{m}|B-b|\right)^{p}$.

Como $p! < p^p$ e $\dfrac{\sqrt{n}}{p} \leqslant \dfrac{1}{\sqrt{n}}$, pois $n \leqslant p$, concluímos que

$$\begin{aligned}
|S(z)| < c_8^p p^p p^{\frac{p}{2}} n^{\frac{-mp}{2}} &< c_8^p p^p p^{\frac{p}{2}} p^{\frac{-mp}{2}} \\
&= c_8^p p^{\frac{p(3-m)}{2}},
\end{aligned} \tag{3.2.16}$$

para todo z no círculo C. Por outro lado,

$$|\zeta| \leqslant |\log\alpha|^{-p}\cdot|S(B)| = |\log\alpha|^{-p}\frac{1}{2\pi}\left|\int_C \frac{S(z)}{z-B}dz\right|.$$

Como o comprimento do caminho de integração é $2\pi\frac{p}{q}$ [4], podemos aplicar 3.2.15 e 3.2.16

[4]Sejam U um subconjunto de $\mathbb{C}$, $[a,b]\subset\mathbb{R}$ um intervalo compacto com $a<b$, $\gamma:[a,b]\to U$ um caminho de classe C^1 por partes, cuja imagem $\Gamma := \gamma([a,b])$ é um compacto e $g: U\to\mathbb{C}$ uma função contínua. Defina:

$$M(g,\gamma) := \sup\{|g(z)| : z\in\Gamma\}, \quad \ell(\gamma) := \int_a^b |\gamma'(t)|\,dt,$$

onde $\ell(\gamma)$ é o comprimento de γ. Então:

$$\left|\int_\gamma g(z)\,dz\right| \leqslant M(g,\gamma)\cdot\ell(\gamma).$$

Além disso, como Γ é compacto e g é contínua em $U\supset\Gamma$, temos $M(g,\gamma) = \max_{z\in\Gamma}|g(z)| < \infty$.

para escrever

$$\begin{aligned}
&< \frac{1}{2\pi}|\log\alpha|^{-p}2\pi\frac{p}{q}c_8^p p^{\frac{p(3-m)}{2}}\frac{2q}{p} \\
&= 2|\log\alpha|^{-p}c_8^p p^{\frac{p(3-m)}{2}} < (2c_8|\log\alpha|^{-1})^p p^{\frac{p(3-m)}{2}} \quad (\text{com} \quad 2 \leqslant 2^p) \\
&= c_9^p p^{\frac{p(3-m)}{2}},
\end{aligned}$$

onde $c_9 = 2c_8|\log\alpha|^{-1}$ e independe de n e p. Portanto,

$$\begin{aligned}
|N(\zeta)| = |\zeta||\zeta^{(2)}|\ldots|\zeta^{(h)}| \leqslant |\zeta|||\zeta||^{h-1} &< c_9^p p^{\frac{p(3-m)}{2}}(\tilde{c}^p p^p)^{h-1} \\
&= c_9^p p^{\frac{p(-2h)}{2}}\tilde{c}^{p(h-1)}p^{p(h-1)} \quad (\text{com} \quad m = 2h+3) \\
&= (c_9\tilde{c}^{h-1})^p p^{-ph}p^{ph-p} = (c_{10})^p p^{-p},
\end{aligned}$$

onde $c_{10} = c_9\tilde{c}^{h-1}$. Por outro lado, pelo lema 3.2.3, temos,

$$\tilde{C}^{-p} \leqslant |N(\zeta)| < c_{10}^p p^{-p} \Rightarrow c_{10}^p p^{-p} > \tilde{C}^{-p} \Rightarrow \tilde{C}c_{10} > p,$$

$\tilde{C}$ e c_{10} são constantes que não dependem de n e p. No entanto, essa desigualdade não se verifica se escolhermos um n suficientemente grande, pois $p \geqslant n$, ou seja, há uma contradição. Portanto, α^β é transcendente. □

Observação 3.2.1. Imediatamente, os números $2^{\sqrt{2}}, i^i$ e $\sqrt{2}^{\sqrt{3}}$ são transcendentes

Observação 3.2.2. Ao contrário do caso real, a função exponencial complexa (e^z ou $exp(z)$) não tem inversa em $\mathbb{C}$, visto que não é injetiva. De fato, $e^{z+2k\pi i} = e^z$, para todo $z \in \mathbb{C}$. Por esse motivo, uma função logaritmo seria multivaluada. Mais precisamente, se $z \in \mathbb{C}$, então

$$\log z = \log|z| + i(arg(z) + 2k\pi), \quad \text{para todo} \quad k \in \mathbb{Z},$$

onde $\arg(z)$, chamado argumento $z = a + bi$, é a medida do ângulo entre os vetores $(1,0)$ e (a,b), onde consideramos a medida positiva quando é medido no sentido contrário aos ponteiros do relógio. Por esta razão, $i^i = e^{i\log i} = e^{-(\frac{4k+1}{2})\pi}$, $k \in \mathbb{Z}$. Para corrigir esse problema, iremos restringir o domínio da função exponencial a conjuntos onde ela é injetiva, como por exemplo a "faixa":

$$\mathbf{\Omega} = \{a + bi \in \mathbb{C} : -\pi < b \leqslant \pi\}.$$

Nesse caso $\exp : \mathbf{\Omega} \to \mathbb{C}^*$ é invertível e sua inversa é chamado de ramo principal do logaritmo. Assim, o valor de α^β, será definido como $e^{\beta\log\alpha}$, onde $\log : \mathbb{C}^* \to \mathbf{\Omega}$ é o ramo principal do logaritmo.

O teorema de Gelfond-Schneider encerrou a questão sobre a natureza aritmética da potenciação de dois algébricos, visto que se $\alpha \in \{0,1\}$ ou se $\beta \in \mathbb{Q}$, então α^β é algébrico. uma formulação equivalente do Teorema de Gelfond-Schneider é a seguinte.

Teorema 3.2.5. Se α e γ são algébricos não nulos, com $\alpha \neq 1$, então

$$\beta = \frac{\ln \gamma}{\ln \alpha},$$

é um número racional ou é transcendente.

Demonstração. Provemos a equivalência de ambos os teoremas.

Suponhamos que se verificam as hipóteses do Teorema 3.2.5, mas β é um número algébrico irracional. Da definição de β resulta que $\alpha^\beta = \gamma$, e aplicando o Teorema de Gelfond-Schneider obtemos que γ é transcendente, contradizendo a hipótese. Portanto, o Teorema de Gelfond-Schneider implica o Teorema 3.2.5. Reciprocamente, se α e β verificam as hipóteses de Gelfond-Schneider, mas $\alpha^\beta = \gamma$ é um número algébrico, então

$$\beta = \frac{\ln(\gamma)}{\ln(\alpha)}$$

e, pelo Teorema 3.2.5, β é racional ou transcendente, novamente contradizendo a hipótese. □

Agora, passaremos para algumas consequências interessantes.

Corolário 3.2.6. Sejam α_1, α_2, β_1, β_2 números algébricos, não nulos, com $\log \alpha_1$, $\log \alpha_2$ linearmente independentes sobre $\mathbb{Q}$. Então

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

Demonstração. Suponha por absurdo que existem α_1, α_2, β_1, β_2, satisfazendo as hipóteses do corolário e tais que

$$\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 = 0. \tag{3.2.17}$$

Portanto,

$$-\frac{\beta_1}{\beta_2} = \frac{\log \alpha_2}{\log \alpha_1},$$

implicando que $\alpha_2 = \alpha_1^{-\frac{\beta_1}{\beta_2}}$ e pelo teorema de Gelfond-Schneider, $\dfrac{\beta_1}{\beta_2} \in \mathbb{Q}$. Então existe $p \in \mathbb{Q}$ tal que $\beta_1 = p\beta_2$. Substituindo em 3.2.17, obtemos

$$p \log \alpha_1 + \log \alpha_2 = 0,$$

contrariando a independência linear de $\log\alpha_1, \log\alpha_2$ sobre $\mathbb{Q}$. Logo,

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

□

Exemplo 3.2.1. O número $\dfrac{\log 3}{\log 2}$ é transcendente. Para ver isto, note que $\log 2$ e $\log 3$ são linearmente independentes sobre $\mathbb{Q}$. Caso contrário, $2^a = 3^b$ para alguns inteiros a, b, o que contradiz o Teorema Fundamental da Aritmética. Assim, se $\dfrac{\log 3}{\log 2} = \alpha \in \overline{\mathbb{Q}}$, então teríamos $\log 3 - \alpha \log 2 = 0$, contrariando o corolário anterior.

Corolário 3.2.7. e^π é transcendente.

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

Observação 3.2.3. e^π é conhecido como a constante de Gelfond

O resultado seguinte implica diretamente os teoremas de Gelfond-Schneider e Hermite-Lindemann. Foi demonstrado por Lang [10] em 1966 como um aperfeiçoamento de um resultado similar atribuído a Schneider, razão pela qual é conhecido como Teorema de Schneider-Lang.

Para enunciar o teorema, precisamos ainda do seguinte:

Teorema 3.2.8. Dados $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$, existe $\beta \in \overline{\mathbb{Q}}$ tal que

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\beta).$$

Definição 3.2.1. Sejam $f_1, \ldots, f_n$ funções analíticas em um domínio $D \subset \mathbb{C}$ e K um subcorpo de $\mathbb{C}$. Dizemos que $f_1, \ldots, f_n$ são algebricamente independentes sobre K se não existe polinômio não nulo $P \in K[x_1, \ldots, x_n]$ tal que

$$P(f_1(z), \ldots, f_n(z)) = 0 \quad \text{para todo } z \in D.$$

Caso contrário, elas são algebricamente dependentes sobre K.

A demonstração do Teorema 3.2.8 pode ser encontrada em [1].

Teorema 3.2.9 (Schneider–Lang, versão com elemento primitivo)**.** Sejam $\alpha_1, \ldots, \alpha_n$ números algébricos e seja

$$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n).$$

Sejam $f_1, \ldots, f_N$ funções meromorfas de ordem finita em $\mathbb{C}$ tais que:

1. Para cada $k = 1, \ldots, N$, a derivada $f_k'(z)$ pertence ao anel $K[f_1(z), \ldots, f_N(z)]$;

2. Pelo menos duas das funções, digamos f_{k_1} e f_{k_2}, são algebricamente independentes sobre K.

Sejam ρ_1, ρ_2 as ordens de f_{k_1} e f_{k_2}, respectivamente. Pelo teorema 3.2.8, existe $\beta \in K$ tal que $K = \mathbb{Q}(\beta)$. Então existem no máximo

$$\deg(\beta) \cdot (\rho_1 + \rho_2)$$

pontos distintos $w \in \mathbb{C}$ tais que $f_i(w) \in K$ para todo $i = 1, \ldots, N$.

Deduzamos o Teorema de Hermite-Lindemann utilizando o Teorema de Schneider-Lang. Suponhamos, por absurdo, que e^α seja algébrico para algum $\alpha \in \overline{\mathbb{Q}} \backslash \{0\}$. Definamos o corpo $K = \mathbb{Q}(\alpha, e^\alpha)$ e as funções $f_1(z) = z$ e $f_2(z) = e^{\alpha z}$. Verificam-se as hipóteses do Teorema de Schneider-Lang: (i) as derivadas são $f_1'(z) = 1$ e $f_2'(z) = \alpha e^{\alpha z} = \alpha f_2(z)$, que são polinômios em f_1, f_2 com coeficientes em K; (ii) f_1 e f_2 são algebricamente independentes sobre K; (iii) ambas têm ordem finita ($\rho_1 = 1$ e $\rho_2 = |\alpha|/(2\pi)$). Pelo teorema 3.2.8, existe $\beta \in K$ tal que $K = \mathbb{Q}(\beta)$, e o Teorema de Schneider-Lang garante então que existem no máximo $\deg(\beta)(\rho_1 + \rho_2)$ pontos $w \in \mathbb{C}$ com $f_1(w), f_2(w) \in K$. Contudo, para todo inteiro $n \in \mathbb{N}$, temos $f_1(n) = n \in \mathbb{Q} \subset K$ e $f_2(n) = (e^\alpha)^n \in K$, o que fornece infinitos tais pontos, que é uma contradição. Portanto, e^α é transcendente.

Analogamente, deduzimos o Teorema de Gelfond-Schneider. Suponhamos, por absurdo, que α^β seja algébrico, com $\alpha \in \overline{\mathbb{Q}} \backslash \{0, 1\}$ e $\beta \in \overline{\mathbb{Q}} \backslash \mathbb{Q}$. Consideremos o corpo $K = \mathbb{Q}(\alpha, \beta, \alpha^\beta)$ e as funções $f_1(z) = e^z$ e $f_2(z) = e^{\beta z}$. Novamente valem as hipóteses: as derivadas são $f_1'(z) = f_1(z)$ e $f_2'(z) = \beta f_2(z)$ (polinômios em f_1, f_2 sobre K); f_1 e f_2 são algebricamente independentes sobre K; ambas têm ordem $\rho_1 = \rho_2 = 1$. Seja $\beta_0 \in K$ um elemento primitivo tal que $K = \mathbb{Q}(\beta_0)$. Pelo Teorema de Schneider-Lang, o número de pontos w com $f_1(w), f_2(w) \in K$ é limitado por $\deg(\beta_0)(\rho_1 + \rho_2)$. Entretanto, para cada $n \in \mathbb{N}$, tomando $w_n = n \ln \alpha$ (fixado um ramo do logaritmo), obtemos $f_1(w_n) = \alpha^n \in K$ e $f_2(w_n) = (\alpha^\beta)^n \in K$, produzindo infinitos pontos distintos gerando uma contradição. Logo, α^β é transcendente.

3.3 Combinações lineares de Logaritmos

A seguir apresentaremos uma generalização do Teorema de Gelfond-Schneider, demonstrada pelo matemático Alan Baker [2] em 1966. Através deste teorema, Baker conseguiu demonstrar a independência algébrica sobre $\mathbb{Q}$ dos logaritmos de n números algébricos, desde que estes logaritmos sejam linearmente independentes sobre $\mathbb{Q}$. Em

toda esta seção, trabalhamos com um ramo fixado da função logaritmo complexo. Os resultados de transcendência permanecem válidos independentemente da escolha do ramo

Teorema 3.3.1 (Baker)**.** Se $\alpha_1, \ldots, \alpha_n$ são números algébricos não nulos e os seus logaritmos $\ln(\alpha_1), \ldots, \ln(\alpha_n)$ são linearmente independentes sobre $\mathbb{Q}$, então $1, \ln(\alpha_1), \ldots, \ln(\alpha_n)$ são linearmente independentes sobre $\mathbb{Q}$.

A demonstração do Teorema acima é, ainda que consideravelmente mais complexa, semelhante à do Teorema de Gelfond-Schneider. Consiste em supor a existência de números algébricos $\beta_0, \beta_1, \ldots, \beta_n$, com pelo menos um deles não nulo, tais que

$$\beta_0 + \beta_1 \ln(\alpha_1) + \cdots + \beta_n \ln(\alpha_n) = 0.$$

A contradição busca-se propondo uma função auxiliar complexa ϕ (neste caso, ϕ é uma função de várias variáveis complexas) e encontrando limites para os valores de ϕ e suas derivadas. O passo final consiste em provar que pelo menos uma das desigualdades dadas pelos limites de ϕ não pode verificar-se sob o inicialmente suposto.

No que respeita à teoria dos números transcendentes, o Teorema 3.3.1 tem os seguintes resultados como principais consequências.

Teorema 3.3.2. Sejam $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}} \backslash \{0\}$ e $\beta_0, \beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$ com $\beta_0 \neq 0$. Suponha que os logaritmos $\ln \alpha_1, \ldots, \ln \alpha_n$ sejam linearmente independentes sobre $\mathbb{Q}$. Então

$$\beta_0 + \beta_1 \ln(\alpha_1) + \cdots + \beta_n \ln(\alpha_n) \neq 0.$$

Demonstração. Suponha, por contradição, que

$$\beta_0 + \beta_1 \ln(\alpha_1) + \cdots + \beta_n \ln(\alpha_n) = 0.$$

Podemos reescrever como

$$-\beta_0 = \beta_1 \ln(\alpha_1) + \cdots + \beta_n \ln(\alpha_n).$$

Pelo Teorema de Baker (Teorema 3.3.1 na forma forte), se $\ln \alpha_1, \ldots, \ln \alpha_n$ são linearmente independentes sobre $\mathbb{Q}$, então $1, \ln \alpha_1, \ldots, \ln \alpha_n$ são linearmente independentes sobre $\overline{\mathbb{Q}}$.

Mas a equação acima é exatamente uma relação de dependência linear sobre $\overline{\mathbb{Q}}$ entre $1, \ln \alpha_1, \ldots, \ln \alpha_n$, com coeficientes $(-\beta_0, \beta_1, \ldots, \beta_n) \in \overline{\mathbb{Q}}^{n+1}$ não todos nulos (pois $\beta_0 \neq 0$). Isso contradiz a independência linear sobre $\overline{\mathbb{Q}}$. Portanto, a soma não pode ser zero. □

Teorema 3.3.3. Se $\alpha_1, \ldots, \alpha_n, \beta_0, \beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$ são tais que $\alpha_k \neq 0$ para $k = 1, \ldots, n$,

então

$$\beta_0 + \beta_1 \ln(\alpha_1) + \cdots + \beta_n \ln(\alpha_n)$$

é transcendente.

Demonstração. Denote

$$\gamma = \beta_0 + \beta_1 \ln(\alpha_1) + \cdots + \beta_n \ln(\alpha_n).$$

Suponha, por absurdo, que γ seja um número algébrico.

Escreva a equação como

$$\beta_0 - \gamma + \beta_1 \ln(\alpha_1) + \cdots + \beta_n \ln(\alpha_n) = 0.$$

Esta é uma relação linear sobre $\overline{\mathbb{Q}}$ entre $1, \ln(\alpha_1), \ldots, \ln(\alpha_n)$, com coeficientes $(\beta_0 - \gamma, \beta_1, \ldots, \beta_n) \in \overline{\mathbb{Q}}^{n+1}$.

Se os logaritmos $\ln(\alpha_1), \ldots, \ln(\alpha_n)$ forem linearmente independentes sobre $\mathbb{Q}$, então pelo Teorema de Baker, $1, \ln(\alpha_1), \ldots, \ln(\alpha_n)$ são linearmente independentes sobre $\overline{\mathbb{Q}}$, o que contradiz a existência da relação acima (já que $\beta_0 - \gamma \neq 0$ porque γ é algébrico e β_0 também, mas a relação exige igualdade).

Se, por outro lado, os logaritmos forem linearmente dependentes sobre $\mathbb{Q}$, existe uma relação não trivial

$$q_1 \ln(\alpha_1) + \cdots + q_n \ln(\alpha_n) = 0,$$

com $q_i \in \mathbb{Q}$ não todos nulos. Então podemos reduzir o número de logaritmos na expressão de γ (substituindo um deles em função dos outros) e repetir o argumento com menos variáveis, eventualmente chegando a uma contradição com o caso de independência linear sobre $\mathbb{Q}$, que já tratamos.

Portanto, γ não pode ser algébrico; logo, é transcendente. □

Corolário 3.3.4. $\pi + \ln(\alpha)$ é transcendente se $\alpha \neq 0$ é um número algébrico.

Demonstração. Da igualdade $e^{i\pi} = -1$ obtemos $\pi = \frac{1}{i}\ln(-1) = -i\ln(-1)$ (recordemos que trabalhamos com algum ramo da função logaritmo no plano complexo). Pelo Teorema 3.3.3,

$$\pi + \ln(\alpha) = -i\ln(-1) + \ln(\alpha)$$

é um número transcendente. □

Teorema 3.3.5. $e^{\beta_0}\alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ é transcendente se $\alpha_1, \ldots, \alpha_n, \beta_0, \beta_1, \ldots, \beta_n$ são números algébricos não nulos.

Demonstração. Se supusermos que $\alpha = e^{\beta_0}\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n}$ é algébrico, então

$$\ln(\alpha) - \beta_1\ln(\alpha_1) - \cdots - \beta_n\ln(\alpha_n) = \beta_0$$

é um número algébrico não nulo, contradizendo o Teorema 3.3.2. □

Corolário 3.3.6. $e^{\alpha\pi+\beta}$ é transcendente se α e β são números algébricos, com $\beta \neq 0$.

Demonstração. Novamente fazemos uso da expressão $\pi = -i\ln(-1)$. Aplicando o Teorema 3.3.5, obtemos que

$$e^{\alpha\pi+\beta} = e^{-i\alpha\ln(-1)}e^{\beta} = e^{\beta}(-1)^{-i\alpha}$$

é um número transcendente. □

3.4 Números algébricos como potências de transcendentes

Um problema recreacional na matemática é o de escrever números "comportados" (ex. naturais, inteiros) como combinação de números "complicados" (ex. irracionais, complexos). Por exemplo

$$2 = \sqrt{\sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}} = \sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\cdot^{\cdot}}}} = e^{\log 2}.$$

Em particular, a última identidade acima mostra como o número natural 2 pode ser escrito como potência de dois transcendentes (consequência do Teorema de Hermite-Lindemann). Este fato parece contrariar um pouco a lógica. O teorema de Gelfond-Schneider diz que a potenciação de números "comportados" (ex. algébricos) é transcendente, a menos de casos triviais. Portanto, somos levados a crer que a potenciação de transcendentes (complicados) deveria ser um número "complicado", que não é o caso. Na verdade tudo é possível na natureza aritmética de z^w, quando pelo menos um desses números é transcendente. Podemos passar para outra outra pergunta: existe algum número algébrico da forma t^t, com t transcendente? Seria razoável, conjecturar que a resposta é " Não ", pois isso condiz com o fato de ser esperado que os números $e^e, \pi^\pi, (\log 2)^{\log 2}$ sejam transcendentes. No entanto, a resposta é "Sim" e é uma consequência imediata do Teorema de Gelfond-Schneider.

z	w	z^w	Natureza aritmética
2	$\log 3/\log 2$	3	algébrica
2	$\sqrt{2}\log 3/\log 2$	$3^{\sqrt{2}}$	transcendente
$2^{\sqrt{2}}$	$\sqrt{2}\log 3/\log 2$	9	algébrica
e	π	e^{π}	transcendente
$2^{\sqrt{2}}$	$\sqrt{2}$	4	algébrica
$2^{\sqrt{2}}$	$i\sqrt{2}$	4^i	transcendente

Tabela 3.1: Possibilidades para z^w quando z ou w é transcendente

O Teorema de Gelfond-Schneider representa uma conquista notável na teoria dos números transcendentais. Sua demonstração combina ideias profundas de análise complexa, teoria dos números e álgebra, ilustrando a interconexão entre diferentes áreas da matemática. A seguir temos mais um resultado que é consequência do teorema de Gelfond-Schneider.

Lema 3.4.1. Se Q é racional, não inteiro, então Q^Q é algébrico, não racional.

Demonstração. Para o caso $Q > 0$, escreva $Q = a/b \in \mathbb{Q}$, com $a, b \in \mathbb{N}$ e $\text{mdc}(a,b) = 1$. O número Q^Q é algébrico, pois é raiz de $x^b - Q^a = 0$.

Suponha, por contradição, que $Q^Q = m/n \in \mathbb{Q}$, com $\text{mdc}(m,n) = 1$. Então:

$$\left(\frac{a}{b}\right)^{a/b} = \frac{m}{n} \Rightarrow \left(\frac{a}{b}\right)^{a} = \left(\frac{m}{n}\right)^{b} \Rightarrow a^a n^b = m^b b^a.$$

Seja $d = \text{mdc}(a^a, b^a)$. Como $\text{mdc}(a,b) = 1$, temos $\text{mdc}(a^a, b^a) = 1$, logo $d = 1$. Portanto, $a^a \mid m^b$ e $b^a \mid n^b$. Existe um primo p tal que $p \mid b$. Seja $v_p(b) = r \geqslant 1$ a valoração p-ádica de [5] b. Então $v_p(b^a) = ar$. De $b^a \mid n^b$, temos $v_p(n^b) = b \cdot v_p(n) \geqslant ar$. Logo $v_p(n) \geqslant \frac{ar}{b}$. Como $v_p(n)$ deve ser inteiro, $b \mid ar$. Mas $\text{mdc}(a,b) = 1$, então $b \mid r$, o que é impossível pois $r = v_p(b) < b$. Contradição.

Para $Q < 0$, o argumento procede como na demonstração original. □

Uma consequência imediata do Lema 3.4.1 e do Teorema de Gelfond-Schneider é que Q^{Q^Q} é transcendente, para todo $Q \in \mathbb{Q}\backslash\mathbb{Z}$.

[5] para um primo p e $n \in \mathbb{Z}\backslash\{0\}$, $v_p(n)$ é o maior inteiro k tal que $p^k \mid n$.

Capítulo 4

Conclusão

A trajetória percorrida ao longo desta monografia permitiu uma imersão no Teorema de Gelfond-Schneider, um dos resultados mais elegantes e influentes da teoria dos números do século XX. Mais do que compreender sua formulação e demonstração, foi possível situá-lo em seu contexto histórico, apreciar a engenhosidade de seus métodos e reconhecer suas repercussões no desenvolvimento da matemática moderna.

O teorema, ao estabelecer a transcendência de números da forma α^β, quando α é algébrico distinto de 0 e 1 e β é algébrico irracional, representou uma solução definitiva ao sétimo problema de Hilbert, encerrando uma questão em aberto por mais de três décadas. Sua demonstração, realizada independentemente por Gelfond e Schneider, uniu técnicas de análise complexa, álgebra e teoria dos números de forma brilhante, marcando um ponto de virada na teoria da transcendência.

Além de exemplos notáveis como $2^{\sqrt{2}}$ e e^π, o teorema abriu caminho para novas linhas de investigação, culminando nos avanços de Alan Baker sobre formas logarítmicas lineares, reconhecidos com a Medalha Fields. Esses desdobramentos evidenciam que conquistas aparentemente abstratas possuem não apenas uma beleza intrínseca, mas também aplicações em áreas como ciência da computação e criptografia.

Em perspectiva mais ampla, a resolução do problema de Hilbert ilustra como questões bem formuladas podem estimular décadas de pesquisa e conduzir a descobertas duradouras. O Teorema de Gelfond-Schneider permanece como um testemunho da força criativa da matemática, unindo rigor técnico e profundidade conceitual.

Por fim, espera-se que este trabalho tenha contribuído não apenas para a compreensão deste resultado específico, mas também para reforçar a convicção de que a matemática, ao buscar a verdade abstrata, revela padrões fundamentais que ampliam nossa compreensão tanto do universo matemático quanto do mundo que procuramos descrever por meio dos números.

Referências Bibliográficas

[1] ALACA, Saban; WILLIAMS, Kenneth S. **Introductory algebraic number theory**. Cambridge: Cambridge University Press, 2004.

[2] BAKER, A. **Transcendental Number Theory**. Cambridge University Press, 1975.

[3] BASTOS, G. G. **Tópicos de Álgebra Abstrata**. Fortaleza: Premius, 2003.

[4] CONWAY, J.B. **Functions of a Complex Variable**. Springer, New York, 1973.

[5] ENDLER, O. **Teoria dos Corpos**. Rio de Janeiro: IMPA (Monografia de Matemática; n. 44), 1987.

[6] FIGUEIREDO, D. G. **Números Irracionais e Transcendentes**. Coleção Fundamentos da Matemática Elementar. SBM, p. 114, 1985.

[7] GELFOND, A. O. **Transcendental and Algebraic Numbers**. Dover Publications, 1960.

[8] GONÇALVES, A. **Introdução à Álgebra**. 5. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1994. (Projeto Euclides).

[9] JENSEN, C.; MARQUES, D. **Some Field Theoretic Properties and an Application on Transcendental Numbers**. Journal of Algebra and its Applications, 9(3), p. 493-500, 2010.

[10] LANG, S. **Introduction to Transcendental Numbers**. Addison-Wesley, 1966.

[11] MARQUES, D. **Alguns Resultados que Geram Números Transcendentes**. Dissertação de Mestrado, Universidade Federal do Ceará, Brasil, 2007.

[12] MARQUES, D. **Teoria dos Números Transcendentes**. Rio de Janeiro: SBM, 2013.

[13] NIVEN, I. **Irrational Numbers**. Rahway, NJ: The Mathematical Association of America, 1956.

[14] LINS NETO, Alcides. **Funções de uma variável complexa**. Rio de Janeiro: IMPA, 1976. (Projeto Euclides).

[15] OLIVEIRA, Josivaldo Reis. **A transcendência de PI, e e dos números de Liouville**. São Cristóvão, 2015. Dissertação de mestrado.

[16] POLLARD, H. **The Theory of Algebraic Numbers**. Baltimore: The Mathematical Association of America (The Carus Mathematical Monographs; v. 9), 1950.

[17] SANTOS, José Plínio de Oliveira. **Introdução a Teoria dos Números**. 3ª ed. Rio de Janeiro: IMPA, 2012.

[18] SONDOW, J.; MARQUES, D. **Algebraic and Transcendental Solutions of Some Exponential Equations**. Annales Mathematicae et Informaticae, 37, p. 151-164, 2010.

[19] USPENSKY, J. **The Theory of Equations**. New York: MacGraw-Hill, 1948.

[20] VINBERG, E. B. **A Concise Course in Algebra**. 1ª ed. Moscou: Mir, 1985.

Apêndice A

Biografias dos Matemáticos

ALEXANDER OSIPOVICH GELFOND	
 *Fonte: MacTutor (2025)*	**Dados Básicos:** • Nascimento: 24 de outubro de 1906 em São Petersburgo • Falecimento: 7 de novembro de 1968 em Moscou **Formação:** • Universidade Estatal de Moscou (1927) • Orientadores: Aleksandr Khinchin e Vyacheslaw Stepanov **Contribuições Principais:** • Teorema de Gelfond-Schneider • Teoria dos números transcendentais • Resolução do Sétimo Problema de Hilbert **Reconhecimentos:** • Prêmio Lenin (1954) • Professor da Universidade Estatal de Moscou

Tabela A.1: Dados biográficos essenciais de Alexander Gelfond

Biografia Detalhada de Alexander Gelfond

O pai de Aleksandr Osipovich Gelfond era Osip Isaacovich Gelfond, um médico que também tinha interesse em filosofia. Gelfond entrou na Faculdade de Física e Matemática da Universidade Estadual de Moscou em 1924 e concluiu seus estudos de graduação em

1927. Ele então começou a pesquisar sob a supervisão de Aleksandr Khinchin e Vyacheslaw Stepanov e concluiu seus estudos de pós-graduação em 1930.

Durante 1929-30, ele lecionou matemática na Faculdade Tecnológica de Moscou, mas já havia publicado alguns artigos importantes: "As propriedades aritméticas de funções inteiras"(1929); "Números transcendentais"(1929); e "Um esboço da história e do estado atual da teoria dos números transcendentais"(1930). O segundo desses artigos de 1929 continha a palestra que Gelfond deu no Primeiro Congresso de Matemática da União realizado em Kharkov em 1930.

Esses artigos de Gelfond representam um grande passo à frente no estudo de números transcendentais. O primeiro dos artigos examina o crescimento de uma função inteira que assume valores inteiros para argumentos inteiros. No segundo dos artigos de 1929, Gelfond aplicou esse resultado para provar que certos números são transcendentais, resolvendo assim um caso especial do Sétimo Problema de Hilbert.

Gelfond descreve a visita de quatro meses que fez em 1930 à Alemanha, onde passou um tempo em Berlim e Göttingen. Ele foi particularmente influenciado por Hilbert, Siegel e Landau durante sua visita. Após seu retorno à Rússia, Gelfond ensinou matemática a partir de 1931 na Universidade Estadual de Moscou, onde ocupou cadeiras de análise, teoria dos números e história da matemática. A partir de 1933, ele também trabalhou no Instituto de Matemática da Academia Russa de Ciências.

Gelfond desenvolveu técnicas básicas no estudo de números transcendentais, ou seja, números que não são a solução de uma equação algébrica com coeficientes racionais. Além de seu importante trabalho na teoria dos números transcendentais, Gelfond fez contribuições significativas para a teoria da interpolação e a aproximação de funções de uma variável complexa. Ele também contribuiu para o estudo de equações diferenciais e equações integrais e à história da matemática.

Fonte: O'CONNOR, J. J.; ROBERTSON, E. F. **Alexander Osipovich Gelfond**. MacTutor History of Mathematics Archive. Disponível em: `https://mathshistory.st-andrews.ac.uk/Biographies/Gelfond/`. Acesso em: 17 set. 2025.

THEODOR SCHNEIDE	
 *Fonte: MacTutor (2025)*	**Dados Básicos:** • Nascimento: 7 de maio de 1911 em Frankfurt am Main, Alemanha • Falecimento: 31 de outubro de 1988 em Zähringen, Freiburg, Alemanha **Formação:** • Universidade de Frankfurt (1929) • Orientador: Carl Ludwig Siegel **Contribuições Principais:** • Teorema de Gelfond-Schneider • Teoria dos números transcendentais • Funções abelianas e elípticas • Equações diofantinas **Reconhecimentos:** • Professor na Universidade de Freiburg • Membro da Academia de Ciências de Heidelberg • Influência fundamental na teoria dos números

Tabela A.2: Dados biográficos essenciais de Theodor Schneider

Biografia Detalhada de Theodor Schneider

Theodor Schneider foi um matemático alemão nascido em Frankfurt am Main. Estudou matemática na Universidade de Frankfurt, onde foi profundamente influenciado por Carl Ludwig Siegel, tornando-se seu orientando de doutorado.

Em 1934, Schneider completou seu doutorado com a tese "Transcendenzuntersuchungen periodischer Funktionen"(Investigações de Transcendência de Funções Periódicas), que já demonstrava seu talento excepcional para a teoria dos números transcendentais.

Em 1935, de forma independente e simultânea ao matemático russo Alexander Gelfond, Schneider provou o que ficou conhecido como o Teorema de Gelfond-Schneider. Este teorema estabelece que se a é um número algébrico diferente de 0 e 1, e b é um número irracional algébrico, então a^b é transcendente. Este resultado resolveu completamente o sétimo problema de Hilbert, um dos 23 problemas propostos por David Hilbert em 1900.

Schneider continuou sua carreira acadêmica na Universidade de Frankfurt antes de se tornar professor na Universidade de Freiburg, onde lecionou por muitos anos. Suas pesquisas se estenderam além da teoria dos números transcendentais, incluindo significantes contribuições para a teoria das funções abelianas, funções modulares e equações diofantinas.

Durante sua carreira, Schneider orientou vários estudantes que também se tornaram importantes matemáticos, perpetuando sua influência na área. Sua abordagem rigorosa e métodos analíticos profundos caracterizaram seu estilo matemático.

Theodor Schneider faleceu em Freiburg em 1988, deixando um legado duradouro na teoria dos números e análise matemática. Seu trabalho continua sendo fundamental para o estudo de números transcendentais e suas aplicações.

Fonte: O'CONNOR, J. J.; ROBERTSON, E. F. **Theodor Schneider**. MacTutor History of Mathematics Archive. Disponível em: `https://mathshistory.st-andrews.ac.uk/Biographies/Schneider/`. Acesso em: 17 set. 2025.

Apêndice B

Problemas de Hilbert

1. **Hipótese do Contínuo**
   Não existe nenhum conjunto cuja cardinalidade esteja estritamente entre a dos números inteiros e a dos números reais.

2. **Provar a consistência dos axiomas da aritmética**
   Demonstrar que os axiomas da aritmética são consistentes.

3. **Problema da decomposição de poliedros**
   Dados dois poliedros de igual volume, é sempre possível cortar o primeiro em um número finito de poliedros que podem ser remontados para formar o segundo?

4. **Problema da geometria: retas como distância mais curta**
   Construir todas as geometrias métricas em que as retas são as geodésicas.

5. **Grupos de Lie sem suposição de diferenciabilidade**
   São os grupos de Lie automaticamente grupos analíticos?

6. **Axiomatização da física**
   Axiomatizar as partes da física em que a matemática é predominante.

7. **Irracionalidade e transcendência de certos números**
   Se a é algébrico e diferente de 0 e 1, e b é algébrico irracional, então a^b é transcendente? (Resolvido pelo Teorema de Gelfond-Schneider)

8. **Problemas sobre números primos**
   Inclui a Hipótese de Riemann e a Conjectura de Goldbach.

9. **Lei da reciprocidade geral em corpos numéricos**
   Encontrar a lei mais geral de reciprocidade em qualquer corpo numérico.

10. **Problema da decidibilidade de equações diofantinas**
    Encontrar um algoritmo que determine se uma equação diofantina tem solução. (Resolvido negativamente por Matiyasevich)

11. **Formas quadráticas com coeficientes algébricos**
    Classificação de formas quadráticas com coeficientes numéricos algébricos.

12. **Extensão do teorema de Kronecker-Weber**
    Estender o teorema de Kronecker-Weber a corpos numéricos arbitrários.

13. **Impossibilidade de resolver equações de 7º grau com funções de apenas dois argumentos**
    Provar a impossibilidade de resolver a equação geral de 7º grau com funções de apenas dois argumentos.

14. **Provar a finitude de certos sistemas de funções**
    Provar que certos sistemas completos de funções são finitos.

15. **Fundamentos rigorosos do cálculo enumerativo de Schubert**
    Estabelecer bases rigorosas para o cálculo enumerativo de Schubert.

16. **Topologia de curvas e superfícies algébricas**
    Problemas sobre a topologia de curvas e superfícies algébricas reais.

17. **Expressão de formas definidas como somas de quadrados**
    Uma função racional definida positiva pode sempre ser representada como uma soma de quadrados de funções racionais?

18. **Existência de poliedros não regulares que preenchem o espaço**
    Existem poliedros anisoédricos? Construir um espaço preenchido por poliedros congruentes que não sejam regulares.

19. **Analiticidade das soluções de equações diferenciais**
    São as soluções das equações variacionais sempre analíticas?

20. **Problema geral de valores de contorno**
    O problema de valores de contorno para equações diferenciais elípticas tem soluções?

21. **Prova da existência de equações diferenciais lineares com grupo de monodromia prescrito**
    Provar que sempre existe uma equação diferencial linear de Fuchs com singularidades e grupo de monodromia prescritos.

22. **Uniformização por funções automórficas**
    Uniformização de relações analíticas por meio de funções automórficas.

23. **Extensão dos métodos do cálculo das variações**
    Desenvolver os métodos do cálculo das variações.

Alguns problemas foram completamente resolvidos, outros parcialmente resolvidos, e alguns permanecem em aberto. O impacto destes problemas na matemática do século XX foi profundo, inspirando gerações de matemáticos.

- **Resolvidos**: 1 (parcialmente), 2 (parcialmente), 3, 5, 7, 9, 10, 11, 13, 14, 15, 17, 18, 19, 21, 22
- **Parcialmente resolvidos**: 4, 6, 8, 12, 16, 23
- **Não resolvidos**: 20 (considerado muito vago)