Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós–Graduação em Matemática
Mestrado em Matemática

Do Teorema de Liouville ao Sétimo Problema de Hilbert e Algumas Consequências

Josenildo da Silva

João Pessoa – PB
Janeiro de 2021

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós–Graduação em Matemática
Mestrado em Matemática

Do Teorema de Liouville ao Sétimo Problema de Hilbert e Algumas Consequências

por

Josenildo da Silva

sob a orientação do

Prof. Dr. Alexandre de Bustamante Simas

João Pessoa – PB
Janeiro de 2021

Catalogação na publicação
Seção de Catalogação e Classificação

S586t Silva, Josenildo da.
Do teorema de Liouville ao sétimo problema de Hilbert e algumas consequências / Josenildo da Silva. - João Pessoa, 2021.
161f.

Orientação: Alexandre de Bustamante Simas.
Dissertação (Mestrado) - UFPB/CCEN.

1. Números algébricos e transcendentes. 2. Número de Liouville. 3. Uma generalização do teorema de Lindemann. 4. Solução do sétimo problema de Hilbert. 5. Teorema de Baker. I. Simas, Alexandre de Bustamante. II. Título.

UFPB/BC CDU 512 (043)

Elaborado por MARILIA RIANNY PEREIRA COSMOS - CRB - 15/862

Do Teorema de Liouville ao Sétimo Problema de Hilbert e Algumas Consequências

por

Josenildo da Silva [1]

Dissertação apresentada ao Corpo Docente do Programa de Pós–Graduação em Matemática da Universidade Federal da Paraíba como requisito parcial para a obtenção do título de Mestre em Matemática.

Área de Concentração: Teoria Algébrica e Analítica dos Números

Aprovada em 14 de Dezembro de 2020.

Banca Examinadora:

Prof. Dr. Alexandre de Bustamante Simas – UFPB
(Orientador)

Prof. Dr. Flank David Morais Bezerra – UFPB
(Examinador Interno)

Prof. Dr. Henrique de Barros Correia Vitório – UFPE
(Examinador Externo)

[1] O autor foi bolsista da CAPES durante a elaboração desta dissertação.

"Dedico este trabalho ao meu eterno Pai, José (in memorian) que já se foi, mas continua sendo minha maior força e inspiração na vida, com todo o meu amor e gratidão".

Agradecimentos

Primeiramente, à Deus, razão da minha existência, por me conceder força e sabedoria e permitir que tudo isso fosse possível.

A meu carinhoso filho, Jheyson Yan do Nascimento Silva, pelo apoio e compreensão mesmo diante da minha ausência, nos momentos dedicados aos estudos.

Ao meu maravilhoso e eterno Pai, José Jezuíno da Silva Irmão (in memorian), a quem dedico este trabalho, pois ele sempre esteve presente e me incentivando a não desistir nos momentos de dificuldade que encontrei pela frente, sempre me apoiando e torcendo pelo meu sucesso, compartilhando minhas dores, tristezas e alegrias; fazendo a vida valer à pena.

A todos os Professores da UFPB, em especial ao Prof. Dr. Alexandre de Bustamante Simas, pela brilhante orientação e tempo dedicado às leituras minuciosas e excelentes sugestões que deixaram o texto mais claro e correto.

Aos membros da banca examinadora: Prof. Dr. Flank David Morais Bezerra, Prof. Dr. Henrique de Barros Correia Vitório, que se dispusera a avaliar esta dissertação e contribuir com suas brilhantes ideias.

Aos meus colegas e amigos, em especial ao Jhon, pelos momentos compartilhados, trocas de experiências e conhecimentos que me fizeram evoluir.

Por fim, a CAPES por fornecer apoio financeiro durante todo o período do mestrado e realização da dissertação.

A eles todo o meu carinho, muito obrigado!

Resumo

Neste trabalho, estudamos o desenvolvimento da teoria dos números algébricos e transcendentes com ênfase em uma solução do *Sétimo Problema de Hilbert*, resultado que reuniu esforços de grandes matemáticos. Para uma melhor compreensão desse processo, apresentamos o resultado obtido por Liouville a partir de um teorema que caracteriza os algébricos, em seguida, construímos um número que não satisfaz tal caracterização, portanto, será transcendente. Provaremos a notável existência de transcendentes via Liouville e por meio de Cantor, mostrando que o infinito dos transcendentes é não enumerável, enquanto, dos algébricos é enumerável, evidenciando que há muito mais números transcendentes do que algébricos. Demonstraremos uma generalização do Teorema de Lindemann estabelecido por Hermite-Lidemann, de consequências mais gerais como a transcendência de certos números e funções: e^{α}, e, π, $\log(\alpha)$, $\sin(\alpha), \cos(\alpha)$ e $\tan(\alpha)$, sendo α algébrico, e ainda, nosso objeto principal de estudo, que é uma solução do *Sétimo Problema de Hilbert* e algumas consequências, problema este que perguntava *se números da forma α^{β}, onde α é um número algébrico diferente de* 0 *e* 1*; e β é um número algébrico e irracional, são todos transcendentes.* Neste sentido, temos uma infinidade de números da forma $2^{\sqrt{2}}$, i^{i}, $\log_{10} 2$, e^{π} e $\frac{\log 3}{\log 2}$ que são transcendentes. Finalmente, como consequência introduziremos um avanço significativo recente de uma formulação mais geral de uma conjectura provada por Baker, o qual diz que, qualquer combinação finita não nula de logaritmos de algébricos com coeficientes algébricos é transcendente, e assim, facilitando a busca por transcendentes e possibilitando o desenvolvimento de outras áreas.

Palavras-chave: Números algébricos e transcendentes; número de Liouville; uma generalização do teorema de Lindemann; solução do sétimo problema de Hilbert; teorema de Baker.

Abstract

In this work, we study the development of the theory of algebraic and transcendent numbers with emphasis on a solution of Hilbert's Seventh Problem, a result that brought together the efforts of great mathematicians. For a better understanding of this process, we present the result obtained by Liouville from a theorem that characterizes algebraics, then we build a number that does not satisfy this characterization, therefore, it will be transcendent. We will prove the remarkable existence of transcendents via Liouville and through Cantor, showing that the infinite of the transcendent is not enumerable, while of the algebraic it is enumerable, showing that there are many more transcendent numbers than algebraic. We will demonstrate a generalization of the Lindemann Theorem established by Hermite-Lidemann, with more general consequences such as the transcendence of certain numbers and functions: e^{α}, e, π, $\log(\alpha)$, $\sin(\alpha), \cos(\alpha)$ and $\tan(\alpha)$, being α algebraic, and yet, our main object of study, which is a solution to Hilbert's Seventh Problem and some consequences. Problem that asked if numbers of the form α^{β}, where α is an algebraic number different from 0 and 1; and β is an algebraic and irrational number, they are all transcendent. In this sense, we have an infinity of numbers in the form $2^{\sqrt{2}}$, i^{i}, $\log_{10} 2$, e^{π} and $\frac{\log 3}{\log 2}$ that are transcendent. Finally, as a consequence, we will introduce a recent significant advance of a more general formulation of a conjecture proved by Baker, which says that any finite non-zero combination of algebraic logarithms with algebraic coefficients is transcendent, and thus, facilitating the search for transcendents and enabling the development of other areas.

Keywords: Algebraic and transcendent numbers; Liouville number; a generalization of Lindemann's theorem, solution of Hilbert's seventh problem; Baker's theorem.

Sumário

Notações

A seguir, listamos algumas notações utilizadas neste trabalho.

- $\mathbb{N}$ denota o conjunto dos números naturais: $\{1, 2, 3, 4, \ldots\}$;
- $\mathbb{Z}$ denota o conjunto dos números inteiros: $\{\ldots, -1, 0, 1, 2, \ldots\}$;
- $\mathbb{Q}$ denota o conjunto dos números racionais: $\{\frac{p}{q};\ \text{com } p, q \in \mathbb{Z}, q \neq 0\}$;
- $\mathbb{R}\backslash\mathbb{Q}$ denota o conjunto dos números irracionais;
- $\mathbb{R}$ denota o conjunto dos números reais;
- $\mathbb{A}$ denota o conjunto dos números algébricos;
- $\mathbb{T}$ denota o conjunto dos números transcendentes;
- $X \times X$ denota o produto cartesiano de X por X: $\{(a, b); \quad a, b \in X\}$;
- min$X$ denota o menor elemento de X;
- ∂P denota o grau do polinômio P;
- $f \circ g$ denota a função composta das funções f e g;
- f' denota a primeira derivada da função f;
- $n!$ denota o fatorial de n: $n \cdot (n-1)(n-2) \cdots 2 \cdot 1$;

As demais notações presentes neste trabalho terão seu significado expresso no decorrer do mesmo.

Introdução

Neste trabalho, motivados por Dijario Figueiredo [5], Marques [10] e pelos incríveis resultados de Gelfond[2] e um problema matemático que ficou conhecido como o *Sétimo Problema de Hilbert*, de enunciado simples, que consistia em estabelecer se certos números eram transcendentes, porém, que exigiu profundos conhecimentos para ser solucionado, o qual veremos ao longo do texto. A teoria dos números algébricos e transcendentes teve início com a busca da resolução de três problemas clássicos geométricos da matemática grega, a saber, a duplicação do cubo, a trissecção do ângulo e a quadratura do círculo, infelizmente, não faremos a prova destes fatos, pois, concentraremonos em resultados mais recentes de consequências interessantes no desenvolvimento da teoria, embora, pouco difundida, é uma área que teve grandes contribuições de matemáticos, como: Euler[3], Liouville[4], Hermite[5], Lindemann[6] e Hilbert[7].

O desenvolvimento da teoria transcendente com o matemático francês Liouville teve início em 1851, quando exibiu o primeiro número transcendente da história conhecido hoje como constante de Liouville, apesar de que já havia alguns problemas sobre irracionalidade. A ideia do Liouville para construir tais números foi desenvolver uma propriedade satisfeita por todos os números algébricos e depois construir um número que não satisfizesse tal propriedade, este número foi chamado de transcendente.

Apesar de o método de Cantor[8] em contraste com o de Liouville, não exibir um número transcendente de forma explícita, ele demonstrou que o infinito dos números transcendentes é não enumerável, enquanto, dos algébricos é enumerável, que evidentemente, justifica completamente este trabalho, visto que vale a pena verificar se um dado número é transcendente, já que em certo sentido, há muito mais números transcendentes do que algébricos.

Provar que algum número particular é transcendente, não é uma tarefa tão simples.

[2]Alexsander Gelfond (1906-1968), nasceu em Petersburgo, na Rússia, foi um matemático soviético.
[3]Leonhard Paul Euler (1707-1783), nasceu em Suiça, na Rússia, foi um matemático e físico
[4]Joseph Liouville (1809-1882), nasceu em Pas-de-Calais, em Paris, exibiu o primeiro transcendente.
[5]Charles Hermite (1822-1901), nasceu em Dieuze, em Paris, foi um matemático francês.
[6]Carl Lindemann (1852-1939), nasceu em Hanôver, Munique, foi um matemático alemão.
[7]David Hilbert (1862-1943), nasceu em Königsberg, capital da Prússia, foi um matemático alemão.
[8]Georg Cantor (1845-1918), nasceu no Império Russo, foi um matemático alemão.

A primeira demonstração de que o número e, base dos logaritmos naturais, é transcendente foi dada por Charles Hermite em 1873 e a demonstração da transcendência de π foi dada por Carl Lindemann em 1882. Veremos em detalhes que a transcendência de e e π são casos especiais de uma generalização de um teorema de Lindemann originado por Hermite-Lindemann..

Vale salientar, o que ilustra a dificuldade de se estabelecer se um particular número é algébrico ou transcendente é o fato desta questão estar em aberto para os números: $e+\pi$, $e\pi$, π^{π}, e^{e} e π^{e}. Para melhor descrever os resultados aqui estudados, especificaremos algumas definições e resultados.

Em 1900, no congresso internacional de matemática em Paris, Hilbert propôs uma lista com 23 problemas que inspirou muitos matemáticos ao longo dos séculos XX e XXI, com profundo significado de certos problemas para o avanço da ciência matemática em geral, em que o Sétimo Problema perguntava *se números da forma α^{β}, onde α é um número algébrico diferente de* 0 *e* 1 *e β é um número algébrico e irracional, são todos transcendentes.* Este resultado, conseguido em 1934 por Gelfond, e em 1935 por Scheneider[9] de forma independente, que ficou conhecido como Teorema de Gelfond-Schneider, foi o ponto culminante de quase quarenta anos de esforços para provar que o chamado *número de Hilbert*, $2^{\sqrt{2}}$ é transcendente, resultado que havia sido considerado extremamente difícil, de modo que Hilbert gostava de mencioná-lo como um problema cuja solução estava ainda no futuro como a *Conjectura de Fermat e a Hipotése de Riemann.* Consequentemente, Gelfond provou que $e^{\pi}=(-1)^{-i}$ é transcendente, os quais veremos detalhadamente.

Como o Teorema de Gelfond-Schneider garante que a potenciação de dois algébricos, gera um transcendente. É razoável pensar que: Será que a potenciação de dois transcendentes sempre gera um transcendente? Não é conhecido um resultado similar para este caso, isto é, em que α^{β} seja transcendente, onde α e β são transcendente, no entanto, sabemos que esta questão tem resposta negativa. Neste sentido, como consequência do Sétimo Problema de Hilbert temos um avanço significativo recente de uma formulação mais geral de uma conjectura que foi provado em 1966 por Baker[10], a saber: *sejam $\alpha_1,\ldots,\alpha_n$ algébricos não nulos tais que $\log\alpha_1,\ldots,\log\alpha_n$ são linearmente independente sobre $\mathbb{Q}$. Então $1,\log\alpha_1,\ldots,\log\alpha_n$ são linearmente independente sobre $\mathbb{A}$ o corpo dos algébricos. Além disso, se $\beta_1,\ldots,\beta_n\in\mathbb{A}$ são algébricos tais que $\beta_1\log\alpha_1+\cdots+\beta_n\log\alpha_n\neq 0$. Então $\beta_1\log\alpha_1+\cdots+\beta_n\log\alpha_n$ é transcendente.* (resultado que rendeu a medalha Fields[11] ao Baker em 1970). O que possibilitou diferentes

[9] Theodor Schneider (1911-1988), nasceu em Freiburg, em Breisgau, foi um matemático alemão.

[10] Alan Baker (1939-2018), nasceu em Londres, em Cambridge, foi um matemático inglês.

[11] A medalha Fields é um prêmio quadrianual concedido a no máximo quatro matemáticos, sendo a maior distinção no ramo da matemática

ramos de estudos na matemática como o desenvolvimento de uma área conhecida como as Formas Lineares e Logartimas de Baker, bem como, soluções de equações Diofantinas.

Estudaremos resultados relacionados aos números algébricos e transcendentes. Além disso, apresentaremos em detalhes os resultados de Liouville, bem como, a transcendência do número e, base do logaritmo neperiano, uma generalização do Teorema de Lindemann estabelecido por Hermite-Lidemann, de consequências mais gerais como a transcendência de certos números e funções: e^{α}, e, π, $\log(\alpha)$, $\sin(\alpha), \cos(\alpha)$ e $\tan(\alpha)$, sendo α algébrico, e ainda, nosso objetivo principal que é uma solução do famoso Sétimo Problema de Hilbert dado pelo Teorema de Gelfond-Schneider, e ainda, algumas consequências interessantes como a transcendência de: $2^{\sqrt{2}}$, i^i, $\log_{10} 2$, e^{π} e $\frac{\log 3}{\log 2}$ e a conjectura provada por Baker.

Para melhor compreensão deste trabalho, a seguir resumimos os capítulos que o compõem.

No *Capítulo* 1, abordamos denifições sobre números algébricos e transcendentes e provamos a enumerabilidade e a não enumerabilidade dos conjuntos Algébricos e Transcendentes, respectivamente.

O *Capítulo* 2, é dedicado a demonstração do Teorema de Liouville e do Número de Liouville. Em seguida, da transcendência da Constante de Liouville, e ainda, faremos uma aplicação da existência dos números transcendentes na prova de um simples resultado que caracteriza o espaço vetorial $\mathbb{R}$ como espaço de dimensão infinita sobre $\mathbb{Q}$.

No *Capítulo* 3, apresentaremos a demonstração em detalhes da transcendência do número e, resultado que foi um desafio aos matemáticos até o século XIX.

Já o *Capítulo* 4, é dedicado à caracterização dos números algébricos via extensões de corpos, alguns resultados preliminares como teorema das funções simétricas, conceitos de conjugado, norma de um algébrico, base integral e discriminante.

No *Capítulo* 5, estudamos alguns resultados preliminares e estabelecemos uma demonstração em detalhes do teorema de Hermite-Lidemann e algumas consequências relacionadas à transcendência de certos números e funções trigonométricas.

O *Capítulo* 6, é destinado aos importantes lemas auxiliares de C. Siegel para sistemas lineares e alguns conceitos analíticos e complexos os quais são de fundamental importância para o nosso objetivo principal que é demonstrar uma solução do Sétimo Problema de Hilbert e como consequência principal o Teorema de Baker 6.5, o qual diz que, qualquer combinação finita não nula de logaritmos de algébricos com coeficientes algébricos é um transcendente.

Por fim, no *Capítulo* 7, apresentamos as considerações finais.

Capítulo 1

Sobre Números Algébricos e Transcendentes

No decorrer deste capítulo, veremos que os números reais podem ser classificados em números algébricos e transcendentes. Mas, nosso objetivo para este capítulo, mais precisamente na Seção 1.2, é demonstrar a existência dos números transcendentes por meio das descobertas de G. Cantor usando a ideia de enumerabilidade. As principais referências utilizadas na elaboração deste capítulo são, Domingues [2] e Figueiredo [5].

1.1 Números Algébricos

Nesta seção, apresentaremos os números algébricos e demonstraremos algumas de suas importantes propriedades, mas antes, caracterizaremos os inteiros algébricos reais.

Definição 1.1. *Qualquer solução real ou complexa de uma equação polinomial não nula da forma*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0 \tag{1.1}$$

em que os coeficientes $a_i \in \mathbb{Z}$, com coeficiente líder $a_n = 1$, para todo $i = 0, 1, \ldots, n \in \mathbb{N}$ é chamada um **inteiro algébrico**.

Posteriormente, veremos algumas propriedades dos inteiros algébrico.

Exemplo 1.1. *Todo número inteiro c é um inteiro algébrico.*

De fato, escrevendo

$$x = c \Longrightarrow x - c = 0. \tag{1.2}$$

Logo, o inteiro c é solução da equação do tipo (1.1), com $n = 1$, $a_0 = -c$ e $a_1 = 1$.

Exemplo 1.2. *O número* $\sqrt{7}$ *é um inteiro algébrico, pois é uma solução da equação*

$$x^2 - 7 = 0. \tag{1.3}$$

De fato, se $x = \sqrt{7}$ implica que $x^2 = (\sqrt{7})^2$, assim, temos que $x^2 = 7$ e segue que $x^2 - 7 = 0$, com $n = 2$, $a_0 = -7$, $a_1 = 0$ e $a_2 = 1$.

Exemplo 1.3. *O número* $\sqrt{2+\sqrt{3}}$ *é um inteiro algébrico, pois é uma solução da equação*

$$x^4 - 4x^2 + 1 = 0. \tag{1.4}$$

De fato, escrevemos $x = \sqrt{2+\sqrt{3}}$ e aplicamos duas quadraturas consecutivas para eliminar os radicais. Vejamos:

$$x = \sqrt{2+\sqrt{3}} \Longrightarrow x^2 = \left(\sqrt{2+\sqrt{3}}\right)^2$$

daí,

$$x^2 = 2 + \sqrt{3} \Longrightarrow x^2 - 2 = \sqrt{3}$$

por conseguinte

$$(x^2 - 2)^2 = (\sqrt{3})^2 \Longrightarrow x^4 - 4x^2 + 4 = 3$$

finalmente

$$x^4 - 4x^2 + 1 = 0$$

com $n = 4$, $a_0 = 1$, $a_1 = 0$, $a_2 = -4$, $a_3 = 0$ e $a_4 = 1$.

Exemplo 1.4. *O número complexo* $i = \sqrt{-1}$ *é um inteiro algébrico, pois é solução da equação*

$$x^2 + 1 = 0 \tag{1.5}$$

De fato,

$$x = \sqrt{-1} \Longrightarrow x^2 = (\sqrt{-1})^2 \Longrightarrow x^2 = -1 \Longrightarrow x^2 + 1 = 0$$

com $n = 2$, $a_0 = 1$, $a_1 = 0$ e $a_2 = 1$.

Exemplo 1.5. *Para todo* b *um número inteiro não nulo, a raiz* m*-ésima de* b*, ou seja,* $\sqrt[m]{b}$ *é um inteiro algébrico.*

De fato,

$$x = \sqrt[m]{b} \Longrightarrow x^m = (\sqrt[m]{b})^m \Longrightarrow x^m = b \Longrightarrow x^m - b = 0$$

esta última equação do tipo (1.1), com $n = m$, $a_0 = -b$ e $a_n = 1$.

Observação 1.1. Podemos concluir dos exemplos acima, que todos os números inteiros são inteiros algébricos, bem como, existem inteiros algébricos irracionais e complexos.

Chamamos atenção para o Teorema 1.1 abaixo, o qual caracteriza os inteiros algébricos reais. Mas antes, daremos uma demonstração da irracionalidade de $\sqrt{2}$.

Lema 1.1. *O número $\sqrt{2}$ é irracional.*

Demonstração. Suponhamos, por contradição, que $\sqrt{2}$ seja um número racional, isto é,

$$\sqrt{2} = \frac{a}{b} \tag{1.6}$$

com a e b inteiros positivos. Suponhamos ainda, sem perda de generalidade que $\frac{a}{b}$ seja uma fração irredutível, ou seja, a e b são primos entre si. Elevando ao quadrado a equação (2.6) e simplificando, obtemos

$$2 = \frac{a^2}{b^2} \Longrightarrow a^2 = 2b^2 \tag{1.7}$$

o termo $2b^2$ representa um inteiro par, de modo que a^2 é um inteiro par, segue que a também é um inteiro par (pois, se a fosse ímpar, então $a = 2k + 1$, com $k \in \mathbb{Z}$ o que implicaria $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, ou seja, a^2 seria ímpar). Assim, se a par, então $a = 2c$, com $c \in \mathbb{Z}$. Substituindo a por $2c$ na equação (2.7), obtemos

$$(2c)^2 = 2b^2 \Longrightarrow 4c^2 = 2b^2 \Longrightarrow 2c^2 = b^2$$

Como b^2 é um inteiro par, pelo mesmo argumento apresentado acima, b também é um inteiro par. Segue que a e b são ambos pares. Se a e b são pares, eles não podem ser primos entre si. Esta contradição nos leva à conclusão de que não é possivel escrever $\sqrt{2}$ na forma $\frac{a}{b}$ com a e b inteiros. Portanto, o número $\sqrt{2}$ é irracional. □

1.1.1 Uma Caracterização de Inteiros Algébricos

Teorema 1.1. *Todo número* **inteiro algébrico** *é um número inteiro ou irracional.*

Demonstração. Suponhamos por absurdo que um inteiro algébrico α seja um número racional não inteiro, isto é, $\alpha = \frac{p}{q}$, com $p, q \in \mathbb{Z}$ sendo $q > 1$ e $mdc(p, q) = 1$ de modo que satisfaça a seguinte equação

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

onde $a_i \in \mathbb{Z}$, com $i = 0, \ldots, n \in \mathbb{N}$, $a_n = 1$. Substituindo x por $\frac{p}{q}$, temos

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

daí, obtemos

$$\frac{p^n}{q^n} = -a_{n-1}\frac{p^{n-1}}{q^{n-1}} - \cdots - a_1\frac{p}{q} - a_0 \Longrightarrow p^n = q^n\left(-a_{n-1}\frac{p^{n-1}}{q^{n-1}} - \cdots - a_1\frac{p}{q} - a_0\right)$$

por conseguinte

$$p^n = \left(-a_{n-1}p^{n-1}q - \cdots - a_1pq^{n-1} - a_0q^n\right)$$

finalmente

$$p^n = q\left(-a_{n-1}p^{n-1} - \cdots - a_1pq^{n-2} - a_0q^{n-1}\right)$$

Considerando $t = (-a_{n-1}p^{n-1} - \cdots - a_1pq^{n-2} - a_0q^{n-1})$ temos que $t \in \mathbb{Z}$. Assim sendo, $p^n = qt$, ou seja, $q|p^n$. Usando o fato de que existe um d fator primo de q, com $d \neq 1$ (note que, se q for um número primo então consideramos $d = q$), segue que $d|p^n$ e sendo d primo isto implica $d|p$. Assim, obtemos que $d|q$ e $d|p$, mas isso é um absurdo, contrariando o fato de p, q serem primos entre si.

Caso q seja um número composto, então ele possui pelo menos um divisor primo, digamos d, e pelo mesmo argumento acima, chegamos ao mesmo absurdo. O absurdo ocorre quando admitimos que um racional não inteiro $\alpha = \frac{p}{q}$ é solução da equação do tipo (1.1). Portanto, um inteiro algébrico α será inteiro ou irracional. □

Exemplo 1.6. *O número $\sqrt{7}$ é irracional.*

Demonstração. De fato, usando o Exemplo 1.2, temos que $\sqrt{7}$ é solução de $x^2 - 7 = 0$. De acordo com nossa notação, $n = 2$, $a_0 = -7$, $a_1 = 0$ e $a_2 = 1$. Então pelo Teorema 2.1, esta solução será um número inteiro ou irracional. Podemos mostrar que $\sqrt{7}$ não é um inteiro. De fato, vejamos que

$$4 < 7 < 9 \Longrightarrow \sqrt{4} < \sqrt{7} < \sqrt{9} \Longrightarrow 2 < \sqrt{7} < 3$$

temos que $\sqrt{7}$ não é um inteiro. **Afirmação:** *Não existe um inteiro entre dois consecutivos,isto é, seja $m \in \mathbb{Z}$, não existe $n \in \mathbb{Z}$ tal que $m < n < m + 1$.*

Com efeito, como $m < n < m + 1$ se, e somente se $0 < n - m < 1$. Basta mostrar que não existe um número natural entre 0 e 1 (note que $n - m$ é um inteiro positivo). Suponhamos por contradição, que existe um $n \in \mathbb{Z}$ com esta propriedade.

Considerando o conjunto

$$S = \{n \in \mathbb{Z}; 0 < n < 1\}$$

não vazio. Portanto, usando o fato que todo subconjunto dos naturais possui elemento mínimo, existe $n_0 \in S$ mínimo.
Assim, temos $0 < n_0 < 1$ e multiplicando esta desigualdade por n_0, obtemos

$$0 < n_0^2 < n_0 < 1 \Longrightarrow 0 < n_0^2 < 1$$

Logo, $n_0^2 \in S$ contrariando o fato de assumirmos que n_0 é o menor elemento de S. Portanto, o conjunto S é vazio, e não existe um número inteiro entre dois inteiros consecutivos ou entre 0 e 1. Portanto, o número $\sqrt{7}$ é irracional. □

Finalmente definiremos um número algébrico.

Definição 1.2 (Número Algébrico)**.** *Qualquer solução real ou complexa de uma equação polinomial não nula da forma*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{1.8}$$

em que cada $a_i \in \mathbb{Q}$, para todo $i = 0, \ldots, n \in \mathbb{N}$ é chamada um número algébrico, isto é, um número α é algébrico quando é possível obter uma equação polinomial com coeficientes racionais, da qual α seja raiz. Por outro lado, veremos na seção seguinte que um número que não é algébrico é dito um número transcendente.

Faremos duas observações a respeito da definição acima, a saber: Os coeficientes da equação polinomial podem ser números inteiros. A outra observação é que, sempre que considerarmos um polinômio para o qual α seja raiz, suponhamos este polinômio de menor grau possível para qual isto ocorre. Posteriormente, veremos esta ideia em detalhes por meio do polinômio minimal de um algébrico.

Exemplo 1.7. *Todo número racional $\alpha = \frac{p}{q}$, com $p, q \in \mathbb{Z}$ e $q \neq 0$ é um número algébrico.*

De fato, escrevendo

$$x = \frac{p}{q} \Longrightarrow x - \frac{p}{q} = 0 \Longrightarrow xq - p = 0.$$

Logo, $\alpha = \frac{p}{q}$ é raiz da equação acima, com $n = 1$, $a_0 = -p$ e $a_1 = q$.

Observação 1.2. Uma vez que todo número racional é algébrico, segue que todo número não algébrico (transcendente) é irracional.

Exemplo 1.8. *Todo inteiro algébrico é um número algébrico.*

De fato, seja α um inteiro algébrico. Então por definição, temos que α é solução de uma equação

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

segue que α é raiz de um polinômio não nulo com coeficientes inteiros, sendo $a_n = 1$. Portanto, α é um número algébrico.

Listaremos no teorema a seguir algumas importantes propriedades de fechamento dos números algébricos que o torna um corpo.

1.1.2 Os Algébricos Formam um Corpo

Veremos a seguir propriedades que caracterizam o conjunto dos números algébricos como um corpo.

Teorema 1.2. *Sejam α, $\beta \in \mathbb{A}$ números algébricos reais. Então valem as seguintes propriedades:*

(i) A soma (ou diferença) $\alpha + \beta$ de dois números algébrico é um número algébrico.

(ii) O produto $\alpha.\beta$ de dois números algébrico é um número algébrico.

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

(iv) O inverso $\alpha^{-1} = \frac{1}{\alpha}$ de um número algébrico $\alpha \neq 0$ é um número algébrico.

Demonstração. **Propriedade (i).** Para demonstrar **(i)** e **(ii)** necessitamos de um fato conhecido em Álgebra Linear. Vejamos o seguinte Lema:

Lema 1.2. *Se L é um espaço vetorial de dimensão n sobre $\mathbb{Q}$. Então qualquer subconjunto de L com mais de n vetores é linearmente dependente (L.D.)*

Demonstração. Seja $B = \{v_1, v_2, \ldots, v_n\}$ uma base de L e $B' = \{w_1, w_2, \ldots, w_m\} \subset L$ um subconjunto de L com m vetores tal que $m > n$. Pretende-se mostrar que B' é (L.D.), para tanto, basta-nos mostrar que existem $r_1, r_2, \ldots, r_m \in \mathbb{Q}$ não todos nulos tais que

$$r_1w_1 + r_2w_2 + \ldots + r_mw_m = 0$$

Como B é uma base de L. Então todo vetor de L é combinação linear dos vetores de B, em particular, os $w_i \in L$, e assim, existem $q_{ij} \in \mathbb{Q}$, $i = 1, \ldots, m$ e $j = 1, \ldots, n \in \mathbb{N}$ tais que

$$\begin{aligned}
w_1 &= q_{11}v_1 + q_{22}v_2 + \ldots + q_{1n}v_n \\
w_2 &= q_{21}v_1 + q_{22}v_2 + \ldots + q_{2n}v_n \\
\vdots \quad &\quad \vdots \quad \vdots \quad \vdots \\
w_m &= q_{m1}v_1 + q_{m2}v_2 + \ldots + q_{mn}v_n
\end{aligned}$$

Substituindo seus valores na relação $(r_1(w_1) + r_2(w_2) + \ldots + r_m(w_m) = 0)$, tem-se

$$r_1\left(q_{11}v_1 + q_{12}v_2 + \ldots + q_{1n}v_n\right) + r_2\left(q_{21}v_1 + q_{22}v_2 + \ldots + q_{2n}v_n\right) + \ldots + r_m\left(q_{m1}v_1 + q_{m2}v_2 + \ldots + q_{mn}v_n\right) = 0$$

Ordenando os elementos de forma adequada, tem-se

$$\left(q_{11}r_1 + q_{21}r_2 + \ldots + q_{m1}r_m\right)v_1 + \left(q_{12}r_1 + q_{22}r_2 + \ldots + q_{m2}r_m\right)v_2 + \ldots + \left(q_{1n}r_1 + q_{2n}r_2 + \ldots + q_{mn}r_m\right)v_n = 0$$

Tendo em vista que $v_1, v_2, \ldots, v_n$ são (L.I.), então os coeficientes dessa combinação são nulos, isto é,

$$\begin{aligned} q_{11}r_1 + q_{21}r_2 + \ldots + q_{m1}r_m &= 0 \\ q_{12}r_1 + q_{22}r_2 + \ldots + q_{m2}r_m &= 0 \\ \vdots \qquad \vdots \qquad\qquad \vdots \qquad &\vdots \\ q_{1n}r_1 + q_{2n}r_2 + \ldots + q_{mn}r_m &= 0 \end{aligned}$$

Esse sistema linear homogêneo possui m variáveis $r_1, r_2, \ldots, r_m$ e n equações. Como $m > n$, existe solução não trivial, isto é, existe um racional $r_i \neq 0$, para algum $i = 1, 2, \ldots, m \in \mathbb{N}$. Portanto, o conjunto $B' = \{w_1, w_2, \ldots, w_m\}$ é (L.D.). □

Vamos agora a demonstração da Propriedade (i):
Sejam α e β números algébricos. Então existem equações polinomiais de menor grau para o quais α e β são raízes, respectivamente:

$$\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \ldots + a_2\alpha^2 + a_1\alpha + a_0 = 0 \tag{1.9}$$

$$\beta^m + b_{m-1}\beta^{m-1} + b_{m-2}\beta^{m-2} + \ldots + b_2\beta^2 + b_1\beta + b_0 = 0 \tag{1.10}$$

com coeficientes racionais (obtidos dividindo-se as equações pelo coeficiente líder). Isolando α^n e β^m, temos

$$\alpha^n = -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \ldots - a_2\alpha^2 - a_1\alpha - a_0 \tag{1.11}$$

$$\beta^m = -b_{m-1}\beta^{m-1} - b_{m-2}\beta^{m-2} - \ldots - b_2\beta^2 - b_1\beta - b_0 \tag{1.12}$$

Note que, o α^n é combinação linear de $1, \alpha, \ldots, \alpha^{n-1}$ com coeficientes racionais. Multiplicando (1.11) por α e substituindo-se o α^n obtido em tal expressão pelo seu valor dado em (1.11), obtemos α^{n+1} expresso ainda como combinação linear de $1, \alpha, \ldots, \alpha^{n-1}$ com coeficientes racionais, isto é,

$$\begin{aligned} \alpha^{n+1} &= -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - a_{n-3}\alpha^{n-2} - \ldots - a_2\alpha^3 - a_1\alpha^2 - a_0\alpha \\ &= -a_{n-1}\left(-a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - \ldots - a_2\alpha^2 - a_1\alpha - a_0\right) - a_{n-2}\alpha^{n-1} - \ldots - a_2\alpha^3 - a_1\alpha^2 - a_0\alpha \\ &= (a_{n-1})^2(-a_{n-2})\alpha^{n-1} - (a_{n-1}a_{n-2}a_{n-3})\alpha^{n-2} - \ldots - (a_{n-1}a_2a_1)\alpha^2 - (a_{n-1}a_1a_0)\alpha + (a_{n-1}a_0) \end{aligned}$$

E assim sucessivamente, todas as potências α^j, para $j = n, n+1, \ldots$, são expressas

como combinações lineares de $1, \alpha, \ldots, \alpha^{n-1}$, com coeficientes racionais.

Como β^m é combinação de $1, \beta, \ldots, \beta^{m-1}$. E pelo mesmo argumento acima, podemos expressar as potências β^k, para $k = m, m+1, \ldots$, como combinações lineares de $1, \beta, \ldots, \beta^{m-1}$ com coeficientes racionais.

Nosso objetivo agora será mostrar que $\alpha + \beta$, satisfaz uma equação polinomial de grau mn com coeficientes racionais, implicando que $\alpha + \beta$ é algébrico.
Consideremos os $mn + 1$ números:

$$1, \alpha + \beta, (\alpha + \beta)^2, \ldots, (\alpha + \beta)^{mn} \tag{1.13}$$

Desenvolvendo as várias potências e usando o que vimos acima sobre a representação das potências α^j, para $j \geq n \in \mathbb{N}$ e β^k, para $k \geq m \in \mathbb{N}$ em combinações lineares; obtemos que os números em (1.13) podem ser expressos como combinações lineares dos mn números:

$$\alpha^j \beta^k, \quad 0 \leq j \leq n-1 \in \mathbb{N}, \quad 0 \leq k \leq m-1 \in \mathbb{N}$$

com coeficientes racionais. Pelo Lema 1.2, consideremos os conjuntos de geradores:
$B = \{v_1, v_2, \ldots, v_{mn}\}$ com mn números $\alpha^j \beta^k$, com $0 \leq j \leq n-1$; $0 \leq k \leq m-1$ e
$B' = \{w_1, w_2, \ldots, w_{mn+1}\}$ com $mn+1$ números $1, \alpha + \beta, (\alpha + \beta)^2, \ldots, (\alpha + \beta)^{mn}$.

Logo, existem racionais $r_0, r_1, r_2, \ldots, r_{mn} \in \mathbb{Q}$ não todos nulos tais que

$$r_0 + r_1(\alpha + \beta) + r_2(\alpha + \beta)^2 + \ldots + r_{mn}(\alpha + \beta)^{mn} = 0$$

o que mostra que $\alpha + \beta$ satisfaz uma equação polinomial de grau mn. Portanto, o número $\alpha + \beta$ é algébrico. □

Demonstração. **Propriedade (ii).** Seguindo o mesmo argumento na Propriedade (i). Consideremos $mn + 1$ números:

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

Utilizando o mesmo raciocínio da demonstração em (i) e usando Lema 1.2, consideremos os v_i, s como sendo os mn números $\alpha^j \beta^k$, com $0 \leq j \leq n-1$; $0 \leq k \leq m-1$ e os w_i, s como sendo os $mn+1$ números $1, \alpha\beta, (\alpha\beta)^2, \ldots, (\alpha\beta)^{mn}$. Logo, existem racionais $s_0, s_1, s_2, \ldots, s_{mn} \in \mathbb{Q}$ não todos nulos tais que

$$s_0 + s_1(\alpha\beta) + s_2(\alpha\beta)^2 + \ldots + s_{mn}(\alpha\beta)^{mn} = 0$$

o que mostra que $\alpha\beta$ satisfaz uma equação polinomial de grau mn. Portanto, o número $\alpha\beta$ é algébrico. □

Demonstração. **Propriedade (iii).** Se α é algébrico, então ele é raiz da seguinte equação polinomial:

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

Portanto, $-\alpha$ é raiz do seguinte polinômio

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

Visto que, aplicando $-\alpha$, tem-se

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

□

Demonstração. **Propriedade (iv).** Se $\alpha \neq 0$ satisfaz à equação da forma:

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0 \tag{1.14}$$

Então $\alpha^{-1} = \frac{1}{\alpha}$ satisfaz o polinômio

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

De fato, multiplicando a equação (1.14) por $\frac{1}{\alpha^n}$, tem-se

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

Portanto, a seguinte equação é satisfeita

$$a_n + a_{n-1}\left(\frac{1}{\alpha}\right) + \cdots + a_1\left(\frac{1}{\alpha}\right)^{n-1} + a_0\left(\frac{1}{\alpha}\right)^n = 0$$

□

Observação 1.3. As propriedades (i), (ii), (iii) e (iv) acima nos diz que o conjunto dos números algébricos reais formam um subcorpo do corpo $\mathbb{R}$ dos reais.

Neste momento, estamos interessados em demonstrar a existência de números transcendentes, porém, antes faremos diversas construções sobre enumerabilidade.

1.2 Enumerabilidade e Existência de Números Transcendentes

Nesta seção apresentaremos a existência de números transcendentes dada por Cantor. Para tanto, necessitaremos de alguns conceitos e importantes resultados sobre enumerabilidade de diversos conjuntos, inclusive, veremos que o conjunto dos números algébricos é enumerável, enquanto o dos transcendente é não enumerável.

Definição 1.3 (Número Transcendente)**.** *Todo número real ou complexo que não é raiz de nenhuma equação polinomial não nula da forma*

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

em que cada $a_i \in \mathbb{Q}$, para todo $i = 0, \ldots, n \in \mathbb{N}$ é chamado um número transcendente, ou seja, um número que não é algébrico.

Definição 1.4. *Um conjunto X é enumerável quando é finito ou quando existe uma correspondência biunívoca com os números naturais. Mais precisamente, X é enumerável se existe uma função bijetiva (isto é, uma função injetiva e sobrejetiva)*

$$f : \mathbb{N} \longrightarrow X$$

No segundo caso, dizemos que X é infinito enumerável (enumerável). Definindo

$$f(1) = x_1, f(2) = x_2, \ldots, f(n) = x_n, \ldots,$$

escrevendo X como sendo $X = \{x_1, x_2, \ldots, x_n, \ldots\}$. Cada bijeção $f : \mathbb{N} \longrightarrow X$ chamamos de uma enumeração (dos elementos) de X. Caso contrário, dizemos que X é não enumerável.

Vale ressaltar que um conjunto X é dito finito quando é vazio ou quando existe, para algum $n \in \mathbb{N}$, uma bijeção $f : I_n \longrightarrow X$, sendo $I_n = \{p \in \mathbb{N}, 1 \leq p \leq n\}$. Caso contrário, X é dito infinito.

Exemplo 1.9. *O conjunto dos números pares positivos é infinito enumerável.*

De fato, seja $\mathbb{P} = \{2n, n \in \mathbb{N}\}$ o conjunto dos números pares positivos, considerando a seguinte função

$$\begin{array}{rccc} f & : & \mathbb{N} & \longrightarrow & \mathbb{P} \\ & & n & \longmapsto & 2n \end{array}$$

definida por $f(n) = 2n$, com $n \in \mathbb{N}$.

Mostraremos que f é bijetiva. Primeiramente provaremos que f é injetiva. Suponhamos que $f(x) = f(y) \in \mathbb{P}$, temos que

$$f(x) = f(y) \Longrightarrow 2x = 2y \Longrightarrow x = y$$

Portanto, f é injetiva.

Mostraremos que f é sobrejetiva, ou seja, $f(\mathbb{N}) = \mathbb{P}$. Usando a definição de conjunto imagem de uma função, temos que $f(\mathbb{N}) \subset \mathbb{P}$. Basta mostrar que $\mathbb{P} \subset f(\mathbb{N})$. Seja $b \in \mathbb{P}$, então $b = 2n_0$ para algum $n_0 \in \mathbb{N}$. Tomando $x = n_0$, temos que $f(x) = f(n_0) = 2n_0 = b$ o que implica $b \in f(\mathbb{N})$, segue que $b = f(x)$. Logo, a função f é sobrejetora. Portanto, f é bijetora e o conjunto $\mathbb{P}$ é infinito enumerável.

Exemplo 1.10. *O conjunto dos números ímpares positivos é infinito enumerável.*

Considerando a seguinte função

$$\begin{array}{rccc} f & : & \mathbb{N} & \longrightarrow & \mathbb{I} \\ & & n & \longmapsto & 2n-1 \end{array}$$

definida por $f(n) = 2n - 1$, com $n \in \mathbb{N}$, sendo $\mathbb{I} = \{2n - 1, n \in \mathbb{N}\}$ o conjunto dos números ímpares positivos. A função f é bijetiva. A demonstração é análogo ao Exemplo (1.9) acima.

Exemplo 1.11. *O conjunto $\mathbb{Z}$ dos números inteiros é infinito enumerável.*

Observe a correspondência abaixo:

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

Descrevendo esta correspondência pela função definida por partes, temos

$$\begin{array}{rccc} f & : & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & & n & \longmapsto & f(n) \end{array}$$

sendo

$$f(n) = \begin{cases} 2n, & \text{se} \quad n > 0 \\ -2n + 1, & \text{se} \quad n \leq 0 \end{cases}$$

De fato, sejam $x, y \in \mathbb{Z}$. Mostraremos que f é injetiva, isto é, suponhamos que $x \neq y$ e provaremos que $f(x) \neq f(y)$. Se x e y são positivos, temos $f(x) = 2x \neq 2y = f(y)$,

uma vez que $2x = 2y$, se $x = y$, contrariando nossa hipótese. Mas, se x e y são números negativos, temos $f(x) = -2x+1 \neq -2y+1 = f(y)$ usando o mesmo argumento acima.

Se $x > 0$ e $y < 0$, temos que $f(x) = 2x \neq -2y+1 = f(y)$, já que $f(x)$ é um número par, enquanto $f(y)$ é um número ímpar. Caso contrário, se $x < 0$ e $y > 0$, pela mesma razão $f(x) = -2x + 1 \neq 2y = f(y)$.

Por outro lado, se $x = 0$ e $y > 0$ (ou $y = 0$ e $x > 0$), usando argumento semelhante $f(x) = f(0) = 1 \neq 2y = f(y)$. Por sua vez, caso $x = 0$ e $y < 0$ (ou $y = 0$ e $x < 0$), temos que $f(x) = f(0) = 1 \neq -2y + 1 = f(y)$. Logo, pelos casos considerados acima, f é injetiva.

Mostraremos que f é sobrejetiva, ou seja, $f(\mathbb{Z}) = \mathbb{N}$. Usando a definição de conjunto imagem de uma função, temos que $f(\mathbb{Z}) \subset \mathbb{N}$. Basta mostrar que $\mathbb{N} \subset f(\mathbb{Z})$.

De fato, seja $n \in \mathbb{N}$. Se n é par então $n = 2k$, com $k \in \mathbb{N} \subset \mathbb{Z}$. Tomando $x = k$, temos

$$n = 2k = f(k) = f(x) \in f(\mathbb{Z})$$

Logo, a função f é sobrejetiva.

Analogamente, se n é ímpar então $n = 2k + 1$, com $k \in \mathbb{N} \cup \{0\}$. Tomando $x = -k \in \mathbb{Z}$, ou seja, $-k \leq 0$, temos

$$n = 2k + 1 = -2(-k) + 1 = f(-k) = f(x) \in f(\mathbb{Z})$$

Logo, a função f é sobrejetiva. Portanto f é bijetiva. Como f é bijetiva, existe uma função inversa bijetiva $g^{-1} : \mathbb{N} \longrightarrow \mathbb{Z}$, assim basta tomar $f = g^{-1}$. Assim, concluímos que $\mathbb{Z}$ é infinito enumerável.

Observação 1.4. Para evitar regressões, enunciaremos um importante resultado sem demonstrá-lo. Se $f : A \longrightarrow B$ é uma função bijetora, então existe uma única função inversa $f^{-1} : B \longrightarrow A$ que também é bijetora. Para maiores detalhes, Ver [2], p. 102.

A partir de agora, queremos demonstrar que os números racionais formam um conjunto infinito enumerável e para isto, necessitaremos de alguns resultados.

Proposição 1.1. *Sejam $f : E \longrightarrow F$ e $g : F \longrightarrow G$ funções bijetoras. Então a função composta $g \circ f : E \longrightarrow G$ é também uma bijeção.*

Demonstração. Sejam $x, y \in E$. Suponhamos que

$$(g \circ f)(x) = (g \circ f)(y) \Longrightarrow g(f(x)) = g(f(y))$$

Como g é injetiva, temos que

$$f(x) = f(y)$$

usando o fato de f ser injetiva, concluímos que

$$x = y$$

Logo, a composta $g \circ f$ é injetiva. Provaremos que $g \circ f$ é sobrejetiva. Seja $z \in G$ mostraremos que existe $x \in E$ tal que $(g \circ f)(x) = z$. De fato, como g é sobrejetiva, então existe $y \in F$ tal que

$$g(y) = z \tag{1.15}$$

usando a fato de f ser sobrejetiva, temos que existe $x \in E$ tal que

$$f(x) = y \tag{1.16}$$

Segue-se de (1.15) e (1.16) que

$$(g \circ f)(x) = g(f(x)) = g(y) = z \Longrightarrow (g \circ f)(x) = z$$

Logo, $g \circ f$ é sobrejetiva. Portanto, a composta $g \circ f$ é bijetiva. □

Observação 1.5. É importante notar que, podemos obter a injetividade da composta $g \circ f$, satisfazendo as condições de uma função injetiva e bastando que a imagem do conjunto E pela função f esteja contida no domínio da função g, isto é, $f(E) \subset F$.

Definição 1.5. *Sejam as funções $f : A \longrightarrow B$ e $g : B \longrightarrow A$, dizemos que g é uma inversa à esquerda para f quando*

$$g \circ f = id_A : A \longrightarrow A$$

ou seja, quando $g(f(x)) = x$ para todo $x \in A$.

Definição 1.6. *Sejam as funções $f : A \longrightarrow B$ e $g : B \longrightarrow A$, dizemos que g é uma inversa à direita para f quando*

$$f \circ g = id_B : B \longrightarrow B$$

ou seja, quando $f(g(y)) = y$ para todo $y \in B$.

Enunciaremos alguns importantes lemas a seguir. Porém, por brevidade, não faremos as suas demonstrações. Para maiores detalhes, Ver [8], p. 22.

Lema 1.3. *Uma função $f : A \longrightarrow B$ possui inversa à esquerda se, e somente se, é injetiva.*

Lema 1.4. *Uma função $f : A \longrightarrow B$ possui inversa à direita se, e somente se, é sobrejetiva.*

Lema 1.5. *Todo subconjunto $X \subset \mathbb{N}$ é enumerável.*

Proposição 1.2. *Se $f : X \longrightarrow Y$ é injetiva e Y é infinito enumerável, então X é infinito enumerável.*

Demonstração. Como Y é infinito enumerável, existe uma bijeção $g : Y \longrightarrow \mathbb{N}$. Considerando a função $\varphi = g \circ f : X \longrightarrow \mathbb{N}$. Como f e g são injetivas, usando a Proposição 1.1, temos que φ é injetiva. Logo,

$$\varphi : X \longrightarrow \varphi(X) \subset \mathbb{N} \tag{1.17}$$

é uma bijeção de X sobre um subconjunto $\varphi(X)$ dos naturais. Assim sendo, usando o Lema 1.5, temos que $\varphi(X)$ é infinito enumerável. Por conseguinte, existe uma bijeção

$$h : \mathbb{N} \longrightarrow \varphi(X) \tag{1.18}$$

Além disso, segue de (1.17) que existe uma bijeção $\varphi^{-1} : \varphi(X) \longrightarrow X$. Fazendo a composição de φ^{-1} com h, temos que

$$\varphi^{-1} \circ h : \mathbb{N} \longrightarrow X$$

também é uma bijeção. Portanto, o conjunto X é infinito enumerável. □

Proposição 1.3. *Se $f : X \longrightarrow Y$ é sobrejetiva e X é infinito enumerável, então Y é infinito enumerável.*

Demonstração. Como f é sobrejetiva, usando o Lema 1.4, existe uma função

$$g : Y \longrightarrow X$$

tal que $f \circ g = id_Y : Y \longrightarrow Y$, sendo $f(g(y)) = y$ para todo $y \in Y$. Logo, a função f é uma inversa à esquerda de g, segue que g é injetiva. Usando a Proposição 1.2. Portanto, o conjunto Y é infinito enumerável. □

Proposição 1.4. *O conjunto $\mathbb{N} \times \mathbb{N}$ é infinito enumerável*

Demonstração. Considerando a seguinte função

$$\begin{array}{rccc} f & : & \mathbb{N} \times \mathbb{N} & \longrightarrow & \mathbb{N} \\ & & (m, n) & \longmapsto & 2^m \cdot 3^n \end{array}$$

definida por $f(m,n) = 2^m \cdot 3^n$, com $m, n \in \mathbb{N}$. Sejam $(m,n),(m',n') \in \mathbb{N} \times \mathbb{N}$.

Suponhamos que

$$f(m,n) = f(m',n') \Longrightarrow 2^m \cdot 3^n = 2^{m'} \cdot 3^{n'}$$

usando o famoso Teorema Fundamental da Aritmética, segue-se que

$$m = m' \text{ e } n = n' \Longrightarrow (m,n) = (m',n')$$

ou seja, usando a unicidade da decomposição de um número em fatores primos, temos que f é injetiva, o que nos fornece uma bijeção

$$f : \mathbb{N} \times \mathbb{N} \longrightarrow f(\mathbb{N} \times \mathbb{N}) \subset \mathbb{N}$$

Como $f(\mathbb{N}\times\mathbb{N}) \subset \mathbb{N}$, usando o Lema 1.5, temos que $f(\mathbb{N}\times\mathbb{N})$ é infinito enumerável. Sendo f injetiva e usando a Proposição 1.2, obtemos que $\mathbb{N} \times \mathbb{N}$ é infinito enumerável. □

Proposição 1.5. *Sejam X, Y conjuntos infinitos enumeráveis. Então o produto cartesiano $X \times Y$ é infinito enumerável.*

Demonstração. Como X e Y são conjuntos infinitos enumeráveis. Então existem funções injetivas

$$\varphi : X \longrightarrow \mathbb{N} \quad \text{e} \quad h : Y \longrightarrow \mathbb{N}$$

Considerando a função

$$g : X \times Y \longrightarrow \mathbb{N} \times \mathbb{N}$$

definida por

$$g(x,y) = (\varphi(x), h(y))$$

Logo, a injetividade de g segue da injetividade das funções φ e h. Usando a Proposição 1.4, temos que $\mathbb{N}\times\mathbb{N}$ é infinito enumerável. Juntamente com a Proposição 1.2, concluímos que o produto cartesiano $X \times Y$ é infinito enumerável. □

Observação 1.6. Usando indução finita, podemos mostrar que, se $X_1, X_2, \ldots, X_n$ são conjuntos enumeráveis, seu produto cartesiano finito $X = X_1 \times X_2 \times \cdots \times X_n$ é enumerável. Para maiores detalhes, Ver [8], p. 51.

Proposição 1.6. *Se X é infinito enumerável e $Y \subset X$ é um conjunto infinito. Então Y é infinito enumerável.*

Demonstração. Como X é infinito enumerável, existe uma bijeção

$$f : X \longrightarrow \mathbb{N}$$

que nos fornece a restrição de f ao subconjunto $Y \subset X$, isto é

$$f|Y : Y \longrightarrow f(Y) \subset \mathbb{N}$$

é também uma bijeção de Y sobre um subconjunto $f(Y) \subset \mathbb{N}$ dos naturais. Assim, usando o Lema 1.5, segue-se que $f(Y)$ é infinito enumerável. Por conseguinte, existe uma bijeção

$$g : \mathbb{N} \longrightarrow f(Y)$$

Além disso, existe uma bijeção $(f|Y)^{-1} : f(Y) \longrightarrow Y$. Fazendo a composição de $(f|Y)^{-1}$ com g, tem-se

$$(f|Y)^{-1} \circ g : \mathbb{N} \longrightarrow Y$$

também é uma bijeção. Portanto, o conjunto Y é infinito enumerável. O que significa que todo subconjunto de um conjunto enumerável é enumerável. □

Teorema 1.3. *O conjunto $\mathbb{Q}$ dos números racionais é infinito enumerável.*

Demonstração. Seja $\mathbb{Z}^*$ o conjunto dos números inteiros não nulos, isto é,

$$\mathbb{Z}^* = \mathbb{Z} - \{0\}$$

Temos que $\mathbb{Z}^* \subset \mathbb{Z}$, como já provamos que $\mathbb{Z}$ é infinito enumerável pelo Exemplo 1.11. Usando a Proposição 1.6, concluímos que o conjunto $\mathbb{Z}^*$ é infinito enumerável. Segue -se da Proposição 1.5, que o produto cartesiano

$$\mathbb{Z} \times \mathbb{Z}^*$$

é infinito enumerável. Considerando a função

$$f : \mathbb{Z} \times \mathbb{Z}^* \longrightarrow \mathbb{Q}$$

definida por

$$f(m, n) = \frac{m}{n}$$

com $m \in \mathbb{Z}$ e $n \in \mathbb{Z}^*$ é sobrejetiva (pela própria definição de $\mathbb{Q}$). Assim, segue-se da Proposição 1.3, que o conjunto $\mathbb{Q}$ é infinito enumerável. □

Listaremos os números do conjunto $\mathbb{Q}$ na tabela abaixo:

$$\begin{array}{ccccccccc}
\frac{1}{1} & \rightarrow & \frac{2}{1} & & \frac{3}{1} & \rightarrow & \frac{4}{1} & & \frac{5}{1} \rightarrow \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & \\
\frac{1}{2} & & \frac{2}{2} & & \frac{3}{2} & & \frac{4}{2} & & \frac{5}{2} \quad \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
\frac{1}{3} & & \frac{2}{3} & & \frac{3}{3} & & \frac{4}{3} & & \frac{5}{3} \quad \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & \\
\frac{1}{4} & & \frac{2}{4} & & \frac{3}{4} & & \frac{4}{4} & & \frac{5}{4} \quad \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
\frac{1}{5} & & \frac{2}{5} & & \frac{3}{5} & & \frac{4}{5} & & \frac{5}{5} \quad \cdots \\
 & \swarrow & & & & & & & \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \quad \ddots
\end{array}$$

Note que na primeira linha contém todas as frações positivas de denominador 1, na segunda linha todas as frações de denominador 2. E assim por diante. Claramente, todo número da forma $\frac{p}{q}$ com $p, q \in \mathbb{N}$ e $q \neq 0$ aparecem nesta formação acima.

Considerando uma função f definida por $f(n) = n$-ésimo elemento que encontraremos percorrendo a ordem de sucessão indicada pelas flechas, omitindo os números que já apareceram, obteremos a seguinte sequência infinita

$$1, 2, 1/2, 1/3, 3, 4, 3/2, 2/3, 1/4, 1/5 \ldots$$

dos números racionais positivos, ou seja,

$$\mathbb{Q}^+ = \left\{ \frac{p}{q} \in \mathbb{Q}; \quad \frac{p}{q} > 0 \right\}$$

Tomando o conjunto dos números racionais negativos, ou seja,

$$\mathbb{Q}^- = \left\{ \frac{p}{q} \in \mathbb{Q}; \quad \frac{p}{q} < 0 \right\}$$

Lembrando que,

$$\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$$

Então, escrevendo uma sequência infinita que contém todos os racionais, isto é,

$$\mathbb{Q} = \{0, -1, 1, -2, 2, -1/2, 1/2, -1/3, 1/3, -3, 3, -4, 4, -3/2, 3/2, -2/3, 2/3, \ldots\}$$

também concluímos a demonstração.

Demonstraremos a seguir, importantes propriedades gerais sobre conjuntos enumeráveis.

1.2.1 Propriedades sobre Conjuntos Enumeráveis

Lema 1.6. *A união de um conjunto finito com um conjunto enumerável é enumerável.*

Demonstração. Sejam $A = \{a_1, a_2, \ldots, a_n\}$ um conjunto finito e $B = \{b_1, b_2, \ldots, b_n, \ldots\}$ um conjunto enumerável. O conjunto $A \cup B$ é enumerável. De fato, basta considerar a correspondência biunívoca entre $\mathbb{N}$ e $A \cup B$ abaixo:

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

Suponhamos sem perda de generalidade que A e B são conjuntos disjuntos, isto é, $A \cap B = \varnothing$. Como A é finito, então A é enumerável. Segue que existe uma função bijetiva

$$f : \{1, 2, \ldots, n\} \longrightarrow A$$

para algum $n \in \mathbb{N}$ definida por $f(k) = a_k$ para $1 \leq k \leq n$.

Como B é enumerável. Segue que existe uma função bijetiva

$$g : \mathbb{N} \longrightarrow B$$

definida por $g(j) = b_j$ para todo $j \in \mathbb{N}$.

Considerando uma função

$$h : \mathbb{N} \longrightarrow A \cup B$$

de modo que

$$h(1) = a_1, h(2) = a_2, \ldots, h(n) = a_n, h(n+1) = b_1, h(n+2) = b_2, \ldots, h(n+j) = b_j, \ldots$$

definida por partes

$$h(i) = \begin{cases} a_i, & \text{se} \quad 1 \leq i \leq n \\ b_{i-n}, & \text{se} \quad i \geq n+1 \end{cases}$$

para todo $n \in \mathbb{N}$. Sejam $h(i), h(j) \in A \cup B$ tal que $h(i) = h(j)$. Provaremos que $i = j$. Como $A \cap B = \varnothing$, então ou $h(i)$ e $h(j)$ pertencem ambos a A, ou ambos a B.
No primeiro caso,

$$h(i) = h(j) \Longrightarrow a_i = a_j \Longrightarrow f(i) = f(j)$$

Como f é injetiva. Logo, $i = j$.
No segundo caso,

$$h(i) = h(j) \Longrightarrow b_{i-n} = b_{j-n} \Longrightarrow g(i-n) = g(j-n)$$

Como g é injetiva. Logo, $i - n = j - n$, ou seja, $i = j$. Portanto, a função h é injetiva. Agora, mostraremos que h é sobrejetiva:

Seja $x \in A \cup B$. Provaremos que x pertence ao conjunto imagem de h, ou seja, $x \in h(\mathbb{N})$. Como $A \cap B = \varnothing$, então ou $x \in A$ ou $x \in B$.

Se $x \in A$, como f é sobrejetora, existe um $i \in \{1, 2, \ldots, n\}$ tal que $x = f(i) = a_i$. Mas $a_i = h(i)$. Logo, $x = h(i) \in h(\mathbb{N})$, para algum i.

Se $x \in B$, como g é sobrejetora, $x = g(j) = b_j$ para algum $j \in \mathbb{N}$. Mas $b_j = h(j+n)$. Logo, $x = h(j+n) \in h(\mathbb{N})$, ou seja, x pertence ao conjunto imagem de h. Segue que h é sobrejetiva. Concluímos que h é uma bijeção que enumera a união dos dois conjuntos, concluímos que $A \cup B$ é enumerável. Mas, se $A \cap B \neq \varnothing$. Basta tomar $C = A - B$ um conjunto tal que $A \cup B = C \cup B$. Assim, C e B são disjuntos por construção. Portanto, o conjunto $A \cup B$ é enumerável. □

Lema 1.7. *A união de dois conjuntos enumeráveis é enumerável.*

Demonstração. Sejam $A = \{a_1, a_2, \ldots\}$ e $B = \{b_1, b_2, \ldots\}$ dois conjuntos enumeráveis. Então $A \cup B$ é enumerável, uma vez que, basta considerar a correspondência biunívoca abaixo:

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

Suponhamos sem perda de generalidade que $A \cap B = \varnothing$. Como A é enumerável, então existe uma função bijetiva, em particular, injetiva

$$f_1 : A \longrightarrow \mathbb{N}$$

Usando o Exemplo 1.10, existe uma função injetiva

$$g_1 : \mathbb{N} \longrightarrow \mathbb{I}$$

sendo $\mathbb{I}$ o conjunto dos números ímpares positivos. Logo, existe uma função injetiva

$$\varphi_1 = g_1 \circ f_1 : A \longrightarrow \mathbb{I}$$

definida por $\varphi_1(a_n) = 2n - 1$ para todo $n \in \mathbb{N}$.

Como B também é enumerável, então existe uma função bijetiva, em particular, injetiva

$$f_2 : B \longrightarrow \mathbb{N}$$

Usando o Exemplo 1.9, existe uma função injetiva

$$g_2 : \mathbb{N} \longrightarrow \mathbb{P}$$

sendo $\mathbb{P}$ o conjuntos dos números pares positivos. Logo, existe uma função injetiva

$$\varphi_2 = g_2 \circ f_2 : B \longrightarrow \mathbb{P}$$

definida por $\varphi_2(b_n) = 2n$ para todo $n \in \mathbb{N}$. Considerando a função

$$\varphi : A \cup B \longrightarrow \mathbb{I} \cup \mathbb{P}$$

definida por

$$\varphi(x) = \begin{cases} \varphi_1(x) = 2x - 1, & \text{se} \quad x \in A \\ \varphi_2(x) = 2x, & \text{se} \quad x \in B \end{cases}$$

que também é injetiva, a qual segue da injetividade de φ_1 e φ_2.

Assim sendo, como $\mathbb{I} \cup \mathbb{P} = \mathbb{N}$ é enumerável e usando a Proposição 1.2, temos que $A \cup B$ é enumerável. Caso $A \cap B \neq \varnothing$. Basta tomar $C = A - B$ um conjunto tal que $A \cup B = C \cup B$. Assim, o conjunto $C \cup B$ é enumerável. Portanto, o conjunto $A \cup B$ é enumerável. □

Lema 1.8. *A união de um número finito de conjuntos enumeráveis é enumerável.*

Demonstração. Sejam $A_1, A_2, \ldots, A_n$ conjuntos enumeráveis, mostraremos que

$$\bigcup_{k=1}^{n} A_k = A_1 \cup A_2 \cup \ldots \cup A_n$$

é enumerável, com $k \in \{1, 2, \ldots, n\}$ e $n \in \mathbb{N}$. Usando o princípio da indução finita. Note que para $k = 1$ a propriedade é válida, pois A_1 é enumerável. Para $k = 2$ é válida pelo Lema 1.7. Suponhamos que a propriedade seja válida para todo $k \in \mathbb{N}$, isto é, se $A_1, A_2, \ldots, A_k$ são enumeráveis, então $A_1 \cup A_2 \cup \ldots \cup A_k$ é enumerável. Mostraremos então que a propriedade é válida para $k + 1$, ou seja, se $A_1, A_2, \ldots, A_k, A_{k+1}$ são enumeráveis, então

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

é enumerável. Note que, escrevendo

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

Considerando $A = (A_1 \cup A_2 \cup \ldots \cup A_k)$, temos que

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

Como A é enumerável por hipótese de indução e $A \cup A_{k+1}$ é enumerável usando o Lema 1.7. Logo, $A_1 \cup A_2 \cup \ldots \cup A_k \cup A_{k+1}$ é enumerável. Portanto, o conjunto $\bigcup_{k=1}^{n} A_k = A_1 \cup A_2 \cup \ldots \cup A_n$ é enumerável. □

Lema 1.9. *A união de um conjunto enumerável de conjuntos finitos é enumerável.*

Demonstração. Seja $A = \{A_1, A_2, \ldots, A_n, \ldots\}$ um conjunto enumerável, em que cada A_i é um conjunto finito para todo $i \in \{1, 2, \ldots, n, \ldots\}$. Mostraremos que

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots$$

é enumerável, para todo $n \in \mathbb{N}$. Suponhamos que

$$A_1 = \{a_{11}, a_{12}, \ldots, a_{1w_1}\}, A_2 = \{a_{21}, a_{22}, \ldots, a_{2w_2}\}, \ldots, A_n = \{a_{n1}, a_{n2}, \ldots, a_{nw_n}\}, \ldots$$

com $w_i \in \mathbb{N}$, $i \in \{1, 2, \ldots, n, \ldots\}$. Então,

$$A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots = \{a_{11}, a_{12}, \ldots, a_{1w_1}, a_{21}, a_{22}, \ldots, a_{2w_2}, \ldots, a_{n1}, a_{n2}, \ldots, a_{nw_n}, \ldots\}$$

De fato, basta considerar a correspondência biunívoca entre $A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots$ e $\mathbb{N}$ definida por

$$\begin{array}{ccccccccccccc}
a_{11}, & \ldots, & a_{1w_1}, & a_{21}, & \ldots, & a_{2w_2}, & \ldots, & a_{n1}, & \ldots, & a_{nw_n}, & \ldots \\
\updownarrow & & \updownarrow & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & \\
1, & \ldots, & w_1, & w_1+1, & \ldots, & w_1+w_2, & \ldots, & 1+\sum_{i=1}^{n-1} w_i, & \ldots, & \sum_{i=1}^{n} w_i, & \ldots
\end{array}$$

Portanto, o conjunto $\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots$ é enumerável. □

Vejamos a seguir a generalização do Lema 1.9.

Lema 1.10. *A união de um conjunto enumerável de conjuntos enumeráveis é enumerável.*

Demonstração. Seja $A = \{A_1, A_2, \ldots, A_n, \ldots\}$ um conjunto enumerável, em que cada A_n é um conjunto infinito enumerável para todo $n \in \mathbb{N}$. Mostraremos que

$$\bigcup_{n=1}^{\infty} A_n = A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots$$

é enumerável. Como $A_1, A_2, \ldots, A_n, \ldots$ são conjuntos enumeráveis, então existem funções sobrejetivas

$$f_1 : \mathbb{N} \longrightarrow A_1, f_2 : \mathbb{N} \longrightarrow A_2, \ldots, f_n : \mathbb{N} \longrightarrow A_n, \ldots$$

ou seja,

$$f_n : \mathbb{N} \longrightarrow A_n$$

é sobrejetiva, para todo $n \in \mathbb{N}$. Tomando $A = \bigcup_{n=1}^{\infty} A_n$.

Considerando uma função

$$f : \mathbb{N} \times \mathbb{N} \longrightarrow A$$

definida por

$$f(n, m) = f_n(m)$$

também é sobrejetiva. De fato, se $x \in A = \bigcup_{n=1}^{\infty} A_n$, então existe um índice $n \in \mathbb{N}$ tal que $x \in A_n$. Como f_n é sobrejetiva, existe $m \in \mathbb{N}$ tal que $f_n(m) = x$.

Segue que $f(n, m) = f_n(m) = x \in f(\mathbb{N} \times \mathbb{N})$. Logo, f é sobrejetiva. Como o conjunto $\mathbb{N} \times \mathbb{N}$ é enumerável, concluímos da Proposição 1.3, que $A = \bigcup_{n=1}^{\infty} A_n$ é enumerável. □

Os resultados sobre enumerabilidade é de suma importância, pois existem conjuntos que não são enumeráveis.

Teorema 1.4. *O conjunto $\mathbb{R}$ dos números reais não é enumerável.*

Demonstração. Demonstraremos que os números reais $x \in (0, 1]$, isto é, $0 < x \leq 1$ não é enumerável. Suponhamos que os números reais $x \in (0, 1]$ seja enumerável, digamos

$$r_1, r_2, r_3, r_4, \ldots$$

Como cada r_i, com $i \in \{1, 2, \ldots, n, \ldots\}$ possui uma representação decimal. Evitando representações decimais finitas pelo uso da forma infinita periódica em tais casos. Por exemplo, o número $1/2$ será escrito como $0,499999\ldots$ e não $0,5$. Assim sendo, podemos escrever os números deste intervalo $(0, 1]$ como elementos de uma sequência infinita e

listá-los da seguinte forma:

$$\begin{aligned} r_1 &= 0, a_{11}a_{12}a_{13}a_{14}\ldots \\ r_2 &= 0, a_{21}a_{22}a_{23}a_{24}\ldots \\ r_3 &= 0, a_{31}a_{32}a_{33}a_{34}\ldots \\ \vdots & \qquad\qquad \vdots \end{aligned}$$

Cada a_{ij} representa algum dos algarismos de 0 a 9. Porém, por mais extensa que seja esta lista, construiremos um número que não pertença a ela através do processo (diagonal de Cantor). Este processo consiste em construir um número que seja diferente de r_1 na primeira casa decimal, diferente de r_2 na segunda casa decimal, diferente de r_3 na terceira casa e assim por diante, de modo que este número não seja igual a nenhum dos números da lista acima.

Seja $b \in (0, 1]$, então temos o seguinte decimal

$$b = 0, b_1b_2b_3\ldots$$

de modo que $b_i = 7$ se $a_{ii} \neq 7$ e $b_i = 3$ se $a_{ii} = 7$. Dessa forma, temos que b é diferente de r_1, pois $b_1 \neq a_{11}$, o número b é diferente de r_2, pois $b_2 \neq a_{22}$, o número b é diferente de r_3, pois $b_3 \neq a_{33}$ e assim por diante. Em geral, b_i é qualquer algarismo não nulo diferente a_{ii}. Logo, o número b é diferente de cada r_i. Porém, o número real b está compreendido entre 0 e 1, contradição. Portanto, o conjunto dos números reais entre 0 e 1 é não enumerável.

Usando a Proposição 1.6, se $\mathbb{R}$ fosse enumerável, então o intervalo $(0, 1] \subset \mathbb{R}$ seria enumerável. Mas, provamos que o intervalo $(0, 1]$ não é enumerável. Portanto, o conjunto $\mathbb{R}$ dos números reais não é enumerável. □

Corolário 1.1. *O conjunto $\mathbb{R}\backslash\mathbb{Q}$ dos números irracionais não é enumerável.*

Demonstração. De fato, temos que o conjunto $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R}\backslash\mathbb{Q})$. Provamos que o conjunto $\mathbb{Q}$ é enumerável. Se o conjunto dos irracionais $\mathbb{R}\backslash\mathbb{Q}$ também o fosse, então o conjunto dos reais $\mathbb{R}$ seria enumerável usando o Lema 1.7, o que um contradição pelo Teorema 1.4, concluímos que o conjunto $\mathbb{R}\backslash\mathbb{Q}$ dos irracionais não é enumerável. □

Provaremos que o conjunto dos números algébricos é enumerável. Mas, inicialmente, precisaremos de alguns resultados a respeito dos polinômios.

Teorema 1.5. *Um número real β é raiz de um polinômio $P(x)$ não nulo com coeficientes inteiros (ou racionais) se, e somente se, o polinômio $x - \beta$ é um fator de $P(x)$, isto é,*

$$P(x) = (x - \beta)q(x)$$

Além disso, o grau do polinômio quociente $q(x)$ é uma unidade menor do que o grau de $P(x)$.

Demonstração. ($\Leftarrow$) Seja $P(x) = (x - \beta)q(x)$. Então, aplicando β em $P(x)$, tem-se

$$P(\beta) = (\beta - \beta)q(x) \Longrightarrow P(\beta) = 0$$

Portanto, o número β é raiz de $P(x)$.

($\Rightarrow$) Suponhamos que β seja raiz de $P(x)$. Dividindo $P(x)$ por $x - \beta$, temos que existe um quociente $q(x)$ e um resto $r(x)$ tal que

$$P(x) = (x - \beta)q(x) + r(x)$$

em que $r(x)$ é um polinômio cujo grau é menor do que o grau do divisor (que no caso, é o polinômio $(x-\beta)$ de grau 1). Então $r(x) = r$, sendo r uma constante independente de x. Então,

$$P(x) = (x - \beta)q(x) + r$$

Como β é raiz de $P(x)$, segue que

$$P(\beta) = 0 \Longrightarrow (\beta - \beta)q(\beta) + r = 0 \Longrightarrow r = 0$$

assim, o resto da divisão de $P(x)$ por $x - \beta$ é zero.

Portanto, o polinômio $P(x) = (x - \beta)q(x)$. Finalmente, qualquer que seja o grau do polinômio $P(x)$, vemos que o grau do quociente $q(x)$ é uma unidade menor. □

Provaremos o teorema fundamental da álgebra para os números reais: Todo polinômio não nulo $P(x)$ com coeficientes inteiros (ou racionais) de grau n tem no máximo n raízes distintas. Vale ressaltar que existe o teorema fundamental da álgebra para os complexos: Todo polinômio não nulo $p(z)$ com coeficientes complexos de uma variável e de grau n possui alguma raiz complexa. Por outras palavras, o corpo dos números complexos é algebricamente fechado e, portanto, tal como com qualquer outro corpo algebricamente fechado, a equação $p(z) = 0$ tem n soluções não necessariamente distintas.

Teorema 1.6 (Teorema Fundamental da Álgebra)**.** *Qualquer equação polinomial da forma*

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{1.19}$$

não nula com coeficientes inteiros (ou racionais), tem no máximo n raízes distintas.

Demonstração. Suponhamos por contradição, que um polinômio $P(x)$ da forma (1.19) com coeficiente $a_n > 0$ tenha $n+1$ raízes distintas, $\beta_1, \beta_2, \beta_3, \ldots, \beta_n, \beta_{n+1}$. Usando o Teorema 1.5, à qual assegura que $x - \beta_1$ é um fator de $P(x)$ se o número β_1 é um raiz de $P(x)$, ou seja, existe um quociente $q_1(x)$ tal que

$$P(x) = (x - \beta_1)q_1(x) \tag{1.20}$$

Como β_2 é outra raiz de $P(x)$, segue que β_2 também é uma raiz de $q_1(x)$.

De fato,

$$P(\beta_2) = 0 \Longrightarrow (\beta_2 - \beta_1)q_1(\beta_2) = 0 \tag{1.21}$$

Como $(\beta_2 - \beta_1) \neq 0$, temos que $q_1(\beta_2) = 0$. Logo, o número β_2 é raiz de $q_1(x)$. Usando novamente o Teorema 1.5, temos que $x - \beta_2$ é um fator de $q_1(x)$, então existe um quociente $q_2(x)$ tal que

$$q_1(x) = (x - \beta_2)q_2(x) \tag{1.22}$$

Segue-se das equações (1.20) e (1.22) que

$$P(x) = (x - \beta_1)q_1(x) = (x - \beta_1)(x - \beta_2)q_2(x) \tag{1.23}$$

Continuando este processo com $\beta_3, \beta_4, \ldots, \beta_n$, observamos que $P(x)$ pode ser fatorado em

$$P(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3)(x - \beta_4)\cdots(x - \beta_n)q_n(x) \tag{1.24}$$

Mas $P(x)$ tem grau n, logo, o polinômio $q_n(x)$ é uma constante. Assim sendo, o polinômio $q_n(x)$ tem que ser $a_n > 0$ para que a fatoração esteja de acordo com a equação (1.19). Considerando agora a raiz β_{n+1} de $P(x)$, que é diferente de todas as outras raízes, temos que $P(\beta_{n+1}) = 0$.

Segue-se de (1.24) que

$$(\beta_{n+1} - \beta_1)(\beta_{n+1} - \beta_2)(\beta_{n+1} - \beta_3)(\beta_{n+1} - \beta_4)\cdots(\beta_{n+1} - \beta_n)a_n = 0$$

o que é impossível, pois o produto de fatores não nulos não pode ser zero. Assim, o teorema está demonstrado. □

1.2.2 Enumerabilidade dos Algébricos

Teorema 1.7. *O conjunto $\mathbb{A}$ dos números algébricos reais é enumerável.*

Demonstração. Sejam $P(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$ um polinômio não nulo com coeficientes racionais e $\mathcal{R}_P$ o conjunto das raízes de P. Usando o Teorema 1.6,

temos que o conjunto $\mathcal{R}_P$ tem no máximo n elementos, ou seja,

$$\mathcal{R}_P = \{k \in \mathbb{R}; P(k) = 0\}$$

é um conjunto finito, logo, enumerável.

Para cada $n \in \mathbb{N}$, existe apenas uma quantidade enumerável de polinômios com coeficientes racionais com grau n. De fato, seja $\mathbb{P}_n$ o conjunto dos polinômios com coeficientes racionais com grau n, isto é,

$$\mathbb{P}_n = \{P \in \mathbb{Q}[x]; \partial P = n, \text{ com } n \in \mathbb{N}\}$$

Considerando uma função

$$f : \mathbb{P}_n \longrightarrow \mathbb{Q}^{n+1} = \underbrace{\mathbb{Q} \times \cdots \times \mathbb{Q}^*}_{n+1 \text{ cópias}}$$

definida por

$$f\left(P(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n\right) = (a_0, \ldots, a_n)$$

é injetiva.

De fato, sejam $f(P(x)) = (a_0, \ldots, a_n), f(G(x)) = (b_0, \ldots, b_n) \in \mathbb{Q}^{n+1}$. Suponhamos que $f(P(x)) = (a_0, \ldots, a_n) = (b_0, \ldots, b_n) = f(G(x))$, então temos que $a_0 = b_0, \ldots, a_n = b_n$. Segue da igualdade de polinômios que $P(x) = G(x)$. Logo, a função f é injetiva. Como $\mathbb{Q}^{n+1} = \mathbb{Q} \times \cdots \times \mathbb{Q}^*$ é enumerável por ser produto cartesiano finito de conjuntos enumeráveis, segue-se que o conjunto $\mathbb{P}_n$ é enumerável.

Considerando o conjunto $\mathcal{B}$ formado por todos os polinômios com coeficientes racionais com grau n, isto é,

$$\mathcal{B} = \bigcup_{n \in \mathbb{N}} \mathbb{P}_n$$

Assim sendo, o conjunto $\mathcal{B}$ é escrito como união enumerável de conjuntos enumeráveis. Logo, usando o Lema 1.10, o conjunto $\mathcal{B}$ é enumerável.

Agora, considerando o conjunto $\mathcal{A}_n$ formado pelos conjuntos de todas as raízes associadas aos polinômios de grau n, ou seja,

$$\mathcal{A}_n = \bigcup_{P \in \mathbb{P}_n} \mathcal{R}_P$$

Usando o que foi feito anteriormente e o fato de que a união enumerável de conjuntos finitos é enumerável, segue do Lema 1.9, que $\mathcal{A}_n$ é enumerável.

Note que, o conjunto dos números algébricos reais é a união de todos os $\mathcal{A}_n$, isto é,

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

Assim sendo, o conjunto do números algébricos reais é escrito como união enumerável de conjuntos enumeráveis. Portanto, segue-se do Lema 1.10, que o conjunto dos números algébrico reais $\mathbb{A}$ é enumerável. □

Finalmente, veremos a demonstração da existência dos números transcendentes via G. Cantor e a sua não enumerabilidade.

1.2.3 Existência de Números Transcendentes

Teorema 1.8 (G. Cantor)**.** *Existem números transcendentes e estes são não enumeráveis.*

Demonstração. Usando o Teorema 1.7, segue que o conjunto $\mathbb{A}$ dos algébricos reais é enumerável. Como o conjunto $\mathbb{R}$ dos reais é não enumerável, então o conjunto dos números $\mathbb{T}$ transcendentes reais deve ser não enumerável. De fato, se fosse enumerável, usando o Lema 1.7, teríamos que $\mathbb{R}$ seria enumerável como a união de dois conjuntos enumeráveis, $\mathbb{R} = (\mathbb{A} \cup \mathbb{T})$. Portanto, o conjunto dos números $\mathbb{T}$ transcendentes são não enumeráveis. □

Finalmente, observamos que os Teoremas 1.7 e 1.8, notavelmente, nos diz que existem ‘‘mais” números transcendentes do que números algébricos, embora, não tenha produzido um exemplo específico de um destes números.

1.2.4 Natureza Aritmética dos Algébricos versus Transcendentes

O teorema a seguir nos dá informações importantes sobre operações entre números algébricos e transcendentes e suas potências.

Teorema 1.9. *Sejam $\alpha \in \mathbb{A}$ um número algébrico e $t \in \mathbb{T}$ um número transcendente. Então valem as seguintes propriedades:*
(i) A soma (ou diferença) $\alpha + t$ de um número algébrico α com um número transcendente t é um número transcendente.
(ii) O produto $\alpha.t$ de um número algébrico $\alpha \neq 0$ com um número transcendente t é um número transcendente.
(iii) O inverso $t^{-1} = \frac{1}{t}$ de um número transcendente t é um número transcendente.

(iv) Se t é um número transcendente. Então t^n é um número transcendente para todo $n \in \mathbb{N}$, com $n \neq 0$.
(v) Se α é um número algébrico. Então $\alpha^{\frac{a}{b}}$ é um número algébrico para todo $\frac{a}{b} \in \mathbb{Q}$.
(vi) Se t é um número transcendente. Então $t^{\frac{a}{b}}$ é um número transcendente para todo $\frac{a}{b} \in \mathbb{Q}$, com $\frac{a}{b} \neq 0$.

Demonstração. **Propriedade (i).** Suponhamos por contradição que $\alpha + t = c \in \mathbb{A}$ seja um número algébrico. Então pelo Teorema 1.2, tem-se

$$t = c - \alpha$$

seria um número algébrico, por ser a diferença de dois algébricos. Contradição, já que por hipótese t é transcendente. Portanto, o número $\alpha + t \in \mathbb{T}$ é transcendente. □

Demonstração. **Propriedade (ii).** Suponhamos por contradição que $\alpha.t = c \in \mathbb{A}$ seja um número algébrico, com $\alpha \neq 0$. Então pelo Teorema 1.2, tem-se

$$t = c.\frac{1}{\alpha}$$

seria um número algébrico, por ser o produto de dois algébricos. Contradição, já que por hipótese t é transcendente. Portanto, o número $\alpha.t \in \mathbb{T}$ é transcendente. □

Demonstração. **Propriedade (iii).** Suponhamos por contradição que $t^{-1} = \frac{1}{t} \in \mathbb{A}$ seja um número algébrico. Então pelo Teorema 1.2, tem-se que o inverso de t^{-1}, isto é, o número $\dfrac{1}{t^{-1}}$ seria um algébrico, mas note que

$$\frac{1}{t^{-1}} = \frac{1}{\frac{1}{t}} = t$$

Daí, o número t também seria algébrico. Contradição, já que por hipótese t é transcendente. Portanto, o número $t^{-1} \in \mathbb{T}$ é transcendente. □

Demonstração. **Propriedade (iv).** Suponhamos por contradição que $t^n \in \mathbb{A}$ seja um número algébrico para todo $n \in \mathbb{N}$, com $n \neq 0$. Então existe um polinômio não nulo

$$P(x) = a_0 + a_1 x + \cdots + a_m x^m$$

com coeficientes inteiros e $m \in \mathbb{N}$ tal que

$$P(t^n) = a_0 + a_1 t^n + \cdots + a_m (t^n)^m \Longrightarrow P(t^n) = 0$$

Considere o polinômio não nulo com coeficientes inteiros a seguir:

$$Q(x) = a_0 + a_1 x^n + \cdots + a_m x^{mn}$$

Aplicando t em $Q(x)$, tem-se

$$Q(t) = a_0 + a_1 t^n + \cdots + a_m t^{mn} \Longrightarrow Q(t) = a_0 + a_1 t^n + \cdots + a_m (t^n)^m \Longrightarrow Q(t) = P(t^n)$$

o que implicaria

$$Q(t) = 0$$

Daí, teríamos que o número t seria algébrico. Contradição, já que por hipótese t é transcendente. Portanto, o número $t^n \in \mathbb{T}$ é transcendente. □

Demonstração. **Propriedade (v).** Suponhamos por contradição que $\alpha^{\frac{a}{b}} = \beta \in \mathbb{T}$ seja um número transcendente para todo $\frac{a}{b} \in \mathbb{Q}$, sem perda de generalidade, podemos supor ainda que $b > 0$. Assim,

$$\alpha^{\frac{a}{b}} = \beta \Longrightarrow \alpha^a = \beta^b$$

Pela Propriedade (iv) acima teríamos que o número β^b seria transcendente. Contradição, já que pelo Teorema 1.2, o número α^a é algébrico, uma vez que o conjuntos dos números algébricos formam um corpo. Portanto, o número $\alpha^{\frac{a}{b}} \in \mathbb{A}$ é algébrico. □

Demonstração. **Propriedade (vi).** Suponhamos por contradição que $t^{\frac{a}{b}} = c \in \mathbb{A}$ seja um número algébrico para todo $\frac{a}{b} \in \mathbb{Q}$, com $\frac{a}{b} \neq 0$. Assim,

$$t^{\frac{a}{b}} = c \Longrightarrow t^a = c^b$$

Pela Propriedade (v) acima teríamos que o número c^b seria algébrico. Contradição, já que como $a \neq 0$ e t é transcendente por hipótese, tem-se pelas Propriedades (iii) e (iv) acima que o número t^a é transcendente. Portanto, o número $t^{\frac{a}{b}} \in \mathbb{T}$ é transcendente. □

O principal resultado do próximo capítulo será apresentar o primeiro número transcendente que hoje é conhecido como (Constante de Liouville) e uma aplicação da

existência de números transcendentes, caracterizando o espaço vetorial $\mathbb{R}$ como espaço de dimensão infinita sobre $\mathbb{Q}$.

Capítulo 2

O Teorema de Liouville e o Número de Liouville

Neste capítulo, apresentaremos o teorema de Liouville e o primeiro número transcendente, que foi o resultado que historicamente iniciou a teoria transcendente. Através do seu trabalho foi possível escrever explicitamente um número transcendente. A principal referência utilizada na elaboração deste capítulo é Figueiredo [5].

2.1 Algumas Aproximações por Racionais

Esta seção será dedicada a ideia do Liouville para provar a existência dos números transcendentes e produzir um exemplo específico de tais números. Mas antes, vale ressaltar que o Teorema 1.8, apresentado no capítulo anterior garante a existência de pelo menos um número transcendente, embora, não esteja explícito. Foi o matemático Liouville, em 1851, que estabeleceu um critério para que um número seja transcendente.

Definição 2.1. *Um número algébrico α é de grau $n \in \mathbb{N}$ se ele for raiz de uma equação polinomial de grau n com coeficientes racionais, e se não existir uma equação desse tipo de menor grau da qual α seja raiz. Veremos posteriormente em detalhes resultados desta definição.*

Observação 2.1. Os números racionais coincidem com os números algébricos de grau 1. Veja o Exemplo 1.7, no capítulo anterior.

Exemplo 2.1. *O número $\sqrt{2}$ é um número algébrico de grau 2.*

Demonstração. Como $\sqrt{2}$ é raiz de $x^2 - 2 = 0$. De fato, escrevendo

$$x = \sqrt{2} \Longrightarrow x^2 = (\sqrt{2})^2 \Longrightarrow x^2 - 2 = 0$$

Segue que $\sqrt{2}$ é uma raiz de um polinômio de grau 2. Porém, $\sqrt{2}$ não é raiz de um polinômio de grau 1, uma vez que $\sqrt{2}$ é irracional e todo número algébrico de grau 1 é racional. Logo, o número $\sqrt{2}$ é um número algébrico de grau 2. □

Definição 2.2. *Um número real α é aproximável na ordem $n \in \mathbb{N}$ por racionais se existirem uma constante $C > 0$ e uma sequência $(\frac{p_j}{q_j})_{j\geq 1}$ de racionais distintos, com $q_j > 0$ e $mdc(p_j, q_j) = 1$ tais que*

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{C}{q_j^n} \tag{2.1}$$

para todo $j \geq 1$.

Obviamente, se um número α for aproximável na ordem n, então ele é aproximável em qualquer ordem k, com $k < n$. Usando (3.1), obtemos que

$$\left|\alpha - \frac{p_j}{q_j}\right| < C \tag{2.2}$$

o que mostra que a sequência $(q_j)_{j\geq 1}$ não se mantém limitada.

Proposição 2.1. *A sequência $(q_j)_{j\geq 1}$ é ilimitada.*

Demonstração. De fato, suponhamos por contradição que a sequência $(q_j)_{j\geq 1}$ seja limitada, então existe $M > 0$ tal que

$$q_j \leq M \quad \text{para todo} \quad j \geq 1.$$

Segue-se de (2.2) que

$$\left|\alpha - \frac{p_j}{q_j}\right| < C \Longrightarrow |\alpha q_j - p_j| < Cq_j$$

Usando uma relação de desigualdade, temos

$$|p_j| - |\alpha q_j| < |\alpha q_j - p_j| < Cq_j \leq CM$$

daí,

$$|p_j| - |\alpha q_j| < CM \Longrightarrow |p_j| < |\alpha||q_j| + CM \leq |\alpha|\, M + CM$$

por conseguinte,

$$|p_j| < (|\alpha| + C)M$$

o que implica uma limitação para a sequência $(p_j)_{j\geq 1}$. Desse modo, teríamos uma sequência de racionais $(\frac{p_j}{q_j})_{j\geq 1}$ com finitos termos distintos, Mas isto contraria o fato

de a sequência ser infinita. Portanto, a sequência $(q_j)_{j\geq 1}$ é ilimitada. Assim sendo, concluímos que a sequência q_j "tende para mais infinito"e escrevemos

$$q_j \to +\infty$$

Logo, usando (2.1) concluímos

$$\lim_{j\to+\infty}\left(\frac{p_j}{q_j}\right) = \alpha \tag{2.3}$$

e dizemos que a sequência $(\frac{p_j}{q_j})_{j\geq 1}$ converge para α. □

Observação 2.2. A importância da Definição 2.2 não é a existência de uma sequência de racionais convergindo para α (tais sequências sempre existem qualquer que seja o real α, esta é a chamada densidade dos racionais no conjunto dos reais), mas no fato de que uma sequência particular de racionais converge para α de acordo com a desigualdade (3.1). Note que, outro fato importante na definição é que podemos tomar racionais todos diferentes, o que implicará, em particular, que possamos tomá-los distintos de α, mesmo no caso deste ser racional.

A seguir estabeleceremos as relações entre os dois conceitos introduzidos nas Definições 2.1 e 2.2 vista anteriormente.

Teorema 2.1. *Todo número racional (número algébrico de grau* 1*) é aproximável na ordem* 1*, e não é aproximável na ordem* k*, para* $k > 1$*.*

Demonstração. **(I)** - Todo número racional é aproximável na ordem 1.

Seja $\frac{p}{q}$ um número racional, com $q > 0$ e $mdc(p, q) = 1$. Como p e q são primos entre si, existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$px_0 - qy_0 = 1 \tag{2.4}$$

Na verdade, a equação

$$px - qy = 1 \tag{2.5}$$

tem um número infinito de soluções da forma

$$x_t = x_0 + qt \quad \text{e} \quad y_t = y_0 + pt \tag{2.6}$$

para todo $t \in \mathbb{Z}$, as quais satisfazem a equação (2.5), isto é,

$$px_t - qy_t = 1. \tag{2.7}$$

Fixando $k \in \mathbb{N}$, tal que $k > \frac{-x_0}{q}$, considerando as sequências $(x_j)_{j\geq 1}$ e $(y_j)_{j\geq 1}$ definidas a partir de (2.6) por

$$x_j = x_0 + q(k+j) \quad \text{e} \quad y_j = y_0 + p(k+j), \text{ com } j \in \mathbb{N} \tag{2.8}$$

Usando a restrição sobre k, temos que $qk > -x_0$, ou seja, $qk + x_0 > 0$.
Como $x_j = x_0 + qk + qj$. Segue que $x_j > qj$ e daí $x_j > 0$, pois $qj > 0$.

Afirmamos que

$$\frac{y_j}{x_j} \neq \frac{y_{j'}}{x_{j'}}, \text{ se } j \neq j'. \tag{2.9}$$

Mas, caso houvesse igualdade entre os racionais $\frac{y_j}{x_j} = \frac{y_{j'}}{x_{j'}}$, usando (2.6), teríamos $j = j'$.
De fato, se

$$\frac{y_j}{x_j} = \frac{y_{j'}}{x_{j'}}$$

Então, usando (2.6), tem-se

$$x_j = x_0 + qj, \quad y_j = y_0 + pj, \quad x_{j'} = x_0 + qj' \quad \text{e} \quad y_{j'} = y_0 + pj'$$

Assim, substituindo

$$\frac{y_j}{x_j} = \frac{y_{j'}}{x_{j'}} = \frac{y_0 + pj}{x_0 + qj} = \frac{y_0 + pj'}{x_0 + qj'} \Longrightarrow (y_0 + pj)(x_0 + qj') = (y_0 + pj')(x_0 + qj)$$

Segue-se que

$$y_0x_0 + y_0qj' + pjx_0 + pjqj' = y_0x_0 + y_0qj + pj'x_0 + pj'qj$$

Eliminando os termos semelhantes na igualdade acima e isolando j e j', tem-se

$$pjx_0 - y_0qj = pj'x_0 - y_0qj' \Longrightarrow (px_0 - qy_0)j = (px_0 - qy_0)j'$$

Logo,

$$j = j'.$$

Uma vez que por (2.4), tem-se $px_0 - qy_0 = 1$. Por outro lado, em virtude de (2.7), tem-se

$$|px_j - qy_j| = 1 \Longrightarrow \left|\frac{px_j}{qx_j} - \frac{qy_j}{qx_j}\right| = \frac{1}{qx_j}$$

por conseguinte

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

Portanto,

$$\left|\frac{p}{q} - \frac{y_j}{x_j}\right| < \frac{C}{x_j}$$

Para todo $j \geq 1$, onde a constante $C = 2$, $(x_j)_{j\geq 1}$ e $(y_j)_{j\geq 1}$ definidas em (2.8) de modo que a sequência $(\frac{y_j}{x_j})_{j\geq 1}$ de racionais distintos, satisfazem a desigualdade acima. O que mostra que $\frac{p}{q}$ é aproximável na ordem 1 por racionais.

(II) - Todo número racional não é aproximável na ordem k, para $k > 1$.

Para todo racional $\frac{v}{u} \neq \frac{p}{q}$, com $u > 0$ e $q > 0$, tem-se $\frac{p}{q} - \frac{v}{u} \neq 0$. Assim,

$$\left|\frac{p}{q} - \frac{v}{u}\right| = \frac{|pu - qv|}{qu} \geq \frac{1}{qu} \tag{2.10}$$

Suponhamos que $\frac{p}{q}$ seja aproximável na ordem 2, então existe uma constante $C > 0$ e uma sequência de racionais $(\frac{v_j}{u_j})_{j\geq 1}$ distintos, com $u_j > 0$ tais que

$$\left|\frac{p}{q} - \frac{v_j}{u_j}\right| < \frac{C}{u_j^2} \tag{2.11}$$

Usando (2.10) e (2.11), tem-se

$$\frac{1}{qu_j} \leq \left|\frac{p}{q} - \frac{v_j}{u_j}\right| < \frac{C}{u_j^2}$$

o que implica

$$\frac{1}{qu_j} < \frac{C}{u_j^2}$$

multiplicando a desigualdade por $qu_j^2 > 0$, segue que

$$u_j < Cq$$

o que é impossível, uma vez que a sequência $u_j \to +\infty$.
Logo, todo $\frac{p}{q}$ não é aproximável na ordem 2 e portanto, também não é aproximável em nenhuma ordem superior. □

Observação 2.3. A parte (II) do Teorema 2.1 é consequência de um resultado mais geral que será demonstrado abaixo, a saber no Corolário 2.1.

Proposição 2.2 (Princípio das Gavetas)**.** *Se $n + 1$ ou mais objetos são colocados em $n \in \mathbb{N}$ ou menos gavetas, então pelo menos uma gaveta recebe mais de um objeto.*

Demonstração. O número médio de objetos por gaveta é maior do que ou igual a

$$\frac{n+1}{n} = 1 + \frac{1}{n} > 1$$

Note que, a expressão é maior que 1. Logo, em alguma gaveta haverá um número de objetos maior que 1. □

2.1.1 Aproximação de Números $\mathbb{R}\backslash\mathbb{Q}$ por $\mathbb{Q}$

Teorema 2.2 (Dirichlet)**.** *Todo número irracional λ é aproximável na ordem 2, isto é, existe uma constante $C > 0$ tal que a desigualdade abaixo se verifica para um número infinito de racionais $\frac{p}{q}$ distintos, com $q > 0$.*

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

Demonstração. Seja α um número irracional e $n \in \mathbb{N}$. Representamos por $[x]$ a parte inteira de um número real x, isto é, o maior inteiro menor do que ou igual a x e a parte fracionária por $x - [x]$. Considerando os $n + 1$ números reais

$$0, \alpha - [\alpha], 2\alpha - [2\alpha], \ldots, n\alpha - [n\alpha] \tag{2.12}$$

Note que, por definição da função maior inteiro $[x]$, tem-se

$$[\alpha] \leq \alpha < [\alpha] + 1 \Longrightarrow 0 \leq \alpha - [\alpha] < 1$$

Assim, os $n + 1$ números reais pertencem ao intervalo $[0, 1)$. Considerando em seguida a partição do intervalo $[0, 1)$ em n intervalos, disjuntos dois a dois da forma

$$\left[\frac{j}{n}, \frac{j+1}{n}\right), \text{ com } j = 0, 1, \ldots, n-1. \tag{2.13}$$

ou seja,

$$\left[0, \frac{1}{n}\right) \cap \left[\frac{1}{n}, \frac{2}{n}\right) \cap, \ldots, \cap \left[\frac{j}{n}, \frac{j+1}{n}\right) \cap, \ldots, \cap \left[\frac{n-1}{n}, 1\right) = \emptyset$$

Usando o Princípio das Gavetas, o qual segue da Proposição 2.2, temos que pelos menos dois dos reais em (2.12) estão em um mesmo intervalo do tipo (2.13). Digamos que eles sejam $n_1\alpha - [n_1\alpha]$ e $n_2\alpha - [n_2\alpha]$, com $0 \leq n_1 < n_2 \leq n$, para os quais temos então

$$|n_2\alpha - [n_2\alpha] - n_1\alpha + [n_1\alpha]| < \frac{1}{n} \Longrightarrow |(n_2 - n_1)\alpha - ([n_2\alpha] - [n_1\alpha])| < \frac{1}{n} \tag{2.14}$$

Sejam $k := n_2 - n_1$ e $h := [n_2\alpha] - [n_1\alpha]$, os quais são inteiros com $k > 0$ e $h \geq 0$.

Logo, a desigualdade (2.14) pode ser escrita como

$$|k\alpha - h| < \frac{1}{n} \Longrightarrow \left|\alpha - \frac{h}{k}\right| < \frac{1}{nk}$$

segue-se que

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{k^2} \tag{2.15}$$

uma vez que, a desigualdade $n_1 < n_2 < n$ implica $n_1 - n_1 < n_2 - n_1 < n - n_1 < n$, ou seja, $0 < k < n$, de onde segue que $\frac{1}{nk} < \frac{1}{k^2}$. Assim sendo, mostramos que para todo $n \in \mathbb{N}$, existe um racional da forma $\frac{h}{k}$, com $k < n$, para qual a desigualdade (2.15) se verifica. Afirmamos que (2.15), verifica-se para um número infinito de racionais $\frac{h}{k}$ distintos.

Suponhamos por contradição que existe apenas um número finito de racionais

$$\frac{h_1}{k_1}, \ldots, \frac{h_r}{k_r}$$

distintos satisfazendo a desigualdade (2.15).

Seja

$$\epsilon = \min\left\{\left|\alpha - \frac{h_1}{k_1}\right|, \ldots, \left|\alpha - \frac{h_r}{k_r}\right|\right\} > 0$$

Tomando $n \in \mathbb{N}$ tal que $\frac{1}{n} < \epsilon$. Mostramos anteriormente que existe um racional $\frac{h}{k}$ tal que

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{nk}$$

Como

$$\frac{1}{nk} < \frac{1}{n} < \epsilon$$

por conseguinte

$$\left|\alpha - \frac{h}{k}\right| < \epsilon$$

segue que $\frac{h}{k} \neq \frac{h_i}{k_i}$ para $i = 1, \ldots, r$. Mas isso é uma contradição, pois o racional $\frac{h}{k}$ satisfaz (2.15). □

Observação 2.4. (1) O Teorema 2.2 afirma que um número irracional é aproximável, pelo menos, na ordem 2. Dependendo do número irracional ele poderá ser aproximável numa ordem superior a 2. O Teorema 2.5 abaixo fornece informações mais precisas sobre essas ordens de aproximação.

(2) Hurwitz provou que a menor constante C que é válida para todos os irracionais na desigualdade do Teorema 2.2 acima é $\frac{1}{\sqrt{5}}$. Mais precisamente, se $A < \frac{1}{\sqrt{5}}$, então existe um número irracional λ tal que para todos os racionais $\frac{p}{q}$, excetuando-se um

número finito deles.

$$\left|\lambda - \frac{p}{q}\right| > \frac{A}{q^2}$$

Para maiores detalhes, confira em Niven [12].

Necessitaremos ainda de alguns resultados analíticos, relativamente simples, porém, por brevidade, apenas enunciaremos.

Lema 2.1. *Todo polinômio $p : \mathbb{R} \longrightarrow \mathbb{R}$ é uma função contínua e derivável. Também é contínua e derivável toda função racional $f(x) = \frac{p(x)}{q(x)}$* (quociente de dois polinômios) *nos pontos onde é definida, isto é, nos pontos onde seu denominador não se anula.*

Demonstração. Ver [8], p. 227. □

O teorema seguinte assegura a existência de valores máximos e mínimos de uma função contínua quando seu domínio é compacto.

Teorema 2.3 (Weirstrass)**.** *Toda função contínua $f : X \longrightarrow \mathbb{R}$ definida no conjunto compacto $X \subset \mathbb{R}$ é limitada e atinge seus extremos, ou seja, existem $x_1, x_2 \in X$ tais que $f(x_1) \leq f(x) \leq f(x_2)$ para todo $x \in X$.*

Demonstração. Ver [8], p. 239. □

Teorema 2.4 (Teorema do Valor Médio, de Lagrange)**.** *Seja $f : [a, b] \longrightarrow \mathbb{R}$ contínua. Se f é derivável em (a, b), existe $c \in (a, b)$ tal que*

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

Um enunciado equivalente seria. Seja $f : [a, a + h] \longrightarrow \mathbb{R}$ contínua. Se f é derivável em $(a, a + h)$, existe $t \in (0, 1)$ tal que

$$f'(a + th) = \frac{f(a + h) - f(a)}{h}.$$

Demonstração. Ver [8], p. 272. □

Apresentaremos um dos nossos principais objeto de estudo deste capítulo. Um resultado que consolidou o trabalho feito por Liouville na busca por números transcendentes.

2.2 O Teorema de Liouville

Teorema 2.5 (Teorema de Liouville)**.** *Seja α um número algébrico real de grau $n \in \mathbb{N}$. Então existe uma constante $A > 0$ tal que*

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{Aq^n} \tag{2.16}$$

para todo racional $\frac{p}{q}$, com $q > 0$. (Se $n = 1$, tomamos $\frac{p}{q} \neq \alpha$).

Demonstração. Seja α um número algébrico real de grau n. Então α é raiz de uma equação polinomial não nula da forma

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \tag{2.17}$$

Então, existe um $\delta > 0$ tal que no intervalo $[\alpha - \delta, \alpha + \delta]$ a única raiz de $f(x)$ é α, ou seja,

$$[\alpha - \delta, \alpha + \delta] \cap \mathcal{R}_f = \{\alpha\}$$

Sendo $\mathcal{R}_f$ o conjunto das raízes de f. A existência de uma tal δ segue do fato da equação polinomial ter no máximo n raízes reais. Logo, δ pode ser qualquer número menor do que a menor das distâncias de α as demais raízes reais.

A seguir observamos que a derivada $f'(x)$ de $f(x)$ é um polinômio de grau $n - 1$, ou seja,

$$f'(x) = na_n x^{n-1} + n - 1a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1$$

Como f' é contínua no intervalo compacto. Usando o teorema de Weirstrass, segue que existe um $M > 0$ tal que

$$|f'(x)| \leq M, \text{ para todo } x \in [\alpha - \delta, \alpha + \delta] \tag{2.18}$$

Para todo racional $\frac{p}{q} \in [\alpha - \delta, \alpha + \delta]$. Como f é contínua e derivável com extremos $\frac{p}{q}$ e α ou α e $\frac{p}{q}$. Logo, usando o teorema do valor médio, existe um $\xi \in (\frac{p}{q}, \alpha)$ tal que

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

Como $f(\alpha) = 0$, tomando o módulo na igualdade acima e usando (2.18), obtemos

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

o que implica

$$\left| f\left(\frac{p}{q}\right)\right| \leq M\left|\alpha - \frac{p}{q}\right| \tag{2.19}$$

Agora, para obter a desigualdade desejada, necessitamos de uma estimativa inferior para $f(\frac{p}{q})$. Assim, tem-se

$$\left| f\left(\frac{p}{q}\right)\right| = \left| a_n\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1\frac{p}{q} + a_0\right|$$

por definição de δ.

$$\left| f\left(\frac{p}{q}\right)\right| = \left|\frac{a_np^n + a_{n-1}qp^{n-1} + \cdots + a_1pq^{n-1} + a_0q^n}{q^n}\right| \neq 0$$

por conseguinte

$$\left| f\left(\frac{p}{q}\right)\right| = \frac{|a_np^n + a_{n-1}qp^{n-1} + \cdots + a_1pq^{n-1} + a_0q^n|}{q^n} \geq \frac{1}{q^n} \tag{2.20}$$

uma vez que $|a_np^n + a_{n-1}qp^{n-1} + \cdots + a_1pq^{n-1} + a_0q^n| \in \mathbb{Z}^*$.

Usando (2.19) e (2.20) segue-se que

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

Logo,

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

ou seja,

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{Mq^n} > \frac{1}{(M+1)q^n}$$

para todo $\frac{p}{q} \in [\alpha - \delta, \alpha + \delta]$.

Se $\frac{p}{q}$ não estiver no intervalo $[\alpha - \delta, \alpha + \delta]$, então

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

pois, $q \geq 1$. Finalmente, tomando

$$\frac{1}{A} = \min\left\{\frac{1}{M+1}, \delta\right\}$$

Portanto, obtemos a relação desejada

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

para todo racional $\frac{p}{q}$. □

Observação 2.5. Uma versão mais forte do Teorema 2.5, segue de um teorema de *Roth-Siegel-Thue*, que estabelece o seguinte: *Seja λ um número algébrico, se existe uma infinidade de racionais distintos $\frac{p}{q}$, com $q > 0$ e $mdc(p, q) = 1$, satisfazendo à desigualdade*

$$\left|\lambda - \frac{p}{q}\right| \leq \frac{C}{q^\tau}$$

então $\tau \leq 2$. Segue daí que se $\omega > 2$, então há apenas um número finito de racionais $\frac{p}{q}$ satisfazendo à desigualdade

$$\left|\lambda - \frac{p}{q}\right| \leq \frac{C}{q^\omega}$$

para um dado número algébrico λ. E finalmente, uma consequência imediata disto é o seguinte resultado. *Sejam um número algébrico λ e um número $\epsilon > 0$, existe uma constante $C > 0$ tal que*

$$\left|\lambda - \frac{p}{q}\right| \geq \frac{C}{q^{2+\epsilon}}$$

para todo os números racionais $\frac{p}{q}$. Este impressionante resultado rendeu a medalha Fields para Roth em 1958. Para maiores detalhes, ver [5], p. 36 e ver [10], p. 88.

Corolário 2.1. *Se α é um número algébrico real de grau $n \in \mathbb{N}$, então α não é aproximável na ordem $n + 1$.*

Demonstração. Suponhamos por contradição, que α seja aproximável na ordem $n + 1$. Então existe uma constante $C > 0$ e uma sequência $(\frac{p_j}{q_j})_{j\geq 1}$ de racionais distintos, com $q_j > 0$ e $mdc(p_j, q_j) = 1$ tais que

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{C}{q_j^{n+1}} \tag{2.21}$$

para tais racionais. Assim, teríamos pelo Teorema de Liouville 2.5 e (2.21) que existe uma constante $A > 0$ tal que

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

multiplicando $Aq_j^{n+1} > 0$, obtemos $q_j < AC$. Mas isso é impossível, pois $q_j \to +\infty$ para todo $j \geq 1$. □

Observação 2.6. Compare o Corolário 2.1 acima com o Teorema 2.1. O corolário não diz que um número algébrico de grau n deva ser aproximável na ordem n.

2.3 Número de Liouville é Transcendente

Definição 2.3 (Número de Liouville)**.** *Um número real α é chamado um número de Liouville, se existe uma sequência de racionais $(\frac{p_j}{q_j})_{j\geq 1}$ distintos, com $q_j > 1$ e $mdc(p_j, q_j) = 1$ tal que*

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j} \tag{2.22}$$

para todo $j \geq 1$.

Em um certo sentido, os números de Liouville são números que podem ser "bem aproximados" tanto quanto se deseje por números racionais.

Corolário 2.2. *Todo número de Liouville é irracional.*

Demonstração. Suponhamos por contradição, que um número racional $\alpha = \frac{p}{q}$, com $q > 0$ é um número de Liouville. Então existem uma sequência de racionais $(\frac{p_j}{q_j})_{j\geq 1}$ distintos, com $q_j > 0$ e $\frac{p_j}{q_j} \neq \frac{p}{q}$, daí, $\frac{p}{q} - \frac{p_j}{q_j} \neq 0$ tais que

$$\left|\frac{p}{q} - \frac{p_j}{q_j}\right| < \frac{1}{q_j^j} \tag{2.23}$$

por outro lado, temos que

$$\left|\frac{p}{q} - \frac{p_j}{q_j}\right| = \left|\frac{pq_j - p_jq}{qq_j}\right| \geq \frac{1}{|q|q_j} \tag{2.24}$$

Combinando (2.23) e (2.24), temos

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

o que implica

$$\frac{1}{|q|q_j} < \frac{1}{q_j^j}$$

multiplicando por $|q|q_j^j$, obtemos

$$q_j^{j-1} < |q|$$

Mas isso é impossível, pois $q_j \to +\infty$ para j suficientemente grande. □

Agora, provaremos que todo número de Liouville é transcendente.

Teorema 2.6. *Todo número de Liouville é transcendente.*

Demonstração. Seja α número de Liouville, usando o Corolário 2.2, o número α não pode ser racional. Assim, suponhamos por contradição, que α é algébrico de grau $n > 1$. Então pelo Teorema de Liouville 2.5, segue-se que a relação:

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

será válida para todo racional. Em particular, para os racionais $\frac{p_j}{q_j}$ da definição de Número de Liouville 2.3. Dessa forma, teríamos

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

para alguma constante $A > 0$ e para todo $j \geq 1$. O que implica

$$\frac{1}{Aq_j^n} < \frac{1}{q_j^j}$$

multiplicando por $Aq_j^j > 0$, obtemos

$$q_j^{j-n} < A \tag{2.25}$$

Mas isso é impossível, pois $q_j \to +\infty$, segue que (2.25) não se verifica para j suficientemente grande. Logo, α não pode ser um número algébrico. Portanto, o número α é transcendente. □

Lema 2.2. *Seja α um número real tal que*

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

sendo $(\frac{v_j}{u_j})_{j\geq 1}$ uma sequência de racionais distintos, com $u_j > 0$. (Atenção: não exigimos que $mdc(v_j, u_j)$ seja 1.) *Então α é número de Liouville.*

Demonstração. Considerando uma sequência $(\frac{p_j}{q_j})_{j\geq 1}$, com $q_j > 0$ e $mdc(p_j, q_j) = 1$ definida por

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

Então,

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

para todo $j \geq 1$. O que mostra que α é um número de Liouville. □

Finalmente, vejamos o exemplo explícito do número transcendente que ficou conhecido como Constante de Liouville.

2.3.1 Constante de Liouville

Exemplo 2.2 (Constante de Liouville)**.** *O número ℓ é um número de Liouville, ou seja,*

$$\ell = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0,110001000000000000000001000\ldots$$

é um número transcendente.

De fato, como

$$\ell = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \cdots$$

Considerando as sequências de inteiros $p_j = \sum_{n=1}^{j} 10^{j!-n!}$ e $q_j = 10^{j!} > 0$. Assim, temos

$$\frac{p_j}{q_j} = \sum_{n=1}^{j} \frac{1}{10^{n!}}$$

Segue-se que

$$\left|\ell - \frac{p_j}{q_j}\right| = \left|\sum_{n=1}^{\infty} \frac{1}{10^{n!}} - \sum_{n=1}^{j} \frac{1}{10^{n!}}\right| = \sum_{n=j+1}^{\infty} \frac{1}{10^{n!}} = \frac{1}{10^{(j+1)!}} + \frac{1}{10^{(j+2)!}} + \frac{1}{10^{(j+3)!}} + \cdots$$

daí,

$$\left|\ell - \frac{p_j}{q_j}\right| = \frac{1}{10^{(j+1)!}} + \frac{1}{10^{(j+2)!}} + \frac{1}{10^{(j+3)!}} + \cdots = \frac{1}{10^{(j+1)!}} \left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + \frac{1}{10^{(j+3)!-(j+1)!}} + \cdots\right)$$

Note que,

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

uma vez que $(j+k)! - (j+1)! > k-1$, para $k \geq 2$.

De fato, note que

$$(j+1)![(j+k)\cdots(j+2) - 1] > k - 1$$

usando a famosa série geométrica, tem-se

$$\left|\ell - \frac{p_j}{q_j}\right| < \frac{1}{10^{(j+1)!}}\left(1 + \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + \cdots\right) = \frac{1}{10^{(j+1)!}}\left(\frac{1}{1-\frac{1}{10}}\right) = \frac{10}{9}\cdot\frac{1}{10^{(j+1)!}}$$

por conseguinte

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

ou seja,

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

para todo $j \geq 1$.
Portanto, o número ℓ é um número de Liouville. Como todo número de Liouville é transcendente. Logo, o número ℓ é transcendente.

Como aplicação da existência de números transcendentes, provaremos um resultado que caracteriza o espaço vetorial $\mathbb{R}$ como espaço de dimensão infinita sobre racionais.

Teorema 2.7. *O conjunto dos números reais $\mathbb{R}$ é um espaço vetorial de dimensão infinita sobre $\mathbb{Q}$.*

Demonstração. Seja t um número real transcendente. Então, o conjunto das potências positivas dos transcendentes, isto é,

$$\mathcal{T} = \{t^n; \quad n \in \mathbb{N}\} \subset \mathbb{R}$$

é linearmente independente (L.I.) e possui infinitos elementos. Suponhamos por contradição que o conjunto $\mathcal{T}$ fosse linearmente dependente (L.D.), então existiria $n_0 \in \mathbb{N}$ e escalares $\alpha_0, \ldots, \alpha_{n_0} \in \mathbb{Q}$ não todos nulos tais que

$$\alpha_0 + \alpha_1 t + \alpha_2 t^2 + \ldots + \alpha_{n_0} t^{n_0} = 0$$

Dessa forma, o número t seria raiz de um polinômio

$$P(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{n_0} x^{n_0}$$

não nulo com coeficientes racionais. Mas isso é uma contradição, uma vez que t é um número transcendente. Como a dimensão de um espaço vetorial se dá pelo número de vetores de uma de suas bases, e como uma base deve gerar todo espaço, em particular, deve gerar o conjunto $\mathcal{T}$. Portanto, o conjunto dos números reais $\mathbb{R}$ é um espaço vetorial de dimensão infinita sobre $\mathbb{Q}$. □

Podemos afirmar mais do que apenas a existência e a não enumerabilidade dos números transcendentes, podemos de fato, exibí-los. Além disso, percebemos que o teorema de Liouville caracteriza os números algébricos como aqueles que não admitem boas aproximações por números racionais, enquanto, os transcendentes de um certa forma são bem aproximados por racionais. O próximo capítulo será dedicado à transcendência do número e base dos logaritmos neperianos.

Capítulo 3

A Transcendência do Número e

Neste capítulo, apresentaremos a demonstração da Transcendência do Número e, resultado que foi um desafio aos matemáticos até o século XIX. Quando em 1873, o matemático Chales Hermite marcou época ao provar a transcendência do número e base dos logaritmos neperianos. As principais referências utilizadas na elaboração deste capítulo são, Figueiredo [5] e Herstein [7].

3.1 O Número e é Transcendente

Esta seção será dedicada a prova em detalhes da transcendência de e, baseada no método de Hermite o qual sofreu simplificações sucessivas por matemáticos famosos como Jordan (1882), Markhoff (1883), Rouché (1883), Weierstrass (1885), Hilbert (1893), Hurwitz (1893) e entre outros. A demonstração que apresentaremos a seguir é baseada na de Hurwitz. Vale ressaltar que, para saber se um dado número é transcendente, em geral, não é uma tarefa tão simples. Dessa forma, para tal prova vamos abordar uma série de lemas que serão necessários no decorrer da demonstração.

Lema 3.1. *Seja P(x) um polinômio arbitrário não nulo que será especificado posteriormente de grau $r \in \mathbb{N}$ com coeficientes inteiros. Defina a função*

$$F(x) = P(x) + P^{(1)}(x) + \ldots + P^{(r)}(x)$$

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

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

Demonstração. Com efeito, convém notar que

$$\begin{aligned}
\tfrac{d}{dx}\left[e^{-x}F(x)\right] &= \tfrac{d}{dx}\left[e^{-x}\left(P(x)+P^{(1)}(x)+\ldots+P^{(r)}(x)\right)\right] \\
&= -e^{-x}\left(P(x)+\ldots+P^{(r)}(x)\right)+e^{-x}\left(P(x)^{(1)}+P^{(2)}(x)+\ldots+P^{(r+1)}(x)\right) \\
&= e^{-x}\left(-P(x)-P^{(1)}(x)-\ldots-P^{(r)}(x)+P(x)^{(1)}+P^{(2)}(x)+\ldots+P^{(r+1)}(x)\right) \\
&= e^{-x}(-P(x)+\underbrace{P^{(r+1)}(x)}_{0}) \\
&= -e^{-x}P(x)
\end{aligned}$$

Levando-se em conta o cancelamento dos termos semelhantes acima e usando o fato de $P^{(r+1)}(x)=0$ (pois $P(x)$ tem grau r), obtemos a seguinte relação

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

em que será usada no lema a seguir. □

Lema 3.2. *Aplicando o teorema do valor médio a função $e^{-x}F(x)$. Mostre que*

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

Para todo número real $k>0$, onde $\theta_k \in (0,1)$.

Demonstração. Consideremos a seguinte aplicação

$$\begin{array}{rccl} H & : & [0,k] & \longrightarrow & \mathbb{R} \\ & & x & \longmapsto & H(x)=e^{-x}F(x) \end{array}$$

Note que para cada número real $k>0$, a aplicação H é contínua no intervalo $[0,k]$ e derivável no aberto $(0,k)$, já que $F(x)$ é a soma de polinômios e juntamente com a função exponencial e^{-x} são infinitamente deriváveis, daí, podemos afirmar que $e^{-x}F(x)$ é infinitamente derivável. Dessa forma, podemos aplicar o Teorema do Valor Médio (TVM) e usar o Lema 3.1, e assim, existe $c\in(0,k)$ tal que

$$H(k)-H(0)=H'(c)(k-0) \Longrightarrow e^{-k}F(k)-e^{-0}F(0)=\left[e^{-c}F(c)\right]'k$$

segue-se que

$$e^{-k}F(k)-F(0)=[e^{-c}F(c)]'k$$

por conseguinte,

$$e^{-k}F(k)-F(0) = -k\left(e^{-c}P(c)\right)$$

Convém observar que como $c\in(0,k)$, com $k>0$, podemos ter um número real

$\theta_k \in (0,1)$ que depende de k tal que

$$c = k.\theta_k$$

Substituindo $c = k\theta_k$ na expressão acima, tem-se

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

Multiplicando ambos membros da igualdade acima por e^k, obtemos

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

e denotando $A_k := F(k) - e^kF(0) = -k\left(e^{k(1-\theta_k)}P(k\theta_k)\right)$ com $k = 1, 2, \ldots, n$ para facilitar a notação, pois usaremos no lema a seguir e posteriormente estimaremos de uma certa forma o tamanho de $A_1, A_2, \ldots, A_n$. □

Lema 3.3. *Sejam $F(x)$ e $A_k = F(k) - e^kF(0)$ definidos nos Lemas 3.1 e 3.2, respectivamente. Suponha por contradição que o número e seja algébrico, ou seja, que satisfaz uma equação polinômial da forma*

$$c_ne^n + c_{n-1}e^{n-1} + \ldots + c_1e + c_0 = 0 \tag{3.1}$$

com coeficientes inteiros $c_0, c_1, \ldots, c_n$. Mostre a seguinte igualdade

$$c_0F(0) + c_1F(1) + \ldots + c_nF(n) = c_1A_1 + \ldots + c_nA_n \tag{3.2}$$

e que podemos tomar sem perda de generalidade $c_0 > 0$.

Demonstração. Note que caso c_0 fosse um inteiro negativo, $c_0 < 0$. Poderíamos considerar:
$(-c_n)e^n + \ldots + (-c_1)e + (-c_0) = 0$, tem-se $u_ne^n + \ldots + u_1e + u_0 = 0$ onde $u_i = (-c_i)$, para $i = 0, 1, \ldots, n \in \mathbb{N}$ e $u_0 = -c_0 > 0$. Seja $A_k = F(k) - e^kF(0)$, para $k = 1, 2, \ldots, n \in \mathbb{N}$, tem-se

$$\begin{aligned} c_1A_1 &= c_1F(1) - c_1e^1F(0) \\ c_2A_2 &= c_2F(2) - c_2e^2F(0) \\ \vdots \quad & \quad \vdots \quad \quad \vdots \\ c_nA_n &= c_nF(n) - c_ne^nF(0) \end{aligned}$$

Somando ambos membros de todas as igualdades acima, obtemos

$$c_1A_1 + \ldots + c_nA_n = c_1F(1) + \ldots + c_nF(n) + F(0)\left(-c_1e^1 - \ldots - c_ne^n\right)$$

Observe que da relação (3.1), tem-se $c_0 = -c_1e^1 - \ldots - c_ne^n$. Segue-se que

$$c_0F(0) + c_1F(1) + \ldots + c_nF(n) = c_1A_1 + \ldots + c_nA_n$$

o que mostra o resultado. □

Toda esta discussão foi feita para a $F(x)$ construída a partir de um polinômio arbitrário $P(x)$. Vejamos agora o que isto implica para um polinômio particular, usado pela primeira vez por Hermite, a saber:

$$P(x) = \frac{1}{(p-1)!}x^{p-1}\,(1-x)^p\,(2-x)^p\,(3-x)^p\cdots(n-x)^p$$

em que p é um número primo qualquer escolhido de modo que $p > n$ e $p > c_0$, cujo o grau de $P(x)$ é $(np + p - 1)$, sendo n e c_0 números dados no Lema 3.3 acima. Agora nosso objetivo é mostrar que o lado esquerdo da igualdade (3.2) do Lema 3.3 é um número inteiro não nulo e não divisível por p, enquanto o lado direito da igualdade tem módulo menor que 1, caracterizando a contradição. Assim, para mostrar o lado esquerdo de tal igualdade usaremos os Lemas 3.4, 3.5, 3.6, 3.7 e 3.8. Já para o lado direito usaremos os Lemas 3.9 e 3.10 os quais serão todos demonstrados a seguir:

Lema 3.4. *Seja $Q(x) = \sum_{j=0}^{r} a_jx^j$ um polinômio não nulo arbitrário com coeficientes inteiros a_j, sendo $j = 0, 1, \ldots, r \in \mathbb{N}$ e $p < r$. Então mostre os seguintes itens:*

(i) $\quad Q^{(i)}(x) = \displaystyle\sum_{j=i}^{r} \frac{j!}{(j-i)!}a_jx^{j-i}, \quad$ *para* $\quad i \leq r \quad$ *e* $\quad i \leq j;$

(ii) $\quad \dfrac{1}{(p-1)!}Q^{(i)}(x), \quad$ *para* $\quad i \geq p \quad$ *e* $\quad i \in \mathbb{N}$

é um polinômio com coeficientes inteiros divisíveis pelo número primo p.

Demonstração. **Item (i).** Mostraremos por indução sobre $k \in \mathbb{N}$ a expressão para $Q^{(i)}(x)$, porém, façamos alguns casos particulares para facilitar o entendimento. Para $r = 4$, tem-se

$$Q(x) = \sum_{j=0}^{4} a_jx^j = a_0x^0 + a_1x^1 + a_2x^2 + a_3x^3 + a_4x^4 \tag{3.3}$$

Vejamos as derivadas de ordem 1 à 4 de $Q(x)$:

$$\begin{aligned}
Q^{(1)}(x) &= 1a_1x^{1-1} + 2a_2x^{2-1} + 3a_3x^{3-1} + 4a_4x^{4-1}\\
Q^{(2)}(x) &= (2-1)2a_2x^{2-2} + (3-1)3a_3x^{3-2} + (4-1)4a_4x^{4-2}\\
Q^{(3)}(x) &= (3-2)(3-1)3a_3x^{3-3} + (4-2)(4-1)4a_4x^{4-3}\\
Q^{(4)}(x) &= (4-3)(4-2)(4-1)4a_4x^{4-4}
\end{aligned}$$

Por outro lado, observe que para $i = 1$ e $j = 1, 2, \ldots, 4$, tem-se

$$\begin{aligned}\sum_{j=1}^{4} \frac{j!}{(j-1)!} a_j x^{j-1} &= \frac{1!}{(1-1)!} a_1 x^{1-1} + \frac{2!}{(2-1)!} a_2 x^{2-1} + \frac{3!}{(3-1)!} a_3 x^{3-1} + \frac{4!}{(4-1)!} a_4 x^{4-1} \\ &= 1a_1 x^{1-1} + 2a_2 x^{2-1} + 3a_3 x^{3-1} + 4a_4 x^{4-1} \\ &= Q^{(1)}(x)\end{aligned}$$

Note ainda que para $i = 2$ e $j = 2, 3, 4$, tem-se

$$\begin{aligned}\sum_{j=2}^{4} \frac{j!}{(j-2)!} a_j x^{j-2} &= \frac{2!}{(2-2)!} a_2 x^{2-2} + \frac{3!}{(3-2)!} a_3 x^{3-2} + \frac{4!}{(4-2)!} a_4 x^{4-2} \\ &= \frac{2(2-1)}{0!} a_2 x^{2-2} + \frac{3(3-1)(3-2)!}{(3-2)!} a_3 x^{3-2} + \frac{4(4-1)(4-2)!}{(4-2)!} a_4 x^{4-2} \\ &= 2(2-1)a_2 x^{2-2} + 3(3-1)a_3 x^{3-2} + 4(4-1)a_4 x^{4-2} \\ &= Q^{(2)}(x)\end{aligned}$$

Analogamente, para $i = 3$ e $j = 3, 4$, tem-se

$$Q^{(3)}(x) = \sum_{j=3}^{4} \frac{j!}{(j-3)!} a_j x^{j-3}$$

e para $i = 4$ e $j = 4$, tem-se

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

Agora vamos a demonstração, verifiquemos que $Q^{(i)}(x)$ é válida para $i = 1$. De fato,

$$\begin{aligned}Q^{(1)}(x) &= [Q(x)]' \\ &= \left[\sum_{j=0}^{r} a_j x^j\right]' \\ &= [a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots + a_r x^r]' \\ &= 1a_1 x^{1-1} + 2a_2 x^{2-1} + \ldots + r a_r x^{r-1} \\ &= \frac{1!}{(1-1)!} a_1 x^{1-1} + \frac{2!}{(2-1)!} a_2 x^{2-1} + \ldots + \frac{r!}{(r-1)!} a_r x^{r-1} \\ &= \sum_{j=1}^{r} \frac{j!}{(j-1)!} a_j x^{j-1}\end{aligned}$$

Logo, $Q^{(1)}(x)$ é válida.
Suponha que $Q^{(k)}(x)$ seja válida por hipótese de indução para um certo $k \in \mathbb{N}$, isto é,

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

Provaremos que

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

é válida para $k+1$. De fato,

$$\begin{aligned}
Q^{(k+1)}(x) = & \left[Q(x)^{(k)}\right]' \\
= & \left[\sum_{j=k}^{r} \frac{j!}{(j-k)!} a_j x^{j-k}\right]' \\
= & \left[\frac{k!}{(k-k)!} a_k x^{k-k} + \frac{(k+1)!}{((k+1)-k)!} a_{k+1} x^{(k+1)-k} + \ldots + \frac{r!}{(r-k)!} a_r x^{r-k}\right]' \\
= & (k+1-k)\cdot \frac{(k+1)!}{((k+1)-k)!} a_{k+1} x^{(k+1)-k-1} + \ldots + (r-k)\cdot \frac{r!}{(r-k)!} a_r x^{r-k-1} \\
= & \frac{(k+1)!}{((k+1)-k)!} a_{k+1} x^{(k+1)-k-1} + \ldots + (r-k)\cdot \frac{r!}{(r-k)\,(r-k-1))!} a_r x^{r-k-1} \\
= & \frac{(k+1)!}{((k+1)-(k+1))!} a_{k+1} x^{((k+1)-(k+1))} + \ldots + \frac{r!}{(r-(k+1))!} a_r x^{(r-(k+1))} \\
= & \sum_{j=k+1}^{r} \frac{j!}{(j-(k+1))!} a_j x^{j-(k+1)}
\end{aligned}$$

Pois, note que escrevemos:

$$\frac{(k+1)!}{((k+1)-k)!} = \frac{(k+1)!}{1!} = \frac{(k+1)!}{0!} = \frac{(k+1)!}{((k+1)-(k+1))!}$$

Portanto, pelo princípio de indução finita é válida a expressão para $Q^{(i)}(x)$, isto é,

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

□

Demonstração. **Item (ii).** Com efeito, substituindo a expressão da $Q^{(i)}(x)$, tem-se

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

Assim, o polinômio acima possui cada coeficiente dado por:

$$b_j := a_j \frac{j!}{(j-i)!(p-1)!}$$

com $i \leq j$, $p < r$ e $i \geq p$. É suficiente mostrar que cada b_j é um número inteiro divisível

por p, isto é, existe $q \in \mathbb{Z}$ tal que $b_j = pq$. Observe que

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

Mas, note que

$$\frac{j!}{(j-i)!\,i!} = \begin{pmatrix} j \\ i \end{pmatrix}$$

é um coeficiente do desenvolvimento Binomial de uma dada expressão, sendo assim, um número inteiro, digamos, $u := \dfrac{j!}{(j-i)!\,i!} \in \mathbb{Z}$. Para $i \geq p$, podemos escrever:

$$\begin{aligned} \frac{j!}{(j-i)!(p-1)!} &= \frac{j!}{(j-i)!\,i!} \cdot \frac{i!}{(p-1)!} \\ &= u \cdot \frac{i}{(p-1)!} \\ &= \frac{u.i(i-1)(i-2)\cdots(p+1)p(p-1)!}{(p-1)!} \\ &= u.i(i-1)(i-2)\cdots(p+1)p \end{aligned}$$

Como $a_j \in \mathbb{Z}$, por hipótese, para $j = i, \ldots, r \in \mathbb{N}$. Segue-se

$$b_j := a_j \frac{j!}{(j-i)!(p-1)!} = a_j.u.i(i-1)(i-2)\cdots(p+1)p \in \mathbb{Z}$$

o qual é um número inteiro. Além disso,

$$b_j := a_j \frac{j!}{(j-i)!(p-1)!} = pq$$

onde $q := a_j.u.i(i-1)(i-2)\cdots(p+1) \in \mathbb{Z}$, isto é, $b_j = pq \in \mathbb{Z}$. Portanto, a expressão

$$\begin{aligned} \frac{1}{(p-1)!}Q^{(i)}(x) &= \sum_{j=i}^{r} a_j \frac{j!}{(j-i)!(p-1)!} x^{j-i} \\ &= \sum_{j=i}^{r} b_j x^{j-i} \\ &= \sum_{j=i}^{r} pqx^{j-i} \end{aligned}$$

é um polinômio com coeficientes inteiros divisíveis por p. □

Lema 3.5. *Considere o polinômio*

$$P(x) = \frac{1}{(p-1)!} x^{p-1} (1-x)^p (2-x)^p (3-x)^p \cdots (n-x)^p$$

definido em $F(x)$, sendo $p > n$ e $p > c_0$. Então mostre os seguintes itens:

$(i)\quad P(x) = \dfrac{(n!)^p}{(p-1)!}x^{p-1} + \dfrac{b_0}{(p-1)!}x^p + \cdots + \dfrac{b_{np-1}}{(p-1)!}x^{np+p-1},$

$(ii)\quad P^{(i)}(k) = 0, \quad para \quad k = 1, \ldots, n \in \mathbb{N}, \quad Se \quad i < p,$

$(iii)\quad P^{(p-1)}(0) = (n!)^p \quad e \quad P^{(i)}(0) = 0, \quad Se \quad i < p-1.$

Demonstração. **Item (i).** Aplicando a fórmula do desenvolvimento Binomial de Newton:

$$(a-x)^n = \sum_{j=0}^{n} \binom{n}{j} a^{n-j}(-x)^j = \sum_{j=0}^{n} \frac{n!}{j!(n-j)!} a^{n-j}(-x)^j, \quad \text{com} \quad n \geq j \in \mathbb{Z},$$

aos números

$$(1-x)^p, (2-x)^p, (3-x)^p \ldots, (n-x)^p$$

fatores do polinômio $P(x)$, sendo p número primo escolhido de modo que $p > n$ e $p > c_0$, sendo $\binom{n}{j} = \dfrac{n!}{j!(n-j)!} = \dfrac{n(n-1)(n-2)\cdots(n-j+1)}{j!}$, tem-se:

$$(1-x)^p = \sum_{j=0}^{p} \frac{p!}{j!(p-j)!} 1^{p-j}(-x)^j = \left(1^p + p1^{p-1}(-x) + \sum_{j=2}^{p} \frac{p!}{j!(p-j)!} 1^{p-j}(-x)^j\right);$$

$$(2-x)^p = \sum_{j=0}^{p} \frac{p!}{j!(p-j)!} 2^{p-j}(-x)^j = \left(2^p + p2^{p-1}(-x) + \sum_{j=2}^{p} \frac{p!}{j!(p-j)!} 2^{p-j}(-x)^j\right);$$

$$(3-x)^p = \sum_{j=0}^{p} \frac{p!}{j!(p-j)!} 3^{p-j}(-x)^j = \left(3^p + p3^{p-1}(-x) + \sum_{j=2}^{p} \frac{p!}{j!(p-j)!} 3^{p-j}(-x)^j\right);$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$(n-x)^p = \sum_{j=0}^{p} \frac{p!}{j!(p-j)!} n^{p-j}(-x)^j = \left(n^p + pn^{p-1}(-x) + \sum_{j=2}^{p} \frac{p!}{j!(p-j)!} n^{p-j}(-x)^j\right).$$

das expressões acima, segue-se que

$$\begin{aligned}
P(x) &= \frac{x^{p-1}}{(p-1)!}\Big(1-x\Big)^p\Big(2-x\Big)^p\Big(3-x\Big)^p\cdots\Big(n-x\Big)^p \\
&= \frac{x^{p-1}}{(p-1)!}\Big(1^p + p1^{p-1}(-x) + \sum_{j=2}^{p}\frac{p!}{j!(p-j)!}1^{p-j}(-x)^j\Big)\cdots\Big(n^p + pn^{p-1}(-x) + \sum_{j=2}^{p}\frac{p!}{j!(p-j)!}n^{p-j}(-x)^j\Big) \\
&= \frac{x^{p-1}}{(p-1)!}\Big(1^p.2^p\cdots n^p - 1^p p2^{p-1}x - 1^p p3^{p-1}x - \ldots - 1^p pn^{p-1}x + \Big(\text{Parcelas com variável } x\Big)\Big) \\
&= \frac{x^{p-1}}{(p-1)!}\Big(\big(\,n!\,\big)^p + x\Big(-p2^{p-1} - p3^{p-1} - \ldots - pn^{p-1}\Big) + \Big(\text{Parcelas com variável } x\Big)\Big)
\end{aligned}$$

Daí, tem-se que $P(x)$ é da forma

$$P(x) = \frac{x^{p-1}}{(p-1)!}\Big(\big(\,n!\,\big)^p + xb_0 + \ldots\Big) = \frac{(n!)^p}{(p-1)!}x^{p-1} + \frac{b_0}{(p-1)!}x^p + \cdots + \frac{b_{np-1}}{(p-1)!}x^{np+p-1}$$

onde $b_0 = (-p2^{p-1} - p3^{p-1} - \ldots - pn^{p-1}), b_1, \ldots, b_{np-1} \in \mathbb{Z}$. □

Demonstração. **Item (ii).** Basta observar que para $k = 1, 2, 3, \ldots, n \in \mathbb{N}$ são raízes de multiplicidade p do polinômio

$$P(x) = \frac{1}{(p-1)!}x^{p-1}\,(1-x)^p\,(2-x)^p\,(3-x)^p\cdots(n-x)^p$$

Como o grau de $P(x)$ é maior que p, tem-se que $k = 1, 2, 3, \ldots, n$ são raízes das derivadas de $P(x)$ de ordens menores que p, isto é,

$$P^{(0)}(k) = P^{(1)}(k) = P^{(2)}(k) = \cdots = P^{(p-1)}(k) = 0$$

sendo $i < p$. Com efeito, como $n \geq k$, podemos escrever:

$$\begin{aligned}
P(x) &= \frac{x^{p-1}}{(p-1)!}(1-x)^p\cdots(k-1-x)^p(k-x)^p(k+1-x)^p\cdots(n-x)^p \\
&= \frac{x^{p-1}}{(p-1)!}\Big((1-x)^p\cdots(k-1-x)^p(k+1-x)^p\cdots(n-x)^p\Big)(k-x)^p \\
&= (k-x)^p g(x)
\end{aligned}$$

onde $g(x) = \dfrac{x^{p-1}}{(p-1)!}\big((1-x)^p\cdots(k-1-x)^p(k+1-x)^p\cdots(n-x)^p\big)$. Assim, derivando $P(x)$, tem-se

$$\begin{aligned}
P^{(1)}(x) &= -p(k-x)^{p-1}g(x) + (k-x)^p g'(x) \\
&= (k-x)^{p-1}\big(-pg(x) + (k-x)g'(x)\big) \\
&= (k-x)^{p-1}g_1(x)
\end{aligned}$$

onde $g_1(x) = \big(-pg(x) + (k-x)g'(x)\big)$. Por sua vez, derivando $P^{(1)}(x)$, tem-se

$$\begin{aligned} P^{(2)}(x) &= -(p-1)(k-x)^{p-2}g_1(x) + (k-x)^{p-1}g_1'(x) \\ &= (k-x)^{p-2}\big(-(p-1)g_1(x) + (k-x)g_1'(x)\big) \\ &= (k-x)^{p-2}g_2(x) \end{aligned}$$

onde $g_2(x) = \big(-(p-1)g_1(x) + (k-x)g_1'(x)\big)$. Prosseguindo dessa forma, generalizando as derivações, teremos:

$$P^{(i)}(x) = (k-x)^{p-i}g_i(x)$$

Portanto, segue-se que $P^{(i)}(k) = 0$, para $k = 1, 2, \ldots, n \in \mathbb{N}$, se $i < p$. □

Demonstração. **Item (iii).** Tomando as derivadas de ordem 1 à $(p+1)$ do polinômio

$$P(x) = \frac{(n!)^p}{(p-1)!}x^{p-1} + \frac{b_0}{(p-1)!}x^p + \frac{b_1}{(p-1)!}x^{p+1} + \ldots + \frac{b_{np-1}}{(p-1)!}x^{np+p-1}$$

Teremos:

$$P^{(1)}(x) = (p-1)\frac{(n!)^p x^{(p-2)}}{(p-1)!} + p\frac{b_0 x^{(p-1)}}{(p-1)!} + (p+1)\frac{b_1 x^p}{(p-1)!} + \big(\text{Parcelas com variável } x\big)$$

$$P^{(2)}(x) = (p-2)(p-1)\frac{(n!)^p x^{(p-3)}}{(p-1)!} + (p-1)p\frac{b_0 x^{(p-2)}}{(p-1)!} + p(p+1)\frac{b_1 x^{(p-1)}}{(p-1)!} + \big(\text{P. V. } x\big)$$

$$P^{(3)}(x) = (p-3)(p-2)(p-1)\frac{(n!)^p x^{(p-4)}}{(p-1)!} + (p-2)(p-1)p\frac{b_0 x^{(p-3)}}{(p-1)!} + (p-1)p(p+1)\frac{b_1 x^{(p-2)}}{(p-1)!} + (\text{P. V. } x)$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$P^{(i)}(x) = (p-i)(p-(i-1))\cdots(p-1)\frac{(n!)^p x^{(p-(i+1))}}{(p-1)!} + (p-(i-1))(p-(i-2))\cdots p\frac{b_0 x^{(p-i)}}{(p-1)!} + \big(\text{P. V. } x\big)$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$P^{(p-1)}(x) = (p-(p-1))(p-(p-2))\cdots(p-1)\frac{(n!)^p x^{(p-p)}}{(p-1)!} + (p-(p-2))(p-(p-3))\cdots p\frac{b_0 x^{(p-(p-1))}}{(p-1)!} + \big(\text{P. V. } x\big)$$

$$P^{(p)}(x) = \underbrace{(p-p)}_{0}(p-(p-1))\cdots(p-1)\frac{(n!)^p x^{(p-(p+1))}}{(p-1)!} + (p-(p-1))(p-(p-2))\cdots p\frac{b_0 x^{\overbrace{(p-p)}^{0}}}{(p-1)!} + \big(\text{P. V. } x\big)$$

$$P^{(p+1)}(x) = \underbrace{(p-p)}_{0}(p-(p-1))(p-(p-2))\cdots p\frac{b_0 x^{(p-(p+1))}}{(p-1)!} + (p-(p-1))\cdots p(p+1)\frac{b_1 x^{\overbrace{(p-p)}^{0}}}{(p-1)!} + \big(\text{P. V. } x\big)$$

Note que denotamos (P. V. x) para indicar que existem mais Parcelas com variável x

nas expressões acima. Agora mostraremos que

$$P^{(p-1)}(0) = (n!)^p \quad \text{e} \quad P^{(i)}(0) = 0, \quad \text{Se} \quad i < p-1.$$

Então da expressão da $P^{(p-1)}(x)$, tem-se:

$$\begin{aligned} P^{(p-1)}(x) &= (p-(p-1))(p-(p-2))\cdots(p-1)\frac{(n!)^p x^{(p-p)}}{(p-1)!} + (p-(p-2))\cdots p\frac{b_0 x^{(p-(p-1))}}{(p-1)!} + \big(\text{P. V. } x\big) \\ &= 1.2.3\cdots(p-3)(p-2)(p-1)\frac{(n!)^p x^0}{(p-1)!} + 1.2.3\cdots(p-2)(p-1)p\frac{b_0 x^1}{(p-1)!} + \big(\text{P. V. } x\big) \\ &= (p-1)!\frac{(n!)^p}{(p-1)!} + (p-1)!p\frac{b_0 x}{(p-1)!} + \big(\text{P. V. } x\big) \\ &= \big(n!\big)^p + pb_0 x + \big(\text{P. V. } x\big) \end{aligned}$$

Segue-se que $P^{(p-1)}(x) = (n!)^p + pb_0x + \big(\text{Parcelas com variável } x\big)$ e aplicando $x = 0$, por conseguinte, $P^{(p-1)}(0) = (n!)^p + pb_0.0 + \big(\text{Parcelas com } x = 0\big) = (n!)^p$.

Logo, concluímos que $P^{(p-1)}(0) = (n!)^p$. Analogamente, tem-se

$$P^{(i)}(0) = 0$$

pois, observe que da expressão da $P^{(i)}(x)$ feita acima, todas as parcelas possuem a variável x. Portanto, aplicando $x = 0$, consequentemente, tem-se que $P^{(i)}(0) = 0$, se $i < p-1$. □

Lema 3.6. *Se d_i são inteiros tais que, para $i = 1, 2, \ldots, r \in \mathbb{N}$, são divisíveis por $p \in \mathbb{Z}$, e para $i = 0$, d_0 é um inteiro não divisível por p. Então $\sum_{i=0}^{r} d_i = d_0 + d_1 + \ldots + d_r$ é um inteiro não divisível por p.*

Demonstração. Suponhamos, por contradição, que $\sum_{i=0}^{r} d_i = d_0 + d_1 + \ldots + d_r$ seja um inteiro divisível por p. Então existe $q \in \mathbb{Z}$ tal que

$$\sum_{i=0}^{r} d_i = pq$$

Como por hipótese, cada d_i é um inteiro divisível por p, para $i = 1, 2, \ldots, r \in \mathbb{N}$. Então existem $q_i \in \mathbb{Z}$ tais que

$$d_i = pq_i, \quad \text{para} \quad i = 1, 2, \ldots, r \in \mathbb{N}$$

Segue-se que

$$pq = \sum_{i=0}^{r} d_i = d_0 + d_1 + \ldots + d_r = d_0 + pq_1 + \ldots + pq_r = d_0 + p(q_1 + \ldots + q_r)$$

daí, tem-se

$$pq = d_0 + p(q_1 + \ldots + q_r), \quad \text{onde} \quad (q_1 + \ldots + q_r) \in \mathbb{Z}$$

por conseguinte,

$$d_0 = pq - p(q_1 + \ldots + q_r) = p\big(q - (q_1 + \ldots + q_r)\big) = pM$$

Logo, $d_0 = pM$ onde $M := (q - (q_1 + \ldots + q_r)\big) \in \mathbb{Z}$, daí, teríamos que d_0 seria divisível por p, o que uma contradição, pois por hipótese, d_0 é um inteiro não divisível por p. Portanto, $\sum_{i=0}^{r} d_i = d_0 + d_1 + \ldots + d_r$ é um inteiro não divisível por p. □

Lema 3.7. *Mostre que $F(k)$ para $k = 1, 2, \ldots, n \in \mathbb{N}$ é inteiro divisível por p. Por outro lado, $F(0)$ é um inteiro não divisível por p, sendo número primo $p > n$.*

Demonstração. Considere a função

$$F(k) = P(k) + P^{(1)}(k) + \ldots + P^{(p-1)}(k) + P^{(p)}(k) + P^{(p+1)}(k) + \ldots + P^{(np+p-1)}(k)$$

para $k = 1, 2, \ldots, n \in \mathbb{N}$ onde $(np + p - 1)$ é o grau do polinômio $P(x)$ definido no Lema 3.5. Usaremos os seguintes fatos já provados:
Pelo Lema 3.5, item (ii), temos que

$$P^{(i)}(k) = 0, \quad \text{para} \quad k = 1, \ldots, n \in \mathbb{N}, \quad \text{Se} \quad i < p;$$

Pelo Lema 3.4, itens (i) e (ii), tem-se que da expressão da $P^{(i)}(x)$ para $i \geq p$, pode ser escrito na forma $\dfrac{1}{(p-1)!}Q^{(i)}(x)$, como um polinômio com coeficientes inteiros divisível por p, para $i \geq p$, sendo $Q^{(i)}(x)$ definido conforme tal Lema. Assim, tem-se que

$$P^{(i)}(k) \ \text{ é um inteiro divisível por } p, \text{ para } i \geq p \ \text{ e } \ k = 1, \ldots, n \in \mathbb{N}.$$

Dos fatos acima, segue-se que

$$F(k) = \underbrace{P(k) + P^{(1)}(k) + \ldots + P^{(p-1)}(k)}_{0} + \underbrace{P^{(p)}(k) + P^{(p+1)}(k) + \ldots + P^{(np+p-1)}(k)}_{\text{inteiro divisível por } p}$$

Portanto, tem-se que $F(k)$ é um inteiro divisível por p, isto é,

$$p | F(k), \quad \text{para} \quad k = 1, \ldots, n \in \mathbb{N}.$$

Por outro lado, mostraremos que $F(0)$ é um inteiro não divisível por p, sendo $p > n$.

Com efeito, seja

$$F(0) = P(0)+P^{(1)}(0)+\ldots+P^{(p-2)}(0)+P^{(p-1)}(0)+P^{(p)}(0)+P^{(p+1)}(0)+\ldots+P^{(np+p-1)}(0)$$

Usaremos outros fatos já demonstrados:
Pelo Lema 3.5, item (iii), temos

$$P^{(p-1)}(0) = (n!)^p \quad \text{e} \quad P^{(i)}(0) = 0, \quad \text{Se} \quad i < p-1;$$

Além disso, note que pelas expressões das derivadas de $P^{(p)}(x)$ e $P^{(p+1)}(x)$ do polinômio

$$P(x) = \frac{(n!)^p}{(p-1)!}x^{p-1} + \frac{b_0}{(p-1)!}x^p + \frac{b_1}{(p-1)!}x^{p+1} + \cdots + \frac{b_{np-1}}{(p-1)!}x^{(np+p-1)}$$

visto na demonstração do Lema 3.5, item (iii), onde $b_0, b_1, \ldots, b_{np-1} \in \mathbb{Z}$. Temos que

$$P^{(p)}(x) = (p-(p-1))(p-(p-2))\cdots p\frac{b_0}{(p-1)!} + (p-(p-2))\cdots p(p+1)\frac{b_1x^{(p-(p-1))}}{(p-1)!} + \big(\text{P. V. } x\big)$$

$$P^{(p+1)}(x) = (p-(p-1))(p-(p-2))\cdots p(p+1)\frac{b_1\overbrace{x^{(p-(p-1)-1)}}^{0}}{(p-1)!} + \big(\text{P. V. } x\big)$$

Dessa forma, aplicando $x = 0$, para $P^{(p)}(x)$, $P^{(p+1)}(x)$, $P^{(p+2)}(x), \ldots, P^{(p+np-1)}(x)$, tem-se

$$\begin{aligned} P^{(p)}(0) &= (p-(p-1))(p-(p-2))\cdots p\frac{b_0}{(p-1)!} + \big(\text{Parcelas com } x=0\big) \\ &= p!\frac{b_0}{(p-1)!} \end{aligned}$$

$$\begin{aligned} P^{(p+1)}(0) &= (p-(p-1))(p-(p-2))\cdots p(p+1)\frac{b_1}{(p-1)!} + \big(\text{Parcelas com } x=0\big) \\ &= (p+1)!\frac{b_1}{(p-1)!} \end{aligned}$$

$$\begin{aligned} P^{(p+2)}(0) &= (p-(p-1))(p-(p-2))\cdots p(p+1)(p+2)\frac{b_2}{(p-1)!} + \big(\text{Parcelas com } x=0\big) \\ &= (p+2)!\frac{b_2}{(p-1)!} \end{aligned}$$

$$\begin{array}{cccccc} \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

$$\begin{aligned} P^{(p+np-1)}(0) &= (p-(p-1))(p-(p-2))\cdots p(p+1)(p+2)\cdots(p+np-1)\frac{b_{np-1}}{(p-1)!} + \big(\text{P. com } x=0\big) \\ &= (p+np-1)!\frac{b_{np-1}}{(p-1)!} \end{aligned}$$

Consequentemente, generalizando as expressões acima, ou seja, derivando i vezes o

polinômio $P(x)$, considerando $i = p + j$, para $j = 0, 1, \ldots, np - 1 \in \mathbb{N}$ e aplicando $x = 0$, teremos:

$$P^{(p+j)}(0) = \frac{(p+j)!}{(p-1)!} b_j, \text{ que é um inteiro divisível por } p.$$

Segue-se dos fatos acima que:

$$\begin{aligned} F(0) &= \underbrace{P(0) + P^{(1)}(0) + \ldots + P^{(p-2)}(0)}_{0} + \underbrace{P^{(p-1)}(0)}_{(n!)^p} + P^{(p)}(0) + P^{(p+1)}(0) + \ldots + P^{(np+p-1)}(0) \\ &= (n!)^p + P^{(p)}(0) + P^{(p+1)}(0) + \ldots + P^{(np+p-1)}(0) \\ &= \underbrace{(n!)^p}_{\text{inteiro não divisível por } p} + \underbrace{\frac{p!b_0}{(p-1)!} + \frac{(p+1)!b_1}{(p-1)!} + \ldots + \frac{(p+np-1)!b_{np-1}}{(p-1)!}}_{\text{inteiro divisível por } p} \end{aligned}$$

Logo, $F(0)$ é um inteiro não divisível por p, pois, caso contrário, pelo Lema 3.6, teríamos que $(n!)^p$ também seria divisível por p, mas note que $(n!)^p = 1^p 2^p \cdots (n-1)^p n^p$, observe que nenhum termo deste produto é divisível por p, digamos, se n^p o fosse, assim, existiria $V \in \mathbb{Z}$ tal que

$$n^p = pV \Longrightarrow \underbrace{n.n \cdots n}_{p-fatores} = pV \Longrightarrow V = \frac{n.n \cdots n}{p}$$

Daí, teríamos que p dividiria n, isto é,

$$p | n$$

Contradição, pois o número primo $p > n$, como $p > n > n - 1 > \cdots > 2 > 1$, usando o mesmo argumento para cada termo do produto $(1^p 2^p \cdots (n-1)^p n^p)$, obtemos que $(n!)^p$ não é divisível por p. Portanto, podemos concluir que $F(0)$ é um inteiro não divisível por p, isto é, $p \nmid F(0)$. □

Lema 3.8. *Como o número primo $p > c_0 > 0$, em que c_0 é um inteiro positivo, assim definido no Lema 3.3, sendo $c_k \in \mathbb{Z}$, com $k = 0, 1, 2, \ldots, n \in \mathbb{N}$. Mostre que*

$$c_0 F(0) + c_1 F(1) + \cdots + c_n F(n)$$

é um inteiro não divisível por p.

Demonstração. Pelo o Lema 3.7, obtemos que $F(k)$, para $k = 1, 2, \ldots, n \in \mathbb{N}$, é um inteiro divisível por p. Por outro lado, $F(0)$ é um inteiro não divisível por p. Segue-se

que, sendo $c_k \in \mathbb{Z}$ para $k = 1, 2, \ldots, n \in \mathbb{N}$ e denotando:

$$d_k := c_k F(k)$$

é um inteiro divisível por p. Além disso, para $k = 0$, sendo c_0 um inteiro positivo e denotando:

$$d_0 := c_0 F(0)$$

é um inteiro não divisível por p, já que o número primo $p > c_0 > 0$. Segue-se que

$$\sum_{k=0}^{n} d_k = d_0 + d_1 + \ldots + d_n \;=\; \underbrace{c_0 F(0)}_{\text{inteiro não divisível por } p} \;+\; \underbrace{c_1 F(1) \,+\, \ldots \,+\, c_n F(n)}_{\text{inteiro divisível por } p}$$

Logo, pelo Lema 3.6, tem-se que $\displaystyle\sum_{k=0}^{n} d_k$ é um inteiro não divisível por p. Portanto, a expressão $c_0 F(0) + c_1 F(1) + \cdots + c_n F(n)$ é um inteiro não divisível por p, isto é, $p \nmid (c_0 F(0) + c_1 F(1) + \cdots + c_n F(n))$. □

Lema 3.9. *Convém observar que para os* $A_k = -k\left(e^{k(1-\theta_k)} P(k\theta_k)\right)$ *definidos no Lema 3.2, substituindo* $x = k\theta_k$ *no polinômio*

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

tem-se a seguinte forma:

$$A_k = -k e^{k(1-\theta_k)} \frac{1}{(p-1)!} (k\theta_k)^{p-1} (1-k\theta_k)^p (2-k\theta_k)^p \cdots (n-k\theta_k)^p$$

onde $\theta_k \in (0,1)$. *Mostre que*

$$|A_k| \;\leq\; \frac{e^n n^p (n!)^p}{(p-1)!}$$

para $k \leq n$, *onde* p *é primo e* $k > 0$ *é considerado um natural positivo.*

Demonstração. Com efeito, se $0 < k \leq n \in \mathbb{N}$ e $0 < \theta_k < 1$. Passando o módulo em

A_k, obtemos

$$\begin{aligned}
|A_k| &= \left| -ke^{k(1-\theta_k)} \frac{1}{(p-1)!} (k\theta_k)^{p-1} (1-k\theta_k)^p (2-k\theta_k)^p \cdots (n-k\theta_k)^p \right| \\
&= \frac{1}{(p-1)!} |-k| . |e^{k(1-\theta_k)}| . |(k\theta_k)^{p-1}| . | (1-k\theta_k)^p | . | (2-k\theta_k)^p | \cdots | (n-k\theta_k)^p | \\
&\leq \frac{1}{(p-1)!} n e^n n^{p-1} |1-n\theta_k|^p |2-n\theta_k|^p \cdots |n-k\theta_k|^p \\
&\leq \frac{1}{(p-1)!} n e^n n^{p-1} 1^p 2^p \cdots n^p \\
&\leq \frac{1}{(p-1)!} n e^n n^p \frac{1}{n} (12 \cdots n)^p \\
&\leq \frac{e^n n^p (n!)^p}{(p-1)!}
\end{aligned}$$

Pois, note que, como $k \leq n$ e $0 < \theta_k < 1$, temos:

• Se $k \leq n$, multiplicando por $(1-\theta_k)$, segue-se

$$k(1-\theta_k) \leq n(1-\theta_k) \leq n \Longrightarrow e^{k(1-\theta_k)} \leq e^n$$

• Como $k^{p-1} \leq n^{p-1}$ e $\theta_k^{p-1} \leq 1$, multiplicando $\theta_k^{p-1} \leq 1$ por k^{p-1}, segue-se

$$k^{p-1}\theta_k^{p-1} \leq k^{p-1} \Longrightarrow (k\theta_k)^{p-1} \leq n^{p-1}$$

• Como $|1-\theta_k|^p |2-\theta_k|^p \ldots |n-\theta_k|^p \leq 1^p 2^p \ldots n^p = (12 \ldots n)^p = (n!)^p$.

Portanto, obtemos que $|A_k| \leq \dfrac{e^n n^p (n!)^p}{(p-1)!}$, para $k \leq n$. □

Lema 3.10. *Mostre que se p é um número primo suficientemente grande. Então*

$$|c_1 A_1 + \ldots + c_n A_n| < 1$$

onde $c_1, \ldots, c_n \in \mathbb{Z}$, dados no Lema 3.3.

Demonstração. Com efeito, pelo Lema 3.9, tem-se que $|A_k| \leq \dfrac{e^n n^p (n!)^p}{(p-1)!}$, para $k \leq n$, onde $k > 0$ é um natural positivo, assim, para $k = 1, 2, \ldots, n$. Segue-se que

$$\begin{aligned}
|c_1 A_1 + \ldots + c_n A_n| &\leq |c_1 A_1| + \ldots + |c_n A_n| \\
&\leq |c_1| \frac{e^n n^p (n!)^p}{(p-1)!} + \ldots + |c_n| \frac{e^n n^p (n!)^p}{(p-1)!} \\
&= \big(|c_1| + \ldots + |c_n| \big) \frac{e^n n^p (n!)^p}{(p-1)!}
\end{aligned}$$

Mostraremos que para p um número primo suficientemente grande, tem-se

$$|c_1A_1 + \ldots + c_nA_n| \leq \big(|c_1| + \ldots + |c_n|\big)\frac{e^n n^p (n!)^p}{(p-1)!} < 1$$

Para tanto, consideremos a sequência $(a_p)_{p\in\mathbb{N}}$, definida por:

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

Dessa forma, mostraremos que $\lim\limits_{p\to+\infty} a_p = 0$. Mas antes, usaremos o seguinte fato sobre séries:

(Se uma dada série $\sum\limits_{n=1}^{+\infty} x_n$ é convergente. Então $\lim\limits_{n\to+\infty} x_n = 0$).

Assim, é suficiente mostrar que a série $\sum\limits_{p=1}^{+\infty} a_p$ é convergente. Observe que

$$\begin{aligned}
\sum_{p=1}^{+\infty} a_p &= \sum_{p=1}^{+\infty} \frac{e^n n^p (n!)^p}{(p-1)!} \\
&= e^n \sum_{p=1}^{+\infty} \frac{(nn!)^p}{(p-1)!} \\
&= e^n \left[\frac{(nn!)^1}{0!} + \frac{(nn!)^2}{1!} + \frac{(nn!)^3}{2!} + \frac{(nn!)^4}{3!} + \ldots\right] \\
&= e^n \sum_{p=0}^{+\infty} \frac{(nn!)^{p+1}}{p!} \\
&= e^n \sum_{p=0}^{+\infty} y_p
\end{aligned}$$

onde definimos a sequência $y_p := \dfrac{(nn!)^{p+1}}{p!}$. Convém notar que, aplicando o Teste da Razão para séries, basta mostrar que

$$\lim_{p\to+\infty} \left|\frac{y_{p+1}}{y_p}\right| < 1$$

Assim, calculemos este limite. Como $y_{p+1} = \dfrac{(nn!)^{p+2}}{(p+1)!}$. Segue-se que

$$\begin{aligned}
\lim_{p\to+\infty}\left|\frac{y_{p+1}}{y_p}\right| &= \lim_{p\to+\infty}\left|\frac{(nn!)^{p+2}}{(p+1)!}\cdot\frac{p!}{(nn!)^{p+1}}\right| \\
&= \lim_{p\to+\infty}\left|\frac{(nn!)^{p+1}(nn!)^{1}}{(p+1)p!}\cdot\frac{p!}{(nn!)^{p+1}}\right| \\
&= \lim_{p\to+\infty}\left|\frac{nn!}{(p+1)}\right| \\
&= 0 < 1
\end{aligned}$$

Logo, pelo Teste da Razão, a série

$$e^n\sum_{p=0}^{+\infty} y_p = \sum_{p=1}^{+\infty} a_p$$

é convergente. Consequentemente, $\lim\limits_{p\to+\infty} a_p = 0$, isto é,

$$\lim_{p\to+\infty}\frac{e^n n^p (n!)^p}{(p-1)!} = 0$$

Portanto, concluímos que

$$|c_1A_1 + \ldots + c_nA_n| < 1$$

para p suficientemente grande. □

Agora, temos resultados suficientes através dos Lemas para provar a transcendência do número de Euler (e), base do logaritmo neperiano.

Teorema 3.1 (Número de Euler)**.** *O número e é transcendente.*

Demonstração. No Lema 3.3, Supomos que o número e fosse algébrico, isto é, existem inteiros $c_0, c_1, \ldots, c_n$, com $c_0 > 0$ tais que satisfaz uma equação polinomial da forma

$$c_ne^n + c_{n-1}e^{n-1} + \ldots + c_1e + c_0 = 0$$

Dessa forma, obtemos

$$c_0F(0) + c_1F(1) + \ldots + c_nF(n) = c_1A_1 + \ldots + c_nA_n$$

Pelo Lema 3.8, segue-se $c_0F(0) + c_1F(1) + \ldots + c_nF(n)$ é um inteiro não divisível por

p, isto é, $p \nmid (c_0F(0) + c_1F(1) + \ldots + c_nF(n))$. Por outro lado, pelo Lema 3.10, temos que $|c_1A_1 + \ldots + c_nA_n| < 1$. Assim, simultaneamente, teríamos nas mesmas condições a seguinte expressão:

$$0 \leq |c_0F(0) + c_1F(1) + \ldots + c_nF(n)| = |c_1A_1 + \ldots + c_nA_n| < 1$$

que é um inteiro não divisível por p cujo o módulo é menor que 1. Como um inteiro tem módulo sempre maior do que ou igual a 0. Como não existe um número inteiro entre 0 e 1, então nossa única conclusão possível é que $c_0F(0) + c_1F(1) + \ldots + c_nF(n) = 0$, o que implicaria ser divisível por p, isto é, $p|(c_0F(0) + c_1F(1) + \ldots + c_nF(n) = 0)$, pois o zero 0 é múltiplo de todo inteiro não nulo, o que contraria o resultado do Lema 3.8, que diz que $p \nmid (c_0F(0) + c_1F(1) + \ldots + c_nF(n))$. Esta contradição, decorre do fato de supormos que e fosse algébrico. Portanto, o número e é transcendente. □

Vale salientar, que o método usado por Hermite para provar a transcendência de e foi estendido por Lindemann em 1822, para demonstrar a transcendência do π, posteriormente a de e^α onde α é algébrico não nulo, no entanto, o Capítulo 5 será dedicado a uma generalização do Teorema de Lindemann, que implica em tais consequências, mas antes, vejamos os resultados essenciais sobre Extensões algébricas no Capítulo 4.

Capítulo 4

Caracterização dos Algébricos Via Extensões de Corpos

Neste capítulo apresentaremos importantes resultados e propriedades algébricas, analíticas e complexas dos números algébricos e transcendentes, que serão necessário para o desenvolvimento de nosso objetivo principal. As principais referências utilizadas na elaboração deste capítulo são, Endler [3] e Pollard; Harry [13].

4.1 Caracterização de Elementos Algébricos

Esta seção será dedicada aos conceitos de extensões de corpos e alguns resultados preliminares. Será dedicado ainda ao teorema das funções simétricas e os conceitos de conjugado, norma de um algébrico, base integral e discriminante, os quais são de fundamental importância.

4.1.1 Extensão de um Corpo

Definição 4.1. *Sejam K e L dois corpos. Dizemos L é uma extensão de K (ou de um corpo K), e será denotado por $L|K$. Quando K for um subcorpo de L. Neste caso, K é um corpo com as operações de L tal que $K \subset L$ e consideramos L como um espaço vetorial sobre K (ou K-espaço vetorial).*

Exemplo 4.1. São exemplos de extensões de corpos $\mathbb{C}|\mathbb{R}$; $\mathbb{R}|\mathbb{Q}$; $\mathbb{C}|\mathbb{Q}$; $\mathbb{Q}(i)|\mathbb{Q}$ *e* $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$. Assim como, $K(x)|K$, onde K é um corpo e x é uma indeterminada sobre K.

Definição 4.2. *Sejam $L|K$ uma extensão de K. Então $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ denotará o menor subcorpo de L contendo $\alpha_1, \alpha_2, \ldots, \alpha_n$ e K. Além disso, uma extensão $L|K$ é*

chamada finitamente gerada sobre K se existir $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ tais que

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

isto é, $\alpha_1, \alpha_2, \ldots, \alpha_n$ geram a extensão L sobre K.

Definição 4.3. *Se existir $\alpha \in L$ tal que $L = K(\alpha)$, dizemos que L é uma extensão simples sobre K e α é chamado um elemento primitivo de L sobre K.*

Recordemos os conceitos de Números Algébricos e Transcendentes, com a finalidade de generalizá-los.

Definição 4.4. *Seja $L|K$ uma extensão de corpos. Dizemos que $\alpha \in L$ é algébrico sobre K, quando existe $P(x) \in K[x]$ não nulo tal que $P(\alpha) = 0$, isto é, quando α for raiz de um polinômio não nulo com coeficientes em K. Caso contrário, α é dito transcendente sobre K. Mais geralmente, os números $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ são ditos* **algebricamente dependentes** *sobre K, se existe $P(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ não nulo tal que $P(\alpha_1, \ldots, \alpha_n) = 0$. Caso contrário, os números $\alpha_1, \alpha_2, \ldots, \alpha_n$ são ditos* **algebricamente independentes** *sobre K.*

Definição 4.5. *Sejam $L|K$ uma extensão de K. Dizemos que L é uma extensão algébrica sobre K, se todo $\alpha \in L$ é algébrico sobre K.*

Exemplo 4.2. Todo elemento $\alpha \in K$ é algébrico sobre K.

De fato, seja $\alpha \in K$. Então basta tomar o polinômio $f(x) = x - \alpha \in K[x]$ não nulo e teremos α como raiz de $f(x)$, isto é, $f(\alpha) = \alpha - \alpha = 0$. Logo, todo α é algébrico sobre K.

Definição 4.6. *Seja $L|K$ uma extensão e suponhamos que α é algébrico sobre K. Então, o polinômio minimal de α sobre K, denotado por $P_{\alpha,K}(x)$ é o polinômio mônico (coeficiente líder igual a 1) de menor grau com coeficientes em K que tem α como raiz, ou seja, $P_{\alpha,K}(\alpha) = 0$. Neste caso, o grau de um número algébrico α é definido como o grau de seu polinômio minimal, isto é, $\partial P_{\alpha,K}(x)$.*

Exemplo 4.3. O número $\alpha = \frac{1}{\sqrt{2}}$ é algébrico de grau 2, uma vez que seu polinômio minimal é $P_{\alpha,\mathbb{Q}}(x) = x^2 - \frac{1}{2}$ sobre os racionais $\mathbb{Q}$ cujo o grau $\partial P_{\alpha,\mathbb{Q}}(x) = 2$.

Proposição 4.1. *Sejam $\mathbb{C}|K$ uma extensão de K e $\alpha \in \mathbb{C}$ um elemento algébrico sobre K. Então o polinômio minimal $P_{\alpha,K}(x)$ de α é irredutível e único sobre K tal que $P_{\alpha,K}(\alpha) = 0$. Ele ainda divide qualquer polinômio que tem α como raiz, isto é, se $m(\alpha) = 0$, então $P_{\alpha,K}(x)|m(x)$.*

Demonstração. Suponhamos por contradição que o polinômio minimal $P_{\alpha,K}(x)$ sobre K seja redutível, isto é,

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

com $f(x)$, $g(x) \in K[x]$ polinômios sobre K de graus menores que $P_{\alpha,K}(x)$. Podemos assumir que $f(x)$ e $g(x)$ são mônicos. Então,

$$P_{\alpha,K}(\alpha) = 0 \Longrightarrow f(\alpha)g(\alpha) = 0$$

como $K[x]$ é um domínio de integridade, tem-se

$$f(\alpha) = 0 \quad \text{ou} \quad g(\alpha) = 0$$

isto é, α é raiz de f ou de g tais que possuem graus menores do que $P_{\alpha,K}(x)$, o que contraria a definição de polinômio minimal $P_{\alpha,K}(x)$. Portanto, o polinômio minimal $P_{\alpha,K}(x)$ é irredutível sobre K. Note que $P_{\alpha,K}(x)$ é único. Suponha que existe outro polinômio minimal $q(x) \in K[x]$ tal que $q(\alpha) = 0$. Então,

$$q(\alpha) = 0 = P_{\alpha,K}(\alpha) \Longrightarrow q(\alpha) = P_{\alpha,K}(\alpha)$$

Como $q(x)$ e $P_{\alpha,K}(x)$ são mônicos e de menor grau para o qual α é raiz. Sendo assim, devemos ter $q(x) = P_{\alpha,K}(x)$. Logo, $P_{\alpha,K}(x)$ é único. Note ainda que $P_{\alpha,K}(x)|m(x)$. Suponha que um polinômio $m(x) \in K[x]$ é tal que $m(\alpha) = 0$. Assim, pelo Algoritmo da Divisão Euclidiana para polinômios, existem $q(x)$, $r(x) \in K[x]$ tais que

$$m(x) = P_{\alpha,K}(x)q(x) + r(x), \quad \text{onde} \quad \partial r(x) < \partial P_{\alpha,K}(x) \quad \text{ou} \quad r(x) = 0.$$

Se $r(x) = 0$. Então $m(x) = P_{\alpha,K}(x)q(x)$. Logo, o polinômio $P_{\alpha,K}(x)|m(x)$. Caso $r(x) \neq 0$, tem-se que $\partial r(x) < \partial P_{\alpha,K}(x)$. Como

$$0 = m(\alpha) = \underbrace{P_{\alpha,K}(\alpha)}_{0} q(\alpha) + r(\alpha) \Longrightarrow r(\alpha) = 0$$

Como α é raiz de $r(x)$ tal que o grau deste é menor do que o grau de $P_{\alpha,K}(x)$, gerando uma contradição com o fato de $P_{\alpha,K}(x)$ ser o polinômio minimal de α sobre K. Portanto, $r(x) = 0$ e $P_{\alpha,K}(x)|m(x)$. □

4.1.2 Grau de uma Extensão e Caracterização de Algébricos

Definição 4.7. *O grau da uma extensão $L|K$, denotado por $[L : K]$ é igual à dimensão*

de L como espaço vetorial sobre K. Dizemos que $L|K$ é uma extensão finita quando $[L : K] = n < \infty$. Caso contrário, tem-se $[L : K] = \infty$. Além disso, dizemos que o conjunto $\mathcal{B}$= $\{B_1, \ldots, B_n\}$ é uma base da extensão $L|K$, quando os elementos de $\mathcal{B}$ forem distintos dois a dois e $\mathcal{B}$ for base do espaço vetorial L sobre K.

Exemplo 4.4. O grau $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, onde $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2};\ \ a, b \in \mathbb{Q}\}$ Por outro lado, já o grau da extensão $[\mathbb{R} : \mathbb{Q}] = \infty$.

De fato, por definição do conjunto $\mathbb{Q}(\sqrt{2})$ segue-se que o conjunto $\{1, \sqrt{2}\}$ é (L.I.) e gera $\mathbb{Q}(\sqrt{2})$ como espaço vetorial sobre $\mathbb{Q}$. Note que todo elemento $\alpha \in \mathbb{Q}(\sqrt{2})$ é da forma $a.1 + b.\sqrt{2} = \alpha$, com $a, b \in \mathbb{Q}$. Logo, $\{1, \sqrt{2}\}$ gera $\mathbb{Q}(\sqrt{2})$. Se $a + b\sqrt{2} = 0$. Suponha por absurdo que $b \neq 0$, então $\sqrt{2} = -\frac{a}{b} \in \mathbb{Q}$, o que é um absurdo, pois $\sqrt{2}$ é irracional. Logo, $b = 0$, daí, $a + 0\sqrt{2} = 0$, e assim $a = 0$, o que implica que o conjunto $\{1, \sqrt{2}\}$ é (L.I.) sobre $\mathbb{Q}$. Portanto, o grau de $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. O caso da extensão $\mathbb{R}|\mathbb{Q}$, segue imediatamente do Teorema 2.7. Portanto, $[\mathbb{R} : \mathbb{Q}] = \infty$.

Note que o corpo $K(\alpha)$ consiste de todo quociente $\dfrac{g(\alpha)}{h(\alpha)}$, onde $g(\alpha)$ e $h(\alpha)$ são polinômios sobre K com $h(\alpha) \neq 0$. No teorema seguinte mostraremos que todo elemento de $K(\alpha)$ pode ser escrito de forma única como um simples polinômio em α, de modo que, podemos identificar $K(\alpha) = K[\alpha]$.

Lema 4.1. *Sejam $L|K$ uma extensão e $\alpha \in L$ um elemento algébrico sobre K de grau n. Então $K(\alpha) = K[\alpha]$ e para todo elemento $\beta \in K(\alpha)$ pode ser escrito de forma única*

$$\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = f(\alpha)$$

onde $a_i \in K$, com $i = 0, \ldots, n-1 \in \mathbb{N}$.

Demonstração. sejam $\beta = \dfrac{g(\alpha)}{h(\alpha)} \in K(\alpha)$, onde $g(x), h(x) \in K[x]$ e $h(\alpha) \neq 0$. Como α é algébrico de grau n. Então seja $P_{\alpha,K}(x)$ o polinômio minimal irredutível de α sobre K cujo o grau $\partial P_{\alpha,K}(x) = n$ tal que $P_{\alpha,K}(\alpha) = 0$. Note que $P_{\alpha,K}(x) \nmid h(x)$ (caso contrário, pela Proposição 4.1, teríamos que $h(\alpha) = 0$). Então $mdc(P_{\alpha,K}(x), h(x)) = 1$. Logo, existem $s(x)$, $t(x) \in K[x]$ tais que

$$s(x)P_{\alpha,K}(x) + t(x)h(x) = 1$$

Aplicando α na expressão acima, tem-se

$$s(\alpha)\underbrace{P_{\alpha,K}(\alpha)}_{0} + t(\alpha)h(\alpha) = 1 \Longrightarrow t(\alpha)h(\alpha) = 1 \Longrightarrow \frac{1}{h(\alpha)} = t(\alpha)$$

E multiplicando a última igualdade por $g(\alpha)$, tem-se

$$\beta = \frac{g(\alpha)}{h(\alpha)} = g(\alpha)t(\alpha) \in K[\alpha]$$

que é um polinômio em α. Para simplificar escrevemos $\beta = f(\alpha) \in K[\alpha]$, o que mostra que $K(\alpha) \subset K[\alpha]$. Como $K[\alpha] \subset K(\alpha)$, concluímos que $K(\alpha) = K[\alpha]$. Além disso, seja $\beta = f(\alpha) \in K(\alpha) = K[x]$. Pelo Algoritmo da divisão Euclidiana existem $q(x), r(x) \in K[x]$, unicamente determinados tais que

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

Em qualquer dos casos, temos que $r(x)$ é um polinômio de grau no máximo $n-1 \in \mathbb{N}$. Assim, podemos escrever

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

com $a_i \in K$, $i = 0, \ldots, n-1 \in \mathbb{N}$. Aplicando α a expressão de $f(x)$, tem-se

$$f(\alpha) = \underbrace{P_{\alpha,K}(\alpha)}_{0} q(\alpha) + r(\alpha) \Longrightarrow f(\alpha) = r(\alpha) \Longrightarrow f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

Resta mostrar a unicidade da expressão $f(\alpha)$. Suponha que

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

onde $a_i, b_i \in K$, com $i = 0, \ldots n-1 \in \mathbb{N}$. Segue imediatamente que o polinômio $q(x) \in K[x]$ onde

$$q(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1}$$

é tal que $q(\alpha) = (a_0 - b_0) + (a_1 - b_1)\alpha + \cdots + (a_{n-1} - b_{n-1})\alpha^{n-1} = f(\alpha) - h(\alpha) = 0$, isto é, $q(\alpha) = 0$ e pela Proposição 4.1, $P_{\alpha,K}(x)|q(x)$, porém $\partial q(x) < \partial P_{\alpha,K}(x) = n$. Assim, devemos ter $q(x) = 0$, daí, $a_i = b_i$, para todo $i = 0, \ldots, n-1 \in \mathbb{N}$. □

Lema 4.2. *Sejam $L|K$ uma extensão e $\alpha \in L$ algébrico sobre K de grau n. Então $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base da extensão $K(\alpha)|K$ e $[K(\alpha) : K] = n = \partial P_{\alpha,K}(x)$, onde $P_{\alpha,K}(x)$ é o polinômio minimal de α sobre K.*

Demonstração. Seja $\alpha \in L|K$ algébrico de grau n. Então o grau de seu polinômio minimal irredutível é $\partial P_{\alpha,K}(x) = n$. Pelo Lema 4.1, cada elemento $\beta = f(\alpha) \in K(\alpha)$

é escrito de forma única

$$\beta = f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \quad \text{com} \quad a_i \in K$$

isto é, todo elemento de $K(\alpha)$ é combinação linear de $1, \alpha, \ldots, \alpha^{n-1}$ sobre K, mostrando que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ gera $K(\alpha)$ sobre K. Além disso, se fosse

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

com coeficientes nem todos nulos, teríamos $f(\alpha) = 0$, isto é, α seria raiz de $f(x)$ tal que $\partial f(x) < \partial P_{\alpha,K}(x) = n$, o que contradiz a minimalidade de $P_{\alpha,K}(x)$. Assim, devemos ter $a_0 = a_1 = \ldots = a_{n-1} = 0$, segue-se que $1, \alpha, \ldots, \alpha^{n-1}$ é (L.I.), logo, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de $K(\alpha)$ sobre K, com n elementos. Portanto, podemos concluir que $[K(\alpha) : K] = n = \partial P_{\alpha,K}(x)$. □

Vejamos o resultado que caracteriza algébricos e transcendentes via extensões de corpos.

Teorema 4.1. *Sejam $L|K$ uma extensão e $\alpha \in L$. Então α é algébrico sobre K se, e somente se, $[K(\alpha) : K] < \infty$.*

Demonstração. Suponhamos que α é algébrico sobre K. Pelo Lema 4.2, tem-se que o grau de extensão

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

Reciprocamente, suponhamos que $[K(\alpha) : K] < \infty$, digamos $[K(\alpha) : K] = n$. Por definição de grau, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base da extensão $K(\alpha)|K$, em particular, é um conjunto (L.I.) Logo, o conjunto $\{1, \alpha, \ldots, \alpha^{n-1}, \alpha^n\}$ é (L.D.) sobre K, pois temos que $n + 1 > n = [K(\alpha) : K]$. Assim, existem coeficientes $a_0, \ldots, a_{n-1}, a_n \in K$ não todos nulos tais que

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

Tomando $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in K[x]$, temos que $f(x) \neq 0$ e $f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, mostrando que α é algébrico sobre K. □

Observação 4.1. Dessa forma, se $L \subset \mathbb{C}$ é um corpo de números algébricos (isto é, uma extensão finita de $\mathbb{Q}$) e θ um algébrico de L. Então todo elemento $\beta \in \mathbb{Q}(\theta)$ pode ser unicamente representado como um polinômio em θ com coeficientes em $\mathbb{Q}$, isto é, $\beta = f(\theta) = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$, com $a_i \in \mathbb{Q}$, onde $n = [\mathbb{Q}(\theta) : \mathbb{Q}]$. Além disso, podemos generalizar este fato da seguinte maneira: Sejam $\theta_1, \ldots, \theta_n$ elementos de L.

Então para todo elemento $\beta \in \mathbb{Q}(\theta_1, \ldots, \theta_n)$, tem-se $\beta = f(\theta_1, \ldots, \theta_n)$, tal que $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$.

Corolário 4.1. *Sejam $L|K$ uma extensão e $\alpha \in L$. Então α é transcendente se, e somente se, $[K(\alpha) : K] = \infty$.*

Demonstração. Segue imediatamente da contra positiva do Teorema 4.1. □

Teorema 4.2 (Multiplicatividade do Grau)**.** *Sejam K, L e M extensões de corpos tais que $K \subseteq L \subseteq M$. Então o grau da extensão $M|K$ é igual ao produto do grau de $M|L$ por $L|K$, isto é,*

$$[M : K] = [M : L].[L : K]$$

Além disso, temos que o grau da extensão $[L : K] = 1$ se , e somente se $L = K$.

Demonstração. **(Parte I).** Dadas as extensões $M|L$ e $L|K$, obtém-se uma base da extensão $M|K$ multiplicando-se os elementos de uma base de $M|L$ pelos de uma base de $L|K$. Com efeito, suponhamos que $\beta = \{B_1, \ldots, B_n\}$ e $\gamma = \{Y_1, \ldots, Y_m\}$ formem uma base $M|L$ e $L|K$, respectivamente, tal que o grau $[M : L] = n$ e $[L : K] = m$. Vamos provar que o conjunto

$$T = \{B_1Y_1, \ldots, B_nY_1;\ B_1Y_2, \ldots, B_nY_2;\ \ldots\ ;\ B_1Y_m, \ldots, B_nY_m\}$$

com nm elementos é base de $M|K$. Note que basta mostrar que

$$\sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}B_iY_j = 0, \quad \text{com} \quad a_{ij} = 0$$

Como $\beta = \{B_1, \ldots, B_n\}$ é base $L|K$, e assim, β é (L.I.) e gera $L|K, (K \subseteq L)$, tem-se

$$\sum_{i=1}^{n} a_{ij}B_i = 0, \quad \text{com} \quad a_{ij} = 0, \quad j = 1, \ldots, m \in \mathbb{N}$$

Como $\gamma = \{Y_1, \ldots, Y_m\}$ é base $M|L$, e assim, γ é (L.I.) e gera $M|L, (L \subseteq M)$, tem-se

$$\sum_{j=1}^{m} a_{ij}Y_j = 0, \quad \text{com} \quad a_{ij} = 0, \quad i = 1, \ldots, n \in \mathbb{N}$$

Como γ é base de $M|L$ sobre L tal que $L \subseteq M$. Então para todo $\delta \in M|L$, existem $w_1, \ldots, w_m \in L$ tais que

$$\delta = \sum_{j=1}^{m} w_jY_j$$

Como β é base de $L|K$ sobre K tal que $K \subseteq L$. Então podemos ter

$$w_j = \sum_{i=1}^{n} a_{ij} B_i, \quad \text{com} \quad a_{ij} \in K, \quad j = 1, \ldots m \in \mathbb{N}$$

Daí, substituindo w_j na expressão de δ acima, tem-se

$$\sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} B_i Y_j, \quad \text{com} \quad a_{ij} \in K$$

Dessa forma, se

$$\sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} B_i Y_j = 0 \Longrightarrow a_{ij} = 0$$

Logo, o conjunto T é base de $M|K$ e portanto $[M : K] = n.m = [M : L].[L : K]$.

(Parte II). Se $[L : K] = 1$, então o conjunto $\{v = 1\}$ é uma base da extensão $L|K$. Resulta que todo $\alpha \in L$ é da forma $\alpha = a.v = a.1$, com $a \in K$. Daí, $\alpha \in K$. Logo, a extensão $L \subseteq K$ e como $K \subseteq L$ por hipótese. Portanto, temos $L = K$.

Reciprocamente, se $L = K$, existe um elemento $v = 1$ que gera L, isto é, $L = K(1)$, e assim, o conjunto $\{v = 1\}$ é base da extensão $L|K$. Portanto, o grau da extensão $[L : K] = 1$.

□

4.1.3 Relação de Girard e Polinômio Simétrico

As "Relações de Girard" são relações estabelecidas entre os coeficientes de um polinômio e suas raízes. Elas se baseiam na igualdade entre a forma desenvolvida e a fatorada de um polinômio, comparando seus coeficientes.

• **Polinômio de grau** 2: Considere $P(x) = ax^2 + bx + c$, com $a \neq 0$, a, b e $c \in \mathbb{R}$ e raízes x_1 e x_2. Decompondo $P(x)$, tem-se

$$\begin{aligned} ax^2 + bx + c &= a(x - x_1)(x - x_2) \\ &= a\big(x^2 - x_1 x - x_2 x + x_1 x_2\big) \\ &= ax^2 - a\big(x_1 + x_2\big)x + a x_1 x_2 \end{aligned}$$

Pela igualdade de polinômio, tem-se

$$\begin{cases} x_1 + x_2 &= -\frac{b}{a} \\ x_1 x_2 &= \frac{c}{a} \end{cases}$$

• **Polinômio de grau** 3: Considere $P(x) = ax^3 + bx^2 + cx + d$, com $a \neq 0$, a, b, c e $d \in \mathbb{R}$ e raízes x_1, x_2 e x_3. Pelo mesmo argumento, tem-se

$$\begin{aligned} ax^3 + bx^2 + cx + d &= a(x - x_1)(x - x_2)(x - x_3) \\ &= a\big(x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3\big) \\ &= ax^3 - a(x_1 + x_2 + x_3)x^2 + a(x_1x_2 + x_1x_3 + x_2x_3)x - ax_1x_2x_3 \end{aligned}$$

Pela igualdade de polinômio, tem-se

$$\begin{cases} x_1 + x_2 + x_3 &= -\frac{b}{a} \\ x_1x_2 + x_1x_3 + x_2x_3 &= \frac{c}{a} \\ x_1x_2x_3 &= -\frac{d}{a} \end{cases}$$

Note que há uma alternância entre os sinais das relações. Na expressão da soma das raízes temos sempre o sinal negativo (-$\frac{b}{a}$). No entanto, a partir das somas de produtos parciais agrupados, ora temos sinal positivo, ora negativo. Essa recorrência permite escrever as relações de Girard para qualquer grau de $P(x)$. Generalizando, o polinômio $P(x)$ de grau de $n \in \mathbb{N}$, resulta:

• **Polinômio de grau** n: Consideremos o polinômio

$$P(x) = a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} \cdots + a_1x + a_0 = \sum_{t=0}^{n} a_tx^t$$

com $a_n \neq 0$, $a_t \in \mathbb{R}$, com $t = 0, \ldots, n \in \mathbb{N}$ e raízes $x_1, x_2, \ldots, x_n$ (podendo haver repetições). Por recorrência, obtemos

$$\begin{aligned} \sum_{t=0}^{n} a_tx^t &= a_n(x - x_1)(x - x_2)\cdots(x - x_n) \\ &= a_n\Big(x^n - \Big(\sum_{i=1}^{n} x_i\Big)x^{n-1} + \Big(\sum_{1\leq i<j\leq n} x_ix_j\Big)x^{n-2} + \cdots + (-1)^n\Big(x_1x_2\cdots x_n\Big)\Big) \\ &= a_nx^n - a_n\Big(\sum_{i=1}^{n} x_i\Big)x^{n-1} + a_n\Big(\sum_{1\leq i<j\leq n} x_ix_j\Big)x^{n-2} + \cdots + a_n(-1)^n\Big(x_1x_2\cdots x_n\Big) \end{aligned}$$

Pela igualdade de polinômio, tem-se

$$\begin{cases} \displaystyle\sum_{i=1}^{n} x_i & = x_1 + x_2 + \cdots + x_n = -\frac{a_{n-1}}{a_n} \\ \displaystyle\sum_{1\leq i<j\leq n} x_i x_j & = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + x_2x_4 + \cdots + x_{n-1}x_n = \frac{a_{n-2}}{a_n} \\ \vdots & \vdots \\ \displaystyle\sum_{1\leq i_1<i_2<\ldots<i_k\leq n} x_{i_1}x_{i_2}\cdots x_{i_k} & = (-1)^k \frac{a_{n-k}}{a_n} \\ \vdots & \vdots \\ x_{i_1}x_{i_2}\cdots x_{i_n} & = (-1)^n \frac{a_0}{a_n} \end{cases}$$

A seguir veremos que as relações de Girard coincide com as funções simétricas elementares, que em particular, são polinômios simétricos, a qual será uma ferramenta útil para a solução de equações algébricas.

Definição 4.8. *Seja $\mathcal{A}$ um anel. Dizemos que um polinômio $P(x_1, \ldots, x_n) \in \mathcal{A}[x_1, \ldots, x_n]$ é simétrico (ou função simétrica) em $x_1, x_2, \ldots, x_n$, se*

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

para toda permutação $\sigma \in S_n$, onde S_n é o conjunto das permutações do conjunto $\{1, 2, \ldots, n\}$, o qual possuem $n!$(n fatorial) permutações, isto é, um polinômio é dito simétrico quando podemos permutar as variáveis de $P(x_1, \ldots, x_n)$ entre si, sem que isso altere o valor da sua expressão original. Além disso, Para todo, $k = 1, 2, \ldots, n \in \mathbb{N}$, os polinômios

$$\begin{aligned} \sigma_1(x_1, \ldots, x_n) &= \sum_{i_1=1}^{n} x_{i_1} \\ \sigma_2(x_1, \ldots, x_n) &= \sum_{1\leq i_1<i_2\leq n} x_{i_1}x_{i_2} \\ \vdots & \quad \vdots \\ \sigma_k(x_1, \ldots, x_n) &= \sum_{1\leq i_1<i_2<\ldots<i_k\leq n} x_{i_1}x_{i_2}\cdots x_{i_k} \\ \vdots & \quad \vdots \\ \sigma_n(x_1, \ldots, x_n) &= x_{i_1}x_{i_2}\cdots x_{i_n} \end{aligned}$$

são simétricos em $x_1, \ldots, x_n$, e são chamados de k-ésima função simétrica elementar.

Observação 4.2. Note que da Definição 4.8, acima temos que a k-ésima função simétrica elementar coincide com as Relações de Girard, e assim, podemos generalizar

$$\sigma_k(x_1, \ldots, x_n) = \sum_{1\leq i_1<i_2<\ldots<i_k\leq n} x_{i_1}x_{i_2}\cdots x_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}$$

para todo $k = 1, \ldots, n \in \mathbb{N}$, onde os a_{n-k} e a_n são coeficientes de algum polinômio não nulo da forma $P(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} \cdots + a_1 x + a_0$, de grau $n \in \mathbb{N}$ que tem $x_1, x_2, \ldots, x_n$ como raízes. Além disso, podemos escrever:

$$\begin{aligned} P(x) &= a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \\ &= a_n(x - x_1)(x - x_2)\cdots(x - x_n) \\ &= a_n\Big(x^n - \big(\sum_{i=1}^{n} x_i\big)x^{n-1} + \big(\sum_{1\leq i<j\leq n} x_i x_j\big)x^{n-2} + \cdots + (-1)^n\big(x_1 x_2 \cdots x_n\big)\Big) \\ &= a_n\Big(x^n - \sigma_1(x_1, x_2, \ldots, x_n)x^{n-1} + \cdots + (-1)^n\sigma_n(x_1, x_2, \ldots, x_n)\Big). \end{aligned}$$

Exemplo 4.5. O polinômio $P(x, y) = x^2 + y^2 \in \mathcal{A}[x, y]$ é simétrico. Além disso, existe um polinômio $\varphi \in \mathcal{A}[x, y]$ escrito em termos de uma função simétrica elementar tal que

$$P(x, y) = \varphi\big(\sigma_1(x, y), \sigma_2(x, y)\big)$$

De fato, $P(x, y) = x^2 + y^2 = y^2 + x^2 = P(y, x)$. Logo, $P(x, y)$ é simétrico. Além disso, podemos escrever

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

Portanto, o polinômio $P(x, y) = \varphi\big(\sigma_1(x, y), \sigma_2(x, y)\big)$ para algum polinômio φ.

Na verdade, esse fato do Exemplo 4.5, acima é bem geral como veremos a seguir no Teorema Fundamental das Funções Simétricas.

Teorema 4.3 (Fundamental das Funções Simétricas)**.** *Seja $P(x_1, \ldots, x_n) \in \mathcal{A}[x_1, \ldots, x_n]$ um polinômio simétrico em n variáveis, com coeficientes em $\mathcal{A}$. Então existe um polinômio $\varphi(x_1, \ldots, x_n) \in \mathcal{A}[x_1, \ldots, x_n]$ tal que*

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

onde $\sigma_k(x_1, \ldots, x_n)$, com $k = 1, \ldots, n \in \mathbb{N}$ denota as funções simétricas elementares em $x_1, \ldots, x_n$, isto é, podemos escrever todo polinômio simétrico como um polinômio em termos de funções simétricas elementares em $x_1, x_2, \ldots, x_n$.

Demonstração. Procederemos por indução sobre n, no número de variáveis e em seguida sobre o grau do polinômio. Se $n = 1$, note que $\sigma_1(x_1) = x_1$ obviamente temos $P(x_1) = P(\sigma_1(x_1))$. Para facilitar a notação, denotaremos:

$$\sigma_1 := \sigma_1(x_1, \ldots, x_n), \sigma_2 := \sigma_2(x_1, \ldots, x_n), \ldots, \sigma_n := \sigma_n(x_1, \ldots, x_n)$$

para as funções simétricas elementares nas variáveis $x_1, \ldots, x_n$.

(Hipótese (I)): Suponha que o teorema seja válido para cada polinômio simétrico $P(x_1,\ldots,x_{n-1}) \in \mathcal{A}[x_1,\ldots,x_{n-1}]$, isto é, existe $g_1(x_1,\ldots,x_{n-1}) \in \mathcal{A}[x_1,\ldots,x_{n-1}]$ tal que $P(x_1,\ldots,x_{n-1}) = g_1(\sigma_1,\ldots,\sigma_{n-1})$ e representamos as funções simétricas elementares em $x_1,\ldots,x_{n-1}$ por:

$$\begin{aligned}
\sigma_1 &:= \sigma_1(x_1,\ldots,x_n) &&= \sum_{j=1}^{n-1} x_j \\
\sigma_2 &:= \sigma_2(x_1,\ldots,x_n) &&= \sum_{1\le i<j\le n-1} x_i x_j \\
&\vdots \qquad\qquad \vdots && \qquad\quad \vdots \\
\sigma_{n-1} &:= \sigma_{n-1}(x_1,\ldots,x_n) &&= x_1 x_2 \cdots x_{n-1}
\end{aligned}$$

as quais podem ser obtidas fazendo $x_n = 0$ em $P(x_1,\ldots,x_{n-1},0)$. Agora, para mostrar que o teorema vale para polinômios em $x_1, x_2, \ldots, x_n$, $P(x_1,\ldots,x_n) \in \mathcal{A}[x_1,\ldots,x_n]$ de grau d, usaremos indução sobre o grau de P, $(\partial P = d)$.

Se $\partial P = 0$, então teríamos apenas polinômios $P(x_1,\ldots,x_n)$ constantes e o resultado seria trivial, pois não depende do número de variáveis.

(Hipótese (II)): Suponhamos que o resultado seja válido para polinômio simétrico $H(x_1,\ldots,x_n) \in \mathcal{A}[x_1,\ldots,x_n]$ de grau menor que d $(\partial H < d)$ e provaremos que ele se verifica para polinômios de grau d. Considere o polinômio
$P(x_1,\ldots,x_{n-1},0) \in \mathcal{A}[x_1,\ldots,x_n]$ fazendo $x_n = 0$ em P. Como $P(x_1,\ldots,x_{n-1},x_n)$ é simétrico, tem-se que $P(x_1,\ldots,x_{n-1},0)$ também é simétrico. Logo, pela (Hipótese (I)), existe $g_1(x_1,\ldots,x_{n-1}) \in \mathcal{A}[x_1,\ldots,x_{n-1}]$ tal que

$$P(x_1,\ldots,x_{n-1},0) = g_1(\sigma_1,\ldots,\sigma_{n-1}) \tag{4.1}$$

onde σ_i, com $i = 1,\ldots,n-1 \in \mathbb{N}$ denota as funções simétricas elementares em $x_1, x_2, \ldots, x_{n-1}$. Assim, temos ainda que

$$P_1(x_1,\ldots,x_n) = P(x_1,\ldots,x_n) - g_1(\sigma_1,\ldots,\sigma_{n-1}) \tag{4.2}$$

é um polinômio simétrico em $x_1, x_2, \ldots, x_n$ por ser a diferença de polinômios simétricos.

Note que fazendo $x_n = 0$ na expressão de $P_1(x_1,\ldots,x_n)$, obtemos

$$P_1(x_1,\ldots,x_{n-1},0) = P(x_1,\ldots,x_{n-1},0) - g_1(\sigma_1,\ldots,\sigma_{n-1})$$

Daí, e de (4.1), tem-se que

$$P_1(x_1,\ldots,x_{n-1},0) = 0$$

Por conseguinte, x_n é um fator comum de $P_1(x_1,\ldots,x_n)$, (pois quando aplicamos

$x_n = 0$ em P_1 e ele zerou, isso significa que na expressão de P_1 temos fatores x_n). Como $P_1(x_1, \ldots, x_n)$ é simétrico em $x_1, x_2, \ldots, x_n$, segue-se que x_j para todo $j = 1, \ldots\ n \in \mathbb{N}$ é fator comum de $P_1(x_1, \ldots, x_n)$ o que implica que $\sigma_n = x_1 x_2 \cdots x_n$ divide $P_1(x_1, \ldots, x_n)$. Logo,

$$P_1(x_1, \ldots, x_n) = \sigma_n P_2(x_1, \ldots, x_n) \tag{4.3}$$

para algum $P_2(x_1, \ldots, x_n) \in \mathcal{A}[x_1, \ldots, x_n]$. Pela simetria de $P_1(x_1, \ldots, x_n)$ e como σ_n é função simétrica elementar, então $P_2(x_1, \ldots, x_n)$ deve ser simétrico e como o grau de P_2 é menor do que o grau de P, $(\partial P_2 < \partial P = d)$. Então pela (Hipótese (II)), existe um polinômio $g_2(x_1, \ldots, x_n) \in \mathcal{A}[x_1, \ldots, x_n]$ tal que

$$P_2(x_1, \ldots, x_n) = g_2(\sigma_1, \ldots, \sigma_n) \tag{4.4}$$

Finalmente, das expressões de (4.2), (4.3) e (4.4), obtemos

$$\begin{aligned} P(x_1, \ldots, x_n) &= P_1(x_1, \ldots, x_n) + g_1(\sigma_1, \ldots, \sigma_{n-1}) \\ &= \sigma_n P_2(x_1, \ldots, x_n) + g_1(\sigma_1, \ldots, \sigma_{n-1}) \\ &= \sigma_n g_2(\sigma_1, \ldots, \sigma_n) + g_1(\sigma_1, \ldots, \sigma_{n-1}) \end{aligned}$$

Como $P(x_1, \ldots, x_n)$ está escrito como soma de funções simétricas elementares em $x_1, x_2, \ldots, x_n$. Portanto, o polinômio $P(x_1, \ldots, x_n) = \varphi\big(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)\big)$, sendo $\varphi(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)) = \sigma_n g_2(\sigma_1, \ldots, \sigma_n) + g_1(\sigma_1, \ldots, \sigma_{n-1})$. □

Lema 4.3. *Sejam $\beta_1, \beta_2, \ldots, \beta_n$ raízes de um polinômio $f(x)$ com coeficientes inteiros,*

$$f(x) = bx^n + c_1 x^{n-1} + \cdots + c_n, \quad \textit{com} \quad b, c_i \in \mathbb{Z}, \quad i = 1, \ldots, n \in \mathbb{N}.$$

Sendo $b \neq 0$. 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 $\partial P = t \in \mathbb{N}$, então $b^t P(\beta_1, \ldots, \beta_n) \in \mathbb{Z}$.

Demonstração. **(1ª Parte).** Seja $P(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ um polinômio simétrico. Pelo Teorema Fundamental das Funções Simétricas 4.3, existe $\varphi(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ tal que

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

Aplicando $\beta_1, \ldots, \beta_n$ a $P(x_1, \ldots, x_n)$, tem-se

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

Como $\beta_1, \ldots, \beta_n$ são raízes de $f(x)$ e $b, c_i \in \mathbb{Z}$, sendo $b \neq 0$. Então por definição de funções simétricas elementares e das Relações de Girard, confirma a Observação 4.2,

que

$$\sigma_i(\beta_1,\ldots,\beta_n) = (-1)^i\frac{c_i}{b} \in \mathbb{Q}, \quad i = 1,\ldots,n \in \mathbb{N}$$

Dessa forma,

$$P(\beta_1,\ldots,\beta_n) = \varphi\big((-1)^1\frac{c_1}{b},\ldots,(-1)^n\frac{c_n}{b}\big) \in \mathbb{Q}$$

Portanto, o polinômio $P(\beta_1,\ldots,\beta_n) \in \mathbb{Q}$ é um racional. Por outro lado,

(2ª Parte). Seja $P(x_1,\ldots,x_n) \in \mathbb{Z}[x_1,\ldots,x_n]$ um polinômio simétrico. Pelo Teorema 4.3, tem-se

$$P(x_1,\ldots,x_n) = \varphi\big(\sigma_1(x_1,\ldots,x_n),\ldots,\sigma_n(x_1,\ldots,x_n)\big) \tag{4.5}$$

para algum $\varphi(x_1,\ldots,x_n) \in \mathbb{Z}[x_1,\ldots,x_n]$, escrevendo o polinômio φ em n variáveis

$$\varphi(x_1,\ldots,x_n) = \sum_{(i)} a_{(i)}x_1^{i_1}\cdots x_n^{i_n}, \quad \text{com} \quad a_{(i)} \in \mathbb{Z}$$

onde denotamos o multi-índice $(i) := i_1,\ldots,i_n \in \mathbb{N}$ para facilitar a notação. Como $\partial P = t$, por (4.5), o grau $\partial\varphi = t$, então o $\max_{(i)}\big\{i_1+i_2+\cdots+i_n; \quad a_{(i)} \neq 0\big\} = t$.

Por outro lado, aplicando $\beta_1,\ldots,\beta_n$ e $\sigma_i(\beta_1,\ldots,\beta_n) = (-1)^i\frac{c_i}{b}$ a igualdade (4.5), com $i = 1,\ldots,n \in \mathbb{N}$, obtemos

$$\begin{aligned}
P(\beta_1,\ldots,\beta_n) &= \varphi\big(\sigma_1(\beta_1,\ldots,\beta_n),\ldots,\sigma_n(\beta_1,\ldots,\beta_n)\big)\\
&= \sum_{(i)} a_{(i)}\sigma_1(\beta_1,\ldots,\beta_n)^{i_1}\cdots\sigma_n(\beta_1,\ldots,\beta_n)^{i_n}\\
&= \sum_{(i)} a_{(i)}(-1)^{i_1}\left(\frac{c_1}{b}\right)^{i_1}\cdots(-1)^{ni_n}\left(\frac{c_n}{b}\right)^{i_n}\\
&= \sum_{(i)}(-1)^{(i_1+2i_2+\cdots+ni_n)}\frac{a_{(i)}}{b^{i_1}\cdots b^{i_n}}c_1^{i_1}\cdots c_n^{i_n}\\
&= \sum_{(i)}(-1)^m\frac{a_{(i)}}{b^{(i_1+\cdots+i_n)}}c_1^{i_1}\cdots c_n^{i_n}
\end{aligned}$$

sendo $m = (i_1+2i_2+\cdots+ni_n) \in \mathbb{N}$. Logo,

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

Como $b, a_{(i)}$ e $c_i \in \mathbb{Z}$ e $t \geq i_1+\cdots+i_n$ para todo multi-índice $(i) = i_1,\ldots,i_n$. Portanto, a expressão $b^tP(\beta_1,\ldots,\beta_n) \in \mathbb{Z}$ é um inteiro. □

Proposição 4.2. *Seja o polinômio $F(x) \in K[x]-\{0\}$ não constante de grau n e $\alpha \in \mathbb{C}$ uma raiz de $F(x)$. Então.*
(a) α é raiz múltipla de F se, e somente se, α é raiz de F', isto é, $F'(\alpha) = 0$.

(b) Se $F(x)$ é irredutível sobre K. Então todas as raízes de $F(x)$ são simples (todas raízes são distintas).

Demonstração. **item (a).** $(\Longrightarrow)$. Se α é raiz múltipla de $F(x)$, sendo de multiplicidade $m > 1$, por definição, temos

$$F(x) = (x-\alpha)^m q(x), \quad q(x) \in \mathbb{C}[x], \quad \text{e} \quad q(\alpha) \neq 0$$

Por derivação, tem-se

$$F'(x) = m(x-\alpha)^{m-1}q(x) + (x-\alpha)^m q'(x), \quad m > 1$$

Daí, aplicando α, segue-se:

$$F'(\alpha) = m\underbrace{(\alpha-\alpha)}_{0}^{m-1}q(\alpha) + \underbrace{(\alpha-\alpha)}_{0}^{m}q'(\alpha) = 0 \Longrightarrow F'(\alpha) = 0.$$

$(\Longleftarrow)$. Reciprocamente, se $F'(\alpha) = 0$. Suponhamos por contradição que α fosse raiz simples de $F(x)$, ou seja, com multiplicidade $m = 1$. Então existe $g(x) \in \mathbb{C}[x]$ tal que

$$F(x) = (x-\alpha)^1 g(x), \qquad g(\alpha) \neq 0$$

Usando regra de derivação, tem-se

$$F'(x) = 1(x-\alpha)^0 g(x) + (x-\alpha)^1 g'(x) \Longrightarrow F'(x) = g(x) + (x-\alpha)g'(x)$$

Aplicando $x = \alpha$, obtemos

$$F'(\alpha) = g(\alpha) + \underbrace{(\alpha-\alpha)}_{0}g'(\alpha) \Longrightarrow F'(\alpha) = g(\alpha)$$

o que uma contradição, visto que, $F'(\alpha) = 0$ e $g(\alpha) \neq 0$. Portanto, o número α é raiz múltipla de F.

item (b). Seja $F(x) \in K[x]$ um polinômio irredutível sobre K e α raiz de $F(x)$ de multiplicidade m. Basta prova que $m = 1$. Seja $P_{\alpha,K}(x)$ o polinômio minimal de α de menor grau para o qual α é raiz. Pelo Algoritmo da divisão Euclidiana existem $q(x), r(x) \in K[x]$, unicamente determinados tais que

$$F(x) = P_{\alpha,K}(x)q(x) + r(x), \quad \text{onde} \quad \partial r(x) < \partial P_{\alpha,K}(x) \quad \text{ou} \quad r(x) = 0.$$

Aplicando α, tem-se

$$F(\alpha) = \underbrace{P_{\alpha,K}(\alpha)}_{0} q(\alpha) + r(\alpha) \Longrightarrow F(\alpha) = 0 = r(\alpha)$$

Pela Proposição 4.1, temos $P_{\alpha,K}(x)|r(x)$, mas $\partial r(x) < \partial P_{\alpha,K}(x)$. Segue-se da minimalidade do grau de $P_{\alpha,K}(x)$ que $r(x) = 0$. Dessa forma, tem-se

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

Logo, pela irredutibilidade de $F(x)$, existe uma constante $c \in K - \{0\}$ tal que $q(x) = c$ ou $P_{\alpha,K}(x) = c$, digamos $q(x) = c$. Então $F(x) = cP_{\alpha,K}(x)$.

Note que, se a multiplicidade de $F(x)$ fosse $m > 1$, pelo item (a), seguiria que

$$F'(\alpha) = cP'_{\alpha,K}(\alpha) = 0$$

Daí, teríamos $P'_{\alpha,K}(\alpha) = 0$ tal que $\partial P'_{\alpha,K}(x) < \partial P_{\alpha,K}(x)$ o que contradiz a minimalidade de $P_{\alpha,K}(x)$. Logo, a multiplicidade de $F(x)$ é $m = 1$. Portanto, todas as raízes de $F(x)$ são simples (todas raízes são distintas). □

Teorema 4.4. *Uma extensão algébrica múltipla de um corpo de números algébricos é uma extensão algébrica simples. Em outras palavras. Se $\alpha_1, \alpha_2, \ldots, \alpha_s$ são algébricos sobre $\mathbb{Q}$. Então existe γ algébrico sobre $\mathbb{Q}$ tal que*

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

isto é, a extensão de $\mathbb{Q}$ por γ e mesma que a extensão de $\mathbb{Q}$ por $\alpha_1, \alpha_2, \ldots, \alpha_s$.

Demonstração. Primeiro, mostraremos que (dados $\alpha, \beta \in \mathbb{L}$ algébricos sobre $\mathbb{K}$ e as extensões $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ finitas, existe um $u \in \mathbb{K}(\alpha, \beta)$ tal que $\mathbb{K}(\alpha, \beta) = \mathbb{K}(u)$.) em seguida estenderemos de modo que existe um elemento algébrico que pode ser obtido como combinação de um número finito de geradores algébricos sobre $\mathbb{Q}$.

A princípio iniciaremos por indução sobre o grau $[\mathbb{L} : \mathbb{K}] < \infty$. Se $[\mathbb{L} : \mathbb{K}] = 1$, pelo Teorema 4.2, (Parte II), tem-se $\mathbb{L} = \mathbb{K}(1)$ e o teorema é válido trivialmente. Suponhamos que $[\mathbb{L} : \mathbb{K}] > 1$. Assim, exite $v_1 \in \mathbb{L}$, $v_1 \notin \mathbb{K}$. Seja $\mathbb{K}_1 := \mathbb{K}(v_1)$, se $\mathbb{K}_1 = \mathbb{L}$, então $\mathbb{L} = \mathbb{K}(v_1)$ o teorema é válido. Mas, se existe $v_2 \in \mathbb{L}$ tal que $v_2 \notin \mathbb{K}_1 = \mathbb{K}(v_1)$. Seja $\mathbb{K}_2 := \mathbb{K}_1(v_2) = \mathbb{K}(v_1)(v_2) = \mathbb{K}(v_1, v_2)$, se $\mathbb{L} = \mathbb{K}_2$, então $\mathbb{L} = \mathbb{K}(v_1, v_2)$. Como por hipótese $[\mathbb{L} : \mathbb{K}] < \infty$ é finito. Conseguimos $v_1, v_2, \ldots, v_r \in \mathbb{L}$ com $r \geq 2 \in \mathbb{N}$ tais que $\mathbb{L} = \mathbb{K}(v_1, \ldots, v_{r-1}, v_r)$ e $v_i \notin \mathbb{K}(v_1, \ldots, v_{i-1})$.

Dessa forma, temos:

$$\mathbb{K} \subseteq \mathbb{K}(v_1) \subseteq \mathbb{K}(v_1, v_2) \subseteq \ldots \subseteq \mathbb{K}(v_1, \ldots, v_{r-1}) \subseteq \mathbb{K}(v_1, \ldots, v_{r-1}, v_r) = \mathbb{L} < \infty$$

Por conseguinte, $[\mathbb{K}(v_1, \ldots, v_{r-1}, v_r) : \mathbb{K}] < \infty$ e temos por hipótese de indução que existe $\alpha \in \mathbb{K}(v_1, \ldots, v_{r-1})$ tal que $\mathbb{K}(v_1, \ldots, v_{r-1}) = \mathbb{K}(\alpha)$, daí, segue-se imediatamente que $\mathbb{L} = \mathbb{K}(v_1, \ldots, v_{r-1}, v_r) = \mathbb{K}(\alpha)(v_r) = \mathbb{K}(\alpha, v_r)$. Fazendo $v_r = \beta \in \mathbb{L}$ temos:

$$\mathbb{L} = \mathbb{K}(\alpha, \beta) \tag{4.6}$$

Agora vamos provar que existe $u \in \mathbb{L}$ tal que $\mathbb{K}(\alpha, \beta) = \mathbb{K}(u)$.
Se $\alpha, \beta \in \mathbb{L}$ são algébricos. Existem os polinômios irredutíveis $P(x) = irr(\alpha, \mathbb{K})$ e $Q(x) = irr(\beta, \mathbb{K})$ de graus $\partial P(x) = m$ e $\partial Q(x) = n$. Pela Proposição 4.2, item (b), $P(x)$ e $Q(x)$ possuem raízes distintas em $\mathbb{C}$. Sejam os conjugados $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(m)}$ e $\beta = \beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(n)}$ raízes distintas de $P(x)$ e $Q(x)$ em $\mathbb{C}$, respectivamente.

Para cada $i = 1, \ldots, m \in \mathbb{N}$ e $j = 2, \ldots, n \in \mathbb{N}$, sejam

$$\lambda_{ij} := \frac{\alpha^{(i)} - \alpha}{\beta - \beta^{(j)}} \in \mathbb{C}, \quad j \neq 1$$

Como $\mathbb{K}$ é um corpo infinito, e há um número finito de soluções em λ_{ij}, podemos escolher um $\lambda \neq 0 \in \mathbb{K}$ diferente de todas as soluções, isto é,

$$\lambda \notin A = \{\lambda_{ij}; \quad 1 \leq i \leq m \in \mathbb{N}, \quad 2 \leq j \leq n \in \mathbb{N}\} \tag{4.7}$$

Seja $u := \alpha + \lambda\beta$, como todo elemento $\zeta \in \mathbb{K}(u)$ pelo Lema 4.1, pode ser escrito de forma única:

$$\begin{aligned} \zeta &= a_0 + a_1 u + \ldots + a_{n-1} u^{n-1} \\ &= a_0 + a_1 (\alpha + \lambda\beta) + \ldots + a_{n-1} (\alpha + \lambda\beta)^{n-1} \end{aligned}$$

Como ζ é combinação de $(\alpha + \lambda\beta)$, então $\zeta \in \mathbb{K}(\alpha, \beta)$, daí, segue-se que

$$\mathbb{K}(u) \subset \mathbb{K}(\alpha, \beta)$$

Basta mostrar que $\mathbb{K}(\alpha, \beta) \subset \mathbb{K}(u)$, para tanto, é suficiente verificar que $\beta, \alpha \in \mathbb{K}(u)$.

Consideremos o polinômio $H(x) = P(u - \lambda x)$ em $\mathbb{K}(u)[x]$. Temos que β é raiz de $H(x)$, pois

$$H(\beta) = P(u - \lambda\beta) = P(\alpha + \lambda\beta - \lambda\beta) = P(\alpha) = 0$$

Como β também é raiz de $Q(x) \in \mathbb{K}[x] \subset \mathbb{K}(u)[x]$, segue-se que $(x - \beta)$ divide $Q(x)$ e $H(x)$. Seja $d(x) = mdc_{\mathbb{C}[x]}(Q(x), H(x))$.

Afirmamos que $d(x) = (x - \beta)$. Como $d(x)|Q(x)$ e $d(x)|H(x)$ as raízes de $d(x)$ em $\mathbb{C}[x]$ são as raízes comuns de $Q(x)$ e $H(x)$. Provaremos que $d\left(\beta^{(1)}\right) = 0$. Com efeito, suponhamos que $d\left(\beta^{(j)}\right) = 0$ para algum $j = 2, \ldots, n \in \mathbb{N}$, e assim, teríamos que $H(\beta^{(j)}) = 0$, o que implicaria $P\left(u - \lambda\beta^{(j)}\right) = 0$, o que significa que $\left(u - \lambda\beta^{(j)}\right)$ é uma das raízes $\alpha = \alpha^{(1)}, \alpha^{(2)} \ldots, \alpha^{(m)}$ de $P(x)$. Logo, existiria um $i = 1, \ldots, m \in \mathbb{N}$ tal que

$$\alpha^{(i)} = u - \lambda\beta^{(j)} = (\alpha + \lambda\beta) - \lambda\beta^{(j)} = \alpha + \lambda\left(\beta - \beta^{(j)}\right),$$

Por conseguinte, para algum $i = 1, \ldots, m \in \mathbb{N}$.

$$\frac{\alpha^{(i)} - \alpha}{\beta - \beta^{(j)}} = \lambda \Longrightarrow \lambda = \lambda_{ij}, \qquad j = 2, \ldots, n \in \mathbb{N}$$

o que um contradição em (4.7) pela escolha de $\lambda \notin A$.

Segue-se que $d\left(\beta^{(1)}\right) = 0$, então $d(\beta) = 0$. Logo, $d(x) = x - \beta$ o que mostra afirmação.

Agora, seja $d_1(x) := mdc_{\mathbb{K}(u)[x]}(Q(x), H(x))$. Como $\mathbb{K}(u)[x] \subset \mathbb{C}[x]$, segue-se o grau $\partial d_1(x) \leq \partial d(x) = 1$. Se $d_1(x) \neq d(x)$ teríamos que $\partial d_1(x) = 0$ e assim, $d_1(x)$ seria constante igual a 1, isto é, $d_1(x) = 1$, já que $d_1(x) = mdc_{\mathbb{K}(u)[x]}(Q(x), H(x))$ e ainda $d_1(x)|d(x)$. Por outro lado, como $d(x) = mdc_{\mathbb{C}[x]}(Q(x), H(x))$ teríamos ainda que

$$d(x)\,|d_1(x) = 1 \Longrightarrow d(x) = 1$$

o que é um absurdo, uma vez que $d(x) = x - \beta$. Logo, podemos concluir que o elemento $d(x) = x - \beta = d_1(x) \in \mathbb{K}(u)[x]$, isto é, $\beta \in \mathbb{K}(u)$. Note que $\alpha = u - \lambda\beta \in \mathbb{K}(u)$, pois $u \in \mathbb{K}(u)$, vimos que $\beta \in \mathbb{K}(u)$ e $\lambda \in \mathbb{K} \subset \mathbb{K}(u)$. Logo, temos $\mathbb{K}(\alpha, \beta) \subset \mathbb{K}(u)$. Portanto, $\mathbb{K}(\alpha, \beta) = \mathbb{K}(u)$.

Fazendo $\mathbb{Q}(\alpha, \beta) := \mathbb{K}(\alpha, \beta)$, segue-se que a extensão $\mathbb{Q}(\alpha, \beta)$ é simples, quando α, β são algébricos sobre $\mathbb{Q}$, isto é, existe $u \in \mathbb{Q}(\alpha, \beta)$ algébrico sobre $\mathbb{Q}$ tal que

$$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(u)$$

Como a extensão $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ pode ser escrita como $\mathbb{Q}(\alpha_1, \alpha_2)(\alpha_3)$.

Pelo caso de dois geradores, existe $w \in \mathbb{Q}(\alpha_1, \alpha_2)(\alpha_3)$ tal que

$$\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(w)$$

Procedendo de maneira análoga, a extensão múltipla, existe $\gamma \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{s-1})(\alpha_s)$ tal que

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

o que prova o teorema. □

Definição 4.9. *Uma extensão algébrica $\mathbb{Q}(\theta)|\mathbb{Q}$ é dita normal se todo polinômio irredutível em $\mathbb{Q}[x]$ que tem pelo menos uma raiz em $\mathbb{Q}(\theta)$, tiver todas as raízes em $\mathbb{Q}(\theta)$.*

Lema 4.4. *Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ uma extensão algébrica, se $\alpha_1, \alpha_2, \ldots, \alpha_s$ são algébricos sobre $\mathbb{Q}$. Então existem θ algébrico sobre $\mathbb{Q}$ e uma extensão $\mathbb{Q}(\theta)|\mathbb{Q}$ normal tal que*

$$\mathbb{Q}(\theta) \supset \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_s)$$

Demonstração. Pelo Teorema 4.4, existe γ algébrico sobre $\mathbb{Q}$ tal que

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

Considere $P_{\gamma,\mathbb{Q}}$ o polinômio minimal de γ. Sejam $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_m$ as m raízes de $P_{\gamma,\mathbb{Q}}$. Aplicando novamente o Teorema 4.4, temos que existe θ algébrico tal que

$$\mathbb{Q}(\theta) = \mathbb{Q}(\gamma_1, \gamma_2, \ldots, \gamma_m) \supset \mathbb{Q}(\gamma) = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_s)$$

Resta-nos provar que a extensão $\mathbb{Q}(\theta)|\mathbb{Q}$ é normal. Com efeito, considere $g(x) \in \mathbb{Q}[x]$ irredutível e mônico com uma raiz $\alpha \in \mathbb{Q}(\theta)$. Mostraremos que toda raiz de $g(x)$ pertence a $\mathbb{Q}(\theta)$. Como $\alpha \in \mathbb{Q}(\theta) = \mathbb{Q}(\gamma_1, \gamma_2, \ldots, \gamma_m)$. Então $\alpha = f(\gamma_1, \gamma_2, \ldots, \gamma_m)$ para algum polinômio $f(x_1, x_2, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$. Defina o seguinte polinômio:

$$G(x) = \prod_{\sigma \in S_m} \Big(x - f(\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \ldots, \gamma_{\sigma(m)}) \Big)$$

onde S_m é o conjunto das permutações de $\{1, \ldots, m\}$, o qual possuem $m!$ permutação.

Assim, o grau $\partial G(x) = m!$ quando o produto é tomado sobre todas as permutações e os coeficientes de $G(x)$ são escritos em termos de funções simétricas em suas raízes: $\{f(\gamma_1, \gamma_2, \ldots, \gamma_m)\}_{\sigma \in S_m}$. Dessa forma, quando permutamos $\{\gamma_1, \gamma_2, \ldots, \gamma_m\}$ em f temos que $\big\{f(\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \ldots, \gamma_{\sigma(m)})\big\}_{\sigma \in S_m}$ fica invariante, isto é,

$$f(\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \ldots, \gamma_{\sigma(m)}) = f(\gamma_1, \gamma_2, \ldots, \gamma_m) = \alpha \in \mathbb{Q}(\theta)$$

Assim, os coeficientes de $G(x)$ são funções simétricas em $\gamma_1, \gamma_2, \ldots, \gamma_m$, em particular, $G(x)$ é polinômio simétrico e pelo Lema 4.3, são racionais, daí $G(x) \in \mathbb{Q}[x]$ e como $G(\alpha) = 0$ e $g(x) = P_{\alpha,\mathbb{Q}}$ é polinômio minimal de α, sendo $g(\alpha) = 0$. Daí, os polinômios $G(x)$ e $g(x)$ tem a raiz α em comum. Pela Proposição 4.1, $g(x)$ divide $G(x)$, isto é

$G(x) = g(x)h(x)$ para algum $h(x) \in \mathbb{Q}[x]$. Sejam $a_1, a_2, \ldots, a_l$ as raízes de $g(x)$, então

$$G(a_j) = \underbrace{g(a_j)}_{0} h(a_j) = 0, \quad \text{com} \quad j = 1, \ldots, l \in \mathbb{N}$$

Por conseguinte, a_j é raiz de $G(x)$ para todo $j = 1, \ldots, l \in \mathbb{N}$. Aplicando a_j na expressão de $G(x)$, tem-se

$$G(a_j) = \prod_{\sigma \in S_m} \Big(a_j - f(\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \ldots, \gamma_{\sigma(m)}) \Big) = 0$$

Dessa forma, deve existir uma permutação $\bar{\sigma} \in S_m$ tal que todas raízes de $g(x)$ estão em $\mathbb{Q}(\theta)$, isto é,

$$a_j = f(\gamma_{\bar{\sigma}(1)}, \gamma_{\bar{\sigma}(2)}, \ldots, \gamma_{\bar{\sigma}(m)}) = f(\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \ldots, \gamma_{\sigma(m)}) \in \mathbb{Q}(\theta)$$

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

□

4.1.4 Conjugado de um Elemento Algébrico

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

Definição 4.10. *Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ um extensão algébrica. Dado $\gamma \in \mathbb{Q}(\theta)$, pelo Lema 4.1, tem-se $\gamma = \sum_{j=0}^{n-1} a_j \theta^j = h(\theta)$ de forma única, para algum $h(x) \in \mathbb{Q}[x]$ e $\partial h \leq n-1$. Seja $\theta = \theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ as n raízes do polinômio minimal de θ sobre $\mathbb{Q}$. Então*

$$\gamma^{(i)} = \sum_{j=0}^{n-1} a_j (\theta^{(i)})^j = h(\theta^{(i)}), \quad 1 \leq i \leq n \in \mathbb{N}.$$

são chamados conjugados de γ sobre $\mathbb{Q}(\theta)$ e para facilitar representamos por:

$$\gamma = \gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(n)}$$

.

Proposição 4.3. *Sejam α e β números algébricos em um corpo K de grau n sobre $\mathbb{Q}$ os racionais. Se os conjugados de α sobre K são $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ e os de β são $\beta = \beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(n)}$. Então*

(i) $(\alpha+\beta)^{(i)} = \alpha^{(i)} + \beta^{(i)}, \quad$ *para* $\quad 1 \leq i \leq n \in \mathbb{N}$;

(ii) $(\alpha.\beta)^{(i)} = \alpha^{(i)}.\beta^{(i)}, \quad$ *para* $\quad 1 \leq i \leq n \in \mathbb{N}$.

Demonstração. **Item (i).** Como $[K : \mathbb{Q}] = n$, então existe θ tal que $K = \mathbb{Q}(\theta)$. Assim, $\alpha = h(\theta) = \sum_{j=0}^{n-1} a_j\theta^j$ e $\beta = g(\theta) = \sum_{j=0}^{n-1} b_j\theta^j$, onde $h(x) = \sum_{j=0}^{n-1} a_jx^j$ e $g(x) = \sum_{j=0}^{n-1} b_jx^j$ estão em $\mathbb{Q}[x]$, com $a_j, b_j \in \mathbb{Q}$. Segue-se que

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

onde $f(x) = \sum_{j=0}^{n-1}(a_j + b_j)x^j \in \mathbb{Q}[x]$. Para $i = 1, \ldots, n \in \mathbb{N}$, aplicando o conjugado, tem-se

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

O item (ii). é análogo. □

Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ uma extensão algébrica de grau n sobre $\mathbb{Q}$. Note que γ tem n conjugados sobre $\mathbb{Q}(\theta)$ no novo tipo, e m conjugados sobre $\mathbb{Q}$ no antigo, onde $m|n$. A relação entre os dois conceitos de conjugados será estabelecida a seguir, no Teorema 4.5.

Teorema 4.5. *Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ uma extensão algébrica de grau n sobre $\mathbb{Q}$. Então*
(i) Os conjugados de γ sobre $\mathbb{Q}(\theta)$ são os conjugados sobre $\mathbb{Q}$ todos repetidos $\frac{n}{m}$ vezes;
(ii) O elemento $\gamma \in \mathbb{Q}$ se, e somente se, todos seus conjugados sobre $\mathbb{Q}(\theta)$ são iguais;
(iii) $\mathbb{Q}(\gamma) = \mathbb{Q}(\theta)$ se, e somente se, todos os conjugados de γ sobre $\mathbb{Q}(\theta)$ são distintos.

Demonstração. **item (i).** Seja $\gamma \in \mathbb{Q}(\theta)$, então $\gamma = r(\theta)$, sendo $r(x) \in \mathbb{Q}[x]$, onde θ é algébrico de grau n tal que $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ são seus conjugados. Considere o seguinte polinômio simétrico mônico:

$$F(x) = \prod_{i=1}^{n} \left(x - r(\theta^{(i)})\right)$$

com coeficientes racionais. Note que

$$F(\gamma) = \prod_{i=1}^{n} \left(r(\theta) - r(\theta^{(i)})\right) = 0$$

pois, considerando $\theta = \theta^{(1)}$, temos $\gamma = r(\theta) = r(\theta^{(1)})$ é raiz de $F(x)$. Como $F(x)$ é simétrico, então Pelo Teorema Fundamental das Funções Simétricas 4.3, ele pode ser expresso em termos de funções simétricas elementares em x. Por outro lado, como podemos escrever $F(x)$ da forma:

$$F(x) = \prod_{i=1}^{n} \left(x - r(\theta^{(i)})\right) = x^n + \sum_{i=1}^{n} \sigma_i(r(\theta), \ldots, r(\theta^{(n)}))x^{n-i}(-1)^i$$

e assim, podemos escrever seus coeficientes como polinômios em x, e estão em $\mathbb{Q}$.

Seja $P_{\gamma,\mathbb{Q}}(x)$ o polinômio minimal (mônico) de γ sobre $\mathbb{Q}$ tal que $P_{\gamma,\mathbb{Q}}(\gamma) = 0$. Então como $F(\gamma) = 0$, tem-se $P_{\gamma,\mathbb{Q}}(x)$ divide $F(x)$. Assim, podemos escrever:

$$F(x) = [P_{\gamma,\mathbb{Q}}(x)]^S \, h(x), \qquad h(x) \in \mathbb{Q}[x].$$

(onde S será especificado posteriormente) e $P_{\gamma,\mathbb{Q}}(x)$ e $h(x)$ são primos entre si.

Mostraremos que $h(x) = 1$. Note que, se $h(x) = c$ é constante, então deve ser igual 1, visto que, $P_{\gamma,\mathbb{Q}}(x)$ e $F(x)$ são mônicos (coeficiente líder igual a 1). Se $h(x)$ não é um polinômio constante, ele possui um dos $r(\theta^{(i)})$ como raiz, digamos $r(\theta^{(1)})$. Então

$$h(r(x)) = 0, \quad \text{quando} \quad x = \theta^{(1)}$$

Seja $G_{\theta,\mathbb{Q}}(x)$ o polinômio minimal de θ tal que para todo $i = 1, \ldots, n \in \mathbb{N}$, $G_{\theta,\mathbb{Q}}(\theta^{(i)}) = 0$, em particular, para $x = \theta^{(1)}$, temos que $G_{\theta,\mathbb{Q}}(x) = 0$, pela Proposição 4.1, segue-se que $G_{\theta,\mathbb{Q}}(x)$ divide $h(r(x))$. Dessa forma, tem-se

$$h(r(x)) = G_{\theta,\mathbb{Q}}(x)u(x), \qquad u(x) \in \mathbb{Q}[x].$$

Daí, aplicando o i-ésimo conjugado de θ, temos

$$h(r(\theta^{(i)})) = \underbrace{G_{\theta,\mathbb{Q}}(\theta^{(i)})}_{0} u(\theta^{(i)}) = 0, \quad i = 1, 2, \ldots, n \in \mathbb{N}.$$

Logo, $h(r(\theta^{(i)})) = 0$, para todo $\theta^{(i)}$, com $i = 1, \ldots, n \in \mathbb{N}$, em particular, para θ.

Assim, temos

$$h(r(\theta)) = h(\gamma) = 0$$

o que é impossível, pois $P_{\gamma,\mathbb{Q}}(\gamma) = 0$ e $P_{\gamma,\mathbb{Q}}(x)$ e $h(x)$ são primos entre si, o que implica que eles não podem possuir raíz em comum. Com efeito, (Suponha que eles possuem uma raiz em comum. Se $mdc\,(P_{\gamma,\mathbb{Q}}(x), h(x)) = 1$, existiria um $q(x), v(x) \in \mathbb{Q}[x]$ tal que $P_{\gamma,\mathbb{Q}}(x)q(x) + h(x)v(x) = 1 \Longrightarrow \underbrace{P_{\gamma,\mathbb{Q}}(\gamma)}_{0} q(\gamma) + \underbrace{h(\gamma)}_{0} v(\gamma) = 1 \Longrightarrow 0 = 1$) o que é uma

contradição. Segue-se que $h(x)$ é constante e essa deve ser 1, $(h(x) = 1)$. Logo,

$$F(x) = [P_{\gamma,\mathbb{Q}}(x)]^S$$

Desde que m é o grau de γ sobre $\mathbb{Q}$, tem-se $S = \frac{n}{m}$ e o polinômio $F(x)$ é uma potência do polinômio minimal. Logo,

$$F(x) = [P_{\gamma,\mathbb{Q}}(x)]^{\frac{n}{m}} = \underbrace{(P_{\gamma,\mathbb{Q}}(x))\,(P_{\gamma,\mathbb{Q}}(x))\cdots(P_{\gamma,\mathbb{Q}}(x))}_{\frac{n}{m}-vezes}$$

Portanto, os conjugados de γ sobre $\mathbb{Q}(\theta)$ são os conjugados sobre $\mathbb{Q}$ todos repetidos $\frac{n}{m}$ vezes. □

Demonstração. **item (ii).** Se $\gamma \in \mathbb{Q}$. Então existem um polinômio minimal (mônico de menor grau para o qual γ é raiz sobre $\mathbb{Q}$):

$$P_{\gamma,\mathbb{Q}}(x) = (x-\gamma)^1 \in \mathbb{Q}[x]$$

tal que $\partial P_{\gamma,\mathbb{Q}}(x) = m = 1$. Usando o item (i) acima, tem-se que $S = \frac{n}{m} = n$. Daí,

$$F(x) = [P_{\gamma,\mathbb{Q}}(x)]^S = [P_{\gamma,\mathbb{Q}}(x)]^n \Longrightarrow F(x) = (x-\gamma)^n$$

Logo, todos os conjugados de $\gamma = \gamma^{(1)} = \gamma^{(2)} = \ldots = \gamma^{(n)}$ devem ser iguais para que sejam raízes de $F(x)$.

Reciprocamente, se todos os conjugados de $\gamma = \gamma^{(i)} = \ldots = \gamma^{(n)}$ são os mesmos, em $F(x) = (x-\gamma)^n$ com coeficientes racionais. Assim, pelo item (i), $S = n$ o que implica $m = 1$. Note que,

$$\begin{aligned} F(x) &= (x-\gamma)(x-\gamma)\cdots(x-\gamma) \\ &= x^n - \big(\sum_{i=1}^{n}\gamma\big)x^{n-1} + \cdots + (-1)^n\big(\prod_{i=1}^{n}\gamma\big) \\ &= x^n - \sigma_1(\gamma,\gamma,\ldots,\gamma)x^{n-1} + \cdots + (-1)^n\sigma_n(\gamma,\gamma,\ldots,\gamma). \end{aligned}$$

Daí, $\sigma_1(\gamma,\gamma,\ldots,\gamma) = \sum_{i=1}^{n}\gamma = n\gamma \in \mathbb{Q}$. Por conseguinte, $n\gamma = \frac{c}{d}$, com $c, d \in \mathbb{Z}$, $d \neq 0$ e $n \in \mathbb{N}^*$. Portanto, o número gama $\gamma = \frac{c}{nd} \in \mathbb{Q}$ é racional. □

Demonstração. **item (iii).** Seja o grau da extensão $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$. Note que usando o Teorema da Multiplicatividade do Grau 4.2 (parte I e em seguida parte II), teremos

$$[\mathbb{Q}(\theta) : \mathbb{Q}] = [\mathbb{Q}(\theta) : \mathbb{Q}(\gamma)]\,.\,[\mathbb{Q}(\gamma) : \mathbb{Q}]$$

e a extensão $\mathbb{Q}(\gamma) = \mathbb{Q}(\theta)$, se, e somente se,

$$n = [\mathbb{Q}(\theta) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\gamma) : \mathbb{Q}(\gamma)]}_{1} . \underbrace{[\mathbb{Q}(\gamma) : \mathbb{Q}]}_{m}$$

e $m = n$ e $S = \frac{m}{m} = 1$ se, e somente se $F(x) = [P_{\gamma,\mathbb{Q}}(x)]^1$ e não teremos repetições de conjugados. Portanto, todos os conjugados de γ são distintos. □

Observação 4.3. A primeiro momento parece que os conjugados $\gamma^{(i)} = h(\theta^{(i)})$ dependem de uma escolha particular de θ. No entanto, eles dependem apenas do corpo que está sendo considerado. Para maiores detalhes Ver [13], p. 66-68.

4.1.5 Norma de um Elemento Algébrico

Definição 4.11. *Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ um extensão algébrica de grau n. Então denotamos (a norma de α) por $N(\alpha)$ e a definimos como o produto dos conjugados de α sobre $\mathbb{Q}(\theta)$, isto é, $N(\alpha) = \alpha^{(1)} \cdot \alpha^{(2)} \cdots \alpha^{(n)}$.*

Lembremos que em uma extensão $K|\mathbb{Q}$. Um número $\alpha \in K$ é dito um **inteiro algébrico** se for raiz de um polinômio mônico com coeficientes inteiros de menor grau para o qual α é raiz.

Proposição 4.4. *Sejam $\mathbb{Q}(\theta)|\mathbb{Q}$ um extensão algébrica de grau $n \in \mathbb{N}$ e α, $\beta \in \mathbb{Q}(\theta)$. Então*
(i) $N(\alpha\beta) = N(\alpha)N(\beta)$;
(ii) $N(\alpha) = 0$ se, e somente se, $\alpha = 0$;
(iii) Se α é inteiro algébrico não nulo. Então $N(\alpha) \in \mathbb{Z} - \{0\}$;
(iv) Se α é racional. Então $N(\alpha) = \alpha^n$, onde $n = [\mathbb{Q}(\theta) : \mathbb{Q}]$.

Demonstração. **Item (i).** Pela Proposição 4.3 item (ii), temos que o conjugado do produto é o produto dos conjugados, segue-se

$$\begin{aligned} N(\alpha\beta) &= (\alpha\beta)^{(1)}(\alpha\beta)^{(2)} \cdots (\alpha\beta)^{(n)} \\ &= (\alpha^{(1)}\beta^{(1)})(\alpha^{(2)}\beta^{(2)}) \cdots (\alpha^{(n)}\beta^{(n)}) \\ &= \alpha^{(1)}\alpha^{(2)} \cdots \alpha^{(n)}\beta^{(1)}\beta^{(2)} \cdots \beta^{(n)} \\ &= N(\alpha)N(\beta). \end{aligned}$$

□

Demonstração. **Item (ii).** Suponha que $N(\alpha) = 0$, como $N(\alpha) = \alpha^{(1)}\alpha^{(2)} \cdots \alpha^{(n)} = 0$,

então $\alpha^{(i)} = 0$ para algum $i \in \{1, \ldots, n\}$, mas

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

Logo, $a_0 = a_1 = \ldots = a_{n-1} = 0$ e portanto, $\alpha = \sum_{j=0}^{n-1} a_j \theta^j = 0$.

Reciprocamente, se $\alpha = 0$ claramente $N(\alpha) = 0$. □

Demonstração. **Item (iii).** Seja α inteiro algébrico, então existe um polinômio minimal (mônico) $P_{\alpha,\mathbb{Z}}(x)$ com coeficientes inteiros tal que suas raízes são os conjugados $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ de α, cujo coeficiente do termo de maior grau é 1, isto é,

$$P_{\alpha,\mathbb{Z}}(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n, \quad a_i \in \mathbb{Z} - \{0\}, \quad i = 1, \ldots, n \in \mathbb{N}.$$

Pela Observação 4.2 e passando os conjugados, temos

$$\begin{aligned} P_{\alpha,\mathbb{Z}}(x) &= (x - \alpha^{(1)})(x - \alpha^{(2)}) \cdots (x - \alpha^{(n)}) \\ &= x^n - \sigma_1(\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}) x^{n-1} + \cdots + (-1)^n \sigma_n(\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}) \end{aligned}$$

Por conseguinte, temos que $\sigma_i(\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}) = (-1)^i a_i \in \mathbb{Z}$, para $i = 1, \ldots, n \in \mathbb{N}$. O resultado segue, pois

$$N(\alpha) = \alpha^{(1)} \alpha^{(2)} \cdots \alpha^{(n)} = \sigma_n(\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}) = (-1)^n a_n \in \mathbb{Z} - \{0\}.$$

□

Demonstração. **Item (iv).** Se $\alpha \in \mathbb{Q} \subset \mathbb{Q}(\theta)$, então $\alpha = h(\theta)$. Pelo Teorema 4.5 item (ii), todos os conjugados de α são iguais sobre $\mathbb{Q}(\theta)$, isto é, $\alpha^{(i)} = h(\theta^{(i)}) = \alpha$ para todo $i = 1, \ldots, n \in \mathbb{N}$. Portanto, a norma de α é:

$$N(\alpha) = \alpha^{(1)} \alpha^{(2)} \cdots \alpha^{(n)} = \underbrace{\alpha.\alpha \cdots \alpha}_{\text{n-fatores}} = \alpha^n.$$

□

Vale salientar que a norma $N(\alpha)$ depende do corpo que está sendo considerado.

4.1.6 Inteiro Algébrico e Base Integral

Definição 4.12. *Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ um extensão algébrica de grau n. O conjunto de inteiros algébricos $\{\alpha_1, \ldots, \alpha_n\}$ é chamada base integral de $\mathbb{Q}(\theta)$, se todo $\alpha \in \mathbb{Q}(\theta)$ inteiro*

algébrico pode ser escrito de forma única como

$$\alpha = b_1\alpha_1 + \cdots + b_n\alpha_n, \quad b_i \in \mathbb{Z}, \quad i = 1, \ldots n \in \mathbb{N}.$$

Definição 4.13. *Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ um extensão algébrica de grau n. O discriminante de um base $\{\alpha_1, \ldots, \alpha_n\}$ de $\mathbb{Q}(\theta)|\mathbb{Q}$ é definido por*

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

onde $\alpha_j^{(i)}$ é o i-ésimo conjugado de α_j, para $1 \leq i, j \leq n \in \mathbb{N}$.

Vejamos alguns resultados referentes a inteiros algébricos que serão úteis posteriormente.

Teorema 4.6. *Se α é um número algébrico. Então existe $r \in \mathbb{Z}$ não nulo tal que $r\alpha$ é um inteiro algébrico.*

Demonstração. Como α é algébrico. Então existe um polinômio minimal (mônico) $P(x) \in \mathbb{Q}[x]$ de grau n, isto é,

$$P(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$$

Como $P(x) \in \mathbb{Q}[x]$, podemos supor sem perda de generalidade que $a_i = \frac{b_i}{c_i} \in \mathbb{Q}$, onde $b_i \in \mathbb{Z}$, $c_i \in \mathbb{Z}$, sendo $c_i > 0$, com $i = 0, \ldots, n-1 \in \mathbb{N}$.

Considere $r = (c_0c_1 \cdots c_{n-2}c_{n-1}) \in \mathbb{Z} - \{0\}$. Substituindo $a_i = \frac{b_i}{c_i}$ em $P(x)$, obtemos

$$P(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1}x + \cdots + \frac{b_{n-1}}{c_{n-1}}x^{n-1} + x^n$$

Como $P(\alpha) = 0$, tem-se

$$0 = \frac{b_0}{c_0} + \frac{b_1}{c_1}\alpha + \cdots + \frac{b_{n-1}}{c_{n-1}}\alpha^{n-1} + \alpha^n$$

Multiplicando a igualdade acima por $r^n = (c_0^nc_1^n \cdots c_{n-2}^nc_{n-1}^n) \in \mathbb{Z} - \{0\}$, temos

$$0 = \frac{b_0}{c_0}(c_0^n \cdots c_{n-1}^n) + \frac{b_1}{c_1}(c_0^nc_1^n \cdots c_{n-2}^nc_{n-1}^n)\alpha + \cdots + \frac{b_{n-1}}{c_{n-1}}(c_0^nc_1^n \cdots c_{n-2}^nc_{n-1}^n)\alpha^{n-1} + r^n\alpha^n$$

Supondo $n > 1 \Longrightarrow n - 2 > -1$, daí, $n - 2 \geq 0$ e cancelando os c_i do denominador,

tem-se

$$0 = b_0(c_0^{n-1}\cdots c_{n-1}^n)+b_1(c_0^n c_1^{n-1}\cdots c_{n-2}^n c_{n-1}^n)\alpha+\cdots+b_{n-1}(c_0^n c_1^n\cdots c_{n-2}^n c_{n-1}^{n-1})\alpha^{n-1}+(r\alpha)^n$$

Daí,

$$0 = b_0(c_0^{n-1}\cdots c_{n-1}^n) + b_1(c_0^{n-1}c_1^{n-2}\cdots c_{n-2}^{n-1}c_{n-1}^{n-1})\underbrace{(c_0c_1\cdots c_{n-2}c_{n-1})}_{r}\alpha+\cdots+$$
$$+\cdots+ b_{n-1}(c_0c_1\cdots c_{n-2})\underbrace{(c_0^{n-1}c_1^{n-1}\cdots c_{n-2}^{n-1}c_{n-1}^{n-1})}_{r^{n-1}}\alpha^{n-1}+(r\alpha)^n$$

Por conseguinte,

$$0 = b_0(c_0^{n-1}\cdots c_{n-1}^n)+b_1(c_0^{n-1}c_1^{n-2}\cdots c_{n-2}^{n-1}c_{n-1}^{n-1})r\alpha+\cdots+b_{n-1}(c_0c_1\cdots c_{n-2})(r\alpha)^{n-1}+(r\alpha)^n$$

Logo, $r\alpha$ é raiz de um polinômio mônico de grau n irredutível com coeficientes inteiros. Portanto, o número $r\alpha$ é um inteiro algébrico. □

O teorema acima afirma que a partir de um número algébrico é sempre possível obter um inteiro algébrico. Dessa forma, convém notar na observação a seguir algumas propriedades dos *inteiros algébricos*.

Observação 4.4. Vale salientar que a soma, diferença e o produto de *inteiros algébricos* são inteiros algébricos. Além disso, se α é um inteiro algébrico, então seus conjugados $\alpha^{(i)}$ também o são, visto que, todo inteiro algébrico é um número algébrico e que o conjunto dos algébricos formam um corpo. Por outro lado, um *inteiro algébrico* é número inteiro ou irracional, confirma o Teorema 1.1.

A seguir vamos demonstrar em detalhes alguns Teoremas clássicos e úteis sobre base integral, discriminante e inteiro algébrico.

Lema 4.5. *Se $\alpha_1, \alpha_2, \ldots, \alpha_n$ formam uma base de K sobre $\mathbb{Q}$ tal que*

$$\beta_k = \sum_{j=1}^{n} c_{jk}\alpha_j, \qquad c_{jk} \in \mathbb{Q}, \quad k = 1, 2, \ldots, n \in \mathbb{N}$$

Então $\beta_1, \beta_2, \ldots, \beta_n$ é também uma base se, e somente se, o determinante da matriz dos coeficientes é não nulo, isto é, $det\,(c_{jk}) \neq 0$.

Demonstração. ($\Longleftarrow$). Suponhamos que o $det\,(c_{jk}) \neq 0$. Como por hipótese β_k está escrito como combinação linear de α_j o qual gera K, então β_k também gera K. Basta

mostrar que os β_k são (L.I.), para todo $k = 1, \ldots, n \in \mathbb{N}$. Suponha

$$\sum_{k=1}^{n} a_k \beta_k = 0, \qquad a_k \in \mathbb{Q}, \quad k = 1, \ldots, n \in \mathbb{N}$$

Então,

$$0 = \sum_{k=1}^{n} a_k \sum_{j=1}^{n} c_{jk} \alpha_j = \sum_{k=1}^{n} a_k c_{jk} \sum_{j=1}^{n} \alpha_j$$

Como os α_j são (L.I.), tem-se ($\alpha_j \neq 0$, para todo $i = 1, \ldots, n \in \mathbb{N}$). Logo,

$$\sum_{k=1}^{n} a_k c_{jk} = 0, \qquad j = 1, \ldots, n \in \mathbb{N}$$

Como por hipótese o determinante da matriz dos coeficientes é não nula, ou seja, $det\,(c_{jk}) \neq 0$. Segue-se que $a_k = 0$, para $k = 1, \ldots, n \in \mathbb{N}$. Logo, os β_k são (L.I.) para todo $k = 1, \ldots, n \in \mathbb{N}$. Portanto, os $\beta_1, \beta_2, \ldots, \beta_n$ também formam uma base.

($\Longrightarrow$). A recíproca, será demostrada pela contrapositiva:

Suponha que $det\,(c_{jk}) = 0$. Refazendo os passos anteriores, ou seja, suponha que

$$\sum_{k=1}^{n} a_k \beta_k = 0 \Longrightarrow \sum_{k=1}^{n} a_k \sum_{j=1}^{n} c_{jk} \alpha_j = \sum_{k=1}^{n} a_k c_{jk} \sum_{j=1}^{n} \alpha_j = 0$$

Como os α_j são (L.I.) Logo,

$$\sum_{k=1}^{n} a_k c_{jk} = 0, \qquad j = 1, \ldots, n \in \mathbb{N}$$

Como por hipótese $det\,(c_{jk}) = 0$, existe pelo menos uma solução não trivial com a_k não todos nulos. Dessa forma, como

$$\sum_{k=1}^{n} a_k \beta_k = 0, \quad a_k \neq 0, \quad \text{para algum} \quad k = 1, \ldots, n \in \mathbb{N}$$

Segue-se que os β_k são (L.D.) Portanto, os $\beta_1, \beta_2, \ldots, \beta_n$ não formam uma base. □

Teorema 4.7. *Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ um extensão algébrica de grau n. Então toda base integral de um corpo K é uma base.*

Demonstração. Seja $\{\alpha_1, \alpha_2, \ldots, \alpha_s\}$ uma base integral de K tal que $\alpha, \alpha_2, \ldots, \alpha_s$ são inteiros algébricos. Dado $\alpha \in K$ inteiro algébrico, pelo Teorema 4.6, existe um número inteiro $r \in \mathbb{Z}$ não nulo tal que $r\alpha \in K$ é um inteiro algébrico. Consequentemente, por

definição de base integral podemos escrever de forma única como:

$$r\alpha = b_1\alpha_1 + b_2\alpha_2 + \ldots + b_s\alpha_s, \qquad b_i \in \mathbb{Z}, \quad i = 1, \ldots, s \in \mathbb{N}$$

Daí,

$$\alpha = \frac{b_1}{r}\alpha_1 + \frac{b_2}{r}\alpha_2 + \ldots + \frac{b_s}{r}\alpha_s, \qquad \frac{b_i}{r} \in \mathbb{Q}, \quad i = 1, \ldots, s \in \mathbb{N}$$

Assim, como todo $\alpha \in K$ é gerado por α_i, com $\dfrac{b_i}{r} \in \mathbb{Q}$, para $i = 1, \ldots, s \in \mathbb{N}$. Basta mostrar que os α_i são (L.I.). Suponhamos que

$$c_1\alpha_1 + c_2\alpha_2 + \ldots + c_s\alpha_s = 0, \qquad c_i \in \mathbb{Q}, \quad i = 1, \ldots, s \in \mathbb{N}$$

Multiplicando a equação acima pelo menor denominador D positivo comum dos c_i, s, $(D.c_i)$ de modo que obtemos a seguinte relação

$$d_1\alpha_1 + d_2\alpha_2 + \ldots + d_s\alpha_s = 0, \qquad d_i \in \mathbb{Z}, \quad i = 1, \ldots, s \in \mathbb{N}$$

e por definição de base integral (essa representação deve ser única) e assim os d_i são todos nulos, $(d_i = 0)$, por conseguinte, os $c_i = \dfrac{d_i}{D} = 0$. Logo, os α_i são (L.I.) sobre $\mathbb{Q}$, para todo $i = 1, \ldots, s \in \mathbb{N}$. Portanto, o conjunto $\{\alpha_1, \alpha_2, \ldots, \alpha_s\}$ é base. Considerando $K := \mathbb{Q}(\theta)$ segue-se imediatamente que $s = n$, visto que o número de elementos de uma base é igual ao grau da extensão $n = [\mathbb{Q}(\theta) : \mathbb{Q}]$. □

Teorema 4.8. *Se $\alpha_1, \ldots, \alpha_n$ formam uma base cujos elementos são inteiros algébricos da extensão algébrica $\mathbb{Q}(\theta)|\mathbb{Q}$ de grau n. Então o discriminante dessa base*

$$\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Z} - \{0\}\,.$$

é um número inteiro não nulo.

Demonstração. Suponhamos que a extensão tem grau $[K : \mathbb{Q}] = n$. Primeiro, vejamos que o discriminante está bem definido, pois seu valor não depende da base, cujos elementos são inteiros algébricos, em seguida veremos que é um racional, para assim concluirmos a demonstração. Em outras palavras, dados $\alpha_1, \alpha_2, \ldots, \alpha_n$ e $\beta_1, \beta_2, \ldots, \beta_n$ duas bases para K, veremos que os discriminantes diferem apenas pelo um fator quadrático.

Note que, se

$$\beta_k = \sum_{j=1}^{n} c_{jk}\alpha_j, \qquad c_{jk} \in \mathbb{Q}, \quad k = 1, 2, \ldots, n \in \mathbb{N}$$

é outra base tal que está escrita como combinação linear da base $\alpha_1, \ldots, \alpha_n$, então pelo Lema 4.5, o $det(c_{jk}) \neq 0$. Aplicando o i-ésimo conjugado, tem-se

$$\beta_k^{(i)} = \sum_{j=1}^{n} c_{jk}\alpha_j^{(i)}, \qquad i, k = 1, 2, \ldots, n \in \mathbb{N}$$

Por uma multiplicação de determinante, obtemos

$$det\left(\beta_k^{(i)}\right) = det\left(c_{jk}.\alpha_j^{(i)}\right) = det\left(c_{jk}\right).det\left(\alpha_j^{(i)}\right)$$

e elevando ao quadrado, temos

$$\left[det\left(\beta_k^{(i)}\right)\right]^2 = \left[det\left(c_{jk}\right)\right]^2 . \left[det\left(\alpha_j^{(i)}\right)\right]^2$$

Logo, resulta em uma importante fórmula:

$$\Delta[\beta_1, \ldots, \beta_n] = \left[det(c_{jk})\right]^2 \Delta[\alpha_1, \ldots, \alpha_n] \tag{4.8}$$

Pelo Lema 4.1, todo elemento de $K := \mathbb{Q}(\theta)$ pode ser escrito de maneira única da forma:

$$a_0 + a_1\theta + a_2\theta^2 + \ldots + a_{n-1}\theta^{n-1} = f(\theta), \qquad a_t \in \mathbb{Q}, \quad t = 0, 1, \ldots, n-1 \in \mathbb{N}$$

Todo elemento de $\mathbb{Q}(\theta)$ é combinação de $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ e pelo Lema 4.2, formam uma base de $\mathbb{Q}(\theta)$ sobre $\mathbb{Q}$ tal que o grau da extensão $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$.

Usando o fato de que $\left(\theta^t\right)^{(i)}$, (o i-ésimo conjugado da t-ésima potência de θ) é o mesmo que $\left(\theta^{(i)}\right)^t$, (a t-ésima potência do i-ésimo conjugado de θ). Assim, para $0 \leq t \leq n-1 \in \mathbb{N}$ e $1 \leq i \leq n \in \mathbb{N}$ encontramos o seguinte discriminante:

$$D(\theta) := \Delta\left[1, \theta, \theta^2, \ldots, \theta^{n-1}\right] = \left[det\left(\theta^t\right)^{(i)}\right]^2 = \left[det\begin{pmatrix} 1 & \theta^{(1)} & \left(\theta^{(1)}\right)^2 & \cdots & \left(\theta^{(1)}\right)^{n-1} \\ 1 & \theta^{(2)} & \left(\theta^{(2)}\right)^2 & \cdots & \left(\theta^{(2)}\right)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta^{(n)} & \left(\theta^{(n)}\right)^2 & \cdots & \left(\theta^{(n)}\right)^{n-1} \end{pmatrix}\right]^2$$

Note que esse é um determinante de Vandermonde (confira a Proposição 6.1), é conhecido por ter o seguinte valor:

$$\prod_{1 \leq t < i \leq n} \left(\theta^{(t)} - \theta^{(i)}\right)^2$$

Segue-se que

$$D(\theta) = \Delta\left[1, \theta, \theta^2, \ldots, \theta^{n-1}\right] = \prod_{1 \leq t < i \leq n} \left(\theta^{(t)} - \theta^{(i)}\right)^2$$

Como os conjugados de θ em $\mathbb{Q}(\theta)$ são distintos, então $D(\theta) \neq 0$. Note que $D(\theta)$ é simétrico em relação ao $\theta^{(i)}$ e enxergando $D(\theta)$ como uma expressão polinomial em que é constituída pelos conjugados de θ que são raízes de certo polinômio, e assim, pelo Lema 4.3, o discriminante $D(\theta) \in \mathbb{Q}$ é um racional.

Em (4.8), fazendo $\alpha_i = \theta^{i-1}$, para todo $i = 1, 2, \ldots, n \in \mathbb{N}$ e como $c_{jk} \in \mathbb{Q}$ tal que $det(c_{jk}) \neq 0$. Logo,

$$\Delta[\beta_1, \ldots, \beta_n] = [det(c_{jk})]^2 D(\theta) \in \mathbb{Q} - \{0\} \tag{4.9}$$

é um racional não nulo. Portanto, mostramos que o discriminante de toda base de $\mathbb{Q}(\theta)|\mathbb{Q}$ é diferente de zero e pertence a $\mathbb{Q}$.

Dessa forma, suponha que $\{\alpha_1, \ldots, \alpha_n\}$ forma uma base integral de $\mathbb{Q}(\theta)|\mathbb{Q}$, então por definição os α_j são inteiros algébricos, em particular, o $\alpha_j^{(i)}$ o i-ésimo conjugado de α_j também são inteiros algébricos. Consequentemente, para $i, j = 1, \ldots, n \in \mathbb{N}$, o discriminante:

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

é um inteiro algébrico, (visto que, no determinante teremos operações de soma, subtração e produto de inteiros algébricos os quais são inteiros algébricos). Por (4.9), temos que o discriminante

$$\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Q} - \{0\}$$

é um racional não nulo. Usando o Teorema 1.1, que diz que um inteiro algébrico é número inteiro ou irracional, sendo o discriminante $\Delta[\alpha_1, \ldots, \alpha_n]$ ao mesmo tempo um inteiro algébrico e racional não nulo, e assim, ele deve ser um inteiro não nulo. Portanto, o discriminante $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Z} - \{0\}$. □

Teorema 4.9. *Todo corpo de números algébricos possui pelo menos uma base integral.*

Demonstração. Seja $K := \mathbb{Q}(\theta)$ um corpo de números algébricos onde assumimos θ um inteiro algébrico. Considere todas as *bases* de K cujos elementos $1, \theta, \ldots, \theta^{n-1}$ são inteiros algébricos, (Não provaremos que $1, \theta, \ldots, \theta^{n-1}$ formam uma base integral, o fato de não ser necessário ficará aparente mais adiante).

Para uma determinada base (formada por inteiros algébricos) que será especificada

posteriormente, pelo Teorema 4.8, o discriminante de tal base é um inteiro não nulo, e assim, existe alguma base $w_1, \ldots, w_n$ de modo que podemos obter o determinante do discriminante de tal base, isto é,

$$det\Big(\Delta\left[w_1, \ldots, w_n\right]\Big) = d, \quad \text{sendo} \quad d \quad \text{mínimo.}$$

Pelo Teorema 4.8, temos $d \neq 0$. Agora, mostraremos que $w_1, \ldots, w_n$ é base integral. Suponhamos que não fosse uma base integral. Porém, em qualquer caso os $w_1, \ldots, w_n$ formam uma base, então existe $w \in K$ tal que

$$w = a_1w_1 + a_2w_2 + \ldots + a_nw_n$$

não de modo único, onde $a_j \in \mathbb{Q}$, com $j = 1, \ldots, n \in \mathbb{N}$, no entanto, não todos inteiros. Sem perda de generalidade, podemos supor que $a_1 \notin \mathbb{Z}$ é um racional não inteiro.

Escrevendo $a_1 = a + r$, com $a \in \mathbb{Z}$, $r \in \mathbb{Q}$ sendo $0 < r < 1$. Definamos

$$w_1^* = w - aw_1; \qquad \text{e} \qquad w_k^* = w_k, \quad \text{para} \quad k = 2, 3, \ldots, n \in \mathbb{N}$$

Daí, e da expressão de w, tem-se

$$w_1^* = w - aw_1 = a_1w_1 + a_2w_2 + \ldots + a_nw_n - aw_1 \qquad \text{e} \qquad w_2^* = w_2, \ldots, w_n^* = w_n.$$

Por conseguinte,

$$\begin{array}{rcl}
w_1^* = w - aw_1 & = & (a_1 - a)\,w_1 + a_2w_2 + a_3w_3 + \ldots + a_nw_n \\
w_2^* = w_2 & = & 0.w_1 + 1.w_2 + 0.w_3 + \ldots + 0.w_n \\
w_3^* = w_3 & = & 0.w_1 + 0.w_2 + 1.w_3 + \ldots + 0.w_n \\
\vdots & & \vdots \qquad \vdots \qquad \vdots \qquad \vdots \\
w_n^* = w_n & = & 0.w_1 + 0.w_2 + 0.w_3 + \ldots + 1.w_n
\end{array} \tag{4.10}$$

Dessa forma, tomando o determinante da matriz dos coeficientes, (que denotaremos por c_{jk}) das últimas igualdades acima, obtemos:

$$det\big(c_{jk}\big) = det\begin{pmatrix} a_1 - a & a_2 & a_3 & \cdots & a_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} = (a_1 - a) = r > 0$$

Segue-se que o determinante da matriz dos coeficientes de $w_1, \ldots, w_n$ é diferente de zero, $det\big(c_{jk}\big) = r \neq 0$. Como $w_1, \ldots w_n$ formam uma base de K, e de (4.10) temos que w_k^* está escrito como combinação linear de $w_1, \ldots, w_n$, isto é,

$$w_k^* = \sum_{j=1}^{n} c_{jk} w_j, \qquad k = 1, 2, \ldots, n \in \mathbb{N}$$

Logo, pelo Lema 4.5, $w_1^*, \ldots, w_n^*$ é também uma base. Aplicando o conjugado, temos

$$(w_k^*)^{(i)} = \sum_{j=1}^{n} c_{jk} w_j^{(i)}, \qquad i, k = 1, 2, \ldots, n \in \mathbb{N}$$

Pela multiplicação de determinante e elevando ao quadrado, segue-se

$$\left[det\left((w_k^*)^{(i)}\right)\right]^2 = \left[det\left(c_{jk}\right)\right]^2 . \left[det\left(w_j^{(i)}\right)\right]^2$$

Por conseguinte,

$$\Delta[w_1^*, \ldots, w_n^*] = [det(r)]^2 \, \Delta[w_1, \ldots, w_n]$$

Daí, resulta em:

$$\Delta[w_1^*, \ldots, w_n^*] = r^2 \Delta[w_1, \ldots, w_n]$$

Tomando o determinante da igualdade acima, e como $0 < r < 1$, obtemos

$$det\Big(\Delta\left[w_1^*, \ldots, w_n^*\right]\Big) = r^2 det\Big(\Delta\left[w_1, \ldots, w_n\right]\Big) < det\Big(\Delta\left[w_1, \ldots, w_n\right]\Big) = d$$

o que contraria escolha do determinante, $det\Big(\Delta\left[w_1, \ldots, w_n\right]\Big) = d$ como mínimo, e tal contradição decorre do fato de supormos que $w_1, \ldots w_n$ não é base integral. Logo, existe pelo menos uma base integral em um corpo de números algébricos. Além disso, por razões que estão claras acima, uma base integral é também chamada de base minimal. □

Próximo capítulo será dedicado à generalização do teorema de Lindemann e algumas consequências.

Capítulo 5

Uma Generalização do Teorema de Lindemann

Neste capítulo apresentaremos em detalhes uma generalização do Teorema de Lindemann estabelecido por Hermite-Lidemann, e ainda, algumas consequências mais gerais como a transcendência de certos números e funções trigonométricas como: e^{α}, e, π, $\log(\alpha)$, $\sin(\alpha), \cos(\alpha)$ e $\tan(\alpha)$, sendo α algébrico. A principal referência utilizada na elaboração deste capítulo é Niven [12].

5.1 Resultados Preliminares

Vimos no Capítulo 3 que o número e é transcendente resultado dado por Hermite em 1873, mais tarde, Lindemann estendeu seu método provar a transcendência de π e e^{α} os quais são casos especiais de um teorema mais geral que será o assunto principal deste capítulo.

Lema 5.1. *Considere q polinômios $P_1(y_1, \ldots, y_m), \ldots, P_q(y_1, \ldots, y_m)$ em m variáveis $y_1, \ldots, y_m$ dados por:*

$$P_j := P_j(y_1, \ldots, y_m) = f_1(x_j)\, y_1 + \ldots + f_m(x_j)\, y_m, \quad j = 1, \ldots, q, \quad i = 1, \ldots, m \in \mathbb{N}$$

com coeficientes $f_i(x_j)$, os quais são polinômios sobre um corpo $\mathbb{K}$. O produto

$$P_1 P_2 \cdots P_q = \prod_{j=1}^{q} \sum_{i=1}^{m} f_i(x_j)\, y_i$$

desses polinômios quando os termos são agrupados em y_i, os coeficientes de $f_i(x_j)$ são polinômios simétricos em $x_1, \ldots, x_q$.

Demonstração. Note que, se

$$\begin{aligned} P_1P_2\cdots P_q &= \sum_{i=1}^{m} f_i(x_1)\,y_i \sum_{i=1}^{m} f_i(x_2)\,y_i \cdots \sum_{i=1}^{m} f_i(x_q)\,y_i \\ &= \prod_{j=1}^{q}\sum_{i=1}^{m} f_i(x_j)\,y_i \end{aligned}$$

Agrupando os termos em y, para facilitar a notação podemos escrever o produto como:

$$P_1P_2\cdots P_q = \sum_{1\le i_1\le i_2\le\cdots\le i_q\le m} C_{i_1,\ldots,i_q} y_{i_1}y_{i_2}\cdots y_{i_q} \tag{5.1}$$

A condição $i_1 \le i_2 \le \cdots \le i_q$ é imposta na soma para indicar que os termos estão sendo agrupados. (Devemos mostrar que cada coeficiente $C_{i_1,\ldots,i_q} = C_{i_1,\ldots,i_q}(x_1,\ldots,x_q)$ é simétrico em $x_1,\ldots,x_q$). Note que toda permutação de $x_1,\ldots,x_q$ deixa o lado esquerdo da igualdade em (5.1) invariante, pois é apenas uma permutação dos polinômios $P_1,P_2,\ldots,P_q$. Logo, essa permutação também deixa o lado direito de (5.1) invariante, e assim, deixa todo coeficiente $C_{i_1,\ldots,i_q}$ que está escrito em termos de $x_1,\ldots,x_q$ invariante. Logo, cada $C_{i_1,\ldots,i_q}$ é polinômio simétrico em $x_1,\ldots,x_q$. Portanto, ao permutar tais polinômios $P_1P_2\cdots P_q = \prod_{j=1}^{q}\sum_{i=1}^{m} f_i(x_j)\,y_i$ temos que quando os termos são agrupados em y_i, obtemos coeficientes de $f_i(x_j)$ que são polinômios simétricos em $x_1,\ldots,x_q$. □

Lema 5.2. *Sejam $\mathbb{Q}(\theta)|\mathbb{Q}$ uma extensão algébrica normal de grau n e $\theta=\theta^{(1)},\theta^{(2)},\ldots,\theta^{(n)}$ os conjugados de θ. Se $F(x)\in\mathbb{Q}[x]$ é um polinômio com coeficientes racionais. Então o conjunto*

$$\left\{F\left(\theta^{(1)}\right),F\left(\theta^{(2)}\right),\ldots,F\left(\theta^{(n)}\right)\right\} \tag{5.2}$$

é permutado quando substituímos θ por $\theta^{(i)}$.

Demonstração. Seja $\theta\in\mathbb{Q}(\theta)$ um número algébrico satisfazendo o polinômio minimal mônico com coeficientes racionais:

$$f(x) = x^n + b_1x^{n-1} + \ldots + b_{n-1}x + b_n$$

Sejam os conjugados de $\theta=\theta^{(1)},\theta^{(2)},\ldots,\theta^{(n)}$ as n raízes de $f(x)$. Como a extensão $\mathbb{Q}(\theta)|\mathbb{Q}$ é normal, então $\theta^{(j)}\in\mathbb{Q}(\theta)$ para todo $j=1,\ldots,n\in\mathbb{N}$ e pelo Lema 4.1 pode ser escrito de modo único como um polinômio em θ com coeficientes racionais:

$$\theta^{(j)} = h_j(\theta) = a_0 + a_1\theta + \ldots + a_{n-2}\theta^{n-2} + a_{n-1}\theta^{n-1}, \quad h_j(x)\in\mathbb{Q}[x], \quad j=1,\ldots,n\in\mathbb{N}$$

Por conseguinte,

$$\begin{aligned}\theta^{(j)} = h_j(\theta) &= a_{n-1}(\theta - x_1)(\theta - x_2)\cdots(\theta - x_{n-1}) \\ &= a_{n-1}\Big(\theta^{n-1} - (\sum_{i=1}^{n-1} x_i)\theta^{n-2} + (\sum_{1\leq i<j\leq n-1} x_i x_j)\theta^{n-3} + \cdots + (-1)^{n-1}\big(x_1 x_2 \cdots x_{n-1}\big)\Big) \\ &= a_{n-1}\Big(\theta^{n-1} - \sigma_1(x_1, x_2, \ldots, x_{n-1})\theta^{n-2} + \cdots + (-1)^{n-1}\sigma_n(x_1, x_2, \ldots, x_{n-1})\Big).\end{aligned}$$

tal que $\sigma_1(x_1, \ldots, x_{n-1}), \ldots, \sigma_n(x_1, \ldots, x_{n-1})$ são funções simétricas elementares de $h_j(\theta)$ para $j = 1, \ldots, n \in \mathbb{N}$. Substituindo θ por $\theta^{(1)}$ em $h_j(\theta)$, tem-se

$$h_j(\theta^{(1)}) = \big(\theta^{(1)}\big)^{(j)} = \theta^{(j)} = h_j(\theta)$$

claramente $h_1(\theta^{(1)}), h_2\left(\theta^{(1)}\right), \ldots, h_n\left(\theta^{(1)}\right)$ tem as mesmas funções simétricas elementares que $h_j(\theta)$. Substituindo θ por $\theta^{(2)}$ em $h_j(\theta)$, satisfaz a mesma relação, e assim, as funções simétricas elementares de $h_1\left(\theta^{(2)}\right), h_2\left(\theta^{(2)}\right), \ldots, h_n\left(\theta^{(2)}\right)$ são também iguais a de $h_j(\theta)$, para $j = 1, \ldots, n \in \mathbb{N}$.

Note que, substituindo θ por $\theta^{(2)}$ em $h_j(\theta)$, temos $\left(\theta^{(2)}\right)^{(j)} = h_j\left(\theta^{(2)}\right)$, e aplicando em $f(x)$, para todo $j = 1, \ldots, n \in \mathbb{N}$, obtemos

$$\begin{aligned}f\left(\left(\theta^{(2)}\right)^{(j)}\right) &= \left(\left(\theta^{(2)}\right)^{(j)}\right)^n + b_1\left(\left(\theta^{(2)}\right)^{(j)}\right)^{n-1} + \ldots + b_{n-1}\left(\theta^{(2)}\right)^{(j)} + b_n \\ &= \left(\left(\theta^{(2)}\right)^n\right)^{(j)} + b_1\left(\left(\theta^{(2)}\right)^{n-1}\right)^{(j)} + \ldots + b_{n-1}\left(\theta^{(2)}\right)^{(j)} + b_n \\ &= 0\end{aligned}$$

o que significa que os elementos do conjunto:

$$\left\{h_1\left(\theta^{(2)}\right), h_2\left(\theta^{(2)}\right), \ldots, h_n\left(\theta^{(2)}\right)\right\}$$

também são raízes de $f(x)$. Outra maneira de afirmar isso, mais geralmente, se $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ são polinômios em θ, e nesses polinômios θ é substituído por $\theta^{(2)}$, resulta apenas em uma permutação dos conjugados $\theta^{(1)}, \ldots, \theta^{(n)}$. Não há nada de especial no $\theta^{(2)}$ nesta análise, na verdade, é válida a generalização quando substituímos θ pelo $\theta^{(i)}$, como $\theta^{(1)}, \ldots, \theta^{(n)}$ são as raízes de $f(x)$. Segue-se que

$$\left\{h_1\left(\theta^{(i)}\right), h_2\left(\theta^{(i)}\right), \ldots, h_n\left(\theta^{(i)}\right)\right\} = \left\{\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}\right\} \tag{5.3}$$

em alguma ordem para $i = 1, \ldots, n \in \mathbb{N}$.

Agora, aplicando $\theta^{(j)} = h_j(\theta)$ em $F(x)$, para cada $j = 1, \ldots, n \in \mathbb{N}$, tem-se $F\left(\theta^{(j)}\right) = F\left(h_j(\theta)\right)$ e substituindo θ por $\theta^{(i)}$ como no argumento anterior em (5.3).

Teremos que o conjunto

$$\left\{F\left(\theta^{(1)}\right), F\left(\theta^{(2)}\right), \ldots, F\left(\theta^{(n)}\right)\right\}$$

também é permutado em alguma ordem. □

Lema 5.3. *Sejam $\mathbb{Q}(\theta)|\mathbb{Q}$ extensão algébrica normal de grau n. Então todo elemento $\gamma \in \mathbb{Q}(\theta)$ e seus conjugados $\gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(n)}$ satisfazem uma equação polinomial $g(x) = 0$ de grau n com coeficientes inteiros.*

Demonstração. Seja $\gamma \in \mathbb{Q}(\theta)$, então existe $F(x) \in \mathbb{Q}[x]$, com $(\partial F(x) \leq n-1)$ tal que $\gamma = F(\theta)$, e aplicando o conjugado, tem-se $\gamma^{(j)} = F\left(\theta^{(j)}\right)$, para cada $j = 1, \ldots, n \in \mathbb{N}$.

Afirmamos que as funções simétricas elementares de $\gamma = \gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(n)}$ são polinômios simétricos em $\theta = \theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$.

De fato, seja σ_k a k-ésima função simétrica elementar dada por:

$$\sigma_k(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}$$

Defina os polinômios $P_k(x_1, x_2, \ldots, x_n) \in \mathbb{Q}[x_1, x_2, \ldots, x_n]$ dado por

$$P_k(x_1, x_2, \ldots, x_n) := \sigma_k\left(F(x_1), F(x_2), \ldots, F(x_n)\right), \qquad k = 1, \ldots, n \in \mathbb{N}$$

Primeiro, mostraremos que os P_k são simétricos com respeito $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$(os conjugados de θ). Note que, aplicando $\theta^{(j)}$ em P_k, para cada $j = 1, \ldots, n \in \mathbb{N}$, tem-se

$$P_k\left(\theta^{(1)}, \ldots, \theta^{(n)}\right) = \sigma_k\left(F\left(\theta^{(1)}\right), \ldots, F\left(\theta^{(n)}\right)\right) = \sigma_k\left(\gamma^{(1)}, \ldots, \gamma^{(n)}\right) \tag{5.4}$$

Daí, se $\zeta \in S_n$ (conjunto das permutações de $\{1, \ldots, n\}$), então permutando os $\theta^{(j)}$ em P_k, para cada $j = 1, \ldots, n \in \mathbb{N}$, tem-se

$$P_k\left(\theta^{(\zeta(1))}, \ldots, \theta^{(\zeta(n))}\right) = \sigma_k\left(\gamma^{(\zeta(1))}, \ldots, \gamma^{(\zeta(n))}\right) = \sigma_k\left(F\left(\theta^{(\zeta(1))}\right), \ldots, F\left(\theta^{(\zeta(n))}\right)\right)$$

Pelo Lema 5.2, o conjunto $\left\{F\left(\theta^{(\zeta(1))}\right), \ldots, F\left(\theta^{(\zeta(n))}\right)\right\}$ é uma permutação do conjunto $\left\{F\left(\theta^{(1)}\right), \ldots, F\left(\theta^{(n)}\right)\right\}$. Como σ_k é simétrico, então

$$\sigma_k\left(F\left(\theta^{(\zeta(1))}\right), \ldots, F\left(\theta^{(\zeta(n))}\right)\right) = \sigma_k\left(F\left(\theta^{(1)}\right), \ldots, F\left(\theta^{(n)}\right)\right)$$

Daí, e de (5.4), segue-se

$$\begin{aligned} P_k\left(\theta^{(\zeta(1))},\ldots,\theta^{(\zeta(n))}\right) &= \sigma_k\left(F\left(\theta^{(1)}\right),\ldots,F\left(\theta^{(n)}\right)\right) \\ &= \sigma_k\left(\gamma^{(1)},\ldots,\gamma^{(n)}\right) \\ &= P_k\left(\theta^{(1)},\ldots,\theta^{(n)}\right) \end{aligned}$$

Isto é, quando permutamos o $\theta^{(j)}$ (j-ésimo conjugado de θ) em P_k, obtemos que os polinômios P_k ficaram invariantes em $\theta=\theta^{(1)},\theta^{(2)},\ldots,\theta^{(n)}$. Logo, os P_k são simétricos em $\theta=\theta^{(1)},\theta^{(2)},\ldots,\theta^{(n)}$.

Dessa forma, temos

$$\sigma_k\left(\gamma^{(1)},\ldots,\gamma^{(n)}\right)=P_k\left(\theta^{(1)},\ldots,\theta^{(n)}\right),\quad k=1,\ldots,n\in\mathbb{N}$$

onde os P_k são polinômios simétricos em $\theta=\theta^{(1)},\theta^{(2)},\ldots,\theta^{(n)}$ com coeficientes racionais tal que ($\theta^{(j)}$ são raízes de um certo polinômio que podemos tomar com coeficientes inteiros) e assim, pelo Lema 4.3, os $P_k\left(\theta^{(1)},\ldots,\theta^{(n)}\right)\in\mathbb{Q}$ são racionais, para cada $k=1,\ldots,n\in\mathbb{N}$, então existem racionais $\frac{a_1}{b_1},\frac{a_2}{b_2},\ldots,\frac{a_n}{b_n}$, com $a_k,b_k\in\mathbb{Z},\ b_k\neq 0$, para todo $k=1,\ldots,n\in\mathbb{N}$ tais que

$$P_1\left(\theta^{(1)},\ldots,\theta^{(n)}\right)=\frac{a_1}{b_1},\ldots,P_n\left(\theta^{(1)},\ldots,\theta^{(n)}\right)=\frac{a_n}{b_n}$$

Considere o polinômio $g(x)$ da seguinte forma:

$$g(x)=b\left(x-\gamma^{(1)}\right)\left(x-\gamma^{(2)}\right)\cdots\left(x-\gamma^{(n)}\right),\quad \text{onde}\quad b=b_1b_2\cdots b_n\in\mathbb{Z}-\{0\}.$$

Claramente, o grau $\partial g(x)=n$ e $\gamma^{(1)},\gamma^{(2)},\ldots,\gamma^{(n)}$ são raízes de $g(x)$. Basta-nos mostrar que $g(x)\in\mathbb{Z}[x]$. De fato, temos que

$$\begin{aligned} g(x) &= b(x-\gamma^{(1)})\cdots(x-\gamma^{(n)}) \\ &= b\big(x^n-\sigma_1(\gamma^{(1)},\ldots,\gamma^{(n)})x^{n-1}+\ \ldots\ +(-1)^n\sigma_n(\gamma^{(1)},\ldots,\gamma^{(n)})\big) \\ &= b\big(x^n-P_1(\theta^{(1)},\ldots,\theta^{(n)})x^{n-1}+\ \ldots\ +(-1)^nP_n(\theta^{(1)},\ldots,\theta^{(n)})\big) \\ &= b_1b_2\cdots b_n\Big(x^n-\frac{a_1}{b_1}x^{n-1}+\ \ldots\ +(-1)^n\frac{a_n}{b_n}\Big) \\ &= b_1b_2\cdots b_nx^n-a_1b_2\cdots b_nx^{n-1}+\ \ldots\ +(-1)^na_nb_1\cdots b_{n-1}\in\mathbb{Z}[x] \end{aligned}$$

Portanto, o polinômio $g(x)\in\mathbb{Z}[x]$, onde $b=b_1b_2\cdots b_n\in\mathbb{Z}-\{0\}$. □

Lema 5.4. *Considere as seguintes funções*

$$f(x)=\sum_{j=1}^{m}a_jx^{\alpha_j},\qquad g(x)=\sum_{j=1}^{t}b_jx^{\beta_j}$$

onde α_j, β_j são números algébricos não nulos. Assuma que os α_j são distintos, e da mesma forma os β_j também o são. Quando o produto $f(x)g(x)$ é formado e todos os termos de igual expoente são combinados. Então existe pelo menos um coeficiente não nulo no resultado.

Demonstração. Note que, pelo Lema 4.4, existe uma extensão normal $\mathbb{Q}(\theta)|\mathbb{Q}$ que contém $\alpha_1, \ldots, \alpha_m; \beta_1, \ldots, \beta_t$. Suponhamos que $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$. Pelo Lema 4.1, podemos escrever α_j e β_j de modo único como um polinômio em θ com coeficiente racionais:

$$\alpha_j = \sum_{i=0}^{n-1} r_{j,i}\theta^i, \quad \text{e} \quad \beta_j = \sum_{i=0}^{n-1} s_{j,i}\theta^i$$

Para cada $j = 1, \ldots, m \in \mathbb{N}$, (respectivamente, $j = 1, \ldots, t \in \mathbb{N}$).

- Dizemos que α_j precede α_k, (respectivamente β_j precede β_k) quando o primeiro termo não nulo da sequência

  $$r_{k,0} - r_{j,0}, \quad r_{k,1} - r_{j,1}, \quad r_{k,2} - r_{j,2}, \ \ldots, \ r_{k,n-1} - r_{j,n-1}$$

  respectivamente,

  $$s_{k,0} - s_{j,0}, \quad s_{k,1} - s_{j,1}, \quad s_{k,2} - s_{j,2}, \ \ldots, \ s_{k,n-1} - s_{j,n-1}$$

  for positivo, para o menor índice possível.

Como os α_j (respectivamente β_j) são distintos, então organizando a notação, podemos supor sem perda de generalidade que $\alpha_1 < \alpha_j$ para $j \in \{2, \ldots, m\}$ (respectivamente, $\beta_1 < \beta_k$, para $k \in \{2, \ldots, t\}$).

Afirmação. $\alpha_1 + \beta_1 < \alpha_j + \beta_k$ ($\alpha_1 + \beta_1$ precede $\alpha_j + \beta_k$) para todo $j = 2, \ldots, m \in \mathbb{N}$ e $k = 2, \ldots, t \in \mathbb{N}$. De fato, como

$$\alpha_1 + \beta_1 = \sum_{i=0}^{n-1} (r_{1,i} + s_{1,i})\,\theta^i \quad \text{e} \quad \alpha_j + \beta_k = \sum_{i=0}^{n-1} (r_{j,i} + s_{k,i})\,\theta^i$$

Então, basta mostrar que a diferença a seguir é o primeiro termo não nulo positivo, isto é,

$$(r_{j,i} + s_{k,i}) - (r_{1,i} + s_{1,i}) > 0, \quad \text{para um certo índice} \quad i \in \{0, \ldots, n-1\}.$$

Como $\alpha_1 < \alpha_j$, para $j \in \{2, \ldots, m\}$ e $\beta_1 < \beta_k$, para $k \in \{2, \ldots, t\}$ e assim, podemos supor $j \neq 1$ e $k \neq 1$, então existem índices mínimos $a, b \in \{0, \ldots, n-1\}$ tais que os

primeiros termos não nulos e positivos são:

$$r_{j,a} - r_{1,a} > 0 \quad \text{e} \quad s_{k,b} - s_{1,b} > 0 \tag{5.5}$$

(valendo a igualdade $r_{j,l} = r_{1,l}$ e $s_{k,l} = s_{1,l}$, para índice l pertencente aos conjuntos $\{0, \ldots, a-1\}$ e $\{0, \ldots, b-1\}$ os quais tem valores menores que a e b, respectivamente).

Considerando $v = min\{a, b\}$, então para todo $l \in \{0, \ldots, v-1\}$ temos as seguintes igualdades $r_{j,l} = r_{1,l}$ e $s_{k,l} = s_{1,l}$, daí, $r_{j,l} + s_{k,l} = r_{1,l} + s_{1,l}$, e assim, para o índice $v = min\{a, b\}$ e de (5.5), obtemos

$$(r_{j,v} + s_{k,v}) - (r_{1,v} + s_{1,v}) = (r_{j,v} - r_{1,v}) + (s_{k,v} - s_{1,v}) > 0$$

Logo, temos que $\alpha_1 + \beta_1 < \alpha_j + \beta_k$ ($\alpha_1 + \beta_1$ precede $\alpha_j + \beta_k$) para todo $j = 2, \ldots, m \in \mathbb{N}$ e $k = 2, \ldots, t \in \mathbb{N}$. Segue-se que, no produto $f(x)g(x)$, o termo $a_1 b_1 x^{\alpha_1 + \beta_1}$ tem único expoente e não pode ser combinado ou cancelado com nenhum dos outros termos, em particular, não teremos um termo com coeficiente que possa anular o $a_1 b_1$. Portanto, existe pelo menos um coeficiente $a_1 b_1 \neq 0$ não nulo no resultado. □

Vejamos na seção a seguir uma Generalização do Teorema de Lindemann.

5.2 Generalização do Teorema de Lindemann

Para provar a Generalização do Teorema de Lindemann, achamos conveniente nesta seção, primeiro estabelecer o Teorema de Lindemann como caso especial sobre $\mathbb{Q}$, e em seguida generalizar tal teorema sobre o conjunto dos algébricos $\mathbb{A}$.

Teorema 5.1 (Lindemann)**.** *Sejam $\alpha_1, \alpha_2, \ldots, \alpha_m$ números algébricos distintos. Então os valores de $e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_m}$ são linearmente independentes sobre o corpo $\mathbb{Q}$ dos números racionais.*

Demonstração. Suponhamos por contradição que vale a seguinte relação

$$\sum_{j=1}^{m} a_j e^{\alpha_j} = 0 \tag{5.6}$$

com coeficientes racionais $a_j \in \mathbb{Q}$ não todos nulos. Descartando os termos com coeficientes nulos caso exista e reordenando a notação, podemos supor que nenhum coeficiente é nulo. Além disso, multiplicando (5.6) por um inteiro adequado, de modo que podemos supor que os coeficientes $a_j \in \mathbb{Z}\text{-}\{0\}$ são inteiros não nulos. Pelo Lema 4.4, existe uma extensão $\mathbb{Q}(\theta)\,|\mathbb{Q}$ normal que contém $\alpha_1, \alpha_2, \ldots, \alpha_m$. Suponha ainda que o grau

$[\mathbb{Q}(\theta):\mathbb{Q}] = n$. Pelo Lema 4.1, todo $\alpha_j \in \mathbb{Q}(\theta)$ é expresso de modo único como um polinômio em θ de grau no máximo $n-1$ com coeficientes racionais, digamos:

$$\alpha_j = \sum_{i=1}^{n-1} r_{ji}\theta^i, \quad j = 1, \ldots, m \in \mathbb{N}$$

Sendo $\theta = \theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ os conjugados de θ, e aplicando o k-ésimo conjugado em α_j sobre $\mathbb{Q}(\theta)$, temos

$$\alpha_j^{(k)} = \sum_{i=1}^{n-1} r_{ji}\left(\theta^{(k)}\right)^i, \quad j = 1, \ldots, m \in \mathbb{N}, \quad k = 1, \ldots, n \in \mathbb{N} \tag{5.7}$$

Note que, que $\theta^{(k)}$ possui característica semelhante ao próprio θ, ou seja, um número algébrico de grau n, sendo raízes de um polinômio minimal, e como α_j são distintos e escritos de modo único como um polinômio em θ. Consequentemente, as expressões polinomiais em (5.7) são únicas em $\theta^{(k)}$, e ainda, os $\alpha_j^{(k)}$ são distintos para todo k fixo.

Formando o seguinte produtório e escrevendo de modo a facilitar à notação, temos

$$0 = \prod_{k=1}^{n}\sum_{j=1}^{m} a_j e^{\alpha_j^{(k)}} = \sum_{j=0}^{r} c_j e^{\beta_j} \tag{5.8}$$

O produtório acima é nulo, do fato que $\alpha_j^{(1)} = \alpha_j$ e da relação $\sum_{j=1}^{m} a_j e^{\alpha_j} = 0$ em (5.6).

Podemos considerar que os β_j são distintos, já que os $\alpha_j^{(k)}$ são distintos para todo k fixo, como os a_j são inteiros, então os c_j também o são (uma vez que o c_j é resultado da multiplicação do produtório e um somatório de parcelas que são coeficientes das exponenciais). Além disso, temos que por hipótese $a_j \neq 0$, para cada $j = 1, \ldots, m \in \mathbb{N}$ e pelo Lema 5.4, existe pelo menos um coeficiente c_j não nulo, digamos $c_0 \neq 0$.

Note que, para cada j fixo, os n conjugados de $\alpha_j^{(k)}$, são permutados quando substituímos θ por $\theta^{(i)}$ na expressão polinomial de $\alpha_j^{(k)} = \sum_{i=1}^{n-1} r_{ji}\left(\theta^{(k)}\right)^i$ de acordo com o Lema 5.2. Logo, substituindo θ por $\theta^{(i)}$ apenas permutamos os fatores do produtório em (5.8), sendo ele indexado por k, de modo que o resultado total do produto fica invariante. Por outro lado, quando substituímos θ por $\theta^{(i)}$ estamos trocando β_j pelo seu i-ésimo conjugado $\beta_j^{(i)}$, já que $\beta_j = \alpha_j^{(k)}$, $i = 1, \ldots, n \in \mathbb{N}$. Portanto, de (5.8) segue-se que

$$0 = \sum_{j=0}^{r} c_j e^{\beta_j^{(1)}} = \sum_{j=0}^{r} c_j e^{\beta_j^{(2)}} = \cdots = \sum_{j=0}^{r} c_j e^{\beta_j^{(n)}} \tag{5.9}$$

Temos que $\beta_j^{(i)}$ são distintos para todo i fixo, (já que $\alpha_j^{(k)}$ são distintos para todo k fixo).

Agora, multiplicando o primeiro somatório em (5.9) por $e^{-\beta_0^{(1)}}$, o segundo somatório

por $e^{-\beta_0^{(2)}}$, até o ultimo somatório por $e^{-\beta_0^{(n)}}$. Defina

$$\gamma_j^{(i)} = \beta_j^{(i)} - \beta_0^{(i)}, \quad i \in \{1, \ldots, n\}, \quad j \in \{1, \ldots, r\}$$

Como $\beta_j^{(i)}$ são distintos para todo i fixo, então $\gamma_j^{(i)}$ são distintos e não nulos para i fixo e $j = 1, \ldots, r \in \mathbb{N}$. Por outro lado, para $j = 0$, temos que $\gamma_0^{(i)} = \beta_0^{(i)} - \beta_0^{(i)} = 0$. Então as equações em (5.9) podem ser reescritas como

$$0 = c_0 + \sum_{j=1}^{r} c_j e^{\gamma_j^{(1)}} = c_0 + \sum_{j=1}^{r} c_j e^{\gamma_j^{(2)}} = \cdots = c_0 + \sum_{j=1}^{r} c_j e^{\gamma_j^{(n)}} \tag{5.10}$$

Pelo Lema 5.3, os conjugados $\gamma_J^{(1)}, \gamma_j^{(2)}, \ldots, \gamma_j^{(n)}$ são raízes de polinômios com coeficientes inteiros de grau n, digamos

$$g_j(z) = b_j z^n + \ldots = b_j \prod_{i=1}^{n} \left(z - \gamma_j^{(i)}\right), \quad j = 1, \ldots, r \in \mathbb{N} \tag{5.11}$$

Podemos tomar os inteiros $b_j > 0$, e como $\gamma_j^{(i)} \neq 0$, segue-se que os termos constantes desses polinômios $g_j(0) \in \mathbb{Z} - \{0\}$ são inteiros não nulos. Com isso terminamos a parte algébrica da demonstração do teorema. Passaremos agora para um aspecto analítico da demonstração.

Seja $f(z)$ um polinômio que será especificado posteriormente. Defina

$$F(z) = f(z) + f'(z) + f''(z) + f'''(z) + \cdots$$

isto é, $F(z)$ é a soma de $f(z)$ e suas derivadas de todas as ordens.

Vejamos a **(Identidade de Hermite)**. Sejam $F(z)$ e $f(z)$ como acima integráveis. Então

$$\frac{d}{dz}\left(F(z)\, e^{-z}\right) = -f(z)\, e^{-z}.$$

De fato, temos que

$$\begin{aligned}
\frac{d}{dz}\left(F(z)\, e^{-z}\right) &= F'(z)\, e^{-z} + F(z)\left(e^{-z}\right)' \\
&= \left(F'(z) - F(z)\right)e^{-z} \\
&= \Big(f'(z) + f''(z) + \ldots - \left(f(z) + f'(z) + f''(z) + \ldots\right)\Big)e^{-z} \\
&= -f(z)\, e^{-z}
\end{aligned}$$

Daí, integrando $-f(z)e^{-z}$, segue-se que

$$\begin{aligned} -\int_0^b f(z)e^{-z}dz &= \int_0^b \frac{d}{dz}\left(F(z)e^{-z}\right)dz \\ &= F(z)e^{-z}\Big|_0^b \\ &= F(b)e^{-b} - F(0)e^{-0} \\ &= F(b)e^{-b} - F(0) \end{aligned}$$

Por conseguinte,

$$F(b)e^{-b} - F(0) = -\int_0^b f(z)e^{-z}dz$$

Multiplicando a expressão acima por $e^b \neq 0$, tem-se

$$F(b) - F(0)e^b = -e^b \int_0^b f(z)e^{-z}dz$$

e substituindo b por $\gamma_j^{(i)}$ (obtido em (5.10)), na expressão acima e multiplicando-a por c_j e somando sobre $j = 1, \ldots, r$ e $i = 1, \ldots, n \in \mathbb{N}$, obtemos

$$\sum_{j=1}^{r}\sum_{i=1}^{n} c_j F\left(\gamma_j^{(i)}\right) - F(0)\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} = -\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z)e^{-z}dz \tag{5.12}$$

Por (5.10), tem-se

$$\sum_{j=1}^{r} c_j e^{\gamma_j^{(1)}} = -c_0, \quad \sum_{j=1}^{r} c_j e^{\gamma_j^{(2)}} = -c_0, \quad \ldots, \quad \sum_{j=1}^{r} c_j e^{\gamma_j^{(n)}} = -c_0$$

Daí, somando essas equações acima, resulta em:

$$\sum_{i=1}^{n}\sum_{j=1}^{r} c_j e^{\gamma_j^{(i)}} = -nc_0$$

e substituindo no primeiro membro de (5.12), obtemos

$$\sum_{j=1}^{r} c_j \left(\sum_{i=1}^{n} F\left(\gamma_j^{(i)}\right)\right) + nc_0 F(0) = -\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z)e^{-z}dz \tag{5.13}$$

Agora, definimos o polinômio $f(z)$ como

$$f(z) = \frac{(b_1 b_2 \cdots b_r)^{prn}}{(p-1)!} z^{p-1} \prod_{j=1}^{r} g_j(z)^p \tag{5.14}$$

onde $\prod_{j=1}^{r} g_j(z)^p$, (é como em (5.11)), $(b_1 b_2 \cdots b_r)^{prn} \in \mathbb{Z}-\{0\}$ e $p \in \mathbb{N}$ é um primo que será especificado posteriormente.

Nosso objetivo a partir de agora será escolher o número primo $p \in \mathbb{N}$ suficientemente grande para que o lado esquerdo de (5.13) seja um inteiro não nulo, enquanto o lado direito em módulo seja arbitrariamente pequeno. Assim, teremos a contradição que estabelece o teorema.

Tomando as derivadas de ordem 0 à $(p-1)$ de $f(z)$, temos

$$f(z) = \frac{(b_1 b_2 \cdots b_r)^{prn}}{(p-1)!} z^{p-1} \prod_{j=1}^{r} g_j(z)^p$$

$$f'(z) = (p-1)\frac{(b_1 b_2 \cdots b_r)^{prn}}{(p-1)!} z^{p-2} \prod_{j=1}^{r} g_j(z)^p + \frac{(b_1 b_2 \cdots b_r)^{prn}}{(p-1)!} z^{p-1} \left(\prod_{j=1}^{r} g_j(z)^p \right)'$$

$$f''(z) = (p-2)(p-1)\frac{(b_1 b_2 \cdots b_r)^{prn}}{(p-1)!} z^{p-3} \prod_{j=1}^{r} g_j(z)^p + \big(\text{Parcelas com variável } z\big)$$

$$f'''(z) = (p-3)(p-2)(p-1)\frac{(b_1 b_2 \cdots b_r)^{prn}}{(p-1)!} z^{p-4} \prod_{j=1}^{r} g_j(z)^p + \big(\text{Parcelas com variável } z\big)$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$f^{(i)}(z) = (p-i)(p-(i-1))\cdots(p-1)\frac{(b_1 b_2 \cdots b_r)^{prn}}{(p-1)!} z^{(p-(i+1))} \prod_{j=1}^{r} g_j(z)^p + \big(\text{Parcelas com variável } z\big)$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$f^{(p-2)}(z) = (p-(p-2))(p-(p-3))\cdots(p-1)\frac{(b_1 b_2 \cdots b_r)^{prn}}{(p-1)!} z^{(p-(p-1))} \prod_{j=1}^{r} g_j(z)^p + \big(\text{Parcelas com variável } z\big)$$

$$f^{(p-1)}(z) = \underbrace{(p-(p-1))(p-(p-2))\cdots(p-1)}_{(p-1)!} \frac{(b_1 b_2 \cdots b_r)^{prn}}{(p-1)!} \underbrace{z^{(p-p)}}_{1} \prod_{j=1}^{r} g_j(z)^p + \big(\text{Parcelas com variável } z\big)$$

Da expressão de $f^{(p-1)}(z)$ acima, temos

$$f^{(p-1)}(z) = (b_1 b_2 \cdots b_r)^{prn} \prod_{j=1}^{r} g_j(z)^p + \big(\text{Parcelas com variável } z\big)$$

Logo, aplicando $z = 0$ em todas as derivações acima, obtemos:

$$0 = f(0) = f'(0) = \cdots = f^{(p-2)}(0) \quad \text{e} \quad f^{(p-1)}(0) = (b_1 b_2 \cdots b_r)^{prn} \prod_{j=1}^{r} g_j(0)^p \in \mathbb{Z}-\{0\}$$

Escolhendo o primo $p > (b_1 b_2 \cdots b_r)^{prn} \in \mathbb{Z}-\{0\}$ e $p > \prod_{j=1}^{r} g_j(0)^p \in \mathbb{Z}-\{0\}$. Então p não é divisor do inteiro não nulo $f^{(p-1)}(0)$, isto é, $p \nmid f^{(p-1)}(0)$.

Por outro lado, tomando a ordem da derivada de $f(z)$ igual à $t \geq p$, e aplicando $z = 0$, argumentamos que $f^{(t)}(0)$ é um inteiro divisível por p, ou seja, $p | f^{(t)}(0)$.
De fato, pensamos em $f(z)$ como uma soma de potências de z de modo que o coeficiente de cada termo em $f^{(t)}(z)$ possui t inteiros consecutivos que entram no processo de diferenciação.

Assim, para $t \geq p$ o produto de t inteiros consecutivos é $(t! = t(t-1)\cdots 2.1)$ que é divisível por $p!$ de modo que eliminamos o $(p-1)!$ envolvido em $f(z)$. Portanto, podemos escrever:

$$f^{(t)}(z) = p\,(b_1 b_2 \cdots b_r)^{prn}\, G_t(z) \tag{5.15}$$

onde $G_t(z)$ é um polinômio com coeficientes inteiros e grau no máximo $prn - 1$.

Como $p\,(b_1 b_2 \cdots b_r)^{prn} \in \mathbb{Z}-\{0\}$ e o polinômio $G_t(0) \in \mathbb{Z}-\{0\}$, segue-se que $f^{(t)}(0)$ é um inteiro não nulo divisível por p, isto é, $p | f^{(t)}(0)$ para $t \geq p$. Usando resultados vistos anteriores e aplicando $z = 0$, para a expressão de $F(z)$, vamos concluir que $p \nmid nc_0 F(0)$ em (5.13). Para tanto, temos:

$$\begin{aligned} F(0) &= \underbrace{f(0) + f'(0) + \ldots + f^{(p-2)}(0)}_{0} + f^{(p-1)}(0) + \sum_{t \geq p} f^{(t)}(0) \\ &= \underbrace{f^{p-1}(0)}_{\text{inteiro não divisível por } p} + \underbrace{p \sum_{t \geq p} (b_1 b_2 \cdots b_r)^{prn}\, G_t(0)}_{\text{inteiro divisível por } p} \end{aligned}$$

Segue-se que o primo p não divide $F(0)$. Podemos supor ainda que $p > n$ e $p > c_0$. Logo, podemos concluir que p não é divisor do inteiro não nulo $nc_0 F(0) \in \mathbb{Z}-\{0\}$, isto é, $p \nmid nc_0 F(0)$.

Agora, estabeleceremos que o outro termo do lado esquerdo de (5.13):

$$\sum_{j=1}^{r} c_j \left(\sum_{i=1}^{n} F\left(\gamma_j^{(i)}\right) \right)$$

é um inteiro divisível por p. De fato, veremos que a soma a seguir de inteiros não nulos

$$\sum_{i=1}^{n} F\left(\gamma_j^{(i)}\right) = \sum_{i=1}^{n} f\left(\gamma_j^{(i)}\right) + \sum_{i=1}^{n} f'\left(\gamma_j^{(i)}\right) + \ldots + \sum_{i=1}^{n} f^{(p-1)}\left(\gamma_j^{(i)}\right) + \sum_{i=1}^{n} \sum_{t \geq p} f^{(t)}\left(\gamma_j^{(i)}\right)$$

é um múltiplo de p. Como vimos que $f(z), f'(z), \ldots, f^{(p-1)}(z)$ tem fatores iguais à $g_j(z)^p = b_j \prod_{i=1}^{n} \left(z - \gamma_j^{(i)}\right)^p$ tal que $\gamma_j^{(i)}$ são raízes de $g_j(z)^p$, para $j = 1, \ldots, r \in \mathbb{N}$,

isto é, temos que $g_j\left(\gamma_j^{(i)}\right)^p = 0$, o que implica

$$\sum_{i=1}^{n} f\left(\gamma_j^{(i)}\right) = 0,\ \sum_{i=1}^{n} f'\left(\gamma_j^{(i)}\right) = 0,\ \ \ldots,\ \ \sum_{i=1}^{n} f^{(p-1)}\left(\gamma_j^{(i)}\right) = 0 \tag{5.16}$$

Por outro lado, tomando o somatório e aplicando $\gamma_j^{(i)}$ na expressão de $f^{(t)}(z)$ em (5.15), obtemos

$$\sum_{i=1}^{n} f^{(t)}\left(\gamma_j^{(i)}\right) = p\left(b_1 b_2 \cdots b_r\right)^{prn} \sum_{i=1}^{n} G_t\left(\gamma_j^{(i)}\right) \tag{5.17}$$

para todo $t \geq p$ cujo o grau de $G_t(z)$ é no máximo $prn - 1$.

Definimos $\varphi\left(x_1, \ldots, x_n\right) \in \mathbb{Z}\left[x_1, \ldots, x_n\right]$ por

$$\varphi\left(x_1, \ldots, x_n\right) = G_t\left(x_1\right) + G_t\left(x_2\right) + \ldots + G_t\left(x_n\right) = \sum_{i=1}^{n} G_t\left(x_i\right)$$

Note que φ é um polinômio simétrico de grau $\partial\varphi = prn - k$, onde $k \geq 1 \in \mathbb{N}$. Como para todo $j = 1, \ldots, r \in \mathbb{N}$, $\gamma_j^{(1)}, \gamma_j^{(2)}, \ldots, \gamma_j^{(n)}$ são as n raízes dos polinômios $g_j(z) = b_j z^n + \ldots = b_j \prod_{i=1}^{n}\left(z - \gamma_j^{(i)}\right)$ em (5.11) com coeficientes inteiros. Segue-se do Lema 4.3, (2ª Parte) que

$$b_j^{prn-k} \sum_{i=1}^{n} G_t\left(\gamma_j^{(i)}\right) := d_{jt} \in \mathbb{Z}, \quad j = 1, \ldots, r \in \mathbb{N}, \quad t \geq p.$$

Daí, temos $\sum_{i=1}^{n} G_t\left(\gamma_j^{(i)}\right) = \dfrac{d_{jt}}{b_j^{prn-k}}$ e substituindo na expressão em (5.17), tem-se

$$\sum_{i=1}^{n} f^{(t)}\left(\gamma_j^{(i)}\right) = p\left(b_1 b_2 \cdots b_r\right)^{prn} \frac{d_{jt}}{b_j^{prn-k}} = p.b_1^{prn} b_2^{prn} \cdots b_j^{k} \cdots b_r^{prn} d_{jt} \in \mathbb{Z} - \{0\}.$$

é um inteiro. Daí, e de (5.16) na expressão $\sum_{i=1}^{n} F\left(\gamma_j^{(i)}\right)$, obtemos

$$\begin{aligned}
\sum_{i=1}^{n} F\left(\gamma_j^{(i)}\right) &= \underbrace{\sum_{i=1}^{n} f\left(\gamma_j^{(i)}\right) + \sum_{i=1}^{n} f'\left(\gamma_j^{(i)}\right) + \ \ldots\ + \sum_{i=1}^{n} f^{(p-1)}\left(\gamma_j^{(i)}\right)}_{0} + \sum_{i=1}^{n}\sum_{t\geq p} f^{(t)}\left(\gamma_j^{(i)}\right) \\
&= \sum_{t\geq p}\sum_{i=1}^{n} f^{(t)}\left(\gamma_j^{(i)}\right) \\
&= \underbrace{p\sum_{t\geq p} b_1^{prn} b_2^{prn} \cdots b_j^{k} \cdots b_r^{prn} d_{jt}}_{\text{inteiro não nulo divisível por } p}
\end{aligned}$$

é inteiro não nulo divisível por p. Como os $c_j \in \mathbb{Z}-\{0\}$ (pois por hipótese $a_j \in \mathbb{Z}-\{0\}$), tem-se que $\sum_{j=1}^{r} c_j \left(\sum_{i=1}^{n} F\left(\gamma_j^{(i)}\right) \right)$ é um inteiro não nulo divisível por p.

Como estabelecemos que $p \nmid nc_0F(0)$, e $p \mid \sum_{j=1}^{r} c_j \left(\sum_{i=1}^{n} F\left(\gamma_j^{(i)}\right) \right)$. Então o lado esquerdo de (5.13) é um inteiro não nulo e não divisível por p. Portanto, o lado direito em módulo é:

$$1 \leq \left| \sum_{j=1}^{r} \sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z)\, e^{-z} dz \right| \tag{5.18}$$

Defina os seguintes máximos para cada i e j:
$m_1 := \max_{1\leq j\leq r}|c_j|$, $m_2 := \max_{\substack{1\leq i\leq n \\ 1\leq j\leq r}}|e^{\gamma_j^{(i)}}|$, $m_3 := \max_{\substack{1\leq i\leq n \\ 1\leq j\leq r}}|\gamma_j^{(i)}|$, $m_4 := \max_{0\leq u\leq 1} e^{-u\gamma_j^{(i)}}$
$m_5 := \max_{0\leq u\leq 1} \prod_{j=1}^{r} g_j\left(u\gamma_j^{(i)}\right)$ e ($m_3^{p-1} := \max|z^{p-1}|$ quando substituímos z por $\gamma_j^{(i)}$ que está no limite de integração).

Por (5.18), obtemos

$$\begin{aligned}
1 &\leq \left| \sum_{j=1}^{r} \sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z)\, e^{-z} dz \right| \\
&= \left| \sum_{j=1}^{r} \sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} \frac{(b_1 b_2 \cdots b_r)^{prn}}{(p-1)!} z^{p-1} \prod_{j=1}^{r} g_j(z)^p\, e^{-z} dz \right| \\
&\leq (rn) m_1 m_2 \frac{(b_1 b_2 \cdots b_r)^{prn}}{(p-1)!} m_3^{p-1} m_5^p m_4 m_3 \\
&= rn m_1 m_2 m_4 \frac{(b_1^{rn} b_2^{rn} \cdots b_r^{rn} m_3 m_5)^p}{(p-1)!}
\end{aligned}$$

Como $r, n, m, m_1, m_2, m_3, m_4, m_5, b_1, b_2, \ldots, b_r$ não depende de p. Para concluir o teorema, basta-nos provar o lema a seguir:

Lema 5.5. *Seja A uma constante não nula. Então* $\lim_{p\to+\infty} \frac{A^p}{(p-1)!} = 0$.

Demonstração. É evidente que o limite desejado equivale a

$$\lim_{p\to+\infty} \frac{(p-1)!}{A^p} = \infty$$

Tomando p, p_0 primos tal que $\frac{p_0-1}{A} > 2$, denotando $K := \frac{(p_0-1)!}{A^{p_0}}$. Como ($n! > 2^n$, para todo $n \geq 4$, segue-se de indução sobre $n \in \mathbb{N}$). Daí, $(p-p_0)! > 2^{p-p_0}$

para todo p suficientemente grande tal que $p > p_0$ e assim, tem-se

$$\frac{(p-1)!}{A^p} = \underbrace{\frac{(p-1)}{A}.\frac{(p-2)}{A}\cdots\frac{p_0}{A}}_{(p-p_0)-\text{vezes}}.\frac{(p_0-1)!}{A^{p_0}} > \underbrace{(p-p_0)\left((p-p_0)-1\right)\cdots 2.1}_{(p-p_0)!}\frac{(p_0-1)!}{A^{p_0}} > 2^{p-p_0}.K$$

Fazendo $p \to \infty$, temos $2^{p-p_0}.K \to \infty$. Logo, como $\dfrac{(p-1)!}{A^p} > 2^{p-p_0}.K$. Então

$$\lim_{p\to+\infty}\frac{(p-1)!}{A^p} = \infty$$

Portanto, o limite $\lim\limits_{p\to+\infty}\dfrac{A^p}{(p-1)!} = 0$. □

Voltando a demonstração do teorema, denotaremos $A := (b_1^{rn}b_2^{rn}\cdots b_r^{rn}m_3m_5)$. Fazendo $p \to \infty$ na expressão seguir e usando o Lema 5.5, obtemos

$$1 \leq rnm_1m_2m_4\frac{(b_1^{rn}b_2^{rn}\cdots b_r^{rn}m_3m_5)^p}{(p-1)!} \implies 1 \leq rnm_1m_2m_4\lim_{p\to+\infty}\frac{A^p}{(p-1)!} = 0$$

o que é uma contradição. Portanto, os valores $e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_m}$ são linearmente independentes sobre $\mathbb{Q}$. □

Agora, usando a versão anterior do teorema, vamos enunciar e demonstrar uma Generalização do Teorema de Lindemann, originada por Hermite-Lindemann e na seção seguinte algumas consequências interessantes de tal generalização.

Teorema 5.2 (Hermite-Lindemann)**.** *Sejam $\alpha_1, \alpha_2, \ldots, \alpha_m$ números algébricos distintos. Então os valores de $e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_m}$ são linearmente independentes sobre o corpo dos números algébricos $\mathbb{A}$.*

Demonstração. Suponhamos sem perda de generalidade que existem $a_1, a_2, \ldots, a_m$ coeficientes algébricos não nulos tais que

$$\sum_{j=1}^{m} a_j e^{\alpha_j} = 0 \tag{5.19}$$

Pelo Lema 4.4, existe uma extensão $\mathbb{Q}(\theta)|\mathbb{Q}$ normal que supomos de grau q contendo $a_1, a_2, \ldots, a_m$, isto é, $a_j \in \mathbb{Q}(\theta)$, para cada $j = 1, \ldots, m \in \mathbb{N}$.

Como a extensão $\mathbb{Q}(\theta)|\mathbb{Q}$ é normal. Então os conjugados de a_j estão em $\mathbb{Q}(\theta)$, isto é, temos que $a_j = a_j^{(1)}, a_j^{(2)}, \ldots, a_j^{(q)} \in \mathbb{Q}(\theta)$, para cada $j = 1, \ldots, m \in \mathbb{N}$.

Por (5.19), onde $(a_j^{(1)} = a_j)$, formamos o seguinte produtório:

$$0 = \prod_{i=1}^{q} \sum_{j=1}^{m} a_j^{(i)} e^{\alpha_j} = \sum_{j=0}^{r} c_j e^{\beta_j}, \quad \beta_j \in \mathbb{A} \tag{5.20}$$

sendo β_j algébricos distintos, e c_j coeficientes em termos do $a_j^{(i)}$. Como $a_j \in \mathbb{Q}(\theta)$ são polinômios em θ. Então os $a_j^{(i)}$ são polinômios em $\theta^{(i)}$, segue-se que c_j também são polinômios em $\theta^{(i)}$.

Pelo Lema 5.1, o produto em (5.20) possui coeficiente c_j que são polinômios simétricos em $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(q)}$. Denotando $c_j := P_j\left(\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(q)}\right)$ para cada $j = 1, \ldots, r \in \mathbb{N}$. Como $P_j\left(\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(q)}\right)$ é simétrico em $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(q)}$ (onde $\theta^{(i)}$ são raízes de um certo polinômio com coeficientes inteiros). Daí, pelo Lema 4.3, temos que $c_j \in \mathbb{Q}$. Além disso, pelo Lema 5.4, no produtório em (5.20), existe pelo menos um coeficiente $c_j \neq 0$ não nulo, para algum $j = 1, \ldots, r \in \mathbb{N}$. Mas, de (5.20), temos

$$\sum_{j=0}^{r} c_j e^{\beta_j} = 0, \qquad \beta_j \in \mathbb{A} \tag{5.21}$$

o que contradiz o Teorema de Lindemann 5.1, pois foi provado que é impossível em (5.21) obter uma solução para coeficientes $c_j \neq 0$ racionais não todos nulos, e como, tal contradição decorre do fato de supormos que os algébricos $a_1, a_2, \ldots, a_m$ são não nulos. Logo, estes são todos nulos em (5.19). Portanto, os valores $e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_m}$ são linearmente independente sobre o corpo $\mathbb{A}$. □

Veremos algumas consequências da Generalização do Teorema de Lindemann.

5.3 Algumas Consequências do Teorema de Hermite-Lindemann

A seguir, aplicando o Teorema de Hermite-Lindemann, obteremos importantes consequências de casos particulares e mais gerais, como a transcendência de certos números e funções trigonométricas.

Corolário 5.1. *Seja α número algébrico não nulo. Então os seguintes números são transcendentes sobre $\mathbb{A}$.*

(a). *(i)*-$\sin(\alpha)$, *(ii)*-$\cos(\alpha)$, *(iii)*-$\tan(\alpha)$, *(iv)*-$\sinh(\alpha)$, *(v)*-$\cosh(\alpha)$, *(vi)*-$\tanh(\alpha)$, *para todo $\alpha \in \mathbb{A}-\{0\}$;*

(b). *(i)*-e^{α}, *(ii)*-e, *(iii)*-π, *para todo $\alpha \in \mathbb{A}-\{0\}$;*

(c). *(i)*-$\log_e(\alpha)$, *para todo $\alpha \in \mathbb{A}-\{0, 1\}$.*

Demonstração. Nas demonstrações abaixo, usaremos as relações já conhecidas de um curso de Funções de uma Variável Complexa:

$$\sin(x) = \frac{e^{ix} - e^{-ix}}{2i}, \qquad \cos(x) = \frac{e^{ix} + e^{-ix}}{2}, \qquad \tan(x) = \frac{e^{ix} - e^{-ix}}{ie^{ix} + ie^{-ix}},$$
$$\sinh(x) = \frac{e^{x} - e^{-x}}{2}, \qquad \cosh(x) = \frac{e^{x} + e^{-x}}{2}, \qquad \tanh(x) = \frac{e^{x} - e^{-x}}{e^{x} + e^{-x}}.$$

Letra (a). item (i). Seja $\alpha \neq 0$ algébrico não nulo, então ($i\alpha \neq 0$). Se $\sin(\alpha)$ fosse algébrico não nulo, digamos $\sin(\alpha) = a \in \mathbb{A} - \{0\}$, teríamos

$$\sin(\alpha) = \frac{e^{i\alpha} - e^{-i\alpha}}{2i} \Longrightarrow 2i\sin(\alpha) - e^{i\alpha} + e^{-i\alpha} = 0 \Longrightarrow 2i\sin(\alpha)e^{0} + (-1)e^{i\alpha} + 1.e^{-i\alpha} = 0$$

Daí,

$$2iae^{0} + (-1)e^{i\alpha} + 1.e^{-i\alpha} = 0$$

cujos expoentes $0, i\alpha, -i\alpha$ são algébricos distintos e os coeficientes $2ia, (-1), 1$ são algébricos não nulos, o que contraria o Teorema de Hermite-Lindemann 5.2. Portanto, o $\sin(\alpha) \in \mathbb{T}$ é transcendente.

Analogamente, por argumento semelhante, temos □

Demonstração. **Letra (a). item (ii).** Se $\cos(\alpha)$ fosse algébrico não nulo, digamos $\cos(\alpha) = b \in \mathbb{A} - \{0\}$, teríamos

$$\cos(\alpha) = \frac{e^{i\alpha} + e^{-i\alpha}}{2} \Longrightarrow 2\cos(\alpha) - e^{i\alpha} + e^{-i\alpha} = 0 \Longrightarrow 2be^{0} + (-1)e^{i\alpha} + (-1)e^{-i\alpha} = 0$$

(Por argumento semelhante ao item (i)), o que contraria o Teorema de Hermite-Lindemann 5.2. Portanto, o $\cos(\alpha) \in \mathbb{T}$ é transcendente. □

Demonstração. **Letra (a). item (iii).** Se $\tan(\alpha)$ fosse algébrico não nulo, digamos $\tan(\alpha) = c \in \mathbb{A}$, teríamos

$$\tan(\alpha) = \frac{e^{i\alpha} - e^{-i\alpha}}{ie^{i\alpha} + ie^{-i\alpha}} \Longrightarrow i\tan(\alpha)e^{i\alpha} + i\tan(\alpha)e^{-i\alpha} - e^{i\alpha} + e^{-i\alpha} = 0$$

Daí,

$$(i\tan(\alpha) - 1)\, e^{i\alpha} + (i\tan(\alpha) + 1)\, e^{-i\alpha} = 0 \Longrightarrow (ic - 1)\, e^{i\alpha} + (ic + 1)\, e^{-i\alpha} = 0$$

o que contraria o Teorema de Hermite-Lindemann 5.2. Portanto, o $\tan(\alpha) \in \mathbb{T}$ é transcendente. □

Demonstração. **Letra (a). item (iv).** Se $\sinh(\alpha)$ fosse algébrico não nulo, digamos $\sinh(\alpha) = d \in \mathbb{A}-\{0\}$, teríamos

$$\sinh(\alpha) = \frac{e^{\alpha} - e^{-\alpha}}{2} \Longrightarrow 2\sinh(\alpha) - e^{\alpha} + e^{-\alpha} = 0 \Longrightarrow 2de^{0} + (-1)e^{\alpha} + 1.e^{-\alpha} = 0$$

o que contraria o Teorema de Hermite-Lindemann 5.2. Portanto, o $\sinh(\alpha) \in \mathbb{T}$ é transcendente. □

Demonstração. **Letra (a). item (v).** Se $\cosh(\alpha)$ fosse algébrico não nulo, digamos $\cosh(\alpha) = u \in \mathbb{A}-\{0\}$, teríamos

$$\cosh(\alpha) = \frac{e^{\alpha} + e^{-\alpha}}{2} \Longrightarrow 2\cosh(\alpha) - e^{\alpha} - e^{-\alpha} = 0 \Longrightarrow 2ue^{0} + (-1)e^{\alpha} + (-1)e^{-\alpha} = 0$$

o que contraria o Teorema de Hermite-Lindemann 5.2. Portanto, o $\cosh(\alpha) \in \mathbb{T}$ é transcendente. □

Demonstração. **Letra (a). item (vi).** Se $\tanh(\alpha)$ fosse algébrico não nulo, digamos $\tanh(\alpha) = v \in \mathbb{A}$, teríamos

$$\tanh(\alpha) = \frac{e^{\alpha} - e^{-\alpha}}{e^{\alpha} + e^{-\alpha}} \Longrightarrow \tanh(\alpha)e^{\alpha} + \tanh(\alpha)e^{-\alpha} - e^{\alpha} + e^{-\alpha} = 0$$

Daí,

$$(\tanh(\alpha) - 1)\, e^{\alpha} + (\tanh(\alpha) + 1)\, e^{-\alpha} = 0 \Longrightarrow (v-1)\, e^{\alpha} + (v+1)\, e^{-\alpha} = 0$$

o que contraria o Teorema de Hermite-Lindemann 5.2. Portanto, o $\tanh(\alpha) \in \mathbb{T}$ é transcendente. □

Vejamos as demonstrações dos itens da Letra (b).

Demonstração. **Letra (b). item (i)**. Seja $\alpha \in \mathbb{A}-\{0\}$. Se e^{α} fosse algébrico não nulo, digamos $e^{\alpha} = \beta \in \mathbb{A}-\{0\}$. Então teríamos

$$e^{\alpha} = \beta \Longrightarrow e^{\alpha} - \beta = 0 \Longrightarrow 1.e^{\alpha} - \beta e^{0} = 0$$

cujos os expoentes $\alpha, 0$ são algébricos distintos e os coeficientes $1, \beta$ são algébricos não nulos, o que contraria o Teorema de Hermite-Lindemann, tal contradição decorre do fato de supormos que e^{α} fosse algébrico. Portanto, o número $e^{\alpha} \in \mathbb{T}$ é transcendente. □

Demonstração. **Letra (b). item (ii)**. É imediato. Fazendo $\alpha = 1 \in \mathbb{A}-\{0\}$ na Letra (b). item (i). Logo, o número $e^{1} \in \mathbb{T}$ é transcendente. □

Demonstração. **Letra (b). item (iii)**. Se $\pi \in \mathbb{A}-\{0\}$ fosse algébrico não nulo. Então $\pi i \in \mathbb{A}-\{0\}$. Logo, pela Letra (b). item (i), o número $e^{\pi i}$ seria transcendente, mas pela relação de Euler, temos que $e^{\pi i} = -1 \in \mathbb{A}$, o que uma contradição. Portanto, o número $\pi \in \mathbb{T}$ é transcendente. □

Vejamos agora, a demonstração do item da Letra (c).

Demonstração. **Letra (c). item (i)**. Se $\alpha \in \mathbb{A}-\{0,1\}$. Se $\log_e \alpha \in \mathbb{A}-\{0\}$ fosse algébrico não nulo. Logo, pela Letra (b). item (i), teríamos que o número $e^{\log_e \alpha}$ seria transcendente, mas temos que $e^{\log_e \alpha} = \alpha \in \mathbb{A}$, que é algébrico por hipótese, o que uma contradição. Portanto, o número $\log_e \alpha \in \mathbb{T}$ é transcendente. □

Finalmente, no próximo capítulo apresentaremos nosso principal objetivo que é demonstrar uma Solução do Sétimo Problema de Hilbert e algumas consequências.

Capítulo 6

Solução do Sétimo Problema de Hilbert e Algumas Consequências

Neste capítulo apresentaremos nosso principal objetivo que é demonstrar em detalhes uma Solução do Sétimo Problema de Hilbert, que ficou conhecido como Teorema de Gelfond-Schneider, o qual garante que a potenciação de dois algébricos sob algumas condições, gera um transcendente, e com isso, obter algumas consequências interessantes e recentes da teoria. As principais referências utilizadas na elaboração deste capítulo são, Marques [10], Niven [12] e Siegel [14].

6.1 Lemas Auxiliares de C. Siegel

Esta seção será dedicada aos Lemas auxiliares de C. Siegel e alguns conceitos analíticos os quais são de fundamental importância para a Solução do Sétimo Problema de Hilbert.

Proposição 6.1. *Considere a matriz com entradas ρ_j^p na j-ésima linha e $(1+p)$-ésima coluna, com $j = 1, 2, \ldots, t$ e $p = 0, 1, \ldots, t-1$. Essa matriz (chamada matriz de Vandermonde) tem determinante nulo se, e somente se existe $k \neq j$ com $\rho_k = \rho_j$.*

$$V[\rho_1, \ldots, \rho_t] = det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \rho_1^1 & \rho_2^1 & \cdots & \rho_t^1 \\ \vdots & \vdots & \ddots & \vdots \\ \rho_1^{t-1} & \rho_2^{t-1} & \cdots & \rho_t^{t-1} \end{pmatrix} = \prod_{1 \leq k < j \leq t} (\rho_k - \rho_j)$$

para facilitar a notação podemos denotar $V[\rho_1, \ldots, \rho_t] := det\left(\rho_j^p\right)$.

Demonstração. É imediato. Mostraremos a equivalência de uma só vez. Note que o determinante da matriz de Vardemonde é o produto de todas as diferenças possíveis

entre seus elementos característicos $(\rho_k - \rho_j)$, com $1 \leq k < j \leq t \in \mathbb{N}$. Dessa forma, temos que

$$\det\left(\rho_j^p\right) = \prod_{1\leq k<j\leq t} (\rho_k - \rho_j) = (\rho_1 - \rho_t)(\rho_2 - \rho_t)\cdots(\rho_{t-1} - \rho_t)(\rho_1 - \rho_{t-1})$$

Logo,

$$\det\left(\rho_j^p\right) = 0 \Longleftrightarrow (\rho_k - \rho_j) = 0 \Longleftrightarrow \rho_k = \rho_j, \quad \text{para algum} \quad k \neq j.$$

□

Vejamos os dois importantes Lemas Auxiliares de C. Siegel relacionados à soluções de sistemas lineares.

Lema 6.1. *Considere as m equações em n incógnitas com $0 < m < n \in \mathbb{N}$,*

$$a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n = 0, \quad 1 \leq k \leq m \tag{6.1}$$

onde $a_{kj} \in \mathbb{Z}$. Seja A um inteiro positivo tal que $|a_{kj}| \leq A$ para todo k e j. Então existe uma solução não trivial de inteiros $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ em (6.1) tal que

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

Demonstração. Denote $y_k = a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n$, com $1 \leq k \leq m \in \mathbb{N}$. Então todo ponto $x = (x_1, \ldots, x_n)$ corresponde a um ponto $y = (y_1, \ldots, y_m)$. Observe que se x é reticulado, isto é, (suas coordenadas x_j são inteiros), então as coordenadas correspondentes y_k também o são, já que os a_{kj} são inteiros, e assim, y é um inteiro.

Seja q um inteiro positivo que será especificado posteriormente. Considere o cubo n-dimensional C definida por $|x_j| \leq q$. Como $-q \leq x_j \leq q$ com $q > 0$, tem-se que existe $(2q+1)$ possibilidades para x_j, com $j = 1, \ldots n \in \mathbb{N}$, então temos $(2q+1)^n$ pontos reticulados dentro do cubo n-dimensional C. Por hipótese $|a_{kj}| \leq A$, com A inteiro positivo. Para correspondentes y, tem-se

$$|y_k| = |\sum_{j=1}^{n} a_{kj}x_j| \leq \sum_{j=1}^{n} |a_{kj}||x_j| \leq \sum_{j=1}^{n} Aq = nAq \Longrightarrow |y_k| \leq nAq$$

Então $-nAq \leq y_k \leq nAq$ e $nAq > 0$, segue-se que existe $(2nAq+1)$ possibilidades para y_k, com $1 \leq k \leq m$ e assim, temos $(2nAq+1)^m$ pontos reticulados dentro do cubo m-dimensional D. Mostraremos que existem mais pontos reticulados em C do que correspondentes em D, daí, existem pontos reticulados em D que tem dois

correspondentes distintos em C. De fato, basta-nos mostrar

$$(2q+1)^n > (2nAq+1)^m$$

Considere o intervalo $I = \left[(nA)^{\frac{m}{n-m}} - 1, (nA)^{\frac{m}{n-m}} + 1\right)$ de comprimento 2, com $0 < m < n \in \mathbb{N}$, e assim, existe um número par em I. Seja q o único inteiro positivo tal que

$$(nA)^{\frac{m}{n-m}} - 1 \leq 2q < (nA)^{\frac{m}{n-m}} + 1$$

Da primeira parte da desigualdade adicionando 1 e elevando a $(n-m)$, tem-se

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

Por outro lado, temos

$$\begin{aligned}
(2nAq+1)^m &= \left[nA(2q+\tfrac{1}{nA})\right]^m \\
&= (nA)^m(2q+\tfrac{1}{nA})^m \\
&< (nA)^m(2q+1)^m \\
&\leq (2q+1)^{n-m}(2q+1)^m \\
&= (2q+1)^n
\end{aligned}$$

Logo, $(2q+1)^n > (2nAq+1)^m$. Dessa forma, segue-se que existe um ponto reticulado $y \in D$ imagem dos pontos reticulados $x' = (x'_1, \ldots, x'_n)$ e $x'' = (x''_1, \ldots, x''_n)$ distintos em C. Defina $x = x' - x''$, mas como $x = (x_1, \ldots, x_n)$, tem-se

$$x = (x_1, \ldots, x_n) = (x'_1 - x''_1, \ldots, x'_n - x''_n)$$

cujas coordenadas são $x_j = x'_j - x''_j$, com $j = 1, \ldots n \in \mathbb{N}$. Como $x' \neq x''$, daí, $x \neq 0$, isto é, pelo menos uma de suas coordenadas é não nula, aplicando-as e usando o fato de y ser imagem de x' e x'' em (6.1), obtemos a solução desejada:

$$\begin{aligned}
a_{k1}x_1 + \cdots + a_{kn}x_n &= a_{k1}(x'_1 - x''_1) + \cdots + a_{kn}(x'_n - x''_n) \\
&= (a_{k1}x'_1 + \cdots + a_{kn}x'_n) - (a_{k1}x''_1 + \cdots + a_{kn}x''_n) \\
&= y - y \\
&= 0
\end{aligned}$$

para $k = 1, \ldots, m \in \mathbb{N}$. Logo, existe uma solução não trivial de inteiros $x_1, \ldots, x_n$ em (6.1). Além disso, usando o fato de $|x_j| \leq q$ e $2q < (nA)^{\frac{m}{n-m}} + 1$ vistos anteriormente. Segue-se que

$$|x_j| \leq 2q < (nA)^{\frac{m}{n-m}} + 1$$

Portanto, temos que $|x_j| < 1 + (nA)^{\frac{m}{n-m}}$, com $j = 1, 2, \ldots, n \in \mathbb{N}$. □

Definição 6.1. *Seja $\alpha \in K$ um número algébrico (ou inteiro algébrico). O* **peso** *de α denotado por $\|\alpha\|$, é o máximo entre os módulos dos conjugados de α, isto é*

$$\|\alpha\| = máx_{1\leq i\leq n}\left\{|\alpha^{(i)}|\right\}$$

onde $\alpha^{(i)}$ é o i-ésimo conjugado de α e $n \in \mathbb{N}$.

Proposição 6.2. *Se α, $\beta \in K$ são algébricos. Então vale as seguintes propriedades:*

(1) $\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$;

(2) $\|\alpha\beta\| \leq \|\alpha\| \cdot \|\beta\|$

Demonstração. **Item** (1). Se os conjugados de α e β sobre K são $\alpha = \alpha^{(i)}$ e $\beta = \beta^{(i)}$, com $i = 1, \ldots, n \in \mathbb{N}$, respectivamente. Segue-se da Proposição 4.3, item (i) e da desigualdade triangular.

$$\begin{aligned}
\|\alpha + \beta\| &= \text{máx}_{1\leq i\leq n}\left\{|(\alpha+\beta)^{(i)}|\right\} \\
&= \text{máx}_{1\leq i\leq n}\left\{|\alpha^{(i)} + \beta^{(i)}|\right\} \\
&\leq \text{máx}_{1\leq i\leq n}\left\{|\alpha^{(i)}| + |\beta^{(i)}|\right\} \\
&\leq \text{máx}_{1\leq i\leq n}\left\{|\alpha^{(i)}|\right\} + \text{máx}_{1\leq i\leq n}\left\{|\beta^{(i)}|\right\} \\
&= \|\alpha\| + \|\beta\|
\end{aligned}$$

O **Item (2)**. é análogo, segue-se da Proposição 4.3, item (ii). □

Vejamos a seguir mais um importante Lema de C. Siegel.

Lema 6.2. *Seja $K|\mathbb{Q}$ uma extensão algébrica. Considere as p equações em q incógnitas com $0 < p < q \in \mathbb{N}$,*

$$\alpha_{k1}\zeta_1 + \alpha_{k2}\zeta_2 + \cdots + \alpha_{kq}\zeta_q = 0, \quad 1 \leq k \leq p \tag{6.2}$$

onde $\alpha_{ki} \in K$ são inteiros algébricos e $[K : \mathbb{Q}] = n$. Seja $A \geq 1$ um inteiro tal que $\|\alpha_{ki}\| \leq A$ para todo k e i. Então existe uma constante $C > 0$ dependendo de K, porém não depende de α_{ki}, p e q tal que o sistema (6.2) *possui uma solução não trivial $\zeta_1, \zeta_2, \ldots, \zeta_q$ em inteiros algébricos sobre K satisfazendo a seguinte estimativa*

$$\|\zeta_i\| < C + C(CqA)^{\frac{p}{q-p}}, \quad i = 1, \ldots, q \in \mathbb{N}.$$

Demonstração. Pelo Teorema 4.9, $K|\mathbb{Q}$ possui pelo menos uma base integral. Seja $\beta_1, \dots \beta_n$ uma base integral de $K|\mathbb{Q}$. Por definição de base integral se α é um inteiro algébrico sobre K, então existem $g_1, \dots, g_n \in \mathbb{Z}$ tal que α é escrito de forma única como

$$\alpha = g_1\beta_1 + \cdots + g_n\beta_n \tag{6.3}$$

Denotando os conjugados de α por $\alpha = \alpha^{(1)}, \alpha^{(2)}, \dots, \alpha^{(n)}$ e $\beta_j = \beta_j^{(1)}, \beta_j^{(2)}, \dots, \beta_j^{(n)}$ para $j = 1, \dots, n \in \mathbb{N}$. Passando o i-ésimo conjugando na igualdade (6.3) e usando o fato que o conjugado da soma é a soma dos conjugados, obtemos o seguinte sistema

$$\alpha^{(i)} = g_1\beta_1^{(i)} + \cdots + g_n\beta_n^{(i)}, \quad i = 1, \dots, n \in \mathbb{N}, \tag{6.4}$$

Considere as matrizes

$$X = \begin{pmatrix} \alpha_1^{(1)} \\ \vdots \\ \alpha_n^{(n)} \end{pmatrix}; B = \begin{pmatrix} \beta_1^{(1)} & \beta_2^{(1)} & \cdots & \beta_n^{(1)} \\ \beta_1^{(2)} & \beta_2^{(2)} & \cdots & \beta_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{(n)} & \beta_2^{(n)} & \cdots & \beta_n^{(n)} \end{pmatrix}; G = \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix}$$

A igualdade em (6.4) tem a seguinte forma matricial:

$$BG = X$$

Por outro lado, como $\{\beta_1, \dots, \beta_n\}$ é uma base integral. Então pelo Teorema 4.8, tem-se

$$\Delta[\beta_1, \dots, \beta_n] = (\det B)^2 \in \mathbb{Z} - \{0\}.$$

Daí, $detB \neq 0$ e logo existe B^{-1}(a matriz inversa de B) que denotaremos por:

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

onde os β_{ji} so dependem das entradas de B. Multiplicando a igualdade $BG = X$ à

esquerda por B^{-1}, obtemos:

$$G = B^{-1}X, \text{ isto é, } \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix} = \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n1} & \beta_{n2} & \cdots & \beta_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1^{(1)} \\ \vdots \\ \alpha_n^{(n)} \end{pmatrix}$$

Por conseguinte,

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

Passando o módulo, tem-se

$$\begin{aligned} |g_j| &= |\beta_{j1}\alpha^{(1)} + \cdots + \beta_{jn}\alpha^n| \\ &\leq |\beta_{j1}||\alpha^{(1)}| + \cdots + |\beta_{jn}||\alpha^n| \\ &\leq (|\beta_{j1}| + \cdots + |\beta_{jn}|)\|\alpha\| \\ &< C_1\|\alpha\| \end{aligned}$$

onde $C_1 = \text{máx}_{1\leq j\leq n}\{|\beta_{j1}| + \cdots + |\beta_{jn}|\} + 1 > 0$. Observe que C_1 depende de K, porém não depende de α. Logo,

$$|g_j| < C_1\|\alpha\|, \quad j = 1, \ldots, n \tag{6.5}$$

Sendo ζ_i, para $i = 1, \ldots, q \in \mathbb{N}$ inteiros algébricos sobre K satisfazendo o sistema (6.2) (Na verdade, mostraremos que o ζ_i é solução não trivial do sistema), como ζ_i são inteiros algébricos, podemos escrevê-lo de forma única como combinação da base integral $\beta_1, \ldots, \beta_n$.

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

O problema então é determinar o comportamento dos números inteiros x_{ij} de modo que possamos utilizar o Lema 6.1. Por (6.2) temos

$$0 = \sum_{i=1}^{q} \alpha_{ki}\zeta_i = \sum_{i=1}^{q} \alpha_{ki} \sum_{j=1}^{n} x_{ij}\beta_j = \sum_{i=1}^{q}\sum_{j=1}^{n} x_{ij}\alpha_{ki}\beta_j \tag{6.6}$$

Como o produto de inteiros algébricos resulta em um inteiro algébrico, então $\alpha_{ki}\beta_j$ é inteiro algébrico, e por sua vez pode ser escrito de forma única como combinação da

base integral. Logo,

$$\alpha_{ki}\beta_j = \sum_{r=1}^{n} m_{kijr}\beta_r, \quad 1 \leq k \leq p, \ 1 \leq i \leq q, \ 1 \leq j \leq n, \text{ com } m_{kijr} \in \mathbb{Z}. \tag{6.7}$$

e substituindo em (6.6), obtemos

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

Como $\{\beta_1, \ldots, \beta_n\}$ é base integral, e pelo Teorema 4.7, em particular, é uma base, daí, é (L.I.) sobre $\mathbb{Q}$, segue-se

$$0 = \sum_{i=1}^{q}\sum_{j=1}^{n} x_{ij}m_{kijr}, \quad k = 1, \ldots, p \quad r = 1, \ldots, n \tag{6.8}$$

ou seja, temos um sistema de pn equações com qn incógnitas tal que $0 < pn < qn \in \mathbb{N}$ com $x_{ij}, m_{kijr} \in \mathbb{Z}$. Para aplicar o Lema 6.1, basta-nos então majorar os números m_{kijr}. Pelo (6.7) e utilizado o mesmo argumento que obtemos a desigualdade (6.5), deduziremos tal fato. Pela relação $\alpha_{ki}\beta_j = \sum_{r=1}^{n} m_{kijr}\beta_r$ em (6.7), temos

$$\alpha_{ki}\beta_j = m_{kij1}\beta_1 + \cdots + m_{kijn}\beta_n$$

Passando o s-ésimo conjugado, tem-se

$$(\alpha_{ki}\beta_j)^{(s)} = m_{kij1}\beta_1^{(s)} + \cdots + m_{kijn}\beta_n^{(s)}, \quad s = 1, \ldots, n \in \mathbb{N},$$

Considere as matrizes

$$D = \begin{pmatrix} (\alpha_{ki}\beta_j)^{(1)} \\ \vdots \\ (\alpha_{ki}\beta_j)^{(n)} \end{pmatrix}; \ B = \begin{pmatrix} \beta_1^{(1)} & \beta_2^{(1)} & \cdots & \beta_n^{(1)} \\ \beta_1^{(2)} & \beta_2^{(2)} & \cdots & \beta_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{(n)} & \beta_2^{(n)} & \cdots & \beta_n^{(n)} \end{pmatrix}; \ M = \begin{pmatrix} m_{kij1} \\ \vdots \\ m_{kijn} \end{pmatrix}$$

com forma matricial igual a $BM = D$, como vimos anteriormente que $\det B \neq 0$, com inversa B^{-1}, então multiplicando a igualdade $BM = D$ por B^{-1} à esquerda, obtemos

$$M = B^{-1}D, \text{ ou seja, } \begin{pmatrix} m_{kij1} \\ \vdots \\ m_{kijn} \end{pmatrix} = \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n1} & \beta_{n2} & \cdots & \beta_{nn} \end{pmatrix}\begin{pmatrix} (\alpha_{ki}\beta_j)^{(1)} \\ \vdots \\ (\alpha_{ki}\beta_j)^{(n)} \end{pmatrix}$$

Daí,

$$m_{kijr} = \beta_{j1}\left(\alpha_{ki}\beta_j\right)^{(1)} + \beta_{j2}\left(\alpha_{ki}\beta_j\right)^{(2)} + \cdots + \beta_{jn}\left(\alpha_{ki}\beta_j\right)^{(n)}, \quad r = 1, \ldots, n$$

Por conseguinte,

$$\begin{aligned}
|m_{kijr}| &\leq |\beta_{j1}||\left(\alpha_{ki}\beta_j\right)^{(1)}| + \cdots + |\beta_{jn}||\left(\alpha_{ki}\beta_j\right)^{(n)}| \\
&\leq \left(|\beta_{j1}| + \cdots + |\beta_{jn}|\right)\|\alpha_{ki}\beta_j\| \\
&< \left(\text{máx}_{1\leq j\leq n}\left\{|\beta_{j1}| + \cdots + |\beta_{jn}|\right\} + 1\right)\|\alpha_{ki}\beta_j\| \\
&= C_1\|\alpha_{ki}\beta_j\| \\
&\leq C_1\|\alpha_{ki}\|.\|\beta_j\| \\
&\leq C_1 A\|\beta_j\| \\
&\leq C_2 A
\end{aligned}$$

onde C_2 é um constante positiva que satisfaz:

$$C_2 \geq C_1\|\beta_j\| \quad \text{e} \quad C_2 A \in \mathbb{Z} - \{0\}.$$

Como $|m_{kijr}| \leq C_2 A$, onde $C_2 A \geq 1$ e $m_{kijr} \in \mathbb{Z}$ são coeficientes de x_{ij}. Logo, aplicando o Lema 6.1, ao sistema (6.8), ou seja, $0 = \sum_{i=1}^{q}\sum_{j=1}^{n} x_{ij}m_{kijr}$. Logo, existe uma solução não trivial x_{ij} em inteiros sobre K tais que

$$|x_{ij}| < 1 + (qnC_2A)^{\frac{pn}{qn-pn}} = 1 + (nC_2qA)^{\frac{p}{q-p}} \tag{6.9}$$

Por outro lado, tomando o peso dos $\zeta_i = \sum_{j=1}^{n} x_{ij}\beta_j$ e aplicando a Proposição 6.2, item i e ii, e usando o fato de que (se $x_{ij} \in \mathbb{Z}$, então pelo Teorema 4.5, item(ii), seus conjugados são todos iguais), e ainda do fato dos $\beta_j = \beta_j^{(1)}, \ldots, \beta_j^{(n)}$, com $j = 1, \ldots, n$ e da desigualdade (6.9). Segue-se que

$$\begin{aligned}
\|\zeta_i\| &= \Big\|\sum_{j=1}^{n} x_{ij}\beta_j\Big\| \\
&\leq \|x_{i1}\|.\|\beta_1\| + \cdots + \|x_{in}\|.\|\beta_n\| \\
&\leq |x_{ij}|.\text{máx}_{1\leq i\leq n}\left\{|\beta_1^{(i)}|\right\} + \cdots + |x_{ij}|.\text{máx}_{1\leq i\leq n}\left\{|\beta_n^{(i)}|\right\} \\
&\leq \Big(\underbrace{|x_{ij}| + \cdots + |x_{ij}|}_{\text{n-parcelas}}\Big)\text{máx}_j\left\{\|\beta_j\|\right\} \\
&\leq n.|x_{ij}|\text{máx}_j\left\{\|\beta_j\|\right\} \\
&< n.\text{máx}_j\left\{\|\beta_j\|\right\}\left(1 + (nC_2qA)^{\frac{p}{q-p}}\right) \\
&= n.\text{máx}_j\left\{\|\beta_j\|\right\} + n.\text{máx}_j\left\{\|\beta_j\|\right\}\left(nC_2qA\right)^{\frac{p}{q-p}}
\end{aligned}$$

Por conseguinte,

$$\|\zeta_i\| < n.\text{máx}_j \{\|\beta_j\|\} + n.\text{máx}_j \{\|\beta_j\|\} \left(nC_2qA\right)^{\frac{p}{q-p}} \tag{6.10}$$

Considere C uma constante positiva tal que $C \geq n.\text{máx}_j \{\|\beta_j\|\}, (j = 1, \ldots, n)$ e $C \geq nC_2$. Logo, a constante C só depende do corpo K, visto que o peso de $\|\beta_j\|$, e C_2 só dependem de K, e voltando à (6.10) concluímos que

$$\|\zeta_i\| < C + C\left(CqA\right)^{\frac{p}{q-p}}, \quad i = 1, \ldots, q$$

Como os $\beta_j = \beta_j^{(1)}, \ldots, \beta_j^{(n)}$ são não nulos e como vimos que os $x_{ij} \neq 0$ por ser uma solução não trivial. Assim, os $\zeta_i \neq 0$. E voltando à (6.6), podemos concluir que ζ_i é solução não trivial em inteiros algébricos do sistema $\alpha_{k1}\zeta_1 + \cdots + \alpha_{kq}\zeta_q = 0$, com $1 \leq k \leq p \in \mathbb{N}$. □

Agora, necessitaremos de dois teoremas clássicos já conhecidos do curso de funções de uma variável complexa, por brevidade, serão apenas enunciados e uma simples propriedade da desigualdade exponencial que será provada.

Teorema 6.1 (Expansão em Série de Taylor)**.** *Seja $f : U \longrightarrow \mathbb{C}$ uma função analítica no disco $D(z_0, R) \subset U$. Então $F(z)$ é dada pela sua série de Taylor de centro z_0:*

$$f(z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(z_0)}{n!}(z - z_0)^n$$

sendo $a_n = \dfrac{f^{(n)}(z_0)}{n!}$ os coeficientes dessa expansão.

Demonstração. Para maiores detalhes Ver [15], p. 80-81. □

Teorema 6.2 (Fórmula Integral de Cauchy)**.** *Seja $f : U \longrightarrow \mathbb{C}$ uma função analítica em $U \subset \mathbb{C}$. Sejam $\bar{D}(z_0, r_0) \subset U$ um disco fechado e simples e C sua fronteira, orientada compativelmente. Se w_0 é um ponto qualquer no interior de $\bar{D}(z_0, r_0)$. Então*

$$f(w_0) = \frac{1}{2\pi i} \int_C \frac{f(z)}{z - w_0} dz$$

Demonstração. Para maiores detalhes Ver [15], p. 114-116. □

Proposição 6.3. *Seja $u \in \mathbb{C}$ um número complexo, onde $u = a + ib$ com $a, b \in \mathbb{R}$. Então vale a seguinte desigualdade*

$$|e^u| \leq e^{|u|}, \quad \textit{para todo} \quad u \in \mathbb{C}.$$

Demonstração. Usaremos o fato de $e^x > 0$, para todo $x \in \mathbb{R}$ e as seguintes identidades: $(e^{ix} = \cos x + i \sin x)$ e $(\cos^2 x + \sin^2 x = 1)$ para todo $x \in \mathbb{R}$. Por um lado, temos

$$|e^u| = |e^a e^{ib}| = e^a |\cos b + i \sin b| = e^a \underbrace{\sqrt{\cos^2 b + \sin^2 b}}_{1} = e^a$$

Por outro lado, temos que

$$e^{|u|} = e^{|a+ib|} = e^{\sqrt{a^2+b^2}}$$

Segue-se que $e^a \leq e^{\sqrt{a^2+b^2}}$, pois se b é um número real, ou negativo ou positivo, daí, $b^2 > 0$ então $e^a < e^{\sqrt{a^2+b^2}}$, se $b = 0$ vale a igualdade, pois, $e^{\sqrt{a^2+0^2}} = e^{\sqrt{a^2}} = e^a$. Portanto, concluímos que $|e^u| \leq e^{|u|}$ para todo $u \in \mathbb{C}$. □

Finalmente, veremos uma solução do Sétimo Problema de Hilbert.

6.2 Solução do Sétimo Problema de Hilbert

Nesta seção apresentaremos em detalhes uma Solução do famoso Sétimo Problema de Hilbert, baseado na demonstração de Gelfond, teorema que ficou conhecido como Teorema de Gelfond-Schneider, pelo fato de Gelfond (1934) e Schneider (1935), independentemente, terem provado o mesmo teorema. Vejamos sua solução a seguir:

Teorema 6.3 (Gelfond-Schneider)**.** *Sejam α e β números algébricos (reais ou complexos) tal que $\alpha \in \mathbb{A} - \{0, 1\}$ e $\beta \in \mathbb{A} - \mathbb{Q}$. Então α^β é um número transcendente.*

Demonstração. Suponha por absurdo que α^β seja algébrico, com $\alpha \notin \{0, 1\}$. Escrevendo $\gamma = \alpha^\beta = e^{\beta \log \alpha}$, onde log representa o logaritmo de base e. Seja $K := \mathbb{Q}(\alpha, \beta, \gamma)$ uma extensão finta de $\mathbb{Q}$ com grau $h \in \mathbb{N}$. Definamos os inteiros positivos m, q, n e t satisfazendo as relações:

$$m = 2h + 3, \quad q > 4m^2, \quad n = \frac{q^2}{2m}, \quad t = q^2 = 2mn \quad \text{e} \quad n > q. \tag{6.11}$$

Defina também

$$\rho_1, \rho_2, \ldots, \rho_t := (r + k\beta) \log \alpha, \quad \text{para} \quad 1 \leq r \leq q;\ 1 \leq k \leq q$$

em alguma ordem. Considere a seguinte função inteira

$$F(z) = \sum_{j=1}^{t} \eta_j e^{z\rho_j} = \eta_1 e^{z\rho_1} + \cdots + \eta_t e^{z\rho_t} \tag{6.12}$$

onde η_j são inteiros algébricos sobre K que serão especificados posteriormente (Na verdade, mostraremos que o η_j é solução não trivial do sistema (6.13), a seguir). Note que $F(z)$ é uma função inteira (isto é, tem derivada em todo plano complexo).

Tomando a derivada de ordem a da função $F(z)$, tem-se

$$F^{(a)}(z) = \sum_{j=1}^{t} \eta_j \rho_j^a e^{z\rho_j}, \quad 0 \leq a \leq n-1 \in \mathbb{N}.$$

Como α, β e γ são algébricos, então pelo Teorema 4.6, existem a_1, a_2, a_3 inteiros positivos tais que $a_1\alpha, a_2\beta$ e $a_3\gamma$ são inteiros algébricos. Tome $C_1 = a_1a_2a_3 \in \mathbb{Z}$, sendo $C_1 > 0$ tal que $C_1\alpha, C_1\beta$ e $C_1\gamma$ são ainda inteiros algébricos. Considere agora as mn equações em $2mn = q^2 = t$ incógnitas η_j (por enquanto, desconhecidas).

$$C_1^{n+2mq} (\log \alpha)^{-a} F^{(a)}(b) = 0, \quad 0 \leq a \leq n-1;\ 1 \leq b \leq m. \tag{6.13}$$

Desejamos obter os coeficientes de η_j no sistema (6.13), isto é,

$$\begin{aligned} C_1^{n+2mq} (\log \alpha)^{-a} \rho_j^a e^{b\rho_j} &= C_1^{n+2mq} (\log \alpha)^{-a} (r+k\beta)^a (\log \alpha)^a e^{b(r+k\beta)\log\alpha} \\ &= C_1^{n+2mq} (r+k\beta)^a e^{\log\left(\alpha^{b(r+k\beta)}\right)} \\ &= C_1^{n+2mq} (r+k\beta)^a \alpha^{b(r+k\beta)} \\ &= C_1^{n+2mq} (r+k\beta)^a \alpha^{br} \left(\alpha^{\beta}\right)^{bk} \\ &= C_1^{n+2mq} (r+k\beta)^a \alpha^{br} \gamma^{bk} \end{aligned}$$

Note que a ultima igualdade é um polinômio em α, β e γ de grau $a + br + bk$. Como os máximos de a, b, r e k são respectivamente $n-1, m, q$ e q. Então

$$a + br + bk \leq n - 1 + mq + mq = n - 1 + 2mq$$

Como $r, k, C_1\alpha, C_1\beta$ e $C_1\gamma$ são inteiros algébricos e o produto e soma de inteiros algébrico é algébrico. Logo, $C_1^{n+2mq} (r+k\beta)^a \alpha^{br}\gamma^{bk}$ é um inteiro algébrico.

Queremos utilizar o Lema 6.2, para o sistema de equações em (6.13). Já mostramos que os coeficientes das incógnitas η_j são inteiros algébricos, logo, bata-nos encontrar um limitante superior para o peso de $C_1^{n+2mq} (r+k\beta)^a \alpha^{br}\gamma^{bk}$ sobre K. Note que, tomando o peso de $r + k\beta$ e usando a Proposição 6.2, item (1) e o fato de $r \leq q$, $k \leq q$, tem-se

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

Defina $C_2 := \max\{\|\alpha\|, \|\gamma\|, 1 + \|\beta\|\} > 0$.

Dessa forma, C_2 não depende de n, q, e t. Além disso, como $a \leq n-1$, $b \leq m$, $r \leq q$, $k \leq q$ e por (6.11) temos ($q^2 = 2mn \Longrightarrow q = \sqrt{2m}.n^{\frac{1}{2}} \Longrightarrow q^n = \left(\sqrt{2m}\right)^n n^{\frac{n}{2}}$) e $n > q$. Segue-se que

$$\begin{aligned}
\|C_1^{n+2mq}\,(r+k\beta)^a\,\alpha^{br}\gamma^{bk}\| &\leq \|C_1^{n+2mq}\|.\|(r+k\beta)^a\,\|.\|\alpha^{br}\|.\|\gamma^{bk}\| \\
&\leq C_1^{n+2mq}\,[q(1+\|\beta\|)]^a\,C_2^{br}C_2^{bk} \\
&\leq C_1^{n+2mq}(qC_2)^a C_2^{br}C_2^{bk} \\
&\leq C_1^{n+2mq}(qC_2)^n C_2^{mq}C_2^{mq} \\
&= C_1^n C_1^{2mq} q^n C_2^n C_2^{2mq} \\
&= (C_1C_2)^n (C_1C_2)^{2mq} q^n \\
&\leq (C_1C_2)^n (C_1C_2)^{2mn} q^n \\
&= (C_1C_2)^{2mn+n} (\sqrt{2m})^n n^{\frac{n}{2}} \\
&= (C_1C_2)^{(2m+1)n} (\sqrt{2m})^n n^{\frac{n}{2}} \\
&= \left((C_1C_2)^{2m+1}\sqrt{2m}\right)^n n^{\frac{n}{2}} \\
&= C_3^n n^{\frac{n}{2}}
\end{aligned}$$

Defina $C_3 := (C_1C_2)^{2m+1}\sqrt{2m} \geq 1$, tal que m não depende de n, e assim, temos a seguinte limitação:

$$\|C_1^{n+2mq}\,(r+k\beta)^a\,\alpha^{br}\gamma^{bk}\| \leq C_3^n n^{\frac{n}{2}}$$

onde C_3 é uma constante que não depende de n. Agora, podemos usar o Lema 6.2, para concluir que o sistema (6.13) tem solução não trivial η_j em inteiros algébricos, para cada j, com a seguinte estimativa:

$$\begin{aligned}
\|\eta_j\| &< C + C\left(C.2mnC_3^n n^{\frac{n}{2}}\right)^{\frac{mn}{2mn-mn}} \\
&= C + C\left(2CmnC_3^n n^{\frac{n}{2}}\right)^{\frac{mn}{mn}} \\
&= C + 2C^2 mnC_3^n n^{\frac{n}{2}} \\
&< C^2 mnC_3^n n^{\frac{n}{2}} + 2C^2 mnC_3^n n^{\frac{n}{2}} \\
&= 3C^2 mnC_3^n n^{\frac{n}{2}}
\end{aligned}$$

onde C depende de K, porém não depende de n. Como $2^n > n$ (por indução sobre n) e $n > q > m$, ou seja, $2^n > n > m$. Por um lado, multiplicando ($2^n > n$) por 2^n, tem-se

$$2^n.2^n > 2^n n \Longrightarrow 2^{2n} = (2^2)^n > 2^n n \Longrightarrow 4^n > 2^n n$$

Por outro lado, multiplicando ($2^n > n > m$) por n, tem-se $2^n n > n^2 > mn$. Combi-

nando as duas ultimas desigualdade encontradas, temos $4^n > mn$, daí,

$$\begin{aligned} \|\eta_j\| &< 3C^2 mnC_3^n n^{\frac{n}{2}} \\ &< 3C^2 4^n C_3^n n^{\frac{n}{2}} \\ &\leq (3C^2)^n (4C_3)^n n^{\frac{n}{2}} \\ &= (12C^2C_3)^n n^{\frac{n}{2}} \\ &= C_4^n n^{\frac{n}{2}} \end{aligned}$$

Defina $C_4 := 12C^2C_3 > 0$, que depende de K. Agora $F(z)$ em (6.12) está completamente definida

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

onde $\eta_1, \ldots, \eta_t$ é solução não trivial de (6.13), isto é, de

$$C_1^{n+2mq} (\log \alpha)^{-a} F^{(a)}(b) = 0, \quad 0 \leq a \leq n-1, \quad 1 \leq b \leq m.$$

.

Agora, faremos alguns Lemas para uma melhor organização.

Lema 6.3. *Escolha $p \geq n$ e B no intervalo $1 \leq B \leq m$ tais que $F^{(a)}(b) = 0$, para $a = 0, \ldots, p-1$, $b = 1, \ldots, m$, e $F^{(p)}(B) \neq 0$ para algum $p \in \{0, 1, \ldots, t-1\}$.*

Demonstração. Note que, existe um primo $p \geq n$, $(p - 1 \geq n - 1)$ tal que de (6.13), temos que:

$$C_1^{n+2mq} (\log \alpha)^{-a} F^{(a)}(b) = 0, \quad 0 \leq a \leq n-1, \quad 1 \leq b \leq m.$$

. Como $C_1^{n+2mq} \neq 0$, $\log \alpha \neq 0$ (pois $\alpha \neq 1$). Assim,

$$F^{(a)}(b) = 0, \quad 0 \leq a \leq p-1, \quad 1 \leq b \leq m$$

Agora, é suficiente mostrar que existe $p \in \{0, 1, \ldots, t-1\}$ tal que $F^{(p)}(1) \neq 0$. Suponha por absurdo que $F^{(p)}(1) = 0$, para todo $p \in \{0, 1, \ldots, t-1\}$, por (6.12), tem-se

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

Para cada $p = 0, \ldots, t-1$, tem-se o seguinte sistema homogêneo:

$$\begin{array}{rcl} F^{(0)}(1) & = & \eta_1\rho_1^0 e^{\rho_1} + \cdots + \eta_t\rho_t^0 e^{\rho_t} = 0 \\ F^{(1)}(1) & = & \eta_1\rho_1^1 e^{\rho_1} + \cdots + \eta_t\rho_1^1 e^{\rho_t} = 0 \\ \vdots & & \vdots \qquad\qquad \vdots \\ F^{(t-1)}(1) & = & \eta_1\rho_1^{t-1} e^{\rho_1} + \cdots + \eta_t\rho_t^{t-1} e^{\rho_t} = 0 \end{array}$$

Passando para a forma matricial, tem-se

$$\begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_t \end{pmatrix} . \begin{pmatrix} \rho_1^0 & \rho_2^0 & \cdots & \rho_t^0 \\ \rho_1^1 & \rho_2^1 & \cdots & \rho_t^1 \\ \vdots & \vdots & \ddots & \vdots \\ \rho_1^{t-1} & \rho_2^{t-1} & \cdots & \rho_t^{t-1} \end{pmatrix} . \begin{pmatrix} e^{\rho_1} \\ e^{\rho_2} \\ \vdots \\ e^{\rho_t} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Como mostramos que η_j's é solução não trivial (não todos nulos), o que implica que o determinante da matriz do coeficientes do sistema homogêneo é zero, isto é,

$$0 = \det\left(\rho_j^p e^{\rho_j}\right) = \det\left(\rho_j^p\right) \prod_j e^{\rho_j}$$

Como $\prod_j e^{\rho_j} \neq 0$, daí, $\det\left(\rho_j^p\right) = 0$, que é um determinante de Vandermonde. Pela Proposição 6.1, esse determinante anula-se quando dois dos seus elementos característico são iguais, digamos $\rho_j = \rho_l$, para algum $j \neq l$. Logo,

$$(r_s + k_s\beta)\log\alpha = (r_v + k_v\beta)\log\alpha, \quad 1 \leq r_s, k_v \leq q \in \mathbb{N}$$

para algum $s \neq v$. Como $\log\alpha \neq 0$ (pois, $\alpha \neq 1$), e assim, seguiria que

$$(r_s + k_s\beta) = (r_v + k_v\beta) \Longrightarrow r_s - r_v = (k_v - k_s)\,\beta \Longrightarrow \beta = \frac{r_s - r_v}{k_v - k_s} \in \mathbb{Q}$$

Daí, teríamos que β seria racional. Absurdo! pois, por hipótese β é algébrico irracional.

□

Usando o Lema 6.3, acima, definimos o seguinte número não nulo,

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

A seguir tomaremos a norma de ζ.

Lema 6.4. *Existe uma constante positiva $\tilde{C}$, que não depende de n e p, com $p \geq n$ tal que*

$$|N(\zeta)| \geq \tilde{C}^{-p}$$

Demonstração. Primeiramente verifiquemos que $C_1^{p+2mq}\zeta$ é inteiro algébrico sobre K. De fato, note que η_j são inteiros algébricos sobre K e $(r+k\beta)^p \alpha^{Br}\gamma^{Bk}$ é um polinômio em α, β e γ com grau $p + Br + Bk \leq p + mq + mq = p + 2mq$, já que $B \leq m$ e $r, k \leq q$ e como $C_1\alpha, C_1\beta$ e $C_1\gamma$ são inteiros algébricos, e a soma e o produto de inteiros algébricos é inteiro algébrico, logo, $C_1^{p+2mq}\zeta = C_1^{p+2mq} \sum_{j=1}^{t} \eta_j (r+k\beta)^p \alpha^{Br}\gamma^{Bk}$ é um inteiro algébrico. Como $q < n \leq p$. Então

$$C_1^{p+2mq} < C_1^{p+2mp} = \left(C_1^{1+2m}\right)^p = C_5^P \quad \left(\text{Defina } C_5 := C_1^{1+2m} \in \mathbb{Z}, \text{sendo } C_5 > 0\right)$$

pois, C_1 é um inteiro positivo. Como $p > q \in \mathbb{N}$, então $p = q + s$ para algum $s \in \mathbb{N}$. Segue-se que

$$C_5^p\zeta = C_1^{p+2mp}\zeta = C_1^{p+2m(q+s)}\zeta = C_1^{p+2mq+2ms}\zeta = C_1^{2ms}\left(C_1^{p+2mq}\right)\zeta$$

Logo, o número $C_5^p\zeta$ também é inteiro algébrico não nulo. Pela Proposição 4.4, item (iii), tem-se que a norma de $C_5^p\zeta$ é um inteiro não nulo, isto é, $N(C_5^p\zeta) \in \mathbb{Z} - \{0\}$. Pela Proposição 4.4, item (i) e item (iv), segue-se que

$$1 \leq |N(C_5^p\zeta)| = |N(C_5^p) \cdot N(\zeta)| = |N(C_5^p)|.|N(\zeta)| = (C_5^p)^h |N(\zeta)|$$

Daí,

$$|N(\zeta)| \geq \frac{1}{C_5^{ph}} = C_5^{-ph} \Longrightarrow |N(\zeta)| \geq \tilde{C}^{-p}, \quad (\text{Defina } \tilde{C} := C_5^h > 0)$$

onde $\tilde{C}$ e h não dependem de n e p. □

Lema 6.5. *Existe uma constante positiva $\bar{C}$, que não depende de n e p, com $p \geq n$ tal que*

$$\|\zeta\| < \bar{C}^p p^p$$

Demonstração. Como $\zeta = \sum_{j=1}^{t} \eta_j \, (r + k\beta)^p \, \alpha^{Br} \gamma^{Bk} \neq 0$. Tomando o peso de ζ, tem-se

$$\begin{aligned} \|\zeta\| &\leq \|\sum_{j=1}^{t} \eta_j\| \cdot \|(r + k\beta)^p\| \cdot \|\alpha^{Br}\| \cdot \|\gamma^{Bk}\| \\ &\leq t \cdot \text{máx}_j \left\{ \|\eta_j\| \cdot \|(r + k\beta)\|^p \cdot \|\alpha\|^{Br} \cdot \|\gamma\|^{Bk} \right\} \end{aligned}$$

Como $p \geq n > q$ e $q > 4m^2$, daí, $(n > 4m^2)$ e multiplicando por $2n$, temos

$$2n.n > 2n.4m^2 \Longrightarrow 2n^2 > 8m^2 n \Longrightarrow 2n^2 > 2mn = t$$

para n suficientemente grande, tem-se $2^n > 2n^2 > 2mn = t$, ou seja, $t < 2^n$.

Como anteriormente obtemos os seguintes resultados: $t < 2^n$, $\|\eta_j\| < C_4^n n^{\frac{n}{2}}$, $\|r + k\beta\| \leq q\,(1 + \|\beta\|) \leq qC_2$, $C_2 = \text{máx}\{\|\alpha\|, \|\gamma\|, 1 + \|\beta\|\}$, $B \leq m$, $r \leq q$ e $k \leq q$. Então substituindo a expressão que majora $\|\zeta\|$ pelos seus respectivos máximos, obtemos:

$$\begin{aligned} \|\zeta\| &\leq t \cdot \text{máx}_j \left\{ \|\eta_j\| \cdot \|(r + k\beta)\|^p \cdot \|\alpha\|^{Br} \cdot \|\gamma\|^{Bk} \right\} \\ &\leq 2^n C_4^n n^{\frac{n}{2}} \, (qC_2)^p \, C_2^{mq} C_2^{mq} \\ &< 2^p C_4^p n^{\frac{n}{2}} q^p C_2^p C_2^{2mp} \\ &= 2^p C_4^p C_2^{p+2mp} n^{\frac{n}{2}} q^p \\ &= \left(2C_4 C_2^{1+2m}\right)^p n^{\frac{n}{2}} q^p \end{aligned}$$

Por outro lado, como $n \leq p$, daí, $n^{\frac{n}{2}} \leq p^{\frac{p}{2}}$, o que implica que

$$q = \sqrt{2mn} \Longrightarrow q^p = \left(\sqrt{2m}\right)^p n^{\frac{p}{2}} \leq \left(\sqrt{2m}\right)^p p^{\frac{p}{2}}$$

e aplicando essa desigualdade a expressão que majora $\|\zeta\|$, resulta em

$$\begin{aligned} \|\zeta\| &< \left(2C_4 C_2^{1+2m}\right)^p n^{\frac{n}{2}} q^p \\ &\leq \left(2C_4 C_2^{1+2m}\right)^p p^{\frac{p}{2}} \left(\sqrt{2m}\right)^p p^{\frac{p}{2}} \\ &= \left(2\sqrt{2m} C_4 C_2^{1+2m}\right)^p p^p \\ &= \bar{C}^p p^p \end{aligned}$$

Defina $\bar{C} := 2\sqrt{2m}C_4C_2^{1+2m} > 0$. Portanto, o peso $\|\zeta\| < \bar{C}^p p^p$ onde $\bar{C}$ não depende de n e p. □

Como $F(z)$ é uma função inteira. Logo, $S(z)$ definida a seguir também é função inteira:

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

Como $F(z)$ é função inteira, em particular, é analítica, então pelo Teorema 6.1, podemos expandir $F(z)$ em série Taylor em torno de $z_0 = B$, isto é,

$$F(z) = \sum_{d=0}^{\infty}\frac{F^{(p+d)}(B)}{(p+d)!}(z-B)^{p+d}$$

Daí,

$$F(z) = \frac{F^{(p)}(B)}{p!}(z-B)^p + \sum_{d=1}^{\infty}\frac{F^{(p+d)}(B)}{(p+d)!}(z-B)^{p+d}$$

Substituindo na expressão de $S(z)$, temos que

$$\begin{aligned}
S(z) &= p!\Big(\frac{F^{(p)}(B)}{p!}(z-B)^p + \sum_{d=1}^{\infty}\frac{F^{(p+d)}(B)}{(p+d)!}(z-B)^{p+d}\Big)\cdot\frac{(B-1)^p\cdots\widehat{(B-B)^p}\cdots(B-m)^p}{(z-1)^p\cdots(z-B)^p\cdots(z-m)^p}\\
&= p!\frac{F^{(p)}(B)(z-B)^p}{p!}\cdot\frac{(B-1)^p\cdots\widehat{(B-B)^p}\cdots(B-m)^p}{(z-1)^p\cdots(z-B)^p\cdots(z-m)^p} + \sum_{d=1}^{\infty}\frac{p!F^{(p+d)}(B)(z-B)^{p+d}}{(p+d)!}\cdot\frac{\prod_{\substack{b=1\\ b\neq B}}^{m}(B-b)^p}{\prod_{b=1}^{m}(z-b)^p}\\
&= F^{(p)}(B)\frac{(B-1)^p\cdots\widehat{(B-B)^p}\cdots(B-m)^p}{(z-1)^p\cdots\widehat{(z-B)^p}\cdots(z-m)^p} + \sum_{d=1}^{\infty}p!\frac{F^{(p+d)}(B)(z-B)^{p+d}}{(p+d)!}\cdot\frac{\prod_{\substack{b=1\\ b\neq B}}^{m}(B-b)^p}{\prod_{b=1}^{m}(z-b)^p}
\end{aligned}$$

Aplicando B em $S(z)$, temos que

$$S(B) = F^{(p)}(B)\underbrace{\frac{(B-1)^p\cdots\widehat{(B-B)^p}\cdots(B-m)^p}{(B-1)^p\cdots\widehat{(B-B)^p}\cdots(B-m)^p}}_{1} + \underbrace{\sum_{d=1}^{\infty}p!\frac{F^{(p+d)}(B)\overbrace{(B-B)^{p+d}}^{0}}{(p+d)!}\cdot\frac{\prod_{\substack{b=1\\ b\neq B}}^{m}(B-b)^p}{\prod_{b=1}^{m}(B-b)^p}}_{0}$$

Logo, $S(B) = F^{(p)}(B)$. Como $\zeta = (\log\alpha)^{-p}F^{(p)}(B) \neq 0$. Segue-se

$$\zeta = (\log\alpha)^{-p}S(B) \tag{6.14}$$

Usando o Teorema 6.2, ou seja, a Fórmula Integral de Cauchy para $S(z)$, temos:

$$S(B) = \frac{1}{2\pi i}\int_C \frac{S(z)}{z-B}dz \tag{6.15}$$

onde C é uma curva simples fechada [1] em torno de $z_0 = B$. Considere C o círculo $|z| = \frac{p}{q}$ de centro 0 e raio $\frac{p}{q}$. Como $p \geq n > q$, $(q^2 = 2mn \Longrightarrow \frac{q}{2m} = \frac{n}{q})$, $q > 4m^2$ e $B \leq m$. Daí, tem-se

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

Segue-se que $z_0 = B$ está no interior do disco cuja a fronteira [2] é C.

Pela Proposição 6.3, sabemos que (se $u \in \mathbb{C}$, então $|e^u| \leq e^{|u|}$), logo, para todo z no círculo $|z| = \frac{p}{q}$, e como $r \leq q$ e $k \leq q$ inteiros positivos, obtemos

$$|e^{z\rho_j}| \leq e^{|z\rho_j|} \leq e^{|\frac{p}{q}(r+k\beta)\log\alpha|} \leq e^{\frac{p}{q}(q+q|\beta|)|\log\alpha|} \leq e^{p(1+|\beta|)|\log\alpha|} = \left(e^{(1+|\beta|)|\log\alpha|}\right)^p = C_6^p$$

Defina $C_6 := e^{(1+|\beta|)|\log\alpha|} > 0$, onde C_6 não depende de n e p.

Agora, encontraremos estimativas para $|F(z)|, |z-b|^{-p}, |z-B|^{-1}, |S(z)|$, $|\zeta|$ e $|N(\zeta)|$, respectivamente. Sabemos que $q < n \leq p$ e $(t = 2mn < 2n^2 < 2^n \leq 2^p)$ para n suficientemente grande, e que $|e^{z\rho_j}| \leq C_6^p$, e vimos ainda que $|\eta_j| \leq \|\eta_j\| < C_4^n n^{\frac{n}{2}}$, e assim, segue-se que

$$|F(z)| = \left|\sum_{j=1}^{t} \eta_j e^{z\rho_j}\right| \leq \sum_{j=1}^{t} |\eta_j||e^{z\rho_j}| \leq tC_4^n n^{\frac{n}{2}} C_6^p < 2^p C_4^p p^{\frac{p}{2}} C_6^p = (2C_4C_6)^p\, p^{\frac{p}{2}}$$

Por conseguinte,

$$|F(z)| < C_7^p p^{\frac{p}{2}} \tag{6.16}$$

Defina $C_7 := 2C_4C_6 > 0$.

Para $b = 1, 2, \ldots, m$, como $q > 4m^2$ temos também:

$$|z-b| \geq |z| - |b| \geq \frac{p}{q} - m \geq \frac{p}{2q} \Longrightarrow |z-b|^{-1} \leq \frac{2q}{p}$$

Daí,

$$|z-b|^{-p} \leq \left(\frac{2q}{p}\right)^p \tag{6.17}$$

[1] A curva $\alpha : [a,b] \longrightarrow \mathbb{C}$ é dita fechada, se $\alpha(a) = \alpha(b)$. Se a função α for injetiva (não possui auto interseções, excetuando a possibilidade de a curva ser fechada) a curva é chamada de simples.

[2] A fronteira de $X \subseteq Y$ é o conjunto dos pontos $x \in Y$ tais que toda bola aberta centrada em x contém pontos de X e de seu complementar $Y \backslash X$.

Analogamente, temos que

$$|z-B|^{-1} \leq \left(\frac{2q}{p}\right) \tag{6.18}$$

Aplicando (6.16), (6.17) e o fato de ($q^2 = 2mn \Longrightarrow q = \sqrt{2mn} \Longrightarrow q = (2mn)^{\frac{1}{2}}$), obtemos:

$$\begin{aligned}
|S(z)| &= |p!F(z)| \left|\prod_{b=1}^{m}(z-b)^{-p}\right| \left|\prod_{\substack{b=1\\b\neq B}}^{m}(B-b)^{p}\right| \\
&\leq p!|F(z)| \prod_{b=1}^{m} |(z-b)|^{-p} \prod_{\substack{b=1\\b\neq B}}^{m} |(B-b)|^{p} \\
&< p!C_7^p p^{\frac{p}{2}} \prod_{b=1}^{m}\left(\frac{2q}{p}\right)^{p} \prod_{\substack{b=1\\b\neq B}}^{m} |(B-b)|^{p} \\
&= p!C_7^p p^{\frac{p}{2}} \left(\frac{2q}{p}\right)^{mp} \prod_{\substack{b=1\\b\neq B}}^{m} |(B-b)|^{p} \\
&= C_7^p \left(\frac{2\left(2mn\right)^{\frac{1}{2}}}{p}\right)^{mp} \prod_{\substack{b=1\\b\neq B}}^{m} |(B-b)|^{p} p!p^{\frac{p}{2}} \\
&= C_7^p 2^{mp}\left(2m\right)^{\frac{mp}{2}} \left(\frac{n^{\frac{1}{2}}}{p}\right)^{mp} \prod_{\substack{b=1\\b\neq B}}^{m} |(B-b)|^{p} p!p^{\frac{p}{2}} \\
&= \left(C_7 2^m \left(2m\right)^{\frac{m}{2}} \prod_{\substack{b=1\\b\neq B}}^{m} |(B-b)|\right)^{p} p!p^{\frac{p}{2}} \left(\frac{\sqrt{n}}{p}\right)^{mp} \\
&= C_8^p p!p^{\frac{p}{2}} \left(\frac{\sqrt{n}}{p}\right)^{mp}
\end{aligned}$$

onde $C_8 := C_7 2^m \left(2m\right)^{\frac{m}{2}} \prod_{\substack{b=1\\b\neq B}}^{m} |(B-b)| > 0$.

Como $p! < p^p$ e $(n \leq p \Longrightarrow \sqrt{n}.\sqrt{n} \leq p \Longrightarrow \frac{\sqrt{n}.\sqrt{n}}{\sqrt{n}.p} \leq \frac{p}{\sqrt{n}.p} \Longrightarrow \frac{\sqrt{n}}{p} \leq \frac{1}{\sqrt{n}})$. Segue-se

$$\begin{aligned} |S(z)| &< C_8^p p! p^{\frac{p}{2}} \left(\frac{\sqrt{n}}{p}\right)^{mp} \\ &< C_8^p p^p p^{\frac{p}{2}} \left(\frac{1}{\sqrt{n}}\right)^{mp} \\ &= C_8^p p^{\frac{3p}{2}} \left(n^{-\frac{1}{2}}\right)^{mp} \\ &\leq C_8^p p^{\frac{3p}{2}} p^{-\frac{mp}{2}} \\ &= C_8^p p^{\frac{p(3-m)}{2}} \end{aligned}$$

Por conseguinte,

$$|S(z)| < C_8^p p^{\frac{p(3-m)}{2}} \tag{6.19}$$

para todo z no círculo C. Por outro lado, de (6.14), (6.15), (6.18), (6.19) e (usando o fato, do comprimento do caminho C da integral é $2\pi.\frac{p}{q}$), obtemos

$$\begin{aligned} |\zeta| &\leq |\log\alpha|^{-p}|S(B)| \\ &\leq |\log\alpha|^{-p}\frac{1}{2\pi i}\left|\int_C \frac{S(z)}{z-B}dz\right| \\ &\leq \frac{1}{2\pi i}|\log\alpha|^{-p}\int_C \frac{|S(z)|}{|z-B|}|dz| \\ &< \frac{1}{2\pi}|\log\alpha|^{-p}C_8^p p^{\frac{p(3-m)}{2}}\left(\frac{2q}{p}\right)2\pi\left(\frac{p}{q}\right) \\ &= 2|\log\alpha|^{-p}C_8^p p^{\frac{p(3-m)}{2}} \\ &< 2^p|\log\alpha|^{-p}C_8^p p^{\frac{p(3-m)}{2}} \\ &= (2|\log\alpha|^{-1}C_8)^p p^{\frac{p(3-m)}{2}} \\ &= C_9^p p^{\frac{p(3-m)}{2}} \end{aligned}$$

Portanto,

$$|\zeta| < C_9^p p^{\frac{p(3-m)}{2}} \tag{6.20}$$

onde $C_9 := (2|\log\alpha|^{-1}C_8)$ e não depende de n e p. Pelo Lema 6.5, tem-se $\|\zeta\| < \bar{C}^p p^p$ e por (6.20), $|\zeta| < C_9^p p^{\frac{p(3-m)}{2}}$ e como $m = 2h+3$, sendo h o grau da extensão K sobre

$\mathbb{Q}$, segue-se

$$\begin{aligned} |N(\zeta)| &= |\zeta||\zeta^{(2)}|\cdots|\zeta^{(h)}| \\ &\leq |\zeta|\cdot\|\zeta\|^{h-1} \\ &< C_9^p p^{\frac{p(3-m)}{2}}\left(\bar{C}^p p^p\right)^{h-1} \\ &= C_9^p p^{\frac{p(-2h)}{2}}\bar{C}^{p(h-1)}p^{p(h-1)} \\ &= \left(C_9\bar{C}^{(h-1)}\right)^p p^{-ph}p^{ph-p} \\ &= \left(C_9\bar{C}^{(h-1)}\right)^p p^{-p} \\ &= C_{10}^p p^{-p} \end{aligned}$$

Logo,

$$|N(\zeta)| < C_{10}^p p^{-p} \tag{6.21}$$

onde $C_{10} := C_9\bar{C}^{(h-1)}$ e não depende de n e p. Por outro lado, pelo Lema 6.4, temos

$$|N(\zeta)| \geq \tilde{C}^{-p} \tag{6.22}$$

Combinando (6.21) e (6.22), tem-se

$$C_{10}^p p^{-p} > |N(\zeta)| \geq \tilde{C}^{-p} \Longrightarrow C_{10}^p p^{-p} > \tilde{C}^{-p}$$

multiplicando a última desigualdade por $\dfrac{\tilde{C}^p}{p^{-p}} > 0$, obtemos:

$$\frac{\tilde{C}^p C_{10}^p p^{-p}}{p^{-p}} > \frac{\tilde{C}^p\tilde{C}^{-p}}{p^{-p}} \Longrightarrow \tilde{C}^p C_{10}^p > \frac{1}{p^{-p}} \Longrightarrow \left(\tilde{C}C_{10}\right)^p > p^p \Longrightarrow \tilde{C}C_{10} > p.$$

Para $\tilde{C}$ e C_{10} constantes positivas que não depende de n e p. O que é uma contradição, pois $p \geq n$ e n é arbitrário, tomado suficientemente grande. Essa contradição decorre do fato de assumirmos que α^β é algébrico. Portanto, o número α^β é transcendente. □

Finalmente, cumprimos nosso objetivo provando o Teorema de Gelfond-Schneider, ou seja, uma solução do Sétimo Problema de Hilbert. A prova desse teorema fornece uma importante ferramenta para construção de números transcendentes e o desenvolvimento de outras áreas mais recentes, como veremos posteriormente por meio de algumas consequências interessantes.

6.3 Algumas Consequências do Teorema de Gelfond-Schneider

Esta seção será dedicada a algumas consequências do Teorema de Gelfond-Schneider, as quais possuem uma enorme relevância no desenvolvimento da teoria transcendente e das Formas Lineares Logaritmas de Baker.

Exemplo 6.1. *O número $2^{\sqrt{2}}$ foi usado como exemplo específico, pelo grande matemático David Hilbert caso fosse resolvido o Sétimo Problema, e assim, pelo Teorema de Gelfond-Schneider 6.3, o número $2^{\sqrt{2}}$ é transcendente.*

Dessa forma, pelo Teorema Gelfond-Schneider 6.3, temos uma infinidade de números transcendentes: $11^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{3}}$, $\sqrt{3}^{\sqrt{4}}$, $\sqrt{7}^{\sqrt{7}}$, $\sqrt{12}^{\sqrt{3}}$, $\sqrt{2}^{i}$, i^i, 3^i, 4^i, 5^i, 6^i, 7^i, 8^i, $2020^i, \ldots$

Vejamos algumas consequências especificas.

Corolário 6.1. *O número e^{π} é transcendente.*

Demonstração. Usando a relação de Euler ($e^{ix} = \cos x + i \sin x$), para todo $x \in \mathbb{R}$. Daí, para $x = \pi$, tem-se

$$e^{i\pi} = \cos \pi + i \sin \pi = -1 + i.0 = -1 \Longrightarrow \left(e^{i\pi}\right)^{-i} = (-1)^{-i} \Longrightarrow e^{\pi} = (-1)^{-i}.$$

Claramente (-1) é algébrico diferente de 0 e 1, e $-i$ é algébrico irracional. Portanto, pelo Teorema de Gelfond-Schneider 6.3, o número e^{π} é transcendente. □

Corolário 6.2. *Mostre que pelo menos um dos números e^e e e^{ei} é transcendente.*

Demonstração. Pelo Exemplo 1.4, sabemos que i é algébrico irracional. Se e^e é algébrico. Então o Teorema de Gelfond-Schneider 6.3, garante que $(e^e)^i$ é transcendente. □

Exemplo 6.2. *O logaritmo decimal de 2, $(\log_{10} 2)$é transcendente.*

Demonstração. Sejam $\alpha = 10$ e $\beta = \log_{10} 2$. Por definição de logaritmo temos que

$$\log_{10} 2 = k \Longleftrightarrow 10^k = 2$$

Segue-se que

$$\alpha^{\beta} = 10^{\log_{10} 2} = 10^k = 2 \Longrightarrow \alpha^{\beta} = 2$$

Note que $\alpha = 10$ é algébrico diferente de 0 e 1. Se $\beta = \log_{10} 2$ fosse algébrico e irracional, assim, pelo Teorema de Gelfond-Schneider 6.3, teríamos que $\alpha^{\beta} = 2$ seria transcendente, porém, 2 é algébrico, logo, $\beta = \log_{10} 2$ é racional ou transcendente. Sabemos que $\log_{10} 2$ é irracional (não é racional). Portanto, devemos ter que $\beta = \log_{10} 2$ é número transcendente. □

Pelo Teorema de Gelfond-Schneider 6.3, e usando o mesmo argumento do Exemplo 6.2 é possível generalizar que $(\log r)$ é transcendente desde que r seja um número racional positivo diferente de potências de 10 e 10^{-1}:

$$\ldots, 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}, 10^{-1}, 10^{0}, 10^{1}, 10^{2}, 10^{3}, 10^{4}, 10^{5}, \ldots$$

Corolário 6.3. *Seja $r \in \mathbb{Q}$ positivo diferente de potências de 10 e 10^{-1}. Se $\log_{10} r$ é irracional. Então $\log_{10} r$ é transcendente.*

Demonstração. Sejam $\alpha = 10$ e $\beta = \log_{10} r$. Por definição de logaritmo temos que

$$\log_{10} r = k \Longleftrightarrow 10^k = r$$

Segue-se que

$$\alpha^{\beta} = 10^{\log_{10} r} = 10^k = r \Longrightarrow \alpha^{\beta} = r$$

Note que $\alpha = 10$ é algébrico diferente de 0 e 1. Se $\beta = \log_{10} r$ fosse algébrico e irracional, assim, pelo Teorema de Gelfond-Schneider 6.3, teríamos que $\alpha^{\beta} = r$ seria transcendente, porém, $r \in \mathbb{Q}$, como todo racional é algébrico, pelo Exemplo 1.7, r é algébrico, segue-se que $\beta = \log_{10} r$ é racional ou transcendente. Se $\log_{10} r$ é irracional. Portanto, devemos ter que $\beta = \log_{10} r$ é transcendente. □

Vejamos uma equivalência interessante do Teorema de Gelfond-Schneider que deu origem posteriormente a uma generalização do Teorema de Alan Baker 6.5.

Teorema 6.4. *Sejam $\alpha_1 \neq 1$, α_2, β_1 e 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. Vamos provar a equivalência. Considere o Teorema de Gelfond-Schneider 6.3. Suponha por absurdo que existem $\alpha_1, \alpha_2, \beta_1$ e β_2, satisfazendo as hipóteses do teorema 6.4 tais que

$$\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 = 0 \tag{6.23}$$

Daí, e multiplicando por $\dfrac{1}{\beta_2 \log \alpha_1}$, tem-se

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

Usando uma mudança de base para o logaritmo, tem-se

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

Por conseguinte,

$$\log_{\alpha_1}\alpha_2 = -\frac{\beta_1}{\beta_2} \Longrightarrow \alpha_2 = \alpha_1^{-\frac{\beta_1}{\beta_2}}$$

Como α_1 é algébrico diferente de 0 e 1.
Se $-\dfrac{\beta_1}{\beta_2}$ fosse algébrico e irracional, teríamos pelo Teorema de Gelfond-Schneider 6.3, que $\alpha_1^{-\frac{\beta_1}{\beta_2}}$ seria transcendente, porém, $\alpha_1^{-\frac{\beta_1}{\beta_2}} = \alpha_2$, contradição, pois α_2 por hipótese é algébrico, logo, $-\frac{\beta_1}{\beta_2}$ é racional ou transcendente, como o quociente de dois números algébricos é um número algébrico, então $-\frac{\beta_1}{\beta_2}$ é um número algébrico. Portanto, devemos ter que $-\frac{\beta_1}{\beta_2} \in \mathbb{Q} - \{0\}$. Então tomando $\frac{\beta_1}{\beta_2} = p$, com $p \in \mathbb{Q} - \{0\}$, temos $\beta_1 = p\beta_2$. Substituindo-o em (6.23), obtemos

$$p\beta_2 \log \alpha_1 \ + \ \beta_2 \log \alpha_2 = 0$$

e multiplicando por $\dfrac{1}{\beta_2} > 0$, resulta em

$$p \log \alpha_1 \ + \ 1. \log \alpha_2 = 0, \quad \text{com} \quad p, 1 \in \mathbb{Q} - \{0\}\,.$$

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

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

Reciprocamente, suponhamos a validade do Teorema 6.4, e provaremos a validade do Teorema de Gelfond-Schneider 6.3. Sejam $\alpha \in \mathbb{A} - \{0, 1\}$ e $\beta \in \mathbb{A} - \mathbb{Q}$. Suponha por absurdo que $\gamma = \alpha^\beta$ seja algébrico. Então

$$\log \gamma = \log \alpha^\beta \Longrightarrow \log \gamma = \beta \log \alpha \Longrightarrow \log \gamma - \beta \log \alpha = 0$$

o que é uma contradição, pois pela validade do Teorema 6.4, devemos ter

$$\log \gamma - \beta \log \alpha \neq 0$$

já que $1, \gamma \neq 1, \beta, \alpha$, são algébricos não nulos. Portanto, tal contradição decorre do fato de assumirmos que α^β é algébrico. Portanto, o número α^β é transcendente, o que completa a demonstração da equivalência. □

Por brevidade, enunciaremos o teorema a seguir mais uma consequência do Teorema de Gelfond-Shneider que é uma versão mais geral do Teorema de Baker. Foi conjecturado que tal resultado seria válido para uma quantidade arbitrária de logaritmos. Essa conjectura foi provada por A. Baker 1996 (e lhe rendeu a medalha Fields em 1970).

Vejamos que, como consequência de tal teorema, temos que qualquer combinação finita de logaritmos de números algébricos não nulos com coeficientes algébricos ou é zero ou é um número transcendente.

Teorema 6.5 (Alan Baker)**.** *Sejam $\alpha_1, \ldots, \alpha_n$ números algébricos não nulos tais que $\log \alpha_1, \ldots, \log \alpha_n$ são linearmente independente sobre $\mathbb{Q}$. Então $1, \log \alpha_1, \ldots, \log \alpha_n$ são linearmente independente sobre $\mathbb{A}$ o corpo dos números algébricos. Além disso, se $\beta_1, \ldots, \beta_n \in \mathbb{A}$ são números algébricos tais que*

$$\gamma = \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \neq 0$$

Então γ é um número transcendente.

Demonstração. Para maiores detalhes Ver [10], p. 191-212. □

Vejamos um exemplo aplicando o Teorema.

Exemplo 6.3. *Mostre que $\dfrac{\log 3}{\log 2}$ é transcendente.*

Demonstração. Note que $\log 2$ e $\log 3$ são linearmente independentes sobre $\mathbb{Q}$. Caso contrário, existiriam $\dfrac{p}{q}, \dfrac{r}{s} \in \mathbb{Q}$ não todos nulos tais que

$$\frac{p}{q} \log 3 - \frac{r}{s} \log 2 = 0$$

Tomando mínimo múltiplo comum de $\frac{p}{q}, \frac{r}{s}$ de modo que tenhamos na expressão acima coeficientes inteiros a, $b \in \mathbb{Z}$ tais que

$$a \log 3 - b \log 2 = 0$$

Por conseguinte,

$$\log 3^a = \log 2^b \Longrightarrow 3^a = 2^b$$

a última igualdade contradiz o Famoso Teorema Fundamental da Aritmética, logo, $\log 2$ e $\log 3$ são (L.I.) sobre $\mathbb{Q}$. Assim, se $\dfrac{\log 3}{\log 2} = \alpha \in \mathbb{A}$ fosse algébrico, teríamos

$$\log 3 - \alpha \log 2 = 0$$

Contrariando o Teorema 6.5. Portanto, o número $\dfrac{\log 3}{\log 2}$ é transcendente. □

Ainda como consequência do Teorema de Gelfond-Schneider é possível generalizar o exemplo acima, o qual é uma conjectura de Hilbert, que na verdade, é uma formulação mais moderna da conjectura de Euler enunciada por volta de 1748.

Teorema 6.6 (Conjectura de Euler)**.** *Sejam α e $\beta \neq 1$ números algébricos não nulos. Então*

$$\gamma = \frac{\log \alpha}{\log \beta}$$

é racional ou transcendente.

Demonstração. Sejam α e $\beta \neq 1$ números algébricos não nulos. Suponha por contradição que $\gamma = \dfrac{\log \alpha}{\log \beta}$ é algébrico e irracional. Note que por uma mudança de base, temos

$$\frac{\log \alpha}{\log \beta} = \log_{\beta} \alpha = \gamma \Longrightarrow \alpha = \beta^{\gamma}$$

Como β é algébrico diferente de 0 e 1. Então pelo Teorema de Gelfond-Schneider 6.3, teríamos que $\beta^{\gamma} = \alpha$ seria transcendente, o que é uma contradição, pois, por hipótese α é algébrico. Logo, tal contradição decorre do fato de assumirmos que γ é algébrico e irracional. Portanto, o número $\gamma = \dfrac{\log \alpha}{\log \beta}$ é racional ou transcendente. □

Diante do exposto, o Teorema de Gelfond-Schneider, ou seja, Solução do Sétimo Probema de Hilbert, não apenas reuniu esforços de diversos grandes matemáticos com o intuito de resolver problemas na área e contribuir para o desenvolvimento da teoria dos números algébricos e transcendentes de modo que conseguimos explicitar tais números, encerrando completamente a natureza da potenciação de dois algébricos, mas também, para o avanço de ramos da matemática conhecido como *Formas Lineares Logaritmas de Baker* e *Soluções de Equações Diofantinas*.

Salientamos que o Teorema de Gelfond-Schneider garante que a potenciação de dois algébricos, gera um transcendente. É razoável pensar que: Será que a potenciação de dois transcendentes sempre gera um transcendente? Não é conhecido um resultado similar para este caso, isto é, em que α^{β} seja transcendente, onde α e β são transcendente, no entanto, sabemos que esta questão tem resposta negativa.

Capítulo 7

Considerações Finais

Este trabalho foi desenvolvido com o objetivo principal de apresentar uma Solução do Sétimo Problema de Hilbert e identificar alguns avanços no desenvolvimento da teoria dos números algébricos e transcendentes. Ao solucionar o sétimo problema proposto por Hilbert, que ficou conhecido como Teorema de Gelfond-Schneider, obtemos não apenas a natureza da potenciação de dois algébricos, bem como, um método para obter a transcendência de infinitos números, e ainda, o desenvolvimento de outras áreas de estudo da matemática.

No que se refere a este estudo, a partir dos resultados do Liouville produzimos um exemplo específico de transcendente e notamos que números algébricos não admitem em um certo sentido, boas aproximações por números racionais, enquanto, os transcendentes são muito bem aproximados por racionais. Por outro lado, no que diz respeito ao resultado do Cantor na teoria transcendente, mostramos que existe não apenas um transcendente, mas uma infinidade deles e que o infinito dos transcendente é maior do que o dos algébricos, em um certo sentido.

Vale ressaltar que, para saber se um dado número é transcendente, em geral, não é uma tarefa tão simples. Dessa forma, tivemos a oportunidade de compreender o método usado por Hermite em uma série de lemas, para provar a transcendência do número e, resultado que foi um desafio aos matemáticos até o século XIX, e ainda, generalizar o Teorema de Lindemann estabelecido por Hermite-Lidemann, de modo que obtivemos consequências mais gerais como a transcendência de certos números e funções trigonométricas: e^{α}, e, π, $\log(\alpha)$, $\sin(\alpha), \cos(\alpha)$ e $\tan(\alpha)$, sendo α algébrico.

Em relação à pesquisa, considerando o objeto de investigação deste estudo, podemos dizer que foi um trabalho complexo e desafiador, pois tivemos que compreender conhecimentos não adquiridos durante o curso, bem como, relacionar diversos deles, a saber: Aproximações, algébricos via extensões de corpos, raízes e polinômios simétricos elementares, conjugado, norma e base integral de inteiros algébricos, assim como, os

sistemas lineares de C. Siegel.

Ao analisar a solução do sétimo problema de Hilbert percebemos com maior clareza que seu método fornece a possibilidade de explicitar uma infinidade de transcendentes, e assim, provamos que o chamado *número de Hilbert*, $2^{\sqrt{2}}$ é transcendente, bem como, $\sqrt{12}^{\sqrt{3}}$, i^i, 3^i, $e^{\pi} = (-1)^{-i}$, $\frac{\log 3}{\log 2}$ são transcendentes, e ainda, garantimos a natureza da potenciação de dois algébricos.

Neste sentido, como consequência do sétimo problema de Hilbert pudemos compreender um avanço significativo recente de uma formulação mais geral de uma conjectura que foi provado em 1966 por Baker, a qual afirmar que qualquer combinação finita de logaritmos de algébricos não nulos com coeficientes algébricos ou é zero ou é transcendente. Além disso, as várias aplicações do método da demostração usado na solução do sétimo problema de Hilbert foram usados para resolver outras teorias.

Referências Bibliográficas

[1] ALENCAR FILHO, Edgard de. *Teoria Elementar dos Números*. São Paulo: Nobel, 1981.

[2] DOMINGUES, Hygino H. & Iezzi, G. *Álgebra Moderna*. 4ª.ed. São Paulo: Atual, 2003.

[3] ENDLER, Otto. *Teoria dos Corpos*. Rio de Janeiro: IMPA (Monografia de Matemática, nº 44), 1987.

[4] EVES, H. *Introdução à história da matemática*. Trad. Hygino H. Domingues. Campinas, São Paulo: Editora da UNICAMP, 2004.

[5] FIGUEIREDO, D.G. *Números Irracionais e Transcendentes*. 3ª.ed. Rio de Janeiro: SBM, Coleção de Iniciação Científica, 2011.

[6] GONÇALVES, A. *Introdução à álgebra*. Rio de Janeiro: IMPA, 1977.

[7] HERSTEIN, I.N. *Tópicos de Álgebra*. São Paulo: Editora Polígono, 1970.

[8] LIMA, Elon Lages. *Curso de Análise - Vol.1*. 14ª.ed. Rio de Janeiro: IMPA, 2013.

[9] MAOR, Eli. *e: A História de um Número; tradução de Jorge Calife*. 4ª.ed. Rio de Janeiro: Record, 2008.

[10] MARQUES, D. *Teoria dos Números Transcendentes*. 1ª.ed. Rio de Janeiro: SBM, 2013.

[11] MORGADO, A.C. et al. *A Matemática do Ensino Médio - Vol.2*. 7ª.ed. Rio de Janeiro. SBM, 2016.

[12] NIVEN, Ivan. *Irrational Numbers*. sixth printing. USA: The Mathematical Association of America (The Carus Mathematical Monographs), 2006.

[13] POLLARD, Harry. *The Theory of Algebraic Numbers*. Baltimore: The Mathematical Association of America (The Carus Mathematical Monographs - Vol.9), 1950.

[14] SIEGEL, C. L. *Transcendental Numbers*. Princeton Universyty Press, 1949.

[15] SOARES, M. G. *Cálculo em uma Variável Complexa*. 5ª.ed. Rio de Janeiro: IMPA, 2014.

[16] TUBBS, Robert. *Hilbert´s Seventh Problem: Solutions and Extensions*. Book Agency: Springer, 2016.

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