UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Diego Marques Ferreira

ALGUNS RESULTADOS QUE GERAM NÚMEROS TRANSCENDENTES

Fortaleza
2007

Diego Marques Ferreira

ALGUNS RESULTADOS QUE GERAM NÚMEROS TRANSCENDENTES

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Matemática da Universidade Federal do Ceará, como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. José Othon Dantas Lopes.

Fortaleza
2007

.

Ferreira, Diego Marques

F44a Alguns resultados que geram números transcendentes.

Diego Marques Ferreira - Fortaleza: 2007.

116 f

Orientador: Prof. Dr. José Othon Dantas Lopes.

Dissertação (mestrado) - Universidade Federal do Ceará, Depto de Matemática, 2007

1. Teoria dos Números.

CDD 512.73

À pessoa mais importante da minha vida, minha mãe.
Aos meus avós Tereza Lopes e Raimundo Rodrigues (in memorian).

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus e aos meus pais, Flávio Gonçalves Ferreira e Maria Margarete Marques, sem eles com certeza nada disso teria acontecido.

À minha esposa Rubéria e à minha filhinha linda, Mabelle, pela alegria que me propiciam diariamente.

Ao meu orientador, Prof. Dr. José Othon Dantas Lopes, pela orientação e por ter aceitado este desafio.

Agradeço aos meus amigos Carlos Henrique, Clodomir Neto, Chico Diego, Paulo Ítalo, Jefferson (Vampiro), Francisco de Assis, Luiz Antonio, Flávio Portela, Ana Paula, Carlos Augusto, Bruno Holanda, Samuel Barbosa e Davi Máximo pelas conversas matemáticas de cada dia.

Agradeço ao Professor Jonathan Sondow, por ter acreditado em mim e aceitado me acompanhar nesse "espinhoso" mas mágico mundo da **T.N.T**, pela última revisão desse trabalho e por aturar meu inglês em conversas diárias no MSN. Thank you Jonathan.

Novamente ao Clodomir Neto, mas agora pelo **very hard** trabalho com o LaTeX.

Aos professores Luquésio Petrola, Jorge Herbert, Alexandre Fernandes e Gervásio Gurgel, aos quais me espelho constantemente.

Ao CNPq pela ajuda financeira.

"*Superar suas próprias limitações e dominar o universo.*"

"Texto na medalha Fields"

"*Uma grande descoberta envolve a solução de um grande problema, mas há uma semente de descoberta na solução de qualquer problema. Seu problema pode ser modesto, porém, se ele desafiar sua curiosidade e fizer funcionar sua capacidade inventiva, e caso você o resolva sozinho, então você poderá experimentar a tensão e o prazer do triunfo da descoberta.*"

George Pólya

"*A Matemática é a rainha das ciências e a Teoria dos Números é a rainha das Matemáticas.*"

Gauss

RESUMO

O propósito da Dissertação é apresentar um pouco da Teoria dos Números Transcendentes, em especial, explicitar exemplos de números transcendentes usando alguns resultados desta teoria. Este trabalho tenta aparecer como um pequeno "survey" em Teoria Transcendente, e nele figuram alguns dos principais resultados dessa teoria.

Sumário

Este trabalho é baseado em cinco resultados principais. O primeiro devido ao grande matemático francês J. Liouville e o mais recente provado pelo britânico, vencedor da medalha fields em 1970, A. Baker. Dizemos que um número complexo é *algébrico* quando for raiz de um polinômio, não nulo, com coeficientes racionais, caso contrário tal número é dito *transcendente*. Iniciamos nossa história em meados do século XIX, com a teoria de Liouville sobre a n-aproximação de um irracional por racionais. Definimos os números de Liouville e mostramos que tais números são transcendentes. Liouville foi o primeiro a exibir exemplos de números transcendentes, quando, em 1851, mostrou que o números da forma

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

onde a_k é um algarismo qualquer de 1 à 9, são números de Liouville. Em 1873, Hermite provou que e é transcendente e em 1882, Lindemann extendeu o método de Hermite para provar que π também é transcendente, além disso, ele demonstrou que a transcendência de e e π são casos especiais de um resultado bem mais geral. O Teorema de Lindemann, como ficou conhecido, afirma que dados m números algébricos distintos $\alpha_1, \ldots, \alpha_m$ então $e^{\alpha_1}, \ldots, e^{\alpha_m}$ são linearmente independentes sobre o corpo dos números algébricos.

Na época de Lindemann os matemáticos não sabiam como se comportavam as potências de números complexos quanto a sua transcendência ou algebricidade. Somente em 1900, no Congresso Internacional de Matemática em Paris, o matemático alemão David Hilbert levantou tal problema. O sétimo problema de Hilbert perguntava se o número $2^{\sqrt{2}}$ é transcendente, mais geralmente; se α^{β}, onde α é algébrico (diferente de zero e um) e β é algébrico (não racional), é transcendente. Hilbert comentou que a solução de tal problema seria uma bela peça da matemática e que talvez moldaria a moderna Teoria dos Números Transcendentes. Esta questão foi resolvida em 1934 por A. O. Gelfond e independentemente em 1935 por T. Schneider. Em 1966 o matemático A. Baker generalizou o resultado de Gelfond

e Schneider, ver [2] p. 10, mostrando que $\alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ é transcendente, para todos números algébricos $\alpha_1, \ldots, \alpha_n$, diferentes de 0 e 1, e todos números algébricos $\beta_1, \ldots, \beta_n$ com $1, \beta_1, \ldots, \beta_n$ linearmente independentes sobre $\mathbb{Q}$. Para potências de números transcendentes por transcendentes ainda não existe nenhum resultado parecido com o de Gelfond e Schneider, mas sabemos que tais potências tanto podem resultar num número algébrico como num número transcendente. A falta de uma resposta convincente para um problema faz então surgir várias "conjecturas". Por exemplo será que T^T é transcendente para todo número transcendente T? Implicando assim na transcendência de e^e e π^π? Alguns resultados sobre soluções algébricas e transcendentes da equação $y = x^x$ foram provados pelo matemático americano J. Sondow e pelo autor. Em particular, mostra-se que existem infinitos números algébricos da forma T^T, com T transcendente.

Capítulo 1

Preliminares

A teoria dos números transcendentes foi originada por Liouville em sua famosa memória de 1844, na qual ele obteve, pela primeira vez, uma classe, *très-étendue* como foi descrito no título do paper, de números que não satisfazem nenhuma equação algébrica com coeficientes inteiros.

1.1 Os Números Algébricos e Transcendentes

Definição 1.1.1 *Seja $L|K$ uma extensão de corpos. Dizemos que $\alpha \in L$ é algébrico sobre K, quando existe $p \in K[x] - \{0\}$ tal que $p(\alpha) = 0$, isto é, quando α for raiz de um polinômio não nulo com coeficientes em K.*

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

Exemplo 1.1.1 *Todo racional, $\alpha = \dfrac{p}{q}$, é algébrico, pois é raiz do polinômio $F(x) = qx - p$.*

Exemplo 1.1.2 *$i, \sqrt{2} + \sqrt{3}$ e $\cos\frac{2\pi}{2007} + i\sin\frac{2\pi}{2007}$ são algébricos, pois são raízes, respectivamente, de $x^2 + 1$, $x^4 - 10x^2 + 1$ e $x^{2007} - 1$.*

Afirmação 1.1.1 *Sejam $K \subset L \subset M$ corpos. Então se $\alpha \in M$ é algébrico sobre K, também o será sobre L, já que, $K[x] \subset L[x]$.*

Denotaremos por $\mathbb{A}$, o conjunto dos números algébricos e por $\mathbb{T}$, o conjunto dos números transcendentes.

As proposições a seguir nos dão a natureza quantitativa dos números transcendentes.

Proposição 1.1.1 *Existem números transcendentes.*

Demonstração

Dado $p(x) = a_0 + a_1x + \ldots + a_nx^n$, denotaremos por R_p, o conjunto das raízes de p. Pelo Teorema Fundamental da Álgebra, se $\partial p = n$ então $\sharp R_p \leqslant n$. Para todo $n \in \mathbb{N}$, existe apenas uma quantidade enumerável de polinômios, em $\mathbb{Q}[x]$, com grau n. De fato, considere $\mathbb{X}_n =$"conjunto dos polinômios com coeficientes racionais e de grau n". Tome $\psi : \underbrace{\mathbb{Q} \times \cdots \times \mathbb{Q}}_{n+1\, cópias} \longrightarrow \mathbb{X}_n$ dada por

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

Vê-se facilmente que ψ é bijeção. Como $\mathbb{Q} \times \cdots \times \mathbb{Q}$ é enumerável, segue-se que $\mathbb{X}_n$ é enumerável.

Definamos $A_n = \bigcup_{\partial p = n} R_p$. Pelos comentários feitos acima e do fato que a união enumerável de conjuntos finitos é enumerável, segue-se que A_n é enumerável. Agora é só observar que $\mathbb{A} = \bigcup_{n \in \mathbb{N}} A_n$. Daí, $\mathbb{A}$ é enumerável (pois é escrito como união de enumeráveis).

Como $\mathbb{R}$ é não enumerável e $\mathbb{C} \supset \mathbb{R}$, segue-se que $\mathbb{C}$ é não enumerável. Escrevamos então $\mathbb{C} = \mathbb{A} \cup \mathbb{T}$. Como $\mathbb{A}$ é enumerável e $\mathbb{C}$ é não-enumerável, temos $\mathbb{T}$ não-enumerável, em particular, $\mathbb{T} \neq \varnothing$.

□

Proposição 1.1.2 *"Quase todos" os números são transcendentes.*

Demonstração

Quando usamos a expressão "quase todos os números são transcendentes", queremos dizer que $\mathbb{C}-\mathbb{T}=\mathbb{A}$ tem medida nula em $\mathbb{C}$. Então, devemos provar a seguinte afirmação:

Afirmação 1.1.1 *$\mathbb{A}$ tem medida nula em $\mathbb{C}$.*

Demonstração

De fato, dado $\varepsilon > 0$, como $\mathbb{A}$ é enumerável (pela Proposição 1.1.1), então podemos considerar $\mathbb{A} = \{a_1, a_2, \ldots, a_n, \ldots\}$. Definamos então

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

Claramente, $\mathbb{A} \subset \bigcup_{n\in\mathbb{N}} B_n$, além disso,

$$\acute{a}rea\left(\bigcup_{n\in\mathbb{N}} B_n\right) \leqslant \sum_{n=1}^{\infty} \acute{a}rea(B_n) = \sum_{n=1}^{\infty} \pi r_n^2 = \frac{3\varepsilon}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{3\varepsilon}{\pi^2}\left(\frac{\pi^2}{6}\right) = \frac{\varepsilon}{2} < \varepsilon$$

Segue-se então o resultado desejado.

□

As proposições 1.1.1 e 1.1.2 nos dizem que de fato números transcendentes existem e, além disso, que existem numa quantidade não enumerável.

1.2 Caracterização de Algébricos via Extensão de Corpos

Definição 1.2.1 *Dados dois corpos L e K, dizemos que L é uma extensão de K, quando K for um subcorpo de L. Neste caso, consideramos L como um K-espaço vetorial.*

O grau da extensão $L|K$, denotada por $[L : K]$, é igual a dimensão de L como K-espaço vetorial.

Seja $[L : K] = n$. Dizemos que $\{\beta_1, \ldots, \beta_n\}$ é uma base da extensão $L|K$, quando formarem uma base do K-espaço L.

Proposição 1.2.1 *(multiplicidade do grau) Sejam K, L e M corpos tal que $K \subseteq L \subseteq M$. Então $[M : K] = [M : L] \cdot [L : K]$.*

Demonstração

Ver [8], p. 26.

□

Observe que o caso de graus infinitos está incluído.

Definição 1.2.2 *Sejam $L|K$ uma extensão e $\alpha \in L$ algébrico sobre K. Definimos o polinômio minimal de α sobre K, e denotamos por $p_{\alpha,K}$, como o polinômio mônico de menor grau com coeficientes em K que tem α como raiz.*

Teorema 1.2.1 *Sejam $L|K$ uma extensão e $\alpha \in L$ algébrico sobre K. Então $[K(\alpha) : K] = \partial p_{\alpha,K}$ e $\left\{1, \alpha, \ldots, \alpha^{\partial p_{\alpha,K}-1}\right\}$ é uma base de $L|K$.*

Demonstração

Ver [8], p. 34.

□

Encerramos essa seção com um resultado que caracteriza os números algébricos e transcendentes.

Teorema 1.2.2 *Sejam $L|K$ uma extensão e $\alpha \in L$. Então α é algébrico sobre K se e só se $[K(\alpha) : K] < \infty$.*

Demonstração

($\Rightarrow$) Suponha que α é algébrico sobre K. Pelo Teorema 1.2.1, temos

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

($\Leftarrow$) Suponha que $[K(\alpha) : K] = n$ então pelo Teorema 1.2.1, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é base da extensão $K(\alpha)|K$, em particular, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é um conjunto linearmente independente maximal sobre K. Portanto, $\{1, \alpha, \ldots, \alpha^{n-1}, \alpha^n\}$ é linearmente dependente sobre K, segue-se que existem $a_0, \ldots, a_{n-1}, a_n \in K$, não todos nulos, tais que

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$$

Mostrando que α é algébrico sobre K.

□

Este teorema é uma ferramenta de grande utilidade para mostrarmos que certos números são, ou não, algébricos. Isso ficará bem claro na próxima seção.

1.3 Aritmética dos Algébricos

Mostraremos a seguir que o conjunto dos números algébricos formam um corpo.

Proposição 1.3.1 *Dados a e $b \in \mathbb{A}$, temos:*

(i) $a \pm b \in \mathbb{A}$*;*

(ii) $a \cdot b \in \mathbb{A}$*;*

(iii) *Se $a \neq 0$ então $a^{-1} \in \mathbb{A}$.*

Demonstração

A idéia principal da demonstração é usar o Teorema 1.2.2.

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

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

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

□

Proposição 1.3.2 *Os números algébricos formam um conjunto denso em* $\mathbb{C}$.

Demonstração

Como $\mathbb{Q} \times \mathbb{Q} \subset \mathbb{A}$ e $\mathbb{Q}$ é denso em $\mathbb{R}$, segue-se o resultado.

□

A Proposição 1.3.2 ainda nos diz que todo número complexos é limite de uma seqüência de números algébricos.

1.4 Aritmética $\mathbb{A}$ versus $\mathbb{T}$

A proposição seguinte nos dá informações sobre o resultado de operações elementares agindo em números algébricos e transcendentes.

Proposição 1.4.1 *Sejam* $a \in \mathbb{A}$ *e* $\beta \in \mathbb{T}$, *então*

(i) $a \pm \beta \in \mathbb{T}$;

(ii) $a \cdot \beta \in \mathbb{T}$ $(a \neq 0)$;

(iii) $\beta^{-1} \in \mathbb{T}$.

Demonstração

(i) Suponha $a \pm \beta = c \in \mathbb{A}$, então pela Proposição1.3.1, β será algébrico. Contradição. Portanto $a \pm \beta \in \mathbb{T}$.

(ii) Suponha $a \cdot \beta = c \in \mathbb{A}$, como $a \neq 0$ então pela Proposição 1.3.1, $\beta = c \cdot \dfrac{1}{a} \in \mathbb{A}$. Contradição. Portanto $a \cdot \beta \in \mathbb{T}$.

(iii) Supondo $\beta^{-1} \in \mathbb{A}$ então pela Proposição 1.3.1, $\dfrac{1}{\beta^{-1}} \in \mathbb{A}$, mas por outro lado, $\dfrac{1}{\beta^{-1}} = \beta$. Assim $\beta \in \mathbb{A}$. Contradicão. Portanto $\beta^{-1} \in \mathbb{T}$.

□

Proposição 1.4.2 *Sejam* $a \in \mathbb{A}$ *e* $\beta \in \mathbb{T}$, *então*

(i) $a^{\frac{s}{t}} \in \mathbb{A}$, *para qualquer* $\dfrac{s}{t} \in \mathbb{Q}$;

(ii) $\beta^{\frac{s}{t}} \in \mathbb{T}$, *para qualquer* $\dfrac{s}{t} \in \mathbb{Q} - \{0\}$.

Demonstração

Usaremos o seguinte lema:

Lema 1.4.1 *Se* $\beta \in \mathbb{T}$ *então* $\beta^n \in \mathbb{T}\ \forall\, n \in \mathbb{N}$.

Demonstração

Suponha que $\beta^n \in \mathbb{A}$, então existe um polinômio

$$p(x) = a_0 + a_1 x + \ldots + a_m x^m \in \mathbb{Z}[x]$$

não nulo, tal que $p\left(\beta^n\right) = 0$. Considere o polinômio a seguir:

$$\tilde{p}(x) = a_0 + a_1 x^n + \ldots + a_m x^{mn}$$

com coeficientes inteiros e não todos nulos. Temos então,

$$\tilde{p}(\beta) = a_0 + a_1\beta^n + \ldots + a_m\beta^{mn} = a_0 + a_1\beta^n + \ldots + a_m\left(\beta^n\right)^m = p\left(\beta^n\right) = 0$$

Portanto, $\beta \in \mathbb{A}$. Contradição. Daí, $\beta^n \in \mathbb{T}$.

□

Voltando à nossa proposição,

(i) Suponha que $a^{\frac{s}{t}} = \gamma$, onde γ é transcendente. Sem perda de generalidade, podemos supor $t > 0$. Daí,

$$a^s = \gamma^t$$

Pelo Lema 1.4.1, $\gamma^t \in \mathbb{T}$. Absurdo! pois a^s é algébrico.

(ii) Se $\beta^{\frac{s}{t}} = c$, onde c é algébrico, então

$$\beta^s = c^t$$

Como $s \neq 0$ então β^s é transcendente, uma contradição com o lado direito da igualdade acima.

□

Capítulo 2

Números de Liouville

Definição 2.1 *Diz-se que um número algébrico α é de grau n se ele for raiz de um polinômio de grau n com coeficientes inteiros e, se não existir um polinômio de grau menor do que n, do qual α é raiz. Assim, os números racionais coincidem com os números algébricos de grau 1.*

Definição 2.2 *Um número real α é aproximável na ordem n por racionais se existirem uma constante $C > 0$ e uma seqüência $\left\{\frac{p_j}{q_j}\right\}$ de racionais distintos, com $q_j > 0$ e $mdc(p_j, q_j) = 1$ tais que*

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

Dizemos simplesmente que um número é n-aproximável quando for aproximável na ordem n por racionais.

Proposição 2.1 *Se α é n-aproximável então:*

i) *α é k-aproximável para $k < n$;*

ii) $\left|\alpha - \frac{p_j}{q_j}\right| < C$;

iii) $\{q_j\}$ *é ilimitada;*

iv) $\lim_{j\to\infty} \frac{p_j}{q_j} = \alpha$.

Demonstração

(i) Basta-nos mostrar que α é $(n-1)$-aproximável. De fato, temos

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

Considere D $= \{q_j \,|\, j \in \mathbb{N}\}$. Pelo Princípio da Boa Ordenação, existe $\tilde{q} \in D$ tal que $\tilde{q} \leqslant q_j, \forall j \in \mathbb{N}$. Considere $\tilde{C} = \frac{C}{\tilde{q}} > 0$. Portanto,

$$\left|\alpha - \frac{p_j}{q_j}\right| < \frac{C}{q_j^n} = \frac{C}{q_j} \cdot \frac{1}{q_j^{n-1}} \leqslant \frac{C}{\tilde{q}} \cdot \frac{1}{q_j^{n-1}} = \frac{\tilde{C}}{q_j^{n-1}}.$$

Daí, α é $(n-1)$-aproximável.

(ii) Como $q_j \in \mathbb{N}, q_j \geqslant 1$, daí $q_j^n \geqslant 1$, portanto:

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

(iii) Suponha que $\{q_j\}$ é limitada. Como $\left\{\frac{p_j}{q_j}\right\}$ são distintos, $\{p_j\}$ deve ser ilimitada, mas $\left|\alpha - \frac{p_j}{q_j}\right| < C$. Contradição, logo $\{q_j\}$ é ilimitada.

(iv) Como $\{q_j\} \subset \mathbb{N}$ é ilimitada, então $\lim_{j\to\infty} q_j = \infty$. Por outro lado,

$$0 < \left|\alpha - \frac{p_j}{q_j}\right| < \frac{C}{q_j^n}.$$

Passando o limite quando j tende ao infinito, obtemos $\lim_{j\to\infty} \frac{p_j}{q_j} = \alpha$.

□

Proposição 2.2 *Todo número racional é* 1*-aproximável e não é* k*-aproximável para* $k \geqslant 2$.

Demonstração

Seja $\frac{p}{q} \in \mathbb{Q}$, com $q > 0$ e $mdc(p, q) = 1$, logo existem x_0 e y_0 inteiros, tais que $x_0 p - y_0 q = 1$.

Observamos também que a equação $xp - yq = 1$ tem infinitas soluções. De fato, sejam $x_t = x_0 + tq$ e $y_t = y_0 + tp$, onde $t \in \mathbb{Z}$. Portanto, para todo t,

$$x_t p - y_t q = x_0 p + tqp - y_0 q - tpq = 1$$

Tome $k > \frac{-x_0}{q}$ e definamos $x_j = x_0 + (k+j)q$ e $y_j = y_0 + (k+j)p$. Note que $x_j = x_0 + (k+j)q > x_0 + \left(\frac{-x_0}{q} + j\right) q = jq > 0$. Agora, afirmamos que

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

De fato, supondo $\frac{y_i}{x_i} = \frac{y_j}{x_j}$, temos

$$\begin{aligned}
\frac{y_i}{x_i} = \frac{y_j}{x_j} \quad &\Rightarrow \quad \frac{y_0 + (k+i)p}{x_0 + (k+i)q} = \frac{y_0 + (k+j)p}{x_0 + (k+j)q} \Rightarrow \\
&\Rightarrow \quad y_0(k+j)q + x_0(k+i)p = y_0(k+i)q + x_0(k+j)p \Rightarrow \\
&\Rightarrow \quad y_0kq + y_0jq + x_0kp + x_0ip = y_0kq + y_0iq + x_0kp + x_0jp \Rightarrow \\
&\Rightarrow \quad y_0jq + x_0ip = y_0iq + x_0jp \Rightarrow \\
&\Rightarrow \quad i = j
\end{aligned}$$

Por outro lado,

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

mostrando que $\frac{p}{q}$ é 1-aproximável.

Para a segunda parte, suponha que $\frac{p}{q}$ é 2-aproximável, então existem $\left\{\frac{p_j}{q_j}\right\} \in \mathbb{Q} - \left\{\frac{p}{q}\right\}$ e $C > 0$ tais que

$$\left|\frac{p}{q} - \frac{p_j}{q_j}\right| < \frac{C}{q_j^2} \tag{2.2}$$

Por outro lado,

$$\left|\frac{p}{q} - \frac{p_j}{q_j}\right| = \frac{|pq_j - qp_j|}{qq_j} \geqslant \frac{1}{qq_j} \quad pois\ pq_j - qp_j \in \mathbb{Z} - \{0\} \tag{2.3}$$

Combinando (2.2) e (2.3), temos

$$\frac{1}{qq_j} \leqslant \left|\frac{p}{q} - \frac{p_j}{q_j}\right| < \frac{C}{q_j^2}$$

Daí, $q_j \leqslant Cq$. Contradição com o item (iii) da Proposição 2.1. Segue-se que $\frac{p}{q}$ não é 2-aproximável e pelo item (i) da mesma proposição, $\frac{p}{q}$ não pode ser k-aproximável para $k \geqslant 2$.

□

Proposição 2.3 *Todo número irracional é 2-aproximável.*

Demonstração

Sejam α um número irracional e $n \in \mathbb{N}$. Denotemos por $\lfloor x \rfloor$ a parte inteira de um número real x, isto é, o maior inteiro menor ou igual a x. Considere agora os $n+1$ números reais

$$0, \alpha - \lfloor \alpha \rfloor, \ldots, n\alpha - \lfloor n\alpha \rfloor \tag{2.4}$$

os quais pertencem ao intervalo $[0, 1)$. Particionando o intervalo $[0, 1)$ em n intervalos, disjuntos dois a dois, da forma

$$\left[\frac{j}{n}, \frac{j+1}{n}\right), \ j = 0, 1, \ldots, n-1 \tag{2.5}$$

observamos que existem pelo menos, dois números reais em (2.4) que estão em um mesmo intervalo do tipo (2.5). Digamos que eles sejam $n_1\alpha - \lfloor n_1\alpha \rfloor$ e $n_2\alpha - \lfloor n_2\alpha \rfloor$, com $0 \leqslant n_1 < n_2 \leqslant n$, temos:

$$|n_2\alpha - \lfloor n_2\alpha \rfloor - n_1\alpha + \lfloor n_1\alpha \rfloor| < \frac{1}{n} \tag{2.6}$$

Sejam $k = n_2 - n_1$ e $h = \lfloor n_2\alpha \rfloor - \lfloor n_1\alpha \rfloor$, os quais são inteiros com $k > 0$ e $h \geqslant 0$. Logo (2.6) pode ser escrito como:

$$|k\alpha - h| < \frac{1}{n} \ \ ou \ \ \left|\alpha - \frac{h}{k}\right| < \frac{1}{nk} \tag{2.7}$$

segue-se que

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{k^2} \tag{2.8}$$

Queremos mostrar que (2.8) se verifica para infinitos racionais. De fato, suponha o contrário, isto é, que existem apenas $\frac{h_1}{k_1}, \ldots, \frac{h_r}{k_r} \in \mathbb{Q}$ tais que

$$\left|\alpha - \frac{h_i}{k_i}\right| < \frac{1}{k_i^2},\ 1 \leqslant i \leqslant r$$

Tome $\varepsilon = min\left\{\left|\alpha - \frac{h_1}{k_1}\right|, \ldots, \left|\alpha - \frac{h_r}{k_r}\right|\right\} > 0$, pela propriedade arquimediana existe um $m \in \mathbb{N}$ tal que $\frac{1}{m} < \varepsilon$, para este m construímos $\frac{h}{k} \in \mathbb{Q}$ satisfazendo

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

essa contradição prova o resultado.

□

A próxima proposição caracteriza os números algébricos de grau n.

Proposição 2.4 *Se α é algébrico de grau $n > 1$ então existe $A > 0$ tal que*

$$\left|\alpha - \frac{p}{q}\right| > \frac{A}{q^n},\ \forall \frac{p}{q} \in \mathbb{Q} \tag{2.9}$$

Demonstração

Seja $f \in \mathbb{Z}[x]$ com $f(\alpha) = 0$ e $\partial f = n$, existe $d > 0$ tal que a única raiz de f em $[\alpha - d, \alpha + d]$ é α (isso deve-se ao fato que um polinômio, não nulo, tem somente um número finito de raízes).

Sabemos que $f'(x)$ também é um polinômio, logo limitado em intervalos limitados, isto é, existe $M > 0$ tal que

$$|f'(x)| \leqslant M,\ \forall x \in [\alpha - d, \alpha + d]$$

Considere $\frac{p}{q}$, $q > 0$, um número racional em $[\alpha - d, \alpha + d]$. Pelo Teorema do Valor Médio, existe $\zeta \in (\alpha - d, \alpha + d)$ para o qual (a menos de uma sinal)

$$f(\alpha) - f\left(\frac{p}{q}\right) = f'(\zeta)\left(\alpha - \frac{p}{q}\right) \tag{2.10}$$

Como $f(\alpha) = 0$, (2.10) pode ser escrito como

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

daí,

$$\left|f\left(\frac{p}{q}\right)\right| \leqslant M\left|\alpha - \frac{p}{q}\right| \tag{2.11}$$

mas $f(x) = a_0 + a_1x + \ldots + a_nx^n$, portanto

$$\left|f\left(\frac{p}{q}\right)\right| = \left|\frac{a_0q^n + a_1pq^{n-1} + \ldots + a_np^n}{q^n}\right| \geqslant \frac{1}{q^n}$$

Substituindo em (2.11), temos

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

Segue-se que

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{1}{Mq^n} \tag{2.12}$$

Tome agora $\frac{p}{q} \notin [\alpha - d, \alpha + d]$ então

$$\left|\alpha - \frac{p}{q}\right| > d \tag{2.13}$$

Como $q^n > 1$ então $\frac{1}{q^n} < 1$, daí (2.13) fica

$$\left|\alpha - \frac{p}{q}\right| > \frac{d}{q^n} \tag{2.14}$$

Considere $A = \frac{1}{2}min\left\{d, \frac{1}{M}\right\}$, portanto para todo $\frac{p}{q} \in \mathbb{Q}$, tem-se

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

□

Corolário 2.1 *Se α é algébrico de grau n então α não é $(n+1)$-aproximável.*

Demonstração

Suponha que α é $(n+1)$-aproximável, então existem infinitos $\frac{p_j}{q_j}$, racionais e $C > 0$ tal que

$$\left|A - \frac{p_j}{q_j}\right| < \frac{C}{q_j^{n+1}} \tag{2.15}$$

pela proposição anterior existe $A > 0$ para o qual

$$\left|\alpha - \frac{p_j}{q_j}\right| > \frac{A}{q_j^n} \tag{2.16}$$

combinando (2.15) com (2.16) obtemos $\frac{A}{q_j^n} < \frac{C}{q_j^{n+1}} \Rightarrow q_j < \frac{C}{A}$. Contradição, pois q_j é ilimitada. Logo α não pode ser $(n+1)$-aproximável.

□

Corolário 2.2 *Se α é n-aproximável para todo $n \in \mathbb{N}$ então α é transcendente.*

Demonstração

Imediato do Corolário 2.1

Definição 2.3 *Um número real α é chamado número de Liouville se existir uma seqüência $\left\{\frac{p_j}{q_j}\right\}, q_j > 0$, $mdc(p_j, q_j) = 1$, com elementos distintos, e tal que*

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

Teorema 2.1 *(***Liouville***) Todo número de Liouville é transcendente.*

Demonstração

Suponha que um número de Liouville α fosse algébrico, digamos, de grau n. Então pela Proposição 2.4 segue-se que a relação (2.9) será válida para todo número racional. Em particular, para os $\frac{p_j}{q_j}$ da Definição 2.3. Assim, teríamos

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

Daí, $q_j^{j-n} < \frac{1}{A}\ \forall j \in \mathbb{N}$, contradição, pois $q_j^{j-n} \to \infty$ quando $j \to \infty$. Portanto, α não pode ser algébrico.

□

Proposição 2.5 *Seja α um número real tal que*

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

onde $\left\{\frac{v_j}{u_j}\right\}$ é uma seqüência de racionais distintos com $u_j > 0$ (não exigimos que $mdc(u_j, v_j) = 1$), então α é um número de Liouville.

Demonstração

Considere a seqüência $\frac{p_j}{q_j}$ de racionais distintos com $q_j > 0$ e $mdc(p_j, q_j) = 1$, definida por $\frac{p_j}{q_j} = \frac{v_j}{u_j}$. Então,

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

pois $p_j u_j = v_j q_j$, logo $q_j | p_j u_j$ como $mdc(q_j, p_j) = 1$, então $q_j | u_j$, portanto $q_j \leqslant u_j$ e daí $\frac{1}{q_j^j} \geqslant \frac{1}{u_j^j}$.

Proposição 2.6 *Qualquer número da forma*

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

onde a_k é um algarismo qualquer de 1 a 9, é um número de Liouville.

Demonstração

Consideremos números inteiros $v_j = \sum_{k=1}^{j} \frac{a_k}{10^{j!-k!}}$ e $u_j = 10^{j!} > 0$. Temos

$$\begin{aligned}\left|\alpha - \frac{v_j}{u_j}\right| &= \sum_{k=j+1}^{\infty} \frac{a_k}{10^{k!}} = \frac{1}{10^{(j+1)!}}\left(a_{j+1} + \frac{a_{j+2}}{10^{(j+2)!-(j+1)!}} + \ldots\right) \leqslant \\ &\leqslant \frac{9}{10^{(j+1)!}}\left(1 + \frac{1}{10^{(j+2)!-(j+1)!}} + \ldots\right) \qquad (2.17)\end{aligned}$$

Note que $10^{(j+k)!-(j+1)!} > 10^{k-1}$, para $k > 1$. Daí podemos majorar (2.17) como

$$\left|\alpha - \frac{v_j}{u_j}\right| \leqslant \frac{9}{10^{(j+1)!}}\left(1 + \frac{1}{10} + \frac{1}{10^2} + \ldots\right) = \frac{9}{10^{(j+1)!}}\frac{10}{9} = \frac{10}{(10^{j!})^j 10^{j!}} < \frac{1}{u_j^j}$$

pela Proposição 2.5, segue-se que α é um número de Liouville.

□

Observe que pelo Teorema 2.1, todo número que têm a forma

$$\alpha = \sum_{k=1}^{\infty} \frac{a_k}{10^{k!}}, \text{ onde } a_k \in \{1, \ldots, 9\}$$

é um número transcendente.

Deve-se ao matemático francês J. Liouville esse feito.

Defina a seguinte seqüência recorrente: $b_1 = 1$, $b_n = (2^n)^{b_{n-1}}$, $n > 1$. Os termos dessa seqüência são, por exemplo; 1, 2^1, 4^{2^1}, $8^{4^{2^1}}$, ... e crescem rapidamente, para se ter uma idéia b_4 possui mais de 10^7 dígitos. O interessante é que o número

$$\alpha = 1 + \frac{1}{2^1} + \frac{1}{4^{2^1}} + \frac{1}{8^{4^{2^1}}} + \ldots = 1,562500000000035527\ldots$$

é transcendente. De fato, mostraremos que α é um número de Liouville e, pelo Teorema 2.1 é transcendente. Observe que,

$$\alpha = 1 + \frac{1}{b_1} + \frac{1}{b_2} + \ldots$$

Afirmação 2.1 $(2^n)^{b_n} \geqslant b_n^n \; \forall\, n \geqslant 1$

Primeiramente perceba que $b_n^{n-1} \geqslant n+1$ para $n > 1$ e portanto,

$$b_n^n \geqslant (n+1)\, b_n$$

Provaremos a afirmação por indução sobre n.
Para $n = 1$ é trivial. Suponha então que $\left(2^k\right)^{b_k} \geqslant b_k^k$, então

$$b_{k+1} = \left(2^{k+1}\right)^{b_k} \geqslant \left(2^k\right)^{b_k} \geqslant b_k^k$$

daí

$$\left(2^{k+1}\right)^{b_{k+1}} \geqslant \left(2^{k+1}\right)^{b_k^k} \geqslant \left(2^{k+1}\right)^{(k+1)b_k} = b_{k+1}^{k+1}$$

Claramente, $b_n > b_k$ para $n > k$ e por indução b_n é potência de 2 para todo $n \in \mathbb{N}$. De fato, para $n = 1$, $b_1 = 2$. Suponha que $b_k = 2^l$ então

$$b_{k+1} = \left(2^{k+1}\right)^{b_k} = 2^{(k+1)2^l}$$

e a indução está completa. Portanto, $b_k | b_n$, $1 \leqslant k \leqslant n$, por isso $mmc(1, b_1, \ldots, b_n) = b_n$. Segue-se então,

$$1 + \frac{1}{b_1} + \frac{1}{b_2} + \ldots + \frac{1}{b_n} = \frac{a_n}{b_n}, \text{ onde } a_n \in \mathbb{Z}$$

Afirmação 2.2 $\dfrac{b_{n+1}}{b_{n+k}} \leqslant \dfrac{1}{2^{k-1}}$ *para* $k \geqslant 1$.

Basta-nos mostrar que $b_{n+k} \geqslant 2^{k-1} b_{n+1}$ para $k \geqslant 1$. Note que

$$\begin{aligned} b_{n+k} &= \left(2^{n+k}\right)^{b_{n+k-1}} = \left(2^{k-1} \cdot 2^{n+1}\right)^{b_{n+k-1}} \geqslant 2^{k-1} \left(2^{n+1}\right)^{b_{n+k-1}} \geqslant \\ &\geqslant 2^{k-1} \left(2^{n+1}\right)^{b_n} = 2^{k-1} b_{n+1} \end{aligned}$$

Considere $\dfrac{a_n}{b_n}$ como acima. Então,

$$\left|\alpha - \frac{a_n}{b_n}\right| = \frac{1}{b_{n+1}} + \frac{1}{b_{n+2}} + \ldots = \frac{1}{b_{n+1}} \left(1 + \frac{b_{n+1}}{b_{n+2}} + \ldots\right) \tag{2.18}$$

pela Afirmação 2.2,

$$1 + \frac{b_{n+1}}{b_{n+2}} + \ldots + \frac{b_{n+1}}{b_{n+k}} + \ldots \leqslant 1 + \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^{k-1}} + \ldots = 2$$

Substituindo em (2.18),

$$\left|\alpha - \frac{a_n}{b_n}\right| < \frac{2}{b_{n+1}} = \frac{2}{\left(2^{n+1}\right)^{b_n}} \leqslant \frac{1}{\left(2^n\right)^{b_n}}$$

e finalmente pela Afirmação 2.1,

$$\left|\alpha - \frac{a_n}{b_n}\right| \leqslant \frac{1}{\left(2^n\right)^{b_n}} \leqslant \frac{1}{b_n^n}$$

mostrando que α é um número de Liouville e conseqüentemente transcendente.

□

Para mais casos e algumas generalizações, veja [16].

Capítulo 3

O Teorema de Lindemann

Os primeiros números transcendentes foram exibidos por Liouville, usando o que vimos no Capítulo 2. Em 1873, Hermite provou que e é transcendente e em 1882, Lindemann estendeu o método para provar que π também é transcendente, além disso, ele mostrou que a transcendência de e e π são casos especiais de um teorema bem mais geral cuja demonstração é o objetivo desse capítulo.

3.1 Preliminares

Definição 3.1.1 *Um polinômio $p(x_1, \cdots, x_n) \in \mathbb{K}[x_1, \cdots, x_n]$, onde $\mathbb{K}$ é um anel, é chamado simétrico ou função simétrica em $x_1, \ldots, x_n$ se $p\left(x_{\alpha(1)}, \ldots, x_{\alpha(n)}\right) = p(x_1, \ldots, x_n)$, para toda permutação $\alpha \in S_n$. Os polinômios*

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

são simétricos em $x_1, \ldots, x_n$ e são chamados de funções simétricas elementares.

Teorema 3.1.1 ***(Fundamental das Funções Simétricas)*** *Seja $p(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ uma função simétrica. Então existe $\varphi \in \mathbb{K}[x_1, \ldots, x_n]$ tal que*

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

Demonstração

Veja [4], p. 77-78.

□

Proposição 3.1.1 *Sejam $\beta_1,\ldots,\beta_n$ raízes de um polinômio*

$$f(x)=bx^n+c_1x^{n-1}+\ldots+c_n$$

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

Demonstração

(1^a parte) Pelo Teorema 3.1.1, existe $\varphi(x_1,\ldots,x_n)\in\mathbb{Q}[x_1,\ldots,x_n]$ tal que $p(x_1,\ldots,x_n)=\varphi(\sigma_1(x_1,\ldots,x_n),\ldots,\sigma_n(x_1,\ldots,x_n))$, logo $p(\beta_1,\ldots,\beta_n)=\varphi(\sigma_1(\beta_1,\ldots,\beta_n),\ldots,\sigma_n(\beta_1,\ldots,\beta_n))$. Por outro lado, como $\beta_1,\ldots,\beta_n$ são raízes de $f(x)=bx^n+c_1x^{n-1}+\ldots+c_n$, então $\sigma_i(\beta_1,\ldots,\beta_n)=(-1)^i\dfrac{c_i}{b}\in\mathbb{Q}$. Daí, $p(\beta_1,\ldots,\beta_n)\in\mathbb{Q}$.

(2^a parte) Se $p(x_1,\ldots,x_n)$ é um polinômio simétrico com coeficientes inteiros, então pelo Teorema 3.1.1,

$$p(x_1,\ldots,x_n)=\varphi(\sigma_1(x_1,\ldots,x_n),\ldots,\sigma_n(x_1,\cdots,x_n)) \qquad (I)$$

onde $\varphi(x_1,\ldots,x_n)\in\mathbb{Z}[x_1,\ldots,x_n]$, daí, $\varphi(x_1,\ldots,x_n)=\sum_{(i)}a_{(i)}x_1^{i_1}\cdots x_n^{i_n}$, onde $a_{(i)}\in\mathbb{Z}$. Por (I), o grau de φ é t, isto é, $max_{(i)}\{i_1+\ldots+i_n\}=t$. Por outro lado, $\sigma_i(\beta_1,\ldots,\beta_n)=(-1)^i\dfrac{c_i}{b}$.

Aplicando a igualdade (I) para $\beta_1,\ldots,\beta_n$, obtemos:

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

onde $m = i_1 + \ldots + ni_n$. Portanto,

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

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

$$b^t p\left(\beta_1, \ldots, \beta_n\right) \in \mathbb{Z}$$

□

Proposição 3.1.2 *Considere os polinômios* $p_1\left(y_1, \cdots, y_m\right), \cdots, p_q\left(y_1, \cdots, y_m\right)$, *onde*

$$p_j = f_1\left(x_j\right) y_1 + \cdots + f_m\left(x_j\right) y_m, \ j = 1, 2, \cdots, q$$

com coeficientes $f_i\left(x_j\right)$, *onde* $f_i(x)$ *são polinômios sobre um corpo* $\mathbb{F}$. *O produto* $p_1 p_2 \cdots p_q$, *quando os termos em y são agrupados, tem coeficientes que são funções simétricas em* $x_1, \cdots, x_q$.

Demonstração

Escrevamos o produto como

$$p_1 p_2 \cdots p_q = \sum_{\substack{ij=1 \\ i_1 \leqslant i_2 \leqslant \cdots \leqslant i_q}}^{m} c y_{i_1} y_{i_2} \cdots y_{i_q} \tag{3.1}$$

A condição $i_1 \leqslant i_2 \leqslant \cdots \leqslant i_q$ é imposta na soma para indicar que os termos estão sendo agrupados. Note que $c = c\left(x_1, \cdots, x_q\right)$. Toda permutação de $x_1, \cdots, x_q$ deixa o lado esquerdo da igualdade (3.1) invariante, pois é apenas uma permutação dos polinômios $p_1, p_2, \cdots, p_q$. Portanto, essa permutação também deixa o lado direito de (3.1) invariante e daí deixa todo coeficiente c invariante. Logo, $c = c\left(x_1, \cdots, x_q\right)$ é uma função simétrica de $x_1, \cdots, x_q$.

□

Proposição 3.1.3 *Sejam* K *um corpo de números algébricos e* θ *um elemento de* K. *Então todo elemento* $\beta \in \mathbb{Q}(\theta)$ *pode ser unicamente representado como um polinômio em* θ *com coeficientes em* $\mathbb{Q}$, *isto é,*

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

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

Demonstração

Imediato do Teorema 1.2.1.

□

A Proposição 3.1.3 é facilmente generalizada da seguinte maneira:

Sejam K um corpo de números algébricos e $\theta_1, \cdots, \theta_s$ elementos de K. Então para todo elemento $\beta \in \mathbb{Q}(\theta_1, \cdots, \theta_s)$, temos:

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

Proposição 3.1.4 *Se* $\alpha_1, \alpha_2, \cdots, \alpha_s$ *são algébricos sobre* $\mathbb{Q}$ *então existe* γ *algébrico sobre* $\mathbb{Q}$*, tal que*

$$\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_s)$$

Demonstração

Segue-se do fato de que toda extensão finita de um corpo perfeito possui elemento primitivo. Ver [8], p. 63.

□

Definição 3.1.2 *Um corpo algébrico* $\mathbb{Q}(\theta)$ *é dito normal sobre* $\mathbb{Q}$ *se todo polinômio em* $\mathbb{Q}[x]$ *que tem pelo menos uma raiz em* $\mathbb{Q}(\theta)$*, tiver todas as raízes em* $\mathbb{Q}(\theta)$*.*

Proposição 3.1.5 *Sejam* $\alpha_1, \alpha_2, \cdots, \alpha_s$ *números algébricos, então existe* θ *algébrico tal que*

$$\mathbb{Q}(\theta) \supset \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_s)$$

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

Demonstração

Pela Proposição 3.1.4, existe γ algébrico sobre $\mathbb{Q}$ tal que

$$\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_s).$$

Considere $p_{\gamma,\mathbb{Q}}$ o polinômio minimal de γ sobre $\mathbb{Q}$. Sejam $\gamma = \gamma_1, \gamma_2, \cdots, \gamma_m$ as m raízes de $p_{\gamma,\mathbb{Q}}$ então aplicando a Proposição 3.1.4 outra vez, temos que existe θ algébrico sobre $\mathbb{Q}$ tal que

$$\mathbb{Q}(\theta) = \mathbb{Q}(\gamma_1, \gamma_2, \cdots, \gamma_m) \supset \mathbb{Q}(\gamma) = \mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_s)$$

Resta-nos provar que $\mathbb{Q}(\theta)|\mathbb{Q}$ é normal. De fato, considere $g(x) \in \mathbb{Q}[x]$ irredutível e mônico, com uma raiz $\alpha \in \mathbb{Q}(\theta)$. Queremos mostrar que toda raiz de $g(x)$ pertence a $\mathbb{Q}(\theta)$. Como $\alpha \in \mathbb{Q}(\theta) = \mathbb{Q}(\gamma_1, \gamma_2, \cdots, \gamma_m)$, então existe um polinômio $f(x_1, x_2, \cdots, x_m) \in \mathbb{Q}[x_1, x_2, \cdots, x_m]$ tal que $\alpha = f(\gamma_1, \gamma_2, \cdots, \gamma_m)$. Defina então o seguinte polinômio:

$$G(x) = \prod_{\sigma \in S_m} \left(x - f\left(\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \cdots, \gamma_{\sigma(m)}\right)\right) \tag{3.2}$$

onde σ é uma permutação de $\{1, 2, \cdots, m\}$. Portanto, $\partial G = m!$ e os coeficientes de $G(x)$ são funções simétricas em $\left\{f\left(\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \cdots, \gamma_{\sigma(m)}\right)\right\}_{\sigma \in S_m}$. Por outro lado, quando permutamos $\{\gamma_1, \gamma_2, \cdots, \gamma_m\}$ temos que $\left\{f\left(\gamma_{\sigma(1)}, \cdots, \gamma_{\sigma(m)}\right)\right\}_{\sigma \in S_m}$ fica invariante. Logo os coeficientes de $G(x)$ são funções simétricas em $\gamma_1, \gamma_2, \cdots, \gamma_m$ e pela Proposição 3.1.1 são racionais, daí $G(x) \in \mathbb{Q}[x]$ e $G(\alpha) = 0$.

Segue-se então que $g(x)|G(x)$, isto é, $G(x) = g(x)h(x)$ para algum $h(x) \in \mathbb{Q}[x]$ (isso deve-se ao fato de que $g(x) = p_{\alpha,\mathbb{Q}}$). Sejam $\alpha = a_1, a_2, \cdots, a_l$ as raízes de $g(x)$ então

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

Daí a_j é raiz de $G(x)$ para todo $j \in \{1, \cdots, l\}$. Olhando para (3.2), observe que existe $\tilde{\sigma} \in S_m$ tal que

$$a_j = f\left(\gamma_{\tilde{\sigma}(1)}, \gamma_{\tilde{\sigma}(2)}, \cdots, \gamma_{\tilde{\sigma}(m)}\right) \in \mathbb{Q}(\theta)\ \forall\, j \in \{1, \cdots, m\}$$

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

□

Suponha $[\mathbb{Q}(\theta):\mathbb{Q}] = n$ e $\mathbb{Q}(\theta)|\mathbb{Q}$ é normal, então θ satisfaz a equação minimal

$$f(x) = x^n + b_1 x^{n-1} + \cdots + b_n = 0 \tag{3.3}$$

Sejam $\theta = \theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}$ as n raízes de 3.3. Como $\mathbb{Q}(\theta)|\mathbb{Q}$ é normal, então $\theta^{(j)} \in \mathbb{Q}(\theta)$ para $j \in \{1, \cdots, n\}$. Pela Proposição 3.1.3 temos

$$\theta^{(j)} = h_j(\theta), \text{ onde } h_j(x) \in \mathbb{Q}[x]$$

Quando substituímos θ por $\theta^{(2)}$ nos $h_j's$ acima, observamos que $\left\{h_1\left(\theta^{(2)}\right), h_2\left(\theta^{(2)}\right), \cdots, h_n\left(\theta^{(2)}\right)\right\}$ é apenas uma permutação de $\left\{\theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}\right\}$, mas geralmente

$$\left\{h_1\left(\theta^{(i)}\right), h_2\left(\theta^{(i)}\right), \cdots, h_n\left(\theta^{(i)}\right)\right\} = \left\{\theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}\right\} \ (1 \leqslant i \leqslant n)$$

Proposição 3.1.6 *Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ normal de grau n e $\theta = \theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}$ os conjugados de θ (isto é, as n raízes do polinômio minimal de θ sobre $\mathbb{Q}$). Se $F(x) \in \mathbb{Q}[x]$, então $\left\{F\left(\theta^{(1)}\right), F\left(\theta^{(2)}\right), \cdots, F\left(\theta^{(n)}\right)\right\}$ é permutado quando substituímos θ por $\theta^{(i)}$.*

Demonstração

$F\left(\theta^{(j)}\right) = F\left(h_j(\theta)\right)$, fazendo $\theta = \theta^{(i)}$ pelo argumento anterior temos que

$$\left\{h_1\left(\theta^{(i)}\right), h_2\left(\theta^{(i)}\right), \cdots, h_n\left(\theta^{(i)}\right)\right\} = \left\{\theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}\right\}$$

logo, $\left\{F\left(\theta^{(1)}\right), F\left(\theta^{(2)}\right), \cdots, F\left(\theta^{(n)}\right)\right\}$ é permutado.

□

Tome $\gamma \in \mathbb{Q}(\theta)$, logo existe $F \in \mathbb{Q}[x]$ $(\partial F \leqslant n-1)$ tal que $\gamma = F(\theta)$. Denote então $\gamma^{(j)} = F\left(\theta^{(j)}\right)$, onde $\theta = \theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}$ são os conjugados de θ. Afirmamos que as funções simétricas elementares de $\gamma = \gamma^{(1)}, \gamma^{(2)}, \cdots, \gamma^{(n)}$ são polinômios simétricos em $\theta = \theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}$. De fato, seja σ_i a i-ésima função simétrica elementar dada por

$$\sigma_i(x_1, \cdots, x_n) = \sum_{1 \leqslant k_1 < k_2 < \cdots < k_i \leqslant n} x_{k_1} x_{k_2} \cdots x_{k_i}$$

defina $p \in \mathbb{Q}[x_1, \cdots, x_n]$ por

$$p_i(x_1, \cdots, x_n) = \sigma_i(F(x_1), \cdots, F(x_n))$$

mostraremos que p_i é simétrico em $\theta = \theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}$, observe que

$$p_i\left(\theta = \theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}\right) = \sigma_i\left(\gamma^{(1)}, \gamma^{(2)}, \cdots, \gamma^{(n)}\right)$$

Seja $\zeta \in S_n$ então

$$\begin{aligned} p_i\left(\theta^{(\zeta(1))}, \cdots, \theta^{(\zeta(n))}\right) &= \sigma_i\left(\gamma^{(\zeta(1))}, \cdots, \gamma^{(\zeta(n))}\right) = \\ &= \sigma_i\left(F\left(\theta^{(\zeta(1))}\right), \cdots, F\left(\theta^{(\zeta(n))}\right)\right) \end{aligned}$$

Pela Proposição 3.1.6 $\left\{F\left(\theta^{(\zeta(1))}\right), \cdots, F\left(\theta^{(\zeta(n))}\right)\right\}$ é uma permutação de $\left\{F\left(\theta^{(1)}\right), \cdots, F\left(\theta^{(n)}\right)\right\}$, como σ_i é simétrico então

$$\sigma_i\left(F\left(\theta^{(\zeta(1))}\right), \cdots, F\left(\theta^{(\zeta(n))}\right)\right) = \sigma_i\left(F\left(\theta^{(1)}\right), \cdots, F\left(\theta^{(n)}\right)\right)$$

logo,

$$\begin{aligned} p_i\left(\theta^{(\zeta(1))}, \cdots, \theta^{(\zeta(n))}\right) &= \sigma_i\left(F\left(\theta^{(1)}\right), \cdots, F\left(\theta^{(n)}\right)\right) = \sigma_i\left(\gamma^{(1)}, \cdots, \gamma^{(n)}\right) = \\ &= p_i\left(\theta^{(1)}, \cdots, \theta^{(n)}\right) \end{aligned}$$

Portanto, p_i é simétrico em $\theta = \theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}$.

□

Proposição 3.1.7 *Todo elemento $\gamma \in \mathbb{Q}(\theta)$ e $\gamma^{(1)}, \gamma^{(2)}, \cdots, \gamma^{(n)}$ como acima satisfazem uma equação polinomial $g(x) = 0$ de grau n ($n = [\mathbb{Q}(\theta) : \mathbb{Q}]$) com coeficientes inteiros.*

Demonstração

Pelos comentários acima, temos que

$$\begin{aligned} \sigma_1\left(\gamma^{(1)}, \cdots, \gamma^{(n)}\right) &= p_1\left(\theta^{(1)}, \cdots, \theta^{(n)}\right), \cdots, \sigma_n\left(\gamma^{(1)}, \cdots, \gamma^{(n)}\right) = \\ &= p_n\left(\theta^{(1)}, \cdots, \theta^{(n)}\right) \end{aligned}$$

onde os $p_i's$ são polinômios simétricos em $\theta^{(1)}, \cdots, \theta^{(n)}$e pela Proposição 3.1.1 existem racionais $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \cdots, \frac{a_n}{b_n}$ tais que

$$p_1\left(\theta^{(1)},\cdots,\theta^{(n)}\right)=\frac{a_1}{b_1},\cdots,p_n\left(\theta^{(1)},\cdots,\theta^{(n)}\right)=\frac{a_n}{b_n}$$

Considere $g(x)$ como abaixo:

$$g(x)=b_1\cdots b_n\left(x-\gamma^{(1)}\right)\cdots\left(x-\gamma^{(n)}\right).$$

Claramente, $\partial g=n$ e $\gamma^{(1)},\cdots,\gamma^{(n)}$ são raízes de $g(x)$. Basta-nos mostrar que $g(x)\in\mathbb{Z}[x]$. De fato, temos

$$\begin{aligned}
g(x) &= b\left(x-\gamma^{(1)}\right)\cdots\left(x-\gamma^{(n)}\right)\\
&= b\left(x^n-\sigma_1\left(\gamma^{(1)},\cdots,\gamma^{(n)}\right)x^{n-1}+\cdots+(-1)^n\sigma_n\left(\gamma^{(1)},\cdots,\gamma^{(n)}\right)\right)\\
&= b\left(x^n-p_1\left(\theta^{(1)},\cdots,\theta^{(n)}\right)x^{n-1}+\cdots+(-1)^np_n\left(\theta^{(1)},\cdots,\theta^{(n)}\right)\right)\\
&= b\left(x^n-\frac{a_1}{b_1}x^{n-1}+\cdots+(-1)^n\frac{a_n}{b_n}\right)=\\
&= b_1\cdots b_nx^n-a_1b_2\cdots b_nx^{n-1}+\cdots+(-1)^na_nb_1\cdots b_{n-1}\in\mathbb{Z}[x]
\end{aligned}$$

onde $b=b_1\cdots b_n$.

□

Proposição 3.1.8 *Considere as funções* $f(x)=\sum_{j=1}^{m}a_jx^{\alpha_j}$, $g(x)=\sum_{j=1}^{t}b_jx^{\beta_j}$ *onde* α_j, β_j *são números complexos não nulos. Assuma que os* $\alpha_j's$ *são distintos e os* $\beta_j's$ *também. Quando* $f(x)g(x)$ *é formado e todos os termos de igual expoente são combinados, existe um menor coeficiente não nulo no resultado.*

Demonstração

Pela Proposição 3.1.5 existe $\mathbb{Q}(\theta)$ extensão normal de $\mathbb{Q}$ que contém $\alpha_1,\cdots,\alpha_m,\beta_1,\cdots,\beta_t$. Suponha que $[\mathbb{Q}(\theta):\mathbb{Q}]=n$ então α_j e β_j podem ser escritos como

$$\alpha_j=\sum_{i=0}^{n-1}r_{j_i}\theta^i \text{ e } \beta_j=\sum_{i=0}^{n-1}s_{j_i}\theta^i$$

Dizemos que α_i antecede α_k (respectivamente β_i antecede β_k) quando o primeiro termo não nulo da seqüência

$$r_{i_0} - r_{k_0},\ r_{i_1} - r_{k_1}, r_{i_2} - r_{k_2}, \cdots$$

respectivamente

$$s_{i_0} - s_{k_0},\ s_{i_1} - s_{k_1}, s_{i_2} - s_{k_2}, \cdots$$

for positivo. Como os α_j (respectivamente β_j) são distintos, então existe α_1 (respectivamente β_1) que antecede todos os α_j (respectivamente β_j).

Afirmação 3.1.1 *$\alpha_1 + \beta_1$ antecede $\alpha_j + \beta_k$ $\forall\,(j,k) \in I_m \times I_t - \{(1,1)\}$ onde $I_s = \{1, 2, \cdots, s\}$.*

De fato, $\alpha_1 + \beta_1 = \sum_{i=0}^{n-1} (r_{1_i} + s_{1_i})\,\theta^i$ e $\alpha_j + \beta_k = \sum_{i=0}^{n-1} (r_{j_i} + s_{k_i})\,\theta^i$ então $r_{1_i} + s_{1_i} - (r_{j_i} + s_{k_i}) = (r_{1_i} - r_{j_i}) + (s_{1_i} - s_{k_i})$, mas existem $q_1,\ q_2 \in \{0, \cdots, n-1\}$ com $r_{1_{q_1}} - r_{j_{q_1}} > 0$ e $s_{1_{q_1}} - s_{k_{q_1}} > 0$ e $r_{i_l} = r_{j_l}$, $s_{1_{\tilde{l}}} = s_{k_{\tilde{l}}},\ l \in \{0, \cdots, q_1 - 1\},\ \tilde{l} \in \{0, \cdots, q_2 - 1\}$.

Tome $q = min\,\{q_1, q_2\}$, note que para $q_3 \in \{0, \cdots, q-1\}$ temos $r_{1_{q_3}} + s_{1_{q_3}} = r_{j_{q_3}} + s_{k_{q_3}}$ e,
$r_{1_q} + s_{1_q} - \left(r_{j_q} + s_{k_q}\right) = \left(r_{1_q} - r_{j_q}\right) + \left(s_{1_q} - s_{k_q}\right) > 0$.

Portanto, $\alpha_1 + \beta_1$ antecede $\alpha_j + \beta_k$.

Assim, 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.

□

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

Definição 3.1.3 *Seja $\mathbb{Q}(\theta)\,|\mathbb{Q}$ uma extensão algébrica. Dado $\gamma \in \mathbb{Q}(\theta)$ temos que $\gamma = h(\theta)$ onde $h(x) \in \mathbb{Q}[x]$ e $\partial h \leqslant n-1$. Seja $\theta = \theta^{(1)}, \theta^{(2)}, \cdots, \theta^{(n)}$ as n raízes do polinômio minimal de θ sobre $\mathbb{Q}$ então $\gamma = \gamma^{(1)}, \gamma^{(2)}, \cdots, \gamma^{(n)}$ são chamados conjugados de γ sobre $\mathbb{Q}(\theta)$ ou $\mathbb{Q}(\theta)$-conjugados de γ, onde*

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

Proposição 3.1.9 *Sejam α e β números algébricos num corpo K de grau n sobre os racionais. Se os conjugados de α sobre K são $\alpha = \alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(n)}$ e os de β são $\beta = \beta^{(1)}, \beta^{(2)}, \cdots, \beta^{(n)}$. Então os conjugados de $\alpha + \beta$ e $\alpha \cdot \beta$ são respectivamente $\alpha^{(1)} + \beta^{(1)}, \cdots, \alpha^{(n)} + \beta^{(n)}$ e $\alpha^{(1)} \cdot \beta^{(1)}, \cdots, \alpha^{(n)} \cdot \beta^{(n)}$.*

Demonstração

Como $[K : \mathbb{Q}] = n$, então existe $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$, logo $\alpha = h(\theta)$ e $\beta = g(\theta)$ onde $h(x) = \sum_{j=0}^{n-1} a_j x^j$, $g(x) = \sum_{j=0}^{n-1} b_j x^j$ com a_j, $b_j \in \mathbb{Q}$.

Portanto,

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

Daí, para $i \in \{1, \cdots, n\}$

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

o caso $\alpha \cdot \beta$ é análogo.

□

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

Proposição 3.1.10 **(i)** *Os conjugados de γ sobre $\mathbb{Q}(\theta)$ são os conjugados sobre $\mathbb{Q}$ todos repetidos $\frac{n}{m}$ vezes*

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

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

Demonstração

Veja [15], p. 53-54.

□

Definição 3.1.4 *Sejam $K|\mathbb{Q}$ uma extensão e $\alpha \in K$. α é dito inteiro algébrico se for raiz de um polinômio mônico com coeficientes inteiros.*

Definição 3.1.5 *Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ uma extensão algébrica de grau n, então $N(\alpha)$ (a norma de α) é definida como o produto dos conjugados de α sobre $\mathbb{Q}(\theta)$.*

Proposição 3.1.11 *Sejam α, $\beta \in \mathbb{Q}(\theta)$, então:*

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

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

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

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

Demonstração

(i) pela Proposição 3.1.9, temos que

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

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

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

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

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

$$p(x) = x^n + a_1x^n + \cdots + a_{n-1}x + a_n \text{ com } a_i \in \mathbb{Z}$$

Por outro lado,

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = (x-\alpha)(x-\alpha^{(2)})\cdots(x-\alpha^{(n)}) =$$
$$= x^n - \sigma_1(\alpha, \alpha^{(2)}, \cdots, \alpha^{(n)})x^{n-1} + \cdots + (-1)^n\sigma_n(\alpha, \alpha^{(2)}, \cdots, \alpha^{(n)}) \quad (3.4)$$

Daí, $a_i = (-1)^i\sigma_i(\alpha, \alpha^{(2)}, \cdots, \alpha^{(n)})$, note que $N(\alpha) = \sigma_n(\alpha, \alpha^{(2)}, \cdots, \alpha^{(n)})$, mas $\sigma_n(\alpha, \alpha^{(2)}, \cdots, \alpha^{(n)}) = (-1)^n a_n \in \mathbb{Z}$.

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

□

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

3.2 O Teorema de Lindemann

Teorema 3.2.1 *Dados m números algébricos distintos $\alpha_1, \cdots, \alpha_m$, então $e^{\alpha_1}, \cdots, e^{\alpha_m}$ são linearmente indenpendentes sobre o corpo dos números racionais.*

A demonstração desse Teorema seguirá aquela feita no ótimo livro de I. Niven, [14] p. 117-131 .

Demonstração

Suponha por absurdo que

$$\sum_{j=1}^{m} a_j e^{\alpha_j} = 0 \quad (3.5)$$

com coeficientes racionais não todos nulos. Descartando os termos com coeficientes nulos e reordenando a notação, podemos supor que nenhum coeficiente é zero. Além disso, multiplicando (3.5) por um número inteiro conveniente, podemos supor que os coeficientes de (3.5) são inteiros não nulos. Usando a Proposição 3.1.5, temos que existe $\mathbb{Q}(\theta)$ extensão normal de $\mathbb{Q}$ que contém os $\alpha_1, \cdots, \alpha_m$. Suponha que $[\mathbb{Q}(\theta) : \mathbb{Q}] = n$, então todo α_j é expresso como único polinômio em θ de grau $n-1$ com coeficientes racionais. Seja

$$\alpha_j = \sum_{i=0}^{n-1} r_{ji}\theta^i,\ j = \{1, \cdots, m\}$$

vimos anteriormente que sendo $\theta = \theta^{(1)}, \cdots, \theta^{(n)}$ conjugados de θ então os conjugados de α_j sobre $\mathbb{Q}(\theta)$ são

$$\alpha_j^{(k)} = \sum_{i=0}^{n-1} r_{ji}\left(\theta^{(k)}\right)^i,\ j = \{1, 2, \cdots, m\},\ k = \{1, 2, \cdots, n\}$$

Claramente os $\alpha_j^{(k)}$ são distintos para todo k fixo. Temos também que

$$0 = \prod_{k=1}^{n}\sum_{j=1}^{m} a_j e^{\alpha_j^{(k)}} = \sum_{j=0}^{r} c_j e^{\beta j} \tag{3.6}$$

O produtório acima é nulo, porque $\alpha_j^{(1)} = \alpha_j$. Podemos considerar que os β_j são distintos, como os a_j são inteiros, então os c_j, também o são. Além disso, como os $a_j's$ são não nulos, a Proposição 3.1.8 nos garante que existe um menor coeficiente c_j, não nulo, digamos $c_0 \neq 0$.

Para cada j fixo, os n conjugados $\alpha_j^{(k)}$ são permutados quando substituímos θ por $\theta^{(i)}$ de acordo com a Proposição 3.1.6. Portanto, trocando θ por $\theta^{(i)}$, apenas permutamos os fatores do produto em (3.6), mas o resultado é deixado invariante. Por outro lado, quando trocamos θ por $\theta^{(i)}$ estamos substituindo β_j pelo seu conjugado $\beta_j^{(i)}$. Portanto, (3.6) implica

$$0 = \sum_{j=0}^{r} c_j e^{\beta_j^{(1)}} = \sum_{j=0}^{r} c_j e^{\beta_j^{(2)}} = \cdots = \sum_{j=0}^{r} c_j e^{\beta_j^{(n)}} \tag{3.7}$$

Notamos facilmente que os $\beta_j^{(1)}$ são distintos. Portanto, os $\beta_j^{(i)}$ são distintos para todo i fixo.

Agora multiplicamos a primeira soma em (3.7) por $e^{-\beta_0^{(1)}}$, a segunda soma por $e^{-\beta_0^{(2)}}$, $\cdots$, a última soma por $e^{-\beta_0^{(n)}}$. Defina

$$\gamma_j^{(i)} = \beta_j^{(i)} - \beta_0^{(i)},\ i = \{1, \cdots, n\},\ j = \{1, \cdots, r\} \tag{3.8}$$

Como $\beta_j^{(i)}$ são distintos para i fixo, então $\gamma_j^{(i)}$ são não nulos para i fixo. Então (3.7) pode ser reescrita como

$$0 = c_0 + \sum_{j=1}^{r} c_j e^{\gamma_j^{(1)}} = c_0 + \sum_{j=1}^{r} c_j e^{\gamma_j^{(2)}} = \cdots = c_0 + \sum_{j=1}^{r} c_j e^{\gamma_j^{(n)}} \tag{3.9}$$

Pela Proposição 3.1.7, os conjugados $\gamma_j^{(1)}, \gamma_j^{(2)}, \cdots, \gamma_j^{(1)}$ são raízes de um polinômio com coeficientes inteiros, digamos

$$g_j(z) = b_j z^n + \cdots = b_j \prod_{i=1}^{n} \left(z - \gamma_j^{(i)} \right) \quad j = \{1, \cdots, r\} \tag{3.10}$$

Podemos tomar $b_j > 0$ e como $\gamma_j^{(i)} \neq 0$ então $g_j(0)$ é um inteiro não nulo, com isso terminamos a parte algébrica da demonstração do teorema. Agora passaremos ao tratamento analítico. Seja $f(z)$ um polinômio, defina

$$F(z) = f(z) + f'(z) + f''(z) + \cdots$$

isto é, $F(z)$ é a soma de $f(z)$ com suas derivadas de todas as ordens.

Lema 3.2.1 *Sejam $f(z)$ e $F(z)$ como acima, então*

$$\frac{d}{dz}\left(F(z)e^{-z}\right) = -f(z)e^{-z}$$

Demonstração

$$\frac{d}{dz}\left(F(z)e^{-z}\right) = F'(z)e^{-z} - F(z)e^{-z} = -f(z)e^{-z}.$$

□

Portanto,

$$\int_0^b f(z)e^{-z}dz = -\int_0^b \frac{d}{dz}\left(F(z)e^{-z}\right)dz = -F(z)e^{-z}\Big|_0^b = -F(b)e^{-b} + F(0)$$

Daí,

$$F(b) - F(0)e^b = -e^b \int_0^b f(z)e^{-z}dz$$

Substituindo b por $\gamma_j^{(i)}$ como em (3.8), multiplicando todas as equações obtidas por c_j e somando sobre $j = 1, \cdots, r$ e $i = 1, \cdots, n$, obtemos

$$\sum_{j=1}^{r}\sum_{i=1}^{n} c_j F\left(\gamma_j^{(i)}\right) - F(0)\sum_{j=1}^{r}\sum_{i=1}^{n} e^{\gamma_j^{(i)}} = -\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^b f(z)e^{-z}dz$$

Por (3.9) temos,

$$0 = c_0 + \sum_{j=1}^{r} e^{\gamma_j^{(1)}} = c_0 + \sum_{j=1}^{r} e^{\gamma_j^{(2)}} = \cdots = c_0 + \sum_{j=1}^{r} e^{\gamma_j^{(n)}}$$

Daí,

$$\sum_{i=1}^{n}\sum_{j=1}^{r} e^{\gamma_j^{(i)}} = -nc_0$$

Logo,

$$\sum_{j=1}^{r} c_j \left\{\sum_{i=1}^{n} F(\gamma_j^{(i)})\right\} + nc_0F(0) = -\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\gamma_j^{(1)}} \int_0^{\gamma_j^{(i)}} f(z)e^{-z}dz \quad (3.11)$$

Agora definiremos o polinômio $f(z)$ como

$$f(z) = \frac{(b_1b_2\cdots b_r)^{prn}}{(p-1)!} z^{p-1} \prod_{j=1}^{r} g_j(z)^p \quad (3.12)$$

onde p é um primo que depois especificaremos.

Pelo fator z^{p-1} em $f(z)$, temos

$$0 = f(0) = f'(0) = \cdots = f^{(p-2)}(0) \text{ e } f^{(p-1)}(0) = (b_1b_2\cdots b_r)^{prn} \prod_{j=1}^{r} g_j(0)^p$$

Escolhendo $p > b_j$ e $p > g_j(0)$ para $j = \{1, 2, \cdots, r\}$ então $p \nmid f^{(p-1)}(0)$. Para $t \geqslant p$, $f^{(t)}(0)$ é um inteiro divisível por p. De fato, o polinômio $h(z) = (p-1)!f(z)$ tem, coeficientes inteiros, portanto, os coeficientes de todo termo em $h^{(t)}(z)$ tem t inteiros consecutivos formando um produto, mas para $t \geqslant p$,

o produto de t inteiros consecutivos é divisível por $p!$. Logo $p!$ divide o polinômio $h(z)$, portanto,

$$f^{(t)}(z) = p\,(b_1 b_2 \cdots b_r)^{prn}\, G_t(z) \tag{3.13}$$

onde $G_t(z)$ é um polinômio com coeficientes inteiros e grau no máximo $prn-1$. Daí, $f^{(t)}(0) \in \mathbb{Z}$ e é divisível por p. Temos que,

$$\begin{aligned} F(0) &= f(0) + f'(0) + \cdots + f^{(p-2)}(0) + f^{(p-1)}(0) + \sum_{t \geqslant p} f^{(t)}(0) = \\ &= f^{(p-1)}(0) + p \sum_{t \geqslant p} (b_1 \cdots b_r)^{prn}\, G_t(0) \end{aligned}$$

Como $p \nmid f^{(p-1)}(0)$ e $p | p \sum_{t \geqslant p} (b_1 \cdots b_r)^{prn}\, G_t(0)$ então p não divide $F(0)$. Podemos supor também que $p > n$ e $p > c_0$. Logo, p não é um divisor de $nc_0F(0)$ em (3.11).

Mostraremos agora que $\sum_{i=1}^{n} F\left(\gamma_j^{(i)}\right)$ é um inteiro divisível por p. De fato, temos que

$$\sum_{i=1}^{n} F\left(\gamma_j^{(i)}\right) = \sum_{i=1}^{n} f\left(\gamma_j^{(i)}\right) + \sum_{i=1}^{n} f'\left(\gamma_j^{(i)}\right) + \cdots \tag{3.14}$$

Como $f(z)$ tem um fator $g_j(z)^p$ é fácil ver por (3.10) que

$$0 = f\left(\gamma_j^{(i)}\right) = f'\left(\gamma_j^{(i)}\right) = \cdots = f^{(p-1)}\left(\gamma_j^{(i)}\right)$$

Por outro lado (3.13) nos mostra que

$$\begin{aligned} \sum_{i=1}^{n} f^{(t)}\left(\gamma_j^{(i)}\right) &= p \sum_{i=1}^{n} (b_1 b_2 \cdots b_r)^{prn}\, G_t\left(\gamma_j^{(i)}\right) = \\ &= p\,(b_1 b_2 \cdots b_r)^{prn} \sum_{i=1}^{n} G_t\left(\gamma_j^{(i)}\right),\ t \geqslant p. \end{aligned} \tag{3.15}$$

Defina $\psi\left(x_1, x_2, \cdots, x_n\right) \in \mathbb{Z}\left[x_1, x_2, \cdots, x_n\right]$ por

$$\psi\left(x_1, x_2, \cdots, x_n\right) = G_t\left(x_1\right) + \cdots + G_t\left(x_n\right)$$

note que ψ é um polinômio simétrico e $\partial\psi = prn - k$ onde $k \geqslant 1$, logo para todo $j \in \{1, \cdots, r\}$ como $\gamma_j^{(1)}, \gamma_j^{(2)}, \cdots, \gamma_j^{(n)}$ são as n raízes do polinômio $g_j(z) = b_j z^n + \cdots$, então pela Proposição 3.1.1

$$b_j^{prn-k} \sum_{j=1}^{n} G_t\left(\gamma_j^{(i)}\right) = d_{jt} \in \mathbb{Z},\ j = 1, \cdots, r$$

substituindo em (3.15) obtemos

$$\sum_{i=1}^{n} f^{(t)}\left(\gamma_j^{(i)}\right) = p\left(b_1 b_2 \cdots b_r\right)^{prn} \frac{d_{jt}}{b_j^{prn-k}} = p b_1^{prn} \cdots b_j^{k} \cdots b_r^{prn} d_{jt} \in \mathbb{Z}$$

Daí,

$$\sum_{i=1}^{n} F\left(\gamma_j^{(i)}\right) = \sum_{t \geqslant p} \sum_{i=1}^{n} f^{(t)}\left(\gamma_j^{(i)}\right) = p \sum_{t \geqslant p} b_1^{prn} \cdots b_j^{k} \cdots b_r^{prn} d_{jt}$$

é um inteiro divisível por p. Segue-se então que $\sum_{j=1}^{r} c_j \left\{ \sum_{i=1}^{n} F\left(\gamma_j^{(i)}\right) \right\}$ é um inteiro divisível por p.

Como $p \nmid nc_0F(0)$ 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 (3.11) é um inteiro não nulo. Portanto,

$$1 \leqslant \left| \sum_{j=1}^{r} \sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z) e^{-z} dz \right| \tag{3.16}$$

Denotaremos então

$m_1 = max_{1 \leqslant j \leqslant r} |c_j|$, $m_2 = max_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant r}} |e^{\gamma_j^{(i)}}|$, $m_3 = max_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant r}} |\gamma_j^{(i)}|$,

$m_4 = max_{0 \leqslant t \leqslant 1} e^{-t\gamma_j^{(i)}}$ e $m_5 = max_{0 \leqslant t \leqslant 1} \prod_{j=1}^{r} g_j(t\gamma_j^{(i)})$.

Por (3.16) temos,

$$\left| \sum_{j=1}^{r} \sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z) e^{-z} dz \right| =$$

$$= \left| \sum_{j=1}^{r} \sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} \frac{(b_1 \cdots b_r)^{prn}}{(p-1)!} z^{p-1} \prod_{j=1}^{r} g_j(z)^p e^{-z} dz \right| \leqslant$$

$$\leqslant rnm_1 m_2 \frac{(b_1 \cdots b_r)^{prn}}{(p-1)!} m_3^{p-1} m_5^p m_4 m_3 =$$

$$= rnm_1 m_2 m_4 \frac{(b_1^{rn} \cdots b_r^{rn} m_3 m_5)^p}{(p-1)!} \qquad (II)$$

Para terminar basta-nos provar o seguinte lema:

Lema 3.2.2 *Seja A uma constante, então* $\lim_{p\to\infty} \frac{A^p}{(p-1)!} = 0$.

Demonstração

É evidente que o limite desejado equivale a mostrar que

$$\lim_{p\to\infty} \frac{(p-1)!}{A^p} = \infty$$

Tome um p_0 primo tal que $\frac{p_0 - 1}{A} > 2$, denote $k = \frac{(p_0-1)!}{A^{p_0}}$. Para todo $p > p_0$, temos

$$\frac{(p-1)!}{A^p} = \frac{(p-1)}{A} \cdot \frac{(p-2)}{A} \cdots \frac{p_0}{A} \cdot \frac{(p_0-1)!}{A^{p_0}} > k \cdot 2^{p-p_0}$$

Fazendo $p \to \infty$ temos $k \cdot 2^{p-p_0} \to \infty$. Logo, como $\frac{(p-1)!}{A^p} > k \cdot 2^{p-p_0}$, então

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

□

Voltando a demonstração do teorema, denote $A = b_1^{rn} \cdots b_r^{rn} m_3 m_5$. Fazendo p tender ao infinito em (II), obtemos

$$1 \leqslant rnm_1 m_4 \lim_{p\to\infty} \frac{A^p}{(p-1)!} = 0 \text{ (pelo Lema 3.1.2)}$$

Absurdo! Portanto, $e^{\alpha_1}, \cdots, e^{\alpha_n}$ são linearmente independentes sobre $\mathbb{Q}$.

□

Teorema 3.2.2 ***(Lindemann)*** *Dados m números algébricos distintos $\alpha_1, \cdots, \alpha_m$ então $e^{\alpha_1}, \cdots, e^{\alpha_m}$ são linearmente independentes sobre o corpo dos números algébricos.*

Demonstração

Suponha, sem perda de generalidade, que existem $a_1, \cdots, a_m$ algébricos, não nulos, tais que

$$\sum_{i=1}^{m} a_i e^{\alpha_i} = 0 \tag{3.17}$$

Seja $\mathbb{Q}(\theta)$ uma extensão normal de $\mathbb{Q}$ de grau q e que contenha $a_1, \cdots, a_m$. Portanto os conjugados de $a_i \in \mathbb{Q}(\theta)$. Por (3.17) temos que

$$0 = \prod_{j=1}^{q} \sum_{i=1}^{m} a_i^{(j)} e^{\alpha_i} = \sum_{i=1}^{r} c_i e^{\tilde{\alpha}_i}, \text{ onde } \tilde{\alpha}_i \in \mathbb{A}.$$

Como $a_i^{(j)}$ são polinômios em $\theta^{(i)}$, pela Proposição 3.1.2, temos que $c_i = p_i\left(\theta^{(1)}, \cdots, \theta^{(n)}\right)$ para $i \in \{1, \cdots, r\}$ com p_i simétrico em $\theta^{(1)}, \cdots, \theta^{(n)}$. Logo, pela Proposição 3.1.1, $c_i \in \mathbb{Q}$ e existe $j \in \{1, \cdots, r\}$ pela Proposição 3.1.8 tal que $c_j \neq 0$. Daí,

$$\sum_{i=1}^{r} c_i e^{\tilde{\alpha}_i} = 0$$

o que contradiz o Teorema 3.2.1.

□

3.3 Aplicações do Teorema de Lindemann

Proposição 3.3.1 *Os seguintes números são transcendentes:*

(a) *e;*

(b) e^{α}, $\sin\alpha$, $\cos\alpha$, $\tan\alpha$, $\sinh\alpha$, $\cosh\alpha$, $\tanh\alpha$, *para todo* $\alpha \in \mathbb{A} - \{0\}$*;*

(c) π*;*

(d) $\log\alpha$, $\arcsin\alpha$, *e em geral as funções inversas daquelas do item (b), para todo* $\alpha \in \mathbb{A} - \{0, 1\}$.

Demonstração

(a) Suponha que $e = a \in \mathbb{A} - \{0\}$ então $e + (-a)e^0 = 0$. Portanto, $e \in \mathbb{T}$.

(b) Suponha que $e^{\alpha} = a \in \mathbb{A} - \{0\}$ então $e^{\alpha} + (-a)e^0 = 0$. Daí, $e^{\alpha} \in \mathbb{T}$. Note que,

$$2i\sin\alpha e^0 + (-1)e^{i\alpha} + e^{-i\alpha} = 0$$
$$2\cos\alpha e^0 + (-1)e^{i\alpha} + (-1)e^{-i\alpha} = 0$$
$$(i\tan\alpha - 1)\, e^{i\alpha} + (i\tan\alpha + 1)\, e^{-i\alpha} = 0$$
$$2\sinh\alpha e^0 + (-1)e^{\alpha} + e^{-}\alpha = 0$$
$$2\cosh\alpha e^0 + (-1)e\alpha^{+}(-1)e^{-}\alpha = 0$$
$$(\tanh\alpha - 1)\, e^{\alpha} + (\tanh\alpha + 1) = 0$$

Supondo $\alpha \neq 0$ então $i\alpha \neq 0$. Portanto, pelo Teorema 3.2.2,

$$\sin\alpha,\ \cos\alpha,\ \tan\alpha,\ \sinh\alpha,\ \cosh\alpha \text{ e } \tanh\alpha$$

são números transcendentes.

(c) Se π fosse algébrico, então $i\pi \in \mathbb{A} - \{0\}$. Logo, $e^{i\pi}$ é transcendente, mas $e^{i\pi} = -1$. Portanto, $\pi \in \mathbb{T}$.

(d) Suponha que $\log\alpha \in \mathbb{A} - \{0\}$. Por (b) $e^{\log\alpha}$ é transcendente, mas $e^{\log\alpha} = \alpha \in \mathbb{A}$, essa contradição mostra que $\log\alpha \in \mathbb{T}$. De modo análogo, mostramos que

$$\arcsin\alpha,\ \arccos\alpha,\ \arctan\alpha,\ argsinh\alpha,\ argcosh\alpha, argtanh\alpha$$

são números transcendentes.

□

3.4 Quadratura do Círculo

Um célebre problema da antigüidade era o de construir, usando régua e compasso, um quadrado com área igual à de um círculo dado. A impossibilidade da construção foi provada por Lindemann quando provou que π é transcendente. A demonstração disso se baseia no fato de que se um número α é construtível por régua e compasso então

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty \text{ (veja [3], p. 112)}$$

em outras palavras, via Teorema 1.2.1, α deve ser algébrico.

A recíproca não é verdadeira, por exemplo, $\sqrt[3]{2} \in \mathbb{A}$, mas não é construtível por régua e compasso (veja [3], p. 113), o que encerra também o famoso problema da duplicação do cubo. Considere um círculo de raio 1, então sua área é π, como a área de um quadrado de lado l é l^2, então queremos construir por régua e compasso o número $\sqrt{\pi}$, mas quando Lindemann provou que π é transcendente, então $\sqrt{\pi}$ também o é, daí

$$[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$$

mostrando que não é possível construir por meio de régua e compasso um quadrado com área igual a de um círculo dado.

3.5 Transcendência da Série Fatorial com Coeficientes Periódicos

Sabemos que todo número real α pode ser expresso como uma série fatorial, veja [7].

$$\alpha = \frac{a_1}{1!} + \frac{a_2}{2!} + \cdots + \frac{a_n}{n!} + \cdots \tag{3.18}$$

onde $a_n \in \{0, \cdots, n-1\}$ (para $n = 2, 3, \cdots$). Essa representação é única para α irracional.

Teorema 3.5.1 *Todo número α representado por uma série fatorial (3.18), com coeficientes periódicos, é transcendente.*

Podemos generalizar o Teorema 3.5.1 com o seguinte teorema:

Teorema 3.5.2 *Se a série de potências*

$$\varphi(z) = \sum_{n=1}^{\infty} \frac{a_n}{n!} z^n \tag{3.19}$$

tem coeficientes algébricos, não todos nulos, que formam uma seqüência periódica, então $\varphi(z)$ é transcendente para todo z algébrico não nulo.

Para $z = 1$ o Teorema 3.5.2 *implica no Teorema* 3.5.1. *Portanto, basta-nos mostrar o último teorema anunciado.*

Demonstração

Podemos supor que o período se inicia com a_1, seja m o período da seqüência $\{a_n\}_{n\in\mathbb{N}}$. Considere w uma raiz primitiva m-ésima da unidade. Então,

$$e^{w^k z} = 1 + \frac{w^k z}{1!} + \frac{w^{2k} z^2}{2!} + \cdots + \frac{w^{km} z^m}{m!} + \cdots \tag{3.20}$$

Afirmação 3.5.1 *Seja w uma raiz primitiva m-ésima da unidade, então*

$$\sum_{k=1}^{m} w^{jk} = 0,$$

para todo $j \in \mathbb{N}$ tal que $m \nmid j$.

Demonstração

$$\begin{aligned} \sum_{k=1}^{m} w^{jk} &= w^j + w^{2j} + \cdots + w^{mj} = \\ &= 1 + w^j + \left(w^j\right)^2 + \cdots + \left(w^j\right)^m - 1 = \frac{\left(w^j\right)^m - 1}{w^j - 1} \end{aligned}$$

note que $m \nmid j$, daí $w^j - 1 \neq 0$, já que w é raiz primitiva m-ésima da unidade. Como $(w^j)^m = (w^m)^j$ e $w^m = 1$, temos

$$\sum_{k=1}^{m} w^{jk} = 0$$

□

Afirmação 3.5.2 *Seja w como na afirmação anterior, então*

$$\sum_{k=1}^{m} w^{jmk} = m. \tag{3.21}$$

Demonstração

De fato, note que

$$\sum_{k=1}^{m} w^{jmk} = \sum_{k=1}^{m} (w^m)^{jk} = \sum_{k=1}^{m} 1 = m$$

□

De volta à demonstração do teorema. Passando na igualdade (3.20) o somatório de k variando entre 1 e m, e usando as afirmações 3.5.1 e 3.5.2, temos:

$$\sum_{k=1}^{m} e^{w^k m} = m + 0 + \cdots + 0 + m\frac{z^m}{m!} + 0 + \cdots + 0 + m\frac{z^{2m}}{(2m)!} + \cdots$$

E portanto,

$$\frac{a_m}{m}\sum_{k=1}^{m} e^{w^k m} = a_m + a_m\frac{z^m}{m!} + a_m\frac{z^{2m}}{(2m)!} + \cdots \tag{3.22}$$

Analogamente para $r = 1, 2, \cdots, m-1$, temos:

$$\frac{a_{m-r}}{m}\sum_{k=1}^{m} w^{kr} e^{w^k z} = a_{m-r}\frac{z^{m-r}}{(m-r)!} + a_{m-r}\frac{z^{2m-r}}{(2m-r)!} + \cdots \tag{3.23}$$

somando (3.21) com (3.22) para $r = 1, 2, \cdots, m-1$, obtemos

$$\sum_{k=1}^{m} e^{w^k z}\left(\frac{1}{m}\sum_{r=0}^{m-1} a_{m-r} w^{kr}\right) = \varphi(z) + a_m \tag{3.24}$$

denotemos $\frac{1}{m}\sum_{r=0}^{m-1} a_{m-r}w^{kr} = A_k\,(k = 1, 2, \cdots, m)$. Temos então

$$\sum_{k=1}^{m} A_k e^{w^k z} - [\varphi(z) + a_m]\, e^0 = 0 \tag{3.25}$$

Os números A_k são algébricos $(k = 1, 2, \cdots, m)$ e não todos nulos. De fato, suponha que $A_k = 0\,(k = 1, 2, \cdots, m)$. Considere o polinômio de grau $(m-1)$ abaixo:

$$p(z) = \sum_{r=0}^{m-1} a_{m-r} z^r$$

Sabemos que $w^k\,(k = 1, 2, \cdots, m)$ são distintos e

$$p\left(w^k\right) = \sum_{r=0}^{m-1} a_{m-r} w^{kr} = mA_k = 0\,(k = 1, 2, \cdots, m)$$

então p tem grau $m-1$ e possui m raízes distintas, segue-se que $p \equiv 0$, isto é,

$$a_1 = a_2 = \cdots = a_m = 0$$

Logo, $a_j = 0\ \forall\, j \in \mathbb{N}$ (já que o período de $\{a_n\}_{n\in\mathbb{N}}$ é m), contradizendo a hipótese de que as $a_j's$ não são todos nulos. Se z é algébrico diferente de zero, então $w^k z$ é algébrico $(k = 1, \cdots, m)$, diferente de zero. Suponha que $\varphi(z) + a_m \in \mathbb{A}$. Então, pelo Teorema de Lindemann (Teorema 3.2.2):

$$\sum_{k=1}^{m} A_k e^{w^k z} - [\varphi(z) + a_m]\, e^0 \in \mathbb{T}$$

Por outro lado,

$$\sum_{k=1}^{m} A_k e^{w^k z} - [\varphi(z) + a_m]\, e^0 = 0$$

Absurdo! Logo, $\varphi(z) + a_m \in \mathbb{T}$, como $a_m \in \mathbb{A}$, segue-se da Proposição 1.4.1 (i) que

$$\varphi(z) = (\varphi(z) + a_m) - a_m \text{ é transcendente.}$$

□

Capítulo 4

O Teorema de Gelfond-Schneider

Em 1900 no Congresso Internacional de Matemática em Paris, o matemático alemão David Hilbert propôs uma lista de 23 problemas. Nenhum dos problemas tinha solução até então, e vários deles acabaram se tornando muito influentes na matemática do século XX. O sétimo problema de Hilbert pergunta se o número α^{β}, onde α é algébrico (diferente de zero e um) e β é algébrico (não racional), é transcendente. Essa questão foi resolvida em 1934 por A. O. Gelfond e independentemente em 1935 por T. Schneider e sua demonstração é detalhada no presente capítulo.

4.1 Preliminares

Definição 4.1.1 *Seja $\mathbb{Q}(\theta)|\mathbb{Q}$ extensão algébrica. O conjunto de inteiros algébricos $\{\alpha_1, \cdots, \alpha_n\}$ é chamada base integral de $\mathbb{Q}(\theta)$, se todo $\alpha \in \mathbb{Q}(\theta)$, inteiro algébrico, pode ser escrito unicamente na forma*

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

Definição 4.1.2 *Sejam $\mathbb{Q}(\theta)|\mathbb{Q}$ uma extensão de grau n e $\{\alpha_1, \cdots, \alpha_n\}$ base de $\mathbb{Q}(\theta)|\mathbb{Q}$. Denote por $\alpha_j^{(i)}$, $i = 1, \cdots, n$, os conjugados de α_j sobre $\mathbb{Q}(\theta)$. O discriminante do conjunto $\{\alpha_1, \cdots, \alpha_n\}$ é definido por*

$$\Delta[\alpha_1, \cdots, \alpha_n] = \left[\det \begin{pmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} & \cdots & \alpha_n^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \cdots & \alpha_n^{(n)} \end{pmatrix}\right]^2 \tag{4.1}$$

Proposição 4.1.1 *Toda base integral é base.*

Proposição 4.1.2 *Se $\alpha_1, \cdots, \alpha_n$ é base integral de $\mathbb{Q}(\theta)|\mathbb{Q}$ então*

$$\Delta[\alpha_1, \cdots, \alpha_n] \in \mathbb{Z} - \{0\}$$

Proposição 4.1.3 *Todo corpo de números algébricos tem pelo menos uma base integral.*

As demonstrações das proposições acima podem ser vistas em [15], p. 64-65.

□

Proposição 4.1.4 *Considere a matriz com entradas ρ_j^a na j-ésima linha e $(1+a)$-ésima coluna, com $j = 1, 2, \cdots, t$ e $a = 0, 1, \cdots, t-1$. Essa matriz é chamada matriz de Vandermonde e seu determinante é zero se e só se existe $j \neq k$ com $\rho_j = \rho_k$.*

Demonstração

Ver [18], p. 214.

□

Proposição 4.1.5 *Se α é um número algébrico, então existe $r \in \mathbb{Z}^+$ tal que $r\alpha$ é inteiro algébrico.*

Demonstração

Como α é algébrico, tome $p(x) \in \mathbb{Q}[x]$ o seu polinômio minimal,

$$p(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \tag{4.2}$$

Como $p(x) \in \mathbb{Q}[x]$, podemos supor sem perda de generalidade que $a_i = \dfrac{p_i}{q_i}$, onde $p_i \in \mathbb{Z}$, $q_i \in \mathbb{Z}^+$, $0 \leqslant i \leqslant n-1$. Considere $r = q_0 q_1 \cdots q_{n-1}$, substituindo $a_i = \dfrac{p_i}{q_i}$, $0 \leqslant i \leqslant n-1$ em (4.2), obtemos

$$p(x) = \frac{p_0}{q_0} + \frac{p_1}{q_1}x + \cdots + \frac{p_{n-1}}{q_{n-1}}x^{n-1} + x^n$$

Como $p(\alpha) = 0$, então

$$0 = \frac{p_0}{q_0} + \frac{p_1}{q_1}\alpha + \cdots + \frac{p_{n-1}}{q_{n-1}}\alpha^{n-1} + \alpha^n \tag{4.3}$$

Agora multiplicando (4.3) por r^n;

$$0 = \frac{p_0}{q_0}(q_0 \cdots q_{n-1})^n + \frac{p_1}{q_1}(q_0 \cdots q_{n-1})^n\alpha + \cdots + \frac{p_{n-1}}{q_{n-1}}(q_0 \cdots q_{n-1})^n\alpha^{n-1} + (r\alpha)^n$$

Suponha $n > 1$ então $n - 2 \geqslant 0$, daí

$$0 = p_0(q_0^{n-1} \cdots q_{n-1}^n) + \cdots + p_{n-1}(q_0 \cdots q_{n-2})(r\alpha)^{n-1} + (r\alpha)^n$$

Portanto, $r\alpha$ é raiz de um polinômio mônico de grau n com coeficientes inteiros, esse polinômio é obviamente irredutível, pois caso contrário α seria raiz de um polinômio em $\mathbb{Q}[x] - \{0\}$ de grau menor do que n. Logo $r\alpha$ é inteiro algébrico.

□

Lema 4.1.1 *Considere as m equações em n incógnitas*

$$a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n = 0,\ k = 1, \cdots, m \tag{4.4}$$

onde $a_{ij} \in \mathbb{Z}$ e $0 < m < n$. Seja A um inteiro positivo tal que $A \geqslant |a_{ij}|$ para todo i e j. Então existe uma solução não trivial $x_1, x_2, \cdots, x_n$ de (4.4) ($x_i \in \mathbb{Z}$, $1 \leqslant i \leqslant n$) tal que

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

Demonstração

Denote y_k por $a_{k1}x_1 + \cdots + a_{kn}x_n$, então todo ponto $x = (x_1, x_2, \cdots, x_n)$ corresponde a um ponto $y = (y_1, y_2, \cdots, y_m)$. Um ponto x é dito *reticulado* se suas coordenadas x_j são números inteiros. Observe que se x é reticulado, então seu correspondente y também o é.

Seja q um inteiro positivo. Considere o cubo n-dimensional C definido por $|x_j| \leqslant q$, $j = 1, \cdots, n$. Note que existem $(2q+1)^n$ pontos reticulados em C. Para os correspondentes y, temos:

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

Portanto, existem $2nAq + 1$ possibilidades para y_k, como $k = 1, \cdots, m$ então temos $(2nAq + 1)^m$ pontos reticulados dentro do cubo m-dimensional D, definido por $|y_k| \leqslant nAq$.

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 que

$$(2q + 1)^n > (2nAq + 1)^m \tag{4.5}$$

Considere o intervalo $I = \left[(nA)^{\frac{m}{n-m}} - 1, (nA)^{\frac{m}{n-m}} + 1\right)$ com comprimento 2, logo existe um número par em I. Para especificar q em (4.5), considere q inteiro positivo tal que

$$(nA)^{\frac{m}{n-m}} - 1 \leqslant 2q < (nA)^{\frac{m}{n-m}} + 1 \tag{4.6}$$

A primeira parte da desigualdade implica que

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

Temos então,

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

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

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

Além disso, por (4.6)

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

□

Notação Seja $\alpha \in K$ um número algébrico. O *peso* de α denotado por $\| \alpha \|$ é o máximo entre os valores absolutos dos conjugados de α. Pela Proposição 3.1.9, temos

$$\| \alpha + \beta \| \leqslant \| \alpha \| + \| \beta \| \text{ e } \| \alpha\beta \| \leqslant \| \alpha \| \cdot \| \beta \|$$

Este último lema encerra esta seção com uma poderosa ferramenta para a demonstração do Teorema de Gelfond-Schneider.

Lema 4.1.2 *Considere as p equações em q incógnitas*

$$\alpha_{k1}\zeta_1 + a_{k2}\zeta_2 + \cdots + a_{kq}\zeta_q = 0, \; k = 1, \cdots \; p \tag{4.7}$$

onde os coeficientes $\alpha_{ij} \in K$ são inteiros algébricos e $[K : \mathbb{Q}] = n$. Assuma que $0 < p < q$. Seja $A \geqslant 1$ tal que $A \geqslant \| \alpha_{ij} \| \; \forall \, i, j$. Então existe uma constante positiva c dependendo de K, mas independente de α_{ij}, p e q, tal que as equações (4.7) tem uma solução não trivial $\zeta_1, \zeta_2, \cdots, \zeta_q$ em inteiros sobre K, satisfazendo

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

Demonstração

Seja $\beta_1, \cdots, \beta_n$ uma base integral de $K|\mathbb{Q}$ (veja Proposição 4.1.1). Se α é inteiro sobre K então existem $g_1, \cdots, g_n \in \mathbb{Z}$ tal que α é escrito unicamente como

$$\alpha = g_1\beta_1 + \cdots + g_n\beta_n \tag{4.8}$$

Denote os conjugados de α (para K) por $\alpha = \alpha^{(1)}, \alpha^{(2)}, \cdots, \alpha^{(n)}$ e de β_j por $\beta_j = \beta_j^{(1)}, \beta_j^{(2)}, \cdots, \beta_j^{(n)}$ para $j = 1, \cdots, n$. Passando o i-ésimo conjugado na igualdade (4.8), obtemos pela Proposição 3.1.9:

$$\alpha^{(i)} = g_1\beta_1^{(i)} + \cdots + g_n\beta_n^{(i)},\ i = 1, \cdots, n \tag{4.9}$$

Considere

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

As igualdades em (4.9) implicam

$$BG = A \tag{4.10}$$

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

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

onde os β_{ij} só dependem das entradas de B. Multiplicando a igualdade (4.10) à esquerda por B^{-1}, obtemos:

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

Portanto,

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

e então

$$|g_j| \leqslant |\beta_{j1}||\alpha^{(1)}| + \cdots + |\beta_{jn}||\alpha^{(n)}| \leqslant (|\beta_{j1}| + \cdots + |\beta_{jn}|) \parallel \alpha \parallel < c_1 \parallel \alpha \parallel$$

onde $c_1 = max_{1 \leqslant j \leqslant n} \{|\beta_{j1}| + \cdots + |\beta_{jn}|\} + 1$.

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

$$|g_j| < c_1 \parallel \alpha \parallel \ \ (j = 1, \cdots, n) \tag{4.11}$$

Sendo ζ_i, $i = 1, 2, \cdots, q$ inteiros algébricos satisfazendo (4.7), nós podemos escrevê-los em termos da base integral,

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

O problema então é determinar o comportamento dos números inteiros x_{ij}. Por (4.7) temos

$$0 = \sum_{i=1}^{q} \alpha_{ki}\zeta_i = \sum_{i=1}^{q}\sum_{j=1}^{n} x_{ij}\alpha_{ki}\beta_j \tag{4.12}$$

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

$$\alpha_{ki}\beta_j = \sum_{r=1}^{n} m_{kijr}\beta_r,\ k = 1, \cdots, p;\ i = 1, \cdots, q;\ j = 1, \cdots, n \tag{4.13}$$

voltando à (4.12), obtemos

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

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

$$0 = \sum_{i=1}^{q} \sum_{j=1}^{n} x_{ij} m_{kijr},\ k = 1, \cdots, p;\ r = 1, \cdots, n \tag{4.14}$$

ou seja, temos um sistema de pn equações com qn incógnitas, para aplicar o Lema 4.1.1, basta-nos então majorar os números m_{kijr}. Por (4.14) e pelo mesmo argumento empregado para concluir a desigualdade em (4.11), concluímos

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

onde c_2 é uma constante positiva que satisfaz:

$$c_2 \geqslant c_1 \parallel \beta_j \parallel \text{ e } c_2 A \in \mathbb{Z}$$

Podemos então aplicar o Lema 4.1.1 ao sistema em (4.14), portanto, existe uma solução não trivial x_{ij} em inteiros sobre K tais que

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

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

$$\parallel \zeta_i \parallel < n \cdot max_j \parallel \beta_j \parallel (1 + (nc_2qA)^{\frac{p}{q-p}}) \tag{4.15}$$

Considere c uma constante positiva tal que $c \geqslant n \parallel \beta_j \parallel (j = 1, \cdots, n)$ e $c \geqslant nc_2$. Portanto, c só depende de K e voltando a (4.15), concluímos que

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

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

4.2 O Teorema de Gelfond-Schneider

Teorema 4.2.1 ***(Gelfond-Schneider)*** *Seja $\alpha \in \mathbb{A} - \{0,1\}$ e $\beta \in \mathbb{A} - \mathbb{Q}$. Então α^β é transcendente.*

Demonstração

Suponha por absurdo que α^β é algébrico. Escreva $\gamma = \alpha^\beta = e^{\beta \log \alpha}$ e seja K uma extensão de $\mathbb{Q}$ com grau h e tal que α, β, $\gamma \in K$. Escreveremos algumas relações que serão utilizadas posteriormente.

$$m = 2h + 3,\ q > 4m^2,\ n = \frac{q^2}{2m},\ t = q^2 = 2mn,\ n > q \tag{4.16}$$

Defina $\rho_1, \rho_2, \cdots, \rho_t$ como os números

$$(r + k\beta)\log\alpha \ para\ r = 1, 2, \cdots, q;\ k = 1, 2, \cdots, q \tag{4.17}$$

Em alguma ordem. Não precisamos especificar exatamente os $\rho_i's$. Considere a função abaixo:

$$F(z) = \sum_{j=1}^{t} \eta_j e^{z\rho_j} \tag{4.18}$$

onde η_j são inteiros algébricos sobre K que serão especificados. Note que $F(z)$ é uma função inteira.

Pela Proposição 4.1.5, existem a_1, a_2, a_3 números inteiros positivos tais que $a_1\alpha$, $a_2\beta$ e $a_3\gamma$ são inteiros algébricos. Tome, $c_1 = a_1a_2a_3$, observe que $c_1 > 0$ e $c_1\alpha$, $c_1\beta$ e $c_1\gamma$ são inteiros algébricos. Considere agora as mn equações em $2mn$ incógnitas η_j.

$$c_1^{n+2mq}(\log\alpha)^{-a}F^{(a)}(b) = 0,\ a = 0, \cdots, n-1;\ b = 1, \cdots, m \tag{4.19}$$

Os coeficientes de η_j em (4.19) são:

$$c_1^{n+2mq}(\log\alpha)^{-a}\rho_j^a e^{b\rho_j} = c_1^{n+2mq}(r+k\beta)^a e^{\log\alpha^{b(r+k\beta)}} = c_1^{n+2mq}(r+k\beta)^a\alpha^{rb}\gamma^{kb} \tag{4.20}$$

Observe que a última expressão em (4.20) é um polinômio em α, β e γ de grau $a + rb + kb$. Como os máximos de a, b, r e k são respectivamente $n-1$, m, q e q então $a+rb+kb \leqslant n-1+2mq$, portanto $c_1^{n+2mq}(r+k\beta)^a\alpha^{rb}\gamma^{kb}$ é um inteiro algébrico.
Queremos utilizar o Lema 4.1.2 para o sistema de equações (4.19). Já mostramos que os coeficientes das incógnitas η_j são inteiros algébricos, portanto, basta-nos encontrar um limitante para os conjugados de $c_1^{n+2mq}(r + k\beta)^a\alpha^{rb}\gamma^{kb}$ sobre K. Note que

$$\| r + k\beta \| \leqslant \| r \| + \| k \| \cdot \| \beta \| \leqslant q + q \| \beta \| = q(1+ \| \beta \|)$$

Defina $c_2 = max\{\| \alpha \|, \| \gamma \|, 1+ \| \beta \|\}$. Note que c_2 independe de n, q, t e além disso,

$$\begin{aligned} \| c_1^{n+2mq}(r + k\beta)^a\alpha^{rb}\gamma^{kb} \| &\leqslant c_1^{n+2mq}(qc_2)^a c_2^{rb}c_2^{kb} \leqslant c_1^{n+2mq}(qc_2)^n c_2^{qm}c_2^{qm} = \\ &= c_1^{n+2mq}(qc_2)^n c_2^{2mq} = (c_1c_2)^n[(c_1c_2)^{2m}]^q(\sqrt{2m})^n n^{\frac{n}{2}}, \\ &\quad por (4.16) \end{aligned}$$

Defina $c_3 = (c_1c_2)^{2m+1}\sqrt{2m}$, podemos então fazer a seguinte limitação:

$$\| c_1^{n+2mq}(r + k\beta)^a\alpha^{rb}\gamma^{kb} \| \leqslant c_3^n n^{\frac{n}{2}}$$

Observe que c_3 independe de n.

Agora pelo Lema 4.1.2, concluímos que as equações (4.19) têm solução não-trivial η_j em inteiros algébricos, com

$$\begin{aligned} \| \eta_j \| &< c + c\left(2cmnc_3^n n^{\frac{n}{2}}\right)^{\frac{mn}{2mn-mn}} = c + c(2cmnc_3^n n^{\frac{n}{2}}) = c + 2c^2mnc_3^n n^{\frac{n}{2}} < \\ &< 3c^2mnc_3^n n^{\frac{n}{2}} \end{aligned}$$

onde c depende de K mas independe de n. Como $2^n > n > q > m$ então $mn < 4^n$, daí:

$$\| \eta_j \| < 3c^2 4^n c_3^n n^{\frac{n}{2}} = 3c^2(4c_3)^n n^{\frac{n}{2}} < c_4^n n^{\frac{n}{2}} \tag{4.21}$$

onde $c_4 = 12c^2c_3$. Usamos na última desigualdade em (4.21) que $3c^2 < (3c^2)^n$ pois a constante c pode ser tomada maior que 1. Agora $F(z)$ em (4.18) está completamente definida

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

onde $\eta_1, \cdots, \eta_t$ é solução não-trivial de (4.19).

Lema 4.2.1 *Existe* $p \geqslant n$ *e* $B \in \{1, \cdots, m\}$ *tal que* $F^{(a)}(b) = 0$, *para* $a = 0, \cdots, p-1$, $b = 1, \cdots, m$ *e* $F^{(p)}(B) \neq 0$.

Demonstração

Se tal inteiro p existe deve ser maior ou igual à n, em vista de (4.19). É suficiente provar que existe $a \in \{0, 1, \cdots, t-1\}$ tal que $F^{(a)}(1) \neq 0$. Assuma que $F^{(a)}(1) = 0$ para todo $a \in \{0, 1, \cdots, t-1\}$, por (4.18)

$$\sum_{j=1}^{t} \eta_j \rho_j^a e^{\rho_j} = 0, \ 0 \leqslant a \leqslant t-1$$

Como os $\eta_j' s$ não são todos nulos, obtemos um determinante nulo,

$$0 = \det\left(\rho_j^a e^{\rho_j}\right) = \det\left(\rho_j^a\right) \prod_j e^{\rho_j}$$

Daí, $\det|\rho_j^a| = 0$. Pela Proposição 4.1.4, esse determinante de Vandermonde se anula quando dois dos $\rho' s$ são iguais, digamos $\rho_j = \rho_k$. Portanto,

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

como $\log\alpha \neq 0$, teríamos $r_s + k_s\beta = r_l + k_l\beta$ e β seria racional. Absurdo!

□

Usando o Lema 4.2.1, definimos o seguinte número não-nulo,

$$\begin{aligned}
\zeta &= (\log\alpha)^{-p} F^{(p)}(B) = (\log\alpha)^{-p} \sum_{j=1}^{t} \eta_j \rho_j^p e^{B\rho_j} = \\
&= \sum_{j=1}^{t} \eta_j (\log\alpha)^{-p} (\log\alpha)^p (r + k\beta)^p e^{B(r+k\beta)\log\alpha} = \\
&= \sum_{j=1}^{t} \eta_j (r + k\beta)^p \alpha^{Br} \gamma^{Bk} \qquad (4.22)
\end{aligned}$$

Lema 4.2.2 *Existe uma constante positiva $\tilde{C}$, independente de n e p, tal que*

$$|N(\zeta)| \geqslant \tilde{C}^{-p}.$$

Demonstração

Primeiramente mostraremos que $c_1^{p+2mq}\zeta$ é inteiro sobre K. De fato, note que η_j são inteiros sobre K e $(r+k\beta)^p\alpha^{Br}\gamma^{Bk}$ é um polinômio sobre α, β e γ com grau $p+Br+Bk \leqslant p+2mq$, já que $B \leqslant m$ e r, $k \leqslant q$, daí $c_1^{p+2mq}\zeta$ é inteiro algébrico. Como $q < n \leqslant p$ então

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

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

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

Portanto, $c_5^p\zeta$ também é inteiro algébrico. Por (ii) e (iii) da Proposição 3.1.11, $N(c_5^p\zeta) \in \mathbb{Z} - \{0\}$. Segue-se que

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

Daí,

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

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

□

Lema 4.2.3 *Existe uma constante positiva $\tilde{c}$, independente de n e p, tal que*

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

Demonstração

Por (4.22), temos

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

Agora, $q < n \leqslant p$ e $t = 2mn < 2n^2 < 2^n$ para n suficientemente grande. Usando (4.21) e substituindo r, k, β, $\| \alpha \|$, $\| \gamma \|$ e $1+ \| \beta \|$ pelos seus máximos q, q, m, c_2, c_2, c_2 respectivamente, obtemos:

$$\| \zeta \| \leqslant 2^n c_4^n n^{\frac{n}{2}} q^p c_2^p c_2^{mq} c_2^{mq} \leqslant 2^p c_4^p n^{\frac{n}{2}} q^p c_2^p c_2^{2mp} = (2c_4 c_2^{1+2m})^p n^{\frac{n}{2}} q^p \qquad (4.23)$$

Por outro lado, $q^2 = 2mn$ então

$$q^p = (\sqrt{2m})^p n^{\frac{p}{2}} \leqslant (\sqrt{2m})^p p^{\frac{p}{2}} \text{ e } n^{\frac{n}{2}} \leqslant p^{\frac{p}{2}} \text{ (já que } n \leqslant p)$$

aplicando essa desigualdade em (4.23),

$$\| \zeta \| \leqslant (2c_4 c_2^{1+2m})^p n^{\frac{n}{2}} q^p \leqslant (2c_4 c_2^{1+2m})^p p^{\frac{p}{2}} (\sqrt{2m})^p p^{\frac{p}{2}} = \tilde{c}^p p^p$$

onde $\tilde{c} = 2\sqrt{2m} c_4 c_2^{1+2m}$.

Pelo Lema 4.2.1, a função inteira $F(z)$ tem zeros, de ordem pelo menos p, nos pontos $z = 1, \cdots, m$. Portanto $S(z)$ definida a seguir também é função inteira.

$$S(z) = p! F(z) \prod_{b=1}^{m} (z-b)^{-p} \prod_{\substack{b=1 \\ b \neq B}}^{m} (B-b)^p \qquad (4.24)$$

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

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

Substituindo em (4.24), obtemos:

$$\begin{aligned} S(z) &= p! \left(\frac{(z-B)^p F^{(p)}(B)}{p!} + \sum_{k=1}^{\infty} \frac{(z-B)^{p+k} F^{(p+k)}(B)}{(p+k)!} \right) \cdot \\ &\cdot \frac{(B-1)^p \cdots \widehat{(B-B)^p} \cdots (B-m)^p}{(z-1)^p \cdots (z-B)^p \cdots (z-m)^p} = \\ &= p! \left(\frac{F^{(p)}(B)}{p!} \cdot \frac{(B-1)^p \cdots \widehat{(B-B)^p} \cdots (B-m)^p}{(z-1)^p \cdots \widehat{(z-B)^p} \cdots (z-m)^p} \right) + \\ &+ p! \left(\sum_{k=1}^{\infty} \frac{(z-B)^{p+k} F^{(p+k)}(B)}{(p+k)!} \cdot \frac{(B-1)^p \cdots \widehat{(B-B)^p} \cdots (B-m)^p}{(z-1)^p \cdots \widehat{(z-B)^p} \cdots (z-m)^p} \right) \end{aligned}$$

Portanto $S(B) = F^{(p)}(B)$. Como $\zeta = (\log \alpha)^{-p} F^{(p)}(B)$, então

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

Pelo Teorema de Cauchy, temos:

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

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

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

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

Segue-se que $z = B$ está no interior do disco cujo bordo é C.

Sabemos que se $u \in \mathbb{C}$, então $|e^u| \leqslant e^{|u|}$, portanto, para todo z no círculo $|z| = \dfrac{p}{q}$,

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

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

Claramente c_6 independe de n e p. Por (4.18) e (4.21), temos

$$\begin{aligned} |F(z)| &= \left| \sum_{j=1}^{t} \eta_j e^{z\rho_j} \right| \leqslant \sum_{j=1}^{t} |\eta_j| |e^{z\rho_j}| \leqslant t c_4^n n^{\frac{n}{2}} c_6^p < 2^p c_4^p n^{\frac{n}{2}} c_6^p = \\ &= (2c_4 c_6)^p n^{\frac{n}{2}} \leqslant c_7^p p^{\frac{p}{2}} \end{aligned} \tag{4.25}$$

onde $c_7 = 2c_4 c_6$. Para $b = 1, 2, \cdots, m$ temos

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

Daí,

$$|z - b|^{-p} \leqslant \left(\frac{2q}{p} \right)^p \tag{4.26}$$

Aplicando (4.24), (4.25) à (4.26), obtemos

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

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

$$|S(z)| < c_8^p p^{\frac{p(3-m)}{2}} \tag{4.27}$$

para todo z no círculo $|z| = \dfrac{p}{q}$. Por outro lado,

$$\begin{aligned}
|\zeta| &\leqslant |\log\alpha|^{-p} \cdot |S(B)| = \frac{1}{2\pi}|\log\alpha|^{-p}\left|\int_C \frac{S(z)}{z-B}dz\right| < \\
&< \frac{1}{2\pi}|\log\alpha|^{-p} 2\pi \left(\frac{p}{q}\right) c_8 p^{\frac{p(3-m)}{2}} \frac{2q}{p} = \\
&= 2|\log\alpha|^{-p} c_8^p p^{\frac{p(3-m)}{2}} < \left(2c_8|\log\alpha|^{-1}\right)^p p^{\frac{p(3-m)}{2}} = c_9^p p^{\frac{p(3-m)}{2}}
\end{aligned}$$

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

$$\begin{aligned}
|N(\zeta)| &= |\zeta||\zeta^{(2)}|\cdots|\zeta^{(h)}| \leqslant |\zeta| \parallel \zeta \parallel^{h-1} < c_9^p p^{\frac{p(3-m)}{2}} \left(\tilde{c}^p p^p\right)^{h-1} = \\
&= c_9^p p^{\frac{p(-2h)}{2}} \tilde{c}^{p(h-1)} p^{p(h-1)} = (c_9\tilde{c}^{h-1})^p p^{-ph} p^{ph-p} = (c_{10})^p p^{-p}
\end{aligned}$$

onde $c_{10} = c_9\tilde{c}^{h-1}$. Por outro lado, pelo Lema 4.2.2, temos,

$$c_{10}^{p} p^{-p} > \tilde{C}^{-p} \Rightarrow \tilde{C} c_{10} > p$$

$\tilde{C}$ e c_{10} são constantes que não dependem de n e p. Contradição, porque $p \geqslant n$ e n pode ser tomado arbitrariamente grande. Logo α^{β} é transcendente.

□

Corolário 4.2.1 *e^{π} é transcendente.*

Demonstração

Como $e^{\pi i} = -1$ então $(e^{\pi i})^{-i} = (-1)^{-i}$, logo $e^{\pi} = (-1)^{-i}$ é transcendente pelo Teorema 4.2.1.

□

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

Corolário 4.2.2 *Sejam α_1, α_2, β_1, β_2 números algébricos, não-nulos, com $\log \alpha_1$, $\log \alpha_2$ linearmente independentes sobre $\mathbb{Q}$. Então*

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

Demonstração

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

$$\beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 = 0 \tag{4.28}$$

Portanto,

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

implica que $\alpha_2 = \alpha_1^{-\frac{\beta_1}{\beta_2}}$ e pelo Teorema de Gelfond-Schneider, $\dfrac{\beta_1}{\beta_2} \in \mathbb{Q}$. Então existe $p \in \mathbb{Q}$ tal que $\beta_1 = p\beta_2$. Substituindo em (4.28), obtemos:

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

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

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

□

Capítulo 5

Valores Algébricos de Funções Meromorfas

5.1 Preliminares

Neste capítulo toda função $f : \Omega \longrightarrow \mathbb{C}$ holomorfa será inteira, isto é, $\Omega = \mathbb{C}$.

Definição 5.1.1 *Uma função f é dita meromorfa, quando toda singularidade de f é pólo. Neste caso podemos escrever*

$$f = \frac{g}{h}$$

onde g, h são funções inteiras.

Definição 5.1.2 *Uma função $f : \mathbb{C} \longrightarrow \mathbb{C}$ holomorfa é dita de ordem finita se existe $\rho > 0$ tal que para todo $R \geqslant 2$ e $z \in \mathbb{C}$ com $|z| \leqslant R$, tem-se*

$$|f(z)| \leqslant e^{R^\rho}$$

Definição 5.1.3 *Uma função f meromorfa é dita de ordem finita se é quociente de duas funções inteiras de ordem finita.*

Definição 5.1.4 *Sejam $L|K$ uma extensão de corpos e $\alpha_1, \cdots \alpha_n$ elementos de L. $\alpha_1, \cdots \alpha_n$ são ditos algebricamente independentes sobre K, se para todo $p(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n] - \{0\}$,*

$$p(\alpha_1, \cdots, \alpha_n) \neq 0$$

caso contrário $\alpha_1, \cdots \alpha_n$ são ditos algebricamente dependentes sobre K.

Existem muitos problemas em aberto sobre a independência algébrica de alguns números, por exemplo, e e π são algebricamente independentes sobre $\mathbb{Q}$?

5.2 Valores Algébricos de Funções Meromorfas

Teorema 5.2.1 *Sejam $K|\mathbb{Q}$ uma extensão finita e $f_1(z), \cdots, f_n(z)$ funções meromorfas de ordem finita. Suponha que o anel $K[f_1, \cdots, f_n]$ é mapeado em si mesmo pela derivação e que $f_1(z)$, $f_2(z)$ são algebricamente indenpendentes sobre K. Então existe somente um número finito de números complexos, $z_1, \cdots, z_m$, que não são pólos de $f_j(z)$ para $j \in \{1, \cdots, n\}$ e tais que*

$$f_j(z_i) \in K,\ 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n$$

Demonstração

Assuma que as hipóteses do Teorema 5.2.1 são satisfeitas e escreva $f_i = \dfrac{g_i}{h_i}$, onde g_i, h_i são funções inteiras e $i \in \{1, \cdots, n\}$. Suponha que exista uma seqüência infinita de números complexos distintos $y_1, y_2, \cdots$, não pólos das f_j, tais que $f_j(y_i) \in K$ para todo i, j. Por $c_1, c_2, \cdots$ denotamos constantes positivas que dependem apenas de algumas quantidades à

serem definidas, m é um inteiro que excede qualquer constante suficientemente grande e k um inteiro suficientemente grande comparado com m, $L = \lfloor k^{\frac{3}{4}} \rfloor$ e $f^{(j)}$ denota a j-ésima derivada de f.

Lema 5.2.1 *Sejam M, N inteiros com $N > M > 0$ e $u_{ij}, (1 \leqslant i \leqslant M,$ $1 \leqslant j \leqslant N)$ são inteiros algébricos com pesos no máximo $U(\geqslant 1)$. Então existem inteiros algébricos $x_1, \cdots, x_N$ em K, não todos nulos, satisfazendo:*

$$\sum_{j=1}^{N} u_{ij} x_j = 0 \ \ (1 \leqslant i \leqslant M)$$
$$\|x_j\| \leqslant c_1 \left(c_1 NU\right)^{\frac{M}{N-M}} \ \ (1 \leqslant j \leqslant N)$$

A demonstração deste lema é análoga à do Lema 4.1.2 da seção 4.1, portanto será omitida.

Lema 5.2.2 *Existem inteiros algébricos $p(\lambda_1, \lambda_2)$ em K, não todos nulos, com pesos no máximo $k^{c_5 k}$, tal que a função*

$$\Phi(z) = \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1, \lambda_2) f_1(z)^{\lambda_1} f_2(z)^{\lambda_2}$$

satisfaz

$$\Phi^{(j)}(y_l) = 0 \ \ (0 \leqslant j \leqslant k, 1 \leqslant l \leqslant m)$$

Demonstração

O número $\Phi^{(j)}(y_l)$ é escrito como forma linear em $p(\lambda_1, \lambda_2)$ com coeficientes que são polinômios em $f_1(y_l), \cdots, f_n(y_l)$. Os polinômios aparecem das derivadas de $f_1, \cdots, f_n$ que, por hipótese, são elementos de $K[f_1, \cdots, f_n]$. Assim, os coeficientes de $p(\lambda_1, \lambda_2)$ estão em K. Esses coeficientes tornam-se inteiros algébricos quando multiplicados por um número inteiro positivo conveniente. Seja c tal número e suponha que o peso desses inteiros algébricos não exceda $U(\geqslant 1)$. Considere o sistema

$$c\Phi^{(j)}(y_l) = 0 \ \ (0 \leqslant j \leqslant k, 1 \leqslant l \leqslant m) \tag{5.1}$$

com $N=(L+1)^2$ incógnitas $p(\lambda_1,\lambda_2)$ e $M=m(k+1)$ equações.

Note que $N=(L+1)^2=\left(\lfloor k^{\frac{3}{4}}\rfloor+1\right)^2>k^{\frac{3}{2}}>2m(k+1)=2M$, para k suficientemente grande. Pelo Lema 5.2.1, o sistema acima tem solução não trivial e além disso,

$$\|p(\lambda_1,\lambda_2)\|\leqslant c_1(c_1NU)^{\frac{M}{N-M}}<c_1^2NU$$

pois $N>2M$.

Afirmação 5.2.1 *Se $U\leqslant k^{c_6k}$, c_6 constante, então $\|p(\lambda_1,\lambda_2)\|\leqslant k^{c_5k}$.*

De fato, se $U\leqslant k^{c_6k}$ então

$$\|p(\lambda_1,\lambda_2)\|\leqslant c_1^2NU\leqslant k^k\left(2\lfloor k^{\frac{3}{4}}\rfloor\right)^2k^{c_6k}\leqslant k^{c_5k}\left(c_5=\frac{7}{2}+c_6\right)$$

□

Afirmação 5.2.2 *Temos $U\leqslant k^{c_6k}$, para alguma constante c_6.*

Seja $R(z)=\sum_{l_1=0}^{d}\cdots\sum_{l_n=0}^{d}q(l_1,\cdots,l_n)f_1(z)^{l_1}\cdots f_n(z)^{l_n}$, como $f_i'(z)=\frac{d}{dz}f_i(z)\in K[f_1,\cdots,f_n]$ então $f_i'(z)=p_i(f_1,\cdots,f_n)$ onde p_i é um polinômio em n variáveis com coeficientes em K $(1\leqslant i\leqslant n)$. Provaremos por indução sobre j que

$$R^{(j)}(z)=\sum_{l_1=0}^{d'}\cdots\sum_{l_n=0}^{d'}r(l_1,\cdots,l_n)f_1(z)^{l_1}\cdots f_n(z)^{l_n}$$

onde $d'\leqslant d+j\delta$ e $\delta=max_{\{1\leqslant i\leqslant n\}}\{\partial p_i\}$.

Para $j=1$, temos

$$\begin{aligned}R'(z)&=\frac{d}{dz}\left(\sum_{l_1=0}^{d}\cdots\sum_{l_n=0}^{d}q(l_1,\cdots,l_n)f_1(z)^{l_1}\cdots f_n(z)^{l_n}\right)\\&=\sum_{l_1=0}^{d'}\cdots\sum_{l_n=0}^{d'}r(l_1,\cdots,l_n)f_1(z)^{l_1}\cdots f_n(z)^{l_n}\end{aligned}$$

trocando $f_i^{'}$ por $p_i\left(f_1,\cdots,f_n\right)$. Note que a maior potência de $f_i(z)$ que aparece em cada parcela do somatório $R(z)$ é d, se $\delta = max_{\{1\leqslant i\leqslant n\}}\left\{\partial p_i\right\}$ então a maior potência de $f_i(z)$ em p_i é δ. Portanto as potências de $f_i(z)$ que aparecem em $R'(z)$ não pode ultrapassar $d+\delta$, daí $d'\leqslant d+\delta$. Suponha que

$$R^{(j)}(z)=\sum_{l_1=0}^{d'}\cdots\sum_{l_n=0}^{d'}r\left(l_1,\cdots,l_n\right)f_1(z)^{l_1}\cdots f_n(z)$$

onde $d'\leqslant d+j\delta$. Então,

$$\begin{aligned}R^{(j+1)}(z)=\left(R^{(j)}(z)\right)^{'} &= \frac{d}{dz}\left(\sum_{l_1=0}^{d'}\cdots\sum_{l_n=0}^{d'}r\left(l_1,\cdots,l_n\right)f_1(z)^{l_1}\cdots f_n(z)^{l_n}\right)\\ &= \sum_{l_1=0}^{d''}\cdots\sum_{l_n=0}^{d''}s\left(l_1,\cdots,l_n\right)f_1(z)^{l_1}\cdots f_n(z)^{l_n}\end{aligned}$$

e $d''\leqslant d'+\delta\leqslant(d+j\delta)+\delta=d+(j+1)\delta$. Portanto a indução está completa. Entretanto, podemos multiplicar $q\left(l_1,\cdots,l_n\right)$ por um inteiro positivo que o torne inteiro algébrico com peso no máximo s, então $R^{(j)}$ pode ser multiplicado por um inteiro positivo tal que $r\left(l_1,\cdots,l_n\right)$ torna-se inteiro algébrico com peso no máximo $S=\left(c_7d\right)^j j!s$.

Para terminar a demonstração da afirmação, aplique o resultado acima com $Q=x_1^{\lambda_1}x_2^{\lambda_2}$ com $j\leqslant k$, portanto $s=1$, $d\leqslant L\leqslant k$ e

$$S=\left(c_7d\right)^j j!s\leqslant\left(k^2\right)^k k^k=k^{c_8k}\ \left(c_8=3\right)$$

Considere k suficientemente grande tal que $\left|f_i\left(y_l\right)\right|\leqslant k$, $l_i\leqslant d'\leqslant c_{10}k$ e $l\leqslant m$ então

$$\left|f_1\left(y_l\right)^{l_1}\cdots f_n\left(y_l\right)^{l_n}\right|\leqslant k^{c_{10}k}\cdots k^{c_{10}k}=k^{c_9k}\ \left(c_9=nc_{10}\right)$$

Logo,

$$U\leqslant k^{c_6k}\ \left(c_6=c_8+c_9\right)$$

□

Lema 5.2.3 *Para todo* $R \geqslant 2$ *e* $z \in \mathbb{C}$ *com* $|z| \leqslant R$, *a função* $\phi = (h_1, \cdots h_n)^L \Phi$ *satisfaz*

$$|\phi(z)| < e^{c_{11}(k \log k + LR^\rho)}$$

além disso, para todo j, l *com* $j \geqslant k$ *e* $l \leqslant m$ *tal que* $\Phi^{(i)}(y_l) = 0$ *para* $i < j$, *o número* $\Phi^{(i)}(y_l)$ *é zero ou* $\left|\phi^{(i)}(y_l)\right| \geqslant j^{-c_{12}j}$, c_{12} *constante positiva.*

Demonstração

Para a primeira parte temos que $\|p(\lambda_1, \lambda_2)\| \leqslant k^{c_5 k}$. Para todo $R \geqslant 2$ e $z \in \mathbb{C}$ com $|z| \leqslant R$,

$$max\{|g_i(z)|, |h_i(z)|\} \leqslant e^{R^\rho} \ (1 \leqslant i \leqslant n)$$

Por outro lado,

$$\phi(z) = \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1, \lambda_2) h_1(z)^{L-\lambda_1} h_2(z)^{L-\lambda_2} h_3(z)^L \cdots h_n(z)^L g_1(z)^{\lambda_1} g_2(z)^{\lambda_2}$$

Portanto, para k suficientemente grande,

$$\begin{aligned} |\phi(z)| &\leqslant \|p(\lambda_1, \lambda_2)\| (L+1)^2 \left(e^{R^\rho}\right)^{L-\lambda_1} \left(e^{R^\rho}\right)^{L-\lambda_2} \left(e^{R^\rho}\right)^{L(n-2)} \left(e^{R^\rho}\right)^{\lambda_1+\lambda_2} \leqslant \\ &\leqslant k^{c_5 k} k^k e^{nLR^\rho} = k^{(1+c_5)k} e^{nLR^\rho} = e^{(1+c_5)k \log k + nLR^\rho} \leqslant e^{c_{11}(k \log k + LR^\rho)} \end{aligned}$$

onde $c_{11} = max\{1 + c_5, n\}$.

Para a segunda parte, note que $\Phi^{(j)}(y_l) \in K$. Então $t\Phi^{(j)}(y_l)$ é inteiro algébrico para algum inteiro positivo t. Por outro lado, para k convenientemente grande e $j > k$,

$$\begin{aligned} \|t\Phi^{(j)}(y_l)\| &\leqslant k^k \|\Phi^{(j)}(y_l)\| \leqslant k^k (L+1)^2 \|p(\lambda_1, \lambda_2)\| U \leqslant k^k k^k k^{c_5 k} k^{c_6 k} \\ &= k^{c_{13} k} < j^{c_{13} j} \ (c_{13} = 2 + c_5 + c_6) \end{aligned}$$

Daí,

$$\|\Phi^{(j)}(y_l)\| < j^{c_{13} j}$$

□

Afirmação 5.2.3 *Seja ϕ como acima, então*

$$\phi^{(j)}(y_l) = (h_1(y_l)\cdots h_n(y_l))^L \Phi^{(j)}(y_l).$$

De fato, como $\phi(z) = (h_1(z)\cdots h_n(z))^L \Phi(z)$ então,

$$\begin{aligned}\phi^{(j)}(z) &= \sum_{i=0}^{j}\binom{j}{i}\left[(h_1(z)\cdots h_n(z))^L\right]^{(j-i)}\Phi^{(i)}(z) = \\ &= \sum_{i=0}^{j-1}\binom{j}{i}\left[(h_1(z)\cdots h_n(z))^L\right]^{(j-i)}\Phi^{(i)}(z) + (h_1(z)\cdots h_n(z))^L\Phi^{(j)}(z)\end{aligned}$$

mas $\Phi^{(i)}(y_l) = 0$ para $i < j$, segue-se que

$$\phi^{(j)}(y_l) = (h_1(y_l)\cdots h_n(y_l))^L \Phi^{(j)}(y_l)$$

□

Voltando à demonstração do lema, como y_l não é pólo de $f_i(z)$ então $h_i(y_l) \neq 0$, $i = 1,\cdots,n$ e $l = 1,\cdots,m$, portanto existe k suficientemente grande, com

$$\left|(h_1(y_l)\cdots h_n(y_l))^L\right| > \frac{1}{k^k} > \frac{1}{j^j} \tag{5.2}$$

Note que $t\Phi^{(j)}(y_l)$ é inteiro algébrico e então $N\left(t\Phi^{(j)}(y_l)\right)$ é inteiro, daí $\left|N\left(t\Phi^{(j)}(y_l)\right)\right| = 0$ ou $\left|N\left(t\Phi^{(j)}(y_l)\right)\right| \geqslant 1$.

Caso 1. $\left|N\left(t\Phi^{(j)}(y_l)\right)\right| = 0$.

Portanto $\Phi^{(j)}(y_l) = 0$ (já que $t \neq 0$). Nesse caso, pela Afirmação 5.2.3, $\phi^{(j)}(y_l) = 0$.

Caso 2. $|N(t\Phi^{(j)})| \geqslant 1$

Temos,

$$1 \leqslant \left|N\left(t\Phi^{(j)}(y_l)\right)\right| \leqslant |N(t)|\left|N\left(\Phi^{(j)}(y_l)\right)\right| < j^j\left|\Phi^{(j)}(y_l)\right| j^{c_{13}j}$$

isto é,

$$|\Phi^{(j)}(y_l)| > j^{-(1+c_{13})j} \tag{5.3}$$

onde c_{13} é o número de conjugados de $\Phi^{(j)}(y_l)$.

Multiplicando as desigualdades (5.2) e (5.3), obtemos:

$$\left|\phi^{(j)}(y_l)\right| > j^{-c_{12}j},\ c_{12} = 2 + c_{13}$$

□

Lema 5.2.4 *Temos que*

$$\Phi^{(j)}(y_l) = 0,\ j \in \mathbb{N}\ e\ 1 \leqslant l \leqslant m.$$

Demonstração

A demonstração será feita por indução sobre j. O caso $j = 1$ segue-se do Lema 5.2.2. Suponha que

$$\Phi^{(i)}(y_l) = 0,\ (0 \leqslant i < j, 1 \leqslant l \leqslant m) \tag{5.4}$$

Para completar a prova basta mostrar que a igualdade (5.4) vale para $i = j$. Pelo Lema 5.2.2, podemos supor $j > k$, denote $A = max_{1 \leqslant l \leqslant m} |y_l|$ e tome k suficientemente grande tal que $\frac{1}{2} j^{\frac{1}{4\rho}} > A$. Considere o círculo C, no plano complexo, centrado na origem e de raio $R = j^{\frac{1}{4\rho}}$. Defina

$$F(z) = (z - y_1) \cdots (z - y_m).$$

Afirmação 5.2.4 *Para $l \in \{1, \cdots, m\}$, temos*

$$\frac{\phi^{(j)}(y_l)}{(F'(y_l))^j} = \frac{j!}{2\pi i} \int_C \frac{\phi(z)}{(z - y_l)(F(z))^j} dz \tag{5.5}$$

Note que $j^{\frac{1}{4\rho}} = R > A \geqslant |y_s|$, $1 \leqslant s \leqslant m$, logo os pontos $y_1, \cdots, y_m$ pertencem ao interior do círculo C. Tome $l \in \{1, \cdots, m\}$ e veja que $f(z) = \frac{\phi(z)}{(z - y_l)(F(z))^j}$ tem pólos y_s ($1 \leqslant s \leqslant m$ e $s \neq l$) de ordem j e y_l de ordem $j + 1$. Pelo Teorema de Resíduos;

$$\int_C \frac{\phi(z)}{(z - y_l)(F(z))^j} dz = \sum_{s=1}^{m} \eta(C, y_s)\, Res(f, y_s)$$

Parametrizando C, por $\gamma(t) = (R\cos t, R\sin t)$, $0 \leqslant t \leqslant 2\pi$, então $\eta(C, y_s) = 1$. Daí,

$$\int_C \frac{\phi(z)}{(z-y_l)\,(F(z))^j} dz = \sum_{s=1}^{m} Res\,(f, y_s) \tag{5.6}$$

Observe que para y_s $(1 \leqslant s \leqslant m \text{ e } s \neq l)$,

$$Res\,(f, y_s) = \frac{1}{(j-1)!} g^{(j-1)}\,(y_s)\,, onde\ g(z) = (z-y_s)^j\, f(z) \tag{5.7}$$

então

$$g(z) = (z-y_s)^j \frac{\phi(z)}{(z-y_l)\,(F(z))^j} = \phi(z) h(z)^{-1}$$

onde $h(z) = (z-y_1)^j \cdots (z-y_l)^{j+1} \cdots \widehat{(z-y_s)} \cdots (z-y_m)$.

Daí,

$$g^{(j-1)}\,(z-y_l) = \sum_{i=0}^{j-1} \binom{j-1}{i} \phi^{(i)}\,(z-y_l)\left(\left(h\,(y_l)\right)^{-1}\right)^{j-1} = 0$$

pois $\phi^{(i)}\,(y_l) = 0$ para $i < j$. Substituindo em (5.7), obtemos

$$Res\,(f, y_s) = 0\ (1 \leqslant s \leqslant m \text{ e } s \neq l)$$

Por outro lado, $Res\,(f, y_l) = \dfrac{1}{j!}\psi^{(j)}\,(y_l)$, onde

$$\psi(z) = (z-y_l)^{j+1}\, f(z) \tag{5.8}$$

Então,

$$\psi(z) = \phi(z) h_1(z)^{-1}$$

onde $h_1(z) = (z-y_1)^j \cdots \widehat{(z-y_l)} \cdots (z-y_m)^j$.

Daí,

$$\psi^{(j)}\,(y_l) = \sum_{i=0}^{j} \binom{j}{i} \phi^{(i)}\,(y_l)\left[\left(h_1\,(y_l)\right)^{-1}\right]^{j-1} = \phi^{(i)}\,(y_l)\, h_1\,(y_l)^{-1}$$

pois $\phi^{(i)}(y_l) = 0$ para $i < j$. Agora observe que $h_1(y_l) = F'(y_l)^j$. Portanto, substituindo em (5.8),

$$Res(f, y_l) = \frac{1}{j!} \cdot \frac{\phi^{(i)}(y_l)}{F'(y_l)^j}$$

provando assim a Afirmação 5.2.4.

□

Faremos agora algumas majorações:

M1) $|z - y_l| > \frac{1}{2}R$, $1 \leqslant l \leqslant m$, $z \in \mathbb{C}$.

$|z - y_l| \geqslant |z| - |y_l| \geqslant R - A > R - \frac{1}{2}R = \frac{1}{2}R$

M2) Se $z \in \mathbb{C}$ então $|F(z)| > j^{\frac{m}{8p}}$.

$|F(z)| = |z - y_1| \cdots |z - y_m| > \left(\frac{1}{2}R\right)^m = \left(\frac{1}{2}j^{\frac{1}{4p}}\right)^m > j^{\frac{m}{8p}}$ para k suficientemente grande.

M3) $LR^p < j$

$LR^p = \lfloor k^{\frac{3}{4}} \rfloor \left(j^{\frac{1}{4p}}\right)^p \leqslant k^{\frac{3}{4}} j^{\frac{1}{4}} < j^{\frac{3}{4}} \cdot j^{\frac{1}{4}} = j$.

M4) $\phi(z) < j^{c_{14}j}$, para alguma constante c_{14}.

Pelo Lema 5.2.3, temos

$$|\phi(z)| < e^{c_{11}(k \log k + LR^p)} < e^{c_{11}(j \log j + j)} \leqslant e^{c_{11}(2j \log j)} = e^{\log j^{2c_{11}j}}$$

onde $c_{14} = 2c_{11}$ e $k > e$.

M5) $|F'(y_l)| < j$ para k suficientemente grande.

$F'(z) = \sum_{l=1}^{m} (z - y_1) \cdots \widehat{(z - y_l)} \cdots (z - y_m)$. Tome k suficientemente grande, tal que $k > \sum_{l=1}^{m} |y_l - y_1| \cdots \widehat{|y_l - y_l|} \cdots |y_l - y_m|$. Portanto, $|F'(y_l)| < k < j$.

Usando as desigualdades M1, M2 e M4 em (5.5),

$$\frac{\left|\phi^{(j)}(y_l)\right|}{\left|F'(y_l)^j\right|} = \frac{j!}{2\pi} \left| \int_C \frac{\phi(z)}{(z - y_l) F(z)^j} dz \right| \leqslant \frac{j!}{2\pi} \cdot \frac{j^{c_{14}j} \cdot 2\pi R \cdot 2}{R j^{\frac{m}{8p}j}} \leqslant j^{2j} \cdot j^{\left(c_{14} - \frac{m}{8p}\right)j} \tag{5.9}$$

Por outro lado, usando M5:

$$\frac{\left|\phi^{(j)}(y_l)\right|}{\left|F'(y_l)^j\right|} > \frac{\left|\phi^{(j)}(y_l)\right|}{j^j} \tag{5.10}$$

Combinando (5.9) e (5.10) obtém-se:

$$\left|\phi^{(j)}(y_l)\right| < j^{c_{15}j-\frac{m}{8\rho}j}, \text{ onde } c_{15} = 3 + c_{14}$$

Supondo que o número m é arbitrário, tome $m > 8\rho(c_{12} + c_{15})$. Então

$$\left|\phi^{(j)}(y_l)\right| < j^{c_{15}j-\frac{m}{8\rho}j} < j^{c_{15}j-(c_{12}+c_{15})j} = j^{-c_{12}j}$$

Pelo Lema 5.2.3, $\phi^{(j)}(y_l) = 0$.

□

Como $\phi^{(j)}(y_l) = (h_1(y_l), \cdots h_n(y_l))\,\Phi^{(j)}(y_l)$. Assim, por indução, concluímos que Φ e todas suas derivadas se anulam em $y_1, \cdots, y_n$. Portanto, $\Phi \equiv 0$, conseqüentemente $f_1(z)$ e $f_2(z)$ são algebricamente dependentes, contradizendo uma hipótese do teorema. Segue-se que $m < 8\rho(c_{12} + c_{15})$ e daí $y_1, y_2, \cdots$ é finita.

□

Alguns resultados importantes seguem-se imediatamente do Teorema 5.2.1.

Corolário 5.2.1 *(**Teorema de Lindemann**) Se α é um número algébrico não nulo, então e^α é transcendente.*

Demonstração

Se $\alpha \in \mathbb{Z}$ o resultado é trivial, considere então $\alpha \in \mathbb{A} - \mathbb{Z}$. Suponha que e^α é algébrico. Considere $K = \mathbb{Q}(\alpha, e^\alpha)$, $f(z) = z$, $g(z) = e^z$ funções inteiras (portanto meromorfas) de ordem finita 1, já que para todo $R \geqslant 2$ e $|z| \leqslant R$;

$$|z| \leqslant e^{|z|} \leqslant e^R \text{ e } |e^z| \leqslant e^{|z|} \leqslant e^R$$

Claramente a derivada mapeia $K[f, g]$ em si mesmo.

Afirmação 5.2.5 *Fixe $n \in \mathbb{N}$. Se $a_k \in K - \{0\}$, $k = 1, \ldots n$ e $0 \leqslant i_1 < \cdots < i_n$, então*

$$\sum_{k=1}^{n} a_k e^{i_k} \neq 0.$$

A demonstração da Afirmação 5.2.5 será feita por indução sobre n. Para $n = 1$ é trivial. Suponha que a afirmação é válida para $1 \leqslant k < n$ e que existem $c_1, \cdots, c_n$, não nulos, tais que

$$\sum_{k=1}^{n} c_k e^{jk} = 0,\ j_1 < j_2 < \cdots < j_n.$$

Então

$$0 = e^{j_1}\left(c_1 + c_2 e^{m_2} + \cdots + c_m e^{m_n}\right), \text{ onde } m_i = j_i - j_1$$

Como $e^{j_1} \neq 0$ então $(c_1 + c_2 e^{m_2} + \cdots + c_m e^{m_n}) = 0$, contradizendo a hipótese de indução. Segue-se então a veracidade da nossa afirmação.

Voltando a demonstração do Corolário 5.2.1, suponha que exista um polinômio

$$p(x, y) = \sum_{s=1}^{n}\sum_{k=1}^{m} a_{i_k j_s} x^{i_k} y^{j_s} \in K[x, y] - \{0\} \tag{5.11}$$

tal que $p(f, g) = 0$.

Podemos supor, sem perda de generalidade, que $a_{i_k j_s} \neq 0$, para todos $k = \{1, \cdots, m\}$ e $s = \{1, \cdots, n\}$.

Substituindo f e g em (6.2.11), obtemos:

$$0 = \sum_{s=1}^{n}\sum_{k=1}^{m} a_{i_k j_s} z^{i_k} e^{j_s z}\ \forall\, z \in \mathbb{C} \tag{5.12}$$

Faça $z = 1$ em (6.2.12), então

$$0 = \sum_{s=1}^{n}\sum_{k=1}^{m} a_{i_k j_s} e^{j_s} = \sum_{s=1}^{n} c_s e^{j_s}, \text{ onde } c_s = \sum_{s=1}^{m} a_{i_k j_s}\ (1 \leqslant s \leqslant n)$$

o que contradiz a Afirmação 5.2.5. Portanto f e g são algebricamente independentes. Considere $z_k = \alpha k$ $(k \geqslant 1)$ seqüência infinita de números complexos distintos. Para esses números temos:

$$f(z_k) = \alpha k \in K \text{ e } g(z_k) = e^{\alpha k} = (e^{\alpha})^k \in K \ \forall k \geqslant 1$$

contradizendo o Teorema 5.2.1. Portanto e^{α} é transcendente se $\alpha \in \mathbb{A} - \{0\}$.

□

Corolário 5.2.2 *(**Teorema de Gelfond-Schneider**) Se α é um número algébrico ($\neq 0$ e 1) e β é um número algébrico não racional, então α^{β} é transcendente.*

Demonstração

Suponha que α^{β} é algébrico. Considere $K = \mathbb{Q}(\alpha, \beta, \alpha^{\beta})$ e proceda analogamente à demonstração do Corolário 5.2.1 com $f(z) = e^z$, $g(z) = e^{\beta z}$ e $z_k = k \log \alpha \, (k = 1, 2, 3, \cdots)$.

□

Antes de enunciar o próximo corolário, vamos à algumas definições e proposições. Fixemos $\lambda_1, \lambda_2 \in \mathbb{C} - \{0\}$ tais que $\dfrac{\lambda_2}{\lambda_1} \notin \mathbb{R}$ e consideremos o conjunto $\Omega = \lambda_1\mathbb{Z} + \lambda_2\mathbb{Z}$.

Definição 5.2.1 *A função $\wp$ de Weierstrass, ver [1], é definida pela série:*

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Omega^*} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right) \tag{5.13}$$

No somatório acima, a notação Ω^* designa o conjunto $\Omega - \{0\}$.

Definição 5.2.2 *Seja f uma função meromorfa em $\mathbb{C}$, com conjunto de pólos Γ. Dizemos que $T \in \mathbb{C}$ é período de f se para todo $z \in \mathbb{C} - T$, temos $z + T \in \mathbb{C} - \Gamma$ e além disso, $f(z+T) = f(z)$. Denotaremos o conjunto de todos os períodos de f por $per(f)$.*

Proposição 5.2.1 *A série em (5.13) converge uniformemente nas partes compactas de $\mathbb{C}$, para uma função duplamente periódica $\wp$, tal que*

$$per(\wp) = \Omega$$

Proposição 5.2.2 *(E.D.O. de $\wp$) A função $\wp$ de Weierstrass satisfaz a seguinte equação diferencial ordinária:*

$$y'^2 = 4y^3 - g_2 y - g_3 \tag{5.14}$$

onde $g_2 = 60 \sum_{w \in \Omega^*} \frac{1}{w^4}$ *e* $g_3 = 140 \sum_{w \in \Omega^*} \frac{1}{w^6}$

Proposição 5.2.3 *(Fórmulas de Adição) A função $\wp$ de Weierstrass satisfaz:*

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 \tag{5.15}$$

As demonstrações desses fatos podem ser encontradas em [12], p. 340-344.

□

O próximo corolário é devido à Schneider.

Corolário 5.2.3 *Se g_2, g_3 são algébricos, então para todo algébrico $\alpha \neq 0$, $\wp(\alpha)$ é transcendente.*

Demonstração

Análoga às demonstrações dos corolários 5.2.1 e 5.2.2, com
$K = \mathbb{Q}(g_2, g_3, \alpha, \wp(\alpha), \wp'(\alpha))$, $f_1(z) = z$, $f_2(z) = \wp(\alpha z)$, $f_3(z) = \wp'(\alpha z)$,
$z_k = 2^k$ e usando as proposições 5.2.2 e 5.2.3.

para mais detalhes e outra demonstração do Teorema 5.2.1, veja os bons livros de Serge Lang [9] e [10].

□

Capítulo 6

Forma Linear em Logaritmos

O Corolário 4.2.2 do Teorema de Gelfond-Schneider afirma que para todos números algébricos não nulos α_1, α_2, β_1, β_2, com $\log \alpha_1$, $\log \alpha_2$ linearmente independentes sobre $\mathbb{Q}$, então

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

É natural conjecturar um teorema análogo para uma quantidade arbitrária de logaritmos de números algébricos. Esta conjectura foi provada em 1966 por Alan Baker e sua demonstração será detalhada neste capítulo.

6.1 Notações

Seja α um número algébrico. Sabe-se que o polinômio minimal de α é mônico, digamos

$$p_{\alpha,\mathbb{Q}}(x) = x^n + a_1 x^{n-1} + \cdots + a_n,\ a_i \in \mathbb{Q},\ (1 \leqslant i \leqslant n)$$

Como $a_i \in \mathbb{Q}$ então $a_i = \dfrac{p_i}{q_i}$, onde p_i, q_i são números inteiros, $1 \leqslant i \leqslant n$. Defina $F_{\alpha,\mathbb{Q}}$ como

$$F_{\alpha,\mathbb{Q}}(x) = a p_{\alpha,\mathbb{Q}} \in \mathbb{Z}[x] \tag{6.1}$$

onde $a = q_1 \cdots q_n$. Como $p_{\alpha,\mathbb{Q}}$ é mônico, o coeficiente líder de $F_{\alpha,\mathbb{Q}}$ é a.

Proposição 6.1.1 *Se α é um número algébrico satisfazendo*

$$A_0\alpha^d + A_1\alpha^{d-1} + \cdots + A_d = 0$$

onde $A_0, \cdots, A_d$ são números inteiros com valor absoluto no máximo A, então para todo inteiro j não negativo, vale

$$(A_0\alpha)^j = A_0^{(j)} + A_1^{(j)}\alpha + \cdots + A_{d-1}^{(j)}\alpha^{d-1} \tag{6.2}$$

para alguns inteiros $A_m^{(j)}$ com valor absoluto no máximo $(2A)^j$.

Demonstração

Para $j < d$ a representação (6.2) é clara. Para $j \geqslant d$ usaremos indução sobre j.

Para $j = d$, temos

$$\begin{aligned}(A_0\alpha)^d &= A_0^{d-1}(A_0\alpha^d) = A_0^{d-1}(-A_d - \cdots - A_1\alpha^{d-1}) = \\ &= A_0^{(d)} + A_1^{(d)}\alpha + \cdots + A_{d-1}^{(d)}\alpha^{d-1}\end{aligned}$$

onde $A_m^{(d)} = -A_0^{d-1}A_{d-m}$.

Suponha que $(A_0\alpha)^j = A_0^{(j)} + A_1^{(j)}\alpha + \cdots + A_{d-1}^{(j)}\alpha^{d-1}$. Portanto,

$$\begin{aligned}(A_0\alpha)^{j+1} &= (A_0\alpha)(A_0\alpha^j) = (A_0\alpha)(A_0^{(j)} + A_1^{(j)}\alpha + \cdots + A_{d-1}^{(j)}\alpha^{d-1}) = \\ &= A_0A_0^{(j)}\alpha + A_0A_1^{(j)}\alpha^2 + \cdots + A_{d-1}^{(j)}A_0\alpha^d = \\ &= A_0A_0^{(j)}\alpha + A_0A_1^{(j)}\alpha^2 + \cdots + A_{d-1}^{(j)}(-A_1\alpha^{d-1} - \cdots - A_d) = \\ &= A_0^{(j+1)} + A_1^{(j+1)}\alpha + \cdots + A_{d-1}^{(j+1)}\alpha^{d-1}\end{aligned}$$

onde $A_m^{(j+1)} = A_0A_{m-1}^{(j)} - A_{d-1}^{(j)}A_{d-m}$.

Portanto, além de demonstrar a primeira parte da proposição, mostramos que vale a seguinte relação de recorrência:

$$A_m^{(j)} = A_0A_{m-1}^{(j-1)} - A_{d-m}A_{d-1}^{(j-1)}\ (0 \leqslant m < d,\ j \geqslant d),\ A_{-1}^{j-1} = 0 \tag{6.3}$$

Demonstraremos a segunda parte também usando indução sobre j.
Para $j = 1$, por (6.3)

$$|A_m^{(1)}| = |A_0 A_{m-1} A^{(0)} - A_{d-m} A_{d-1}^{(0)}| \leqslant 2A, \text{ já que } A_m^{(0)} = 0$$

Suponha que $|A_m^{(j)}| \leqslant (2A)^j$, usando novamente (6.3), obtemos:

$$\begin{aligned} |A_m^{(j+1)}| &= |A_0 A_{m-1}^{(j)} - A_{d-m} A_{d-1}^{(j)}| \leqslant |A_0|(2A)^j + |A_{d-m}|(2A)^j \leqslant \\ &\leqslant A(2A)^j + A(2A)^j = (2A)^{j+1} \end{aligned}$$

□

Seja d o máximo dos graus de $\alpha_1, \cdots, \alpha_n, \beta_0, \cdots, \beta_{n-1}$ e sejam $a_1, \cdots, a_n, b_0, \cdots, b_{n-1}$ os coeficientes líderes de

$$F_{\alpha_1,\mathbb{Q}}(x), \cdots, F_{\alpha_n,\mathbb{Q}}(x), F_{\beta_0,\mathbb{Q}}(x), \cdots, F_{\beta_{n-1},\mathbb{Q}}(x)$$

respectivamente, então pela proposição anterior

$$(a_r\alpha_r)^j = \sum_{s=0}^{d-1} a_{rs}^{(j)} \alpha_r^s, \; (b_r\beta_r)^j = \sum_{t=0}^{d-1} b_{rt}^{(j)} \beta_r^t \tag{6.4}$$

onde $a_{rs}^{(j)}$, $b_{rt}^{(j)}$ são números inteiros com valor absoluto no máximo c_1^j e $c_3 = max\{a_1, \cdots, a_n, b_0, \cdots, b_{n-1}\}$.

Para facilitar a notação, escreveremos

$$f_{m_0,\cdots,m_{n-1}}(z_0, \cdots, z_{n-1}) = \left(\frac{\partial}{\partial z_0}\right)^{m_0} \cdots \left(\frac{\partial}{\partial z_{n-1}}\right)^{m_{n-1}} f(z_0, \cdots, z_{n-1})$$

onde f é uma função inteira e $m_0, \cdots, m_{n-1}$ são inteiros não negativos.

6.2 O Teorema de Baker

Teorema 6.2.1 *(**Baker**) Sejam $\alpha_1, \cdots, \alpha_n$ números algébricos não nulos tais que $\log \alpha_1, \cdots, \log \alpha_n$ são linearmente independentes sobre $\mathbb{Q}$. Então $1, \log \alpha_1, \cdots, \log \alpha_n$ são linearmente independentes sobre o corpo de todos os números algébricos.*

Demonstração

Suponha que o teorema é falso, então existem números algébricos $\beta_0, \beta_1, \cdots, \beta_n$, não todos nulos, tais que

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n = 0 \tag{6.5}$$

Queremos então obter uma contradição. Como, pelo menos, um dos $\beta_1, \cdots, \beta_n$ é não nulo, podemos supor sem perda de generalidade que $\beta_n \neq 0$. Note que a equação (6.5) continua válida para $\beta'_j = \dfrac{-\beta_j}{\beta_n}$ no lugar de β_j, podemos supor que $\beta_n = -1$. Daí

$$e^{\beta_0} \alpha_1^{\beta_1} \cdots \alpha_{n-1}^{\beta_{n-1}} = \alpha_n \tag{6.6}$$

Denotaremos por $c, c_1, c_2, \cdots$ constantes positivas que dependem apenas dos $\alpha's$, $\beta's$ e $\log \alpha's$ e por h um inteiro positivo, suficientemente grande, que excede quaisquer das constantes c como acima.

Lema 6.2.1 *Sejam M, N inteiros com $N > M > 0$ e se*

$$u_{ij} \, (1 \leqslant i \leqslant M, \, 1 \leqslant j \leqslant N)$$

denota inteiros com valor absoluto no máximo $U(\geqslant 1)$. Então existem inteiros $x_1, \cdots, x_N$ não todos nulos, com valor absoluto no máximo $(NU)^{\frac{M}{N-M}}$ tais que

$$\sum_{j=1}^{N} u_{ij} x_j = 0, \; 1 \leqslant i \leqslant M$$

Demonstração

Análoga à demonstração do Lema 4.1.1 da Seção 4.1.

□

Lema 6.2.2 *Existem inteiros $p(\lambda_0, \cdots, \lambda_n)$, não todos nulos, com valor absoluto no máximo e^{h^3}, tal que a função*

$$\Phi(z_0, \cdots, z_{n-1}) = \sum_{\lambda_0=0}^{L} \cdots \sum_{\lambda_n=0}^{L} p(\lambda_0, \cdots, \lambda_n) z_0^{\lambda_0} e^{\lambda_n \beta_0 z_0} \alpha_1^{\gamma_1 z} \cdots \alpha_{n-1}^{\gamma_{n-1} z_{n-1}},$$

onde $\gamma_r = \lambda_r + \lambda_n\beta_r\,(1 \leqslant r < n)$ *e* $L = \lfloor h^{2-\frac{1}{4n}} \rfloor$, *satisfaz*

$$\Phi_{m_0,\cdots,m_{n-1}}(l,\cdots,l) = 0 \tag{6.7}$$

para todos os inteiros l *com* $1 \leqslant l \leqslant h$ *e todos inteiros não negativos* $m_0,\cdots,m_{n-1}$ *com* $m_0+\cdots+m_{n-1} \leqslant h^2$.

Demonstração

Usando (6.6) temos que

$$\begin{aligned} e^{\lambda_n\beta_0 l}\alpha_1^{\gamma_1 l}\cdots\alpha_{n-1}^{\gamma_{n-1}l} &= e^{\lambda_n\beta_0 l}\alpha_1^{(\lambda_1+\lambda_n\beta_1)l}\cdots\alpha_{n-1}^{(\lambda_{n-1}+\lambda_n\beta_{n-1})l} \\ &= \alpha_1^{\lambda_1 l}\cdots\alpha_{n-1}^{\lambda_{n-1}l}(e^{\beta_0}\alpha_1^{\beta_1}\cdots\alpha_{n-1}^{\beta_{n-1}})^{\lambda_n l} \\ &= \alpha_1^{\lambda_1 l}\cdots\alpha_{n-1}^{\lambda_{n-1}l}\alpha_n^{\lambda_n l} \end{aligned}$$

então

$$\begin{aligned} \Phi_{m_0,\cdots,m_{n-1}}(l,\cdots,l) &= P\sum_{\lambda_0=0}^{L}\cdots\sum_{\lambda_n=0}^{L} p(\lambda_0,\cdots,\lambda_n)q(\lambda_0,\lambda_n,l)\cdot \\ &\cdot\ \alpha_1^{\lambda_1 l}\cdots\alpha_n^{\lambda_n l}\gamma_1^{m_1}\cdots\gamma_{n-1}^{m_{n-1}} \end{aligned}$$

onde $P = (\log\alpha_1)^{m_1}\cdots(\log\alpha_{n-1})^{m_{n-1}} \neq 0$, já que, $\log\alpha_1,\cdots,\log\alpha_n$ são linearmente independentes sobre $\mathbb{Q}$ e

$$q(\lambda_0,\lambda_n,z) = \sum_{\mu_0=0}^{m_0}\binom{m_0}{\mu_0}\lambda_0(\lambda_0-1)\cdots(\lambda_0-\mu_0+1)(\lambda_n\beta_0)^{m_0-\mu_0}z^{\lambda_0-\mu_0}.$$

Portanto é suficiente determinar $p(\lambda_0,\cdots,\lambda_n)$ tal que

$$\sum_{\lambda_0=0}^{L}\cdots\sum_{\lambda_n=0}^{L} p(\lambda_0,\cdots,\lambda_n)q(\lambda_0,\lambda_n,l)\alpha_1^{\lambda_1 l}\cdots\alpha_n^{\lambda_n l}\gamma_1^{m_1}\cdots\gamma_{n-1}^{m_{n-1}} = 0 \tag{6.8}$$

Multiplique (6.8) por

$$P' = (a_1\cdots a_n)^{Ll}b_0^{m_0}\cdots b_{n-1}^{m_{n-1}} \tag{6.9}$$

Note que

$$\gamma_r^{m_r} = \sum_{\mu_r=0}^{m_r} \binom{m_r}{\mu_r} \lambda_r^{m_r-\mu_r} (\lambda_n\beta_r)^{\mu_r}$$

e substituindo de (6.4) as potências de $a_r\alpha_r$ e $b_r\beta_r$, como resultado, obtemos

$$\sum_{s_1=0}^{d-1} \cdots \sum_{s_n=0}^{d-1} \sum_{t_0=0}^{d-1} \cdots \sum_{t_{n-1}=0}^{d-1} A(s,t)\alpha_1^{s_1}\cdots\alpha_n^{s_n}\beta_1^{t_0}\cdots\beta_{n-1}^{t_{n-1}} = 0$$

onde

$$A(s,t) = \sum_{\lambda_0=0}^{L} \cdots \sum_{\lambda_n=0}^{L} \sum_{\mu_0}^{m_0} \cdots \sum_{\mu_{n-1}=0}^{m_{n-1}} p(\lambda_0,\cdots,\lambda_n) q' q'' q''' \tag{6.10}$$

e q', q'', q''' são fixados por

$q' = \prod_{r=1}^{n} \{a_r^{(L-\lambda_r)l} a_{r,s_r}^{(\lambda_r l)}\}$;

$q'' = \prod_{r=1}^{n-1} \left\{ \binom{m_r}{\mu_r} (b_r\lambda_r)^{m_r-\mu_r} \lambda_n^{\mu_r} b_{r,t_r}^{(\mu_r)} \right\}$;

$q''' = \binom{m_0}{\mu_0} \lambda_0(\lambda_0-1)\cdots(\lambda_0-\mu_0+1)\lambda_n^{m_0-\mu_0} b_n^{\mu_0} l^{\lambda_0-\mu_0} b_{0,t_0}^{(m_0-\mu_0)}$.

Assim (6.7) será satisfeita se as d^{2n} equações $A(s,t) = 0$ são válidas. Observando (6.10) percebamos que $A(s,t)$ representa equações lineares em $p(\lambda_0,\cdots,\lambda_n)$ com coeficientes inteiros.

Como $l \leqslant h$ e $2^{m_r} = (1+1)^{m_r} = \sum_{\mu_r=0}^{m_r} \binom{m_r}{\mu_r} \geqslant \binom{m_r}{\mu_r}$, temos

$$|q'| \leqslant \prod_{r=1}^{n} a_r^{(L-\lambda_r)l} c_1^{\lambda_r l} \leqslant \prod_{r=1}^{n} c_3^{(L-\lambda_r)l} c_1^{\lambda_r l} \leqslant \prod_{r=1}^{n} c_3^{Ll} c_1^{Ll} \leqslant c_2^{Lh},\ (c_2 = (c_1c_3)^n)$$

$$|q''| \leqslant \prod_{r=1}^{n-1} 2^{m_r} c_1^{m_r} c_3^{m_r} L^{m_r} = \prod_{r=1}^{n-1} (c_5 L)^{m_r},\ (c_5 = 2c_1c_3)$$

$$\begin{aligned} |q'''| &\leqslant 2^{m_0}\lambda_0^{\mu_0}\lambda_n^{m_0-\mu_0} b_n^{\mu_0} l^{\lambda_0-\mu_0} c_1^{m_0-\mu_0} = 2^{m_0}(\lambda_0 b_n)^{\mu_0}(c_1\lambda_n)^{m_0-\mu_0} l^{\lambda_0-\mu_0} \leqslant \\ &\leqslant (2\lambda_0 b_n c_1 L)^{m_0 l^{\lambda_0}} \leqslant (c_6 L)^{m_0} h^L,\ (c_6 = 2\lambda_0 b_n c_1) \end{aligned}$$

Considere $c_7 = \{c_5, c_6\}$, então

$$|q''| \leqslant \prod_{r=1}^{n-1}(c_7 L)^{m_r} \text{ e } |q'''| \leqslant (c_7 L)^{m_0} h^L$$

Perceba que $(m_0+1)\cdots(m_{n-1}+1) \leqslant 2^{m_o+\cdots+m_{n-1}} \leqslant 2^{h^2}$. O coeficiente de $p(\lambda_0, \cdots, \lambda_r)$ em $A(s,t)$ é $\sum_{\mu_0=0}^{m_0} \cdots \sum_{\mu_{n-1}=0}^{m_{n-1}} q'q''q'''$ e

$$U = \left| \sum_{\mu_0=0}^{m_0} \cdots \sum_{\mu_{n-1}=0}^{m_{n-1}} q'q''q''' \right| \leqslant 2^{h^2}|q'||q''||q'''| \leqslant 2^{h^2} c_2^{Lh} (c_7 L)^{h^2} h^L \leqslant (2c_7 L)^{h^2} c_4^{L^h}$$

onde $c_4 = ec_2$.

Por outro lado, existem no máximo $h(h^2+1)^n$ conjuntos distintos de inteiros $l, m_0, \cdots, m_{n-1}$ satisfazendo as hipóteses do teorema e, portanto existem $M \leqslant d^{2n}h(h^2+1)^n$ equações $A(s,t) = 0$. Entretanto, existem $N = (L+1)^{n+1}$ indeterminadas $p(\lambda_0, \cdots, \lambda_n)$ e vale

$$\begin{aligned} N &= (L+1)^{n+1} = (\lfloor h^{2-\frac{1}{4n}} \rfloor + 1)^{n+1} > (h^{2-\frac{1}{4n}})^{n+1} = \\ &= h^{2(n+1)-\frac{1}{4n}(n+1)} \geqslant h^{2n+\frac{3}{2}} > 2d^{2n}h(h^2+1)^n \geqslant 2M \end{aligned}$$

para h suficientemente grande. Assim, pelo Lema 6.2.1, as equações podem ser resolvidas não trivialmente e os inteiros $p(\lambda_0, \cdots, \lambda_n)$ podem ser escolhidos com valor absoluto no máximo

$$(NU)^{\frac{M}{N-M}} \leqslant NU \leqslant h^{2n+2}(2c_3 L)^{h^2} c_4^{Lh} \leqslant e^{h^3}$$

para h suficientemente grande.

□

Lema 6.2.3 *Sejam $m_0, \cdots, m_{n-1}$ inteiros não negativos com*

$$m_0 + \cdots + m_{n-1} \leqslant h^2$$

e

$$f(z) = \Phi_{m_0,\cdots,m_{n-1}}(z, \cdots, z) \tag{6.11}$$

Então:

(i) *Para todo* z, $|f(z)| \leqslant c_{12}^{h^3+L|z|}$;

(ii) *Se* l *é inteiro positivo, então* $f(l) = 0$ *ou* $|f(l)| > c_{15}^{-h^3-Ll}$

Demonstração

(i) Temos que

$$f(z) = P \sum_{\lambda_0=0}^{L} \cdots \sum_{\lambda_n=0}^{L} p(\lambda_0, \cdots, \lambda_n) q(\lambda_0, \lambda_n, z) \alpha_1^{\lambda_1 z} \cdots \alpha_n^{\lambda_n z} \gamma_1^{m_1} \cdots \gamma_{n-1}^{m_{n-1}}$$

onde $q(\lambda_0, \lambda_n, z)$ e P são definidos no Lema 6.2.2. Seja
$c_8 = max\{\alpha_1, \cdots, \alpha_n, \beta_0, \cdots, \beta_{n-1}\}$ e $c_9 = max\{\log \alpha_1, \cdots, \log \alpha_{n-1}, \log \alpha_n\}$.

Seguem-se algumas majorações importantes:

M1)

$$|q(\lambda_0, \lambda_n, z)| \leqslant L^{\mu_0} (L c_8)^{m_0 - \mu_0} (|z| + 1)^L \sum_{\mu_0=0}^{m_0} \binom{m_0}{\mu_0} = (2c_8 L)^{m_0} (|z| + 1)^L$$

M2)

$|\alpha_1^{\lambda_1 z} \cdots \alpha_n^{\lambda_n z}| \leqslant c_8^{L|z|}$

M3)

$$\begin{aligned} |P\gamma_1^{m_1} \cdots \gamma_{n-1}^{m_{n-1}}| &= |(\log \alpha_1)^{m_1} \cdots (\log \alpha_{n-1})^{m_{n-1}} \gamma_1^{m_1} \cdots \gamma_{n-1}^{m_{n-1}}| \leqslant \\ &\leqslant c_9^{m_1} \cdots c_9^{m_{n-1}} L^{m_1} \cdots L^{m_{n-1}} \\ &= (c_9 L)^{m_1 + \cdots + m_{n-1}} \end{aligned}$$

Observe também que $L \leqslant h^2$, $m_0 + \cdots + m_{n-1} \leqslant h^2$ e $|p(\lambda_0, \cdots, \lambda_n)| \leqslant e^{h^3}$. Portanto, se $c_{10} = max\{2c_7, c_9\}$.

$$\begin{aligned} |f(z)| &\leqslant (L+1)^{n+1} e^{h^3} (2c_7 L)^{m_0} (|z| + 1)^L (c_9 L)^{m_1 + \cdots + m_{n-1}} c_8^{L|z|} \\ &\leqslant (h^2+1)^{n+1} e^{h^3} (c_{10} L)^{h^2} (|z| + 1)^L c_8^{L|z|} \end{aligned}$$

Como $e^x > 1 + x > x$ para $x > 0$, então

$$\begin{aligned} |f(z)| &\leqslant e^{h^2(n+1)} e^{h^3} (c_{10} L)^{h^2} e^{L|z|} c_8^{L|z|} \leqslant (e^{n+1})^{h^3} e^{h^3} e^{h^3} e^{L|z|} c_8^{L|z|} \leqslant \\ &\leqslant c_{11}^{3h^3 + L|z|} \leqslant c_{12}^{h^3 + L|z|}, \text{ onde } c_{12} = (max = \{e^{n+1}, c_8\})^3 \end{aligned}$$

Usamos que $(c_{10}L)^{h^2} \leqslant e^{h^3}$ para h suficientemente grande.

□

(ii) Para a prova da segunda afirmação, definamos o número $f' = \frac{P'}{P} f(l)$, onde P' é definido em (6.9).

$$\begin{aligned}
f' &= \frac{P'}{P} P \sum_{\lambda_0=0}^{L} \cdots \sum_{\lambda_n=0}^{L} p(\lambda_0, \cdots, \lambda_n) q(\lambda_0, \lambda_n, l) \alpha_1^{\lambda_1 l} \cdots \alpha_n^{\lambda_n l} \gamma_1^{m_1} \cdots \gamma_{n-1}^{m_{n-1}} \\
&= (a_1 \cdots a_n)^{Ll} b_0^{m_0} \cdots b_{n-1}^{m_{n-1}} \sum_{\lambda_0=0}^{L} \cdots \sum_{\lambda_n=0}^{L} p(\lambda_0, \cdots, \lambda_n) q(\lambda_0, \lambda_n, l) \cdot \\
&\cdot \quad \alpha_1^{\lambda_1 l} \cdots \alpha_n^{\lambda_n l} \gamma_1^{m_1} \cdots \gamma_{n-1}^{m_{n-1}} = \\
&= \sum_{\lambda_0=0}^{L} \cdots \sum_{\lambda_n=0}^{L} \sum_{\mu_0=0}^{m_0} p(\lambda_0, \cdots, \lambda_n) \binom{m_0}{\mu_0} \lambda_0(\lambda_0 - 1) \cdots (\lambda_0 - \mu_0 + 1) \cdot \\
&\cdot \quad (\lambda_n b_0 \beta_0)^{m_0 - \mu_0} l^{\lambda_0 - \mu_0} \cdot (a_1 \alpha_1)^{\lambda_1 l} \cdots (a_n \alpha_n)^{\lambda_n l} \cdot \\
&\cdot \quad (b_1 \lambda_1 + \lambda_n b_1 \beta_1)^{m_1} \cdots (b_{n-1} \lambda_{n-1} + \lambda_n b_{n-1} \beta_{n-1})^{m_{n-1}} \cdot \\
&\cdot \quad b_0^{\mu_0} a_1^{(L-\lambda_1)l} \cdots a_n^{(L-\lambda_n)l}
\end{aligned}$$

Como $a_1\alpha_1, \cdots, a_n\alpha_n, b_0\beta_0, \cdots, b_{n-1}\beta_{n-1}$ são inteiros algébricos, f' é inteiro algébrico de grau no máximo d^{2n}. Por outro lado, pela estimativa em (i), vemos que todo conjugado de f', obtido pela substituição arbitrária dos conjugados de α_r, β_r, tem valor absoluto no máximo $c_{13}^{h^3+Ll}$; que para h suficientemente grande também é um limitante para $\frac{P'}{P}$. Como f' é inteiro algébrico, devemos considerar dois casos:

Caso 1 $N(f') = 0$

Nesse caso $f' = 0$ implicando que $f(l) = 0$, já que $\frac{P'}{P} \neq 0$.

Caso 2 $|N(f')| \geqslant 1$

Denotando $f', (f')^{(2)}, \cdots, (f')^{(s)}$ os conjugados de f' onde s é um inteiro positivo menor ou igual à d^{2n}. Temos

$$1 \leqslant |N(f')| = |f'||(f')^{(2)}| \cdots |(f')^{(s)}| \leqslant |f'| c_{13}^{d^{2n}(h^3+Ll)}$$

daí,

$$|f'| \geqslant c_{14}^{-h^3-Ll}, \text{ onde } c_{14} = c_{13}^{d^{2n}} \tag{6.12}$$

e

$$\left|\frac{P}{P'}\right| \geqslant c_{13}^{-h^3-Ll} \tag{6.13}$$

Multiplicando as desigualdades (6.12) e (6.13), obtemos

$$|f(l)| = |f'|\left|\frac{P}{P'}\right| \geqslant c_{15}^{-h^3-Ll}, \text{ onde } c_{15} = c_{13}c_{14}$$

□

Lema 6.2.4 *Seja J um inteiro satisfazendo $0 \leqslant J \leqslant (8n)^2$. Então (6.7) vale para todo inteiro l com $1 \leqslant l \leqslant h^{1+\frac{J}{8n}}$ e todos inteiros não negativos $m_0, \cdots, m_{n-1}$ com $m_0 + \cdots + m_{n-1} \leqslant \dfrac{h^2}{2^J}$.*

Demonstração

Alguns fatos que ajudam:

(I) $(x_1 + \cdots + x_n)^m = \sum \dfrac{m!}{i_1! \cdots i_n!} x_1^{i_1} \cdots x_n^{i_n}$, onde o somatório é sobre todos os inteiros não negativos $i_1, \cdots, i_n$ com $i_1 + \cdots + i_n = m$;

(II) Se $f(a) = f'(a) = \cdots = f^{(n)}(a) = 0$ então $f(z) = (z-a)^n g(z)$;

(III) (Princípio do Módulo Máximo) Seja $f : \Omega \longrightarrow \mathbb{C}$ uma função holomorfa (Ω limitado). Então, $max_{z\in\bar{\Omega}}|f(z)| = max_{z\in\partial\Omega}|f(z)|$.

Para demonstrar o Lema 6.2.4, usaremos indução sobre J.

Para $J = 0$ o resultado é válido pelo Lema 6.2.2. Seja K um inteiro com $0 \leqslant K < (8n)^2$ e assuma que o lema vale para $J = 0, 1, \cdots, K$. Basta-nos mostrar o resultado para $J = K + 1$. Defina

$$R_J = \lfloor h^{1+\frac{J}{8n}} \rfloor,\ S_J = \left\lfloor \frac{h^2}{2^J} \right\rfloor \ (J = 0, 1, \ldots)$$

Então, é suficiente mostrar que para todo l com $R_K < l \leqslant R_{K+1}$ e $m_0, \cdots, m_{n-1}$ inteiros não negativos quaisquer, temos $f(l) = 0$.

Afirmação 6.2.1 *$f_m(r) = 0$ para todos r e m com $1 \leqslant r \leqslant R_K$ e $0 \leqslant m \leqslant S_{K+1}$.*

De fato, $f_m(r)$ é dada por

$$\left(\frac{\partial}{\partial z_0}+\cdots+\frac{\partial}{\partial z_{n-1}}\right)^m \Phi_{m_0,\cdots,m_{n-1}}(z_0,\cdots,z_{n-1})$$

quando $z_0=\cdots=z_{n-1}=r$, por (I)

$$\left(\frac{\partial}{\partial z_0}+\cdots+\frac{\partial}{\partial z_{n-1}}\right)^m \Phi_{m_0,\cdots,m_{n-1}}(z_0,\cdots,z_{n-1}) =$$
$$=\sum \frac{m!}{j_0!\cdots j_{n-1}!}\left(\frac{\partial}{\partial z_0}\right)^{j_0}\cdots\left(\frac{\partial}{\partial z_{n-1}}\right)^{j_{n-1}} \Phi_{m_0,\cdots,m_{n-1}}(z_0,\cdots,z_{n-1})$$

Portanto,

$$f_m(r)=\sum \frac{m!}{j_0!\cdots j_{n-1}!}\Phi_{m_0+j_0,\cdots,m_{n-1}+j_{n-1}}(r,\cdots,r)$$

onde a soma é sobre todos os inteiros não negativos $j_0,\cdots,j_{n-1}$ com $j_0+\cdots+j_{n-1}=m$. Observe que,

$$\begin{aligned}(m_0+j_0)+\cdots+(m_{n-1}+j_{n-1}) &= (m_0+\cdots+m_{n-1})+(j_0+\cdots+j_{n-1})\leqslant\\ &\leqslant 2S_{k+1}=2\left\lfloor\frac{h^2}{2^{k+1}}\right\rfloor\leqslant\left\lfloor\frac{h^2}{2^k}\right\rfloor=S_K\end{aligned}$$

Assim, por hipótese de indução, $f_m(r)=0$ para todos r e m $(1\leqslant r\leqslant R_k,\ 0\leqslant m\leqslant S_{k+1})$. Por (II), $f(z)=\{(z-1)\cdots(z-R_k)\}^{S_{k+1}}g(z)$ onde $g(z)$ é holomorfa. Portanto,

$$\frac{f(z)}{F(z)},\ \text{onde } F(z)=\{(z-1)\cdots(z-R_k)\}^{S_{k+1}}$$

é holomorfa no fecho do círculo C centrado na origem e de raio $R=R_{k+1}h^{\frac{1}{8n}}$. Pelo Princípio do Módulo Máximo,

$$|g(l)|\leqslant max_{z\in C}\left|\frac{f(z)}{F(z)}\right|\leqslant\frac{max_{z\in C}|f(z)|}{min_{z\in C}|F(z)|} \tag{6.14}$$

Definindo, $\theta=max_{z\in C}|f(z)|$ e $\Theta=min_{z\in C}|F(z)|$, (6.14) nos garante que

$$\theta|F(l)|\geqslant\Theta|f(l)| \tag{6.15}$$

Note que, para h suficientemente grande, $l \leqslant \frac{R}{2}$.

Algumas majorações importantes:

M4)

$|z-j| > \frac{1}{2}R$, $j = 1, \cdots, R_k$ e $z \in C$

De fato, $|z-j| \geqslant |z| - |j| = R - j > R - \frac{1}{2}R = \frac{1}{2}R$.

M5)

$|F(z)| \geqslant \left(\frac{1}{2}R\right)^{R_k S_{k+1}}$, $z \in C$

Note que, $|F(z)| = |(z-1)\cdots(z-R_k)|^{S_{k+1}} > \left(\frac{1}{2}R\right)^{R_k S_{k+1}}$, por M4.

M6)

$\Theta \geqslant \left(\frac{1}{2}R\right)^{R_k S_{k+1}}$

Diretamente de M5, pois $\Theta = min_{z\in C}|F(z)|$.

M7)

$|f(z)| \leqslant c_{12}^{h^3+LR}$, $z \in C$

Pelo Lema 6.2.3.

M8)

$\theta \leqslant c_{12}^{h^3+LR}$

Temos, $\theta = max_{z\in C}|f(z)| \leqslant c_{12}^{h^3+LR}$

M9)

$|l-j| \leqslant R_{k+1}$; $R_k < l < R_{k+1}$, $j = 1, \cdots, R_k$

$|l-j| \leqslant |R_{k+1} - 1| \leqslant R_{k+1}$

M10)

$|F(l)| \leqslant R_{k+1}^{R_k S_{k+1}}$

Basta usar M9 na expressão de $|F(l)|$.

Pelo Lema 6.2.3, ou $f(l) = 0$ ou $|f(l)| > c_{15}^{-h^3-LR}$. Suponha que $|f(l)| >$

$c_{15}^{-h^3-LR}$ e substituindo M6, M8, M10 em (6.15), obtemos:

$$\begin{aligned} c_{12}^{h^3+LR} R_{k+1}^{R_k S_{k+1}} &\geqslant \left(\frac{1}{2}R\right)^{R_k S_{k+1}} c_{15}^{-h^3-LR} \Longleftrightarrow (c_{12}c_{15})^{h^3+LR} \geqslant \\ &\geqslant \left(\frac{1}{2}h^{\frac{1}{8n}}\right)^{R_k S_{k+1}} \end{aligned} \tag{6.16}$$

Por outro lado,

$$LR = \left\lfloor h^{2-\frac{1}{4n}} \right\rfloor R_{k+1} h^{\frac{1}{8n}} \leqslant h^{2-\frac{1}{4n}} h^{1+\frac{k+1}{8n}} h^{\frac{1}{8n}} = h^{3+\frac{k}{8n}}$$

e

$$2^{k+3} R_k S_{k+1} = 2^{k+3} \left\lfloor h^{1+\frac{k}{8n}} \right\rfloor \left\lfloor \frac{h^2}{2^{k+1}} \right\rfloor \geqslant 2^{k+3} \frac{1}{2^2} h^{1+\frac{k}{8n}} \frac{h^2}{2^{k+1}} = h^{3+\frac{k}{8n}}$$

daí

$$LR \leqslant 2^{k+3} R_k S_{k+1} \Longrightarrow h^3 + LR \leqslant h^3 + 2^{k+3} R_k S_{k+1}$$

Voltando à (6.16),

$$(c_{12}c_{15})^{h^3+2^{k+3}R_k S_{k+1}} \geqslant \left(\frac{1}{2}h^{\frac{1}{8n}}\right)^{R_k S_{k+1}}$$

então

$$c_{16}^{h^3} \geqslant \left(\frac{1}{2} \cdot \frac{h^{\frac{1}{8n}}}{c_{16}^{2^{k+3}}}\right)^{R_k S_{k+1}} = \left(\frac{h^{\frac{1}{8n}}}{c_{17}^{2^{k+3}}}\right)^{R_k S_{k+1}} \tag{6.17}$$

onde $c_{16} = c_{12}c_{15}$ e $c_{17} = 2c_{16}$. Entretanto,

$$R_k S_{k+1} = \left\lfloor h^{1+\frac{k}{8n}} \right\rfloor \left\lfloor \frac{h^2}{2^{k+1}} \right\rfloor > \frac{1}{2^{k+3}} h^{3+\frac{k}{8n}}$$

Substituindo em (6.17),

$$c_{16}^{h^3} \geqslant \left(\frac{h^{\frac{1}{8n}}}{c_{17}^{2^{k+3}}}\right)^{\frac{1}{2^{k+3}}h^{3+\frac{k}{8n}}} = \frac{h^{\frac{h^{3+\frac{k}{8n}}}{2^{k+6}.n}}}{c_{17}^{h^{3+\frac{k}{8n}}}}$$

daí

$$\left(c_{16}^{h^3} \cdot c_{17}^{h^{3+\frac{k}{8n}}}\right)^{2^{k+6}\cdot n} \geqslant h^{h^{3+\frac{k}{8n}}}$$

seja $c_{19} = (max\{c_{16}, c_{17}\})^{2^{k+6}\cdot n}$, então

$$c_{19}^{2\left(h^3+\frac{k}{4n}\right)} \geqslant h^{h^{3+\frac{k}{8n}}}$$

Finalmente,

$$c_{20}^{h^3+\frac{k}{4n}} \geqslant h^{h^{3+\frac{k}{8n}}},\ c_{20} = c_{19}^2 \tag{6.18}$$

Mas para h suficientemente grande a desigualdade acima não é satisfeita. Portanto, $f(l) = 0$ e o lema segue-se por indução.

□

Lema 6.2.5 *Escrevendo $\phi(z) = \Phi(z, \cdots, z)$, temos*

$$|\phi_j(0)| < e^{-h^{8n}}\ (0 \leqslant j \leqslant h^{8n}) \tag{6.19}$$

Demonstração

Defina $X = h^{8n}$, $Y = \left\lfloor \dfrac{h^2}{2^{(8n)^2}} \right\rfloor$. Pelo Lema 6.2.4, (6.7) vale para todo inteiro l e inteiros não negativos $m_0, \cdots, m_{n-1}$ satisfazendo:

$$1 \leqslant l \leqslant X \text{ e } m_0 + \cdots + m_{n-1} \leqslant Y$$

Analogamente à demonstração do Lema 6.2.4, mostramos que $\phi_m(r) = 0$ para todos inteiros r e m com $1 \leqslant r \leqslant X$, $0 \leqslant m \leqslant Y$. Segue-se que $\dfrac{\phi(z)}{E(z)}$, onde

$$E(z) = \{(z-1)\cdots(z-X)\}^Y$$

é holomorfa no fecho do círculo Γ de centro na origem e de raio $R = Xh^{\frac{1}{8n}}$. pelo Princípio do Módulo Máximo, temos para todo w com $|w| < X$ $(w \neq 1, \cdots, X-1)$,

$$|\phi(w)| \leqslant \zeta\Xi^{-1}|E(w)| \tag{6.20}$$

onde $\zeta = max_{z\in\Gamma}|\phi(z)|$, $\Xi = min_{z\in\Gamma}|E(z)|$.

Algumas majorações:

M11
$|E(w)| \leqslant (2X)^{XY}$

Basta-nos mostrar que para $1 \leqslant j \leqslant X$, $|w - j| \leqslant 2X$. De fato,

$$|w - j| \leqslant |w| + |j| < X + X = 2X$$

M12
$|\Xi| \geqslant \left(\frac{1}{2}R\right)^{XY}$

Temos que $|E(z)| = \{|z-1| \cdots |z-X|\}^Y > \left(\frac{1}{2}R\right)^{XY}$, já que

$$|z - j| > \frac{1}{2}R \text{ para } 1 \leqslant j \leqslant X \text{ e } z \in \Gamma$$

Portanto,

$$|\Xi| = min_{z\in\Gamma}|E(z)| \geqslant \left(\frac{1}{2}R\right)^{XY}$$

M13
$\zeta \leqslant c_{12}^{h^3+LR}$

Segue-se do Lema 6.2.3 para $m_0 = \cdots = m_{n-1} = 0$.

Substituindo M11, M12, M13 em (6.20);

$$|\phi(w)| \leqslant c_{12}^{h^3+LR}\left(\frac{1}{2}R\right)^{-XY}(2X)^{XY} = c_{12}^{h^3+LR}\left(\frac{1}{4}h^{\frac{1}{8n}}\right)^{-XY}$$

e como

$$LR = \left\lfloor h^{2-\frac{1}{4n}} \right\rfloor \cdot Xh^{\frac{1}{8n}} \leqslant h^{2-\frac{1}{4n}} \cdot h^{8n} \cdot h^{\frac{1}{8n}} \leqslant h^{8n+2} \leqslant 2^{(8n)^2+1}XY$$

Então

$$|\phi(w)| \leqslant c_{12}^{h^3+2^{(8n)^2+1}XY}\left(\frac{1}{4}h^{\frac{1}{8n}}\right)^{-XY} \tag{6.21}$$

Afirmação 6.2.2 *Para h suficientemente grande, temos*

$$c_{12}^{h^3+2^{(8n)^2+1}XY}\left(\frac{1}{4}h^{\frac{1}{8n}}\right)^{-XY} < e^{-XY}$$

Demonstração

Sejam $d_0 = \log c_{12}$ e $d_1 = \log \frac{1}{4}$. Tome $h > e^{8n(1+2^{(8n)^2+1}d_0 - d_1)}$ então

$$\log h > 8n(2 + 2^{(8n)^2+1}d_0 - d_1)$$

daí

$$\frac{1}{8n}\log h > 2 + 2^{(8n)^2+1}d_0 - d_1$$

Portanto,

$$-1 - 2^{(8n)^2+1}d_0 + d_1 + \frac{1}{8n}\log h > 1 \tag{6.22}$$

Claramente para h suficientemente grande

$$h^3 d_0 < XY \; (já \; que X = h^{8n}) \tag{6.23}$$

Multiplicando as desigualdades (6.22) e (6.23), obtemos

$$h^3 d_0 \leqslant XY\left(-1 - 2^{(8n)^2+1}d_0 + d_1 + \frac{1}{8n}\log h\right)$$

Daí, $\log\left(c_{12}^{h^3+2^{(8n)^2+1}XY}\left(\frac{1}{4}h^{\frac{1}{8n}}\right)^{-xy}\right) < -XY$, e finalmente

$$c_{12}^{h^3+2^{(8n)^2+1}XY}\left(\frac{1}{4}h^{\frac{1}{8n}}\right)^{-XY} < e^{-XY}$$

□

Portanto $|\phi(w)| < e^{-XY}$. Entretanto, pela fórmula integral de Cauchy, temos

$$\phi_j(0) = \frac{j!}{2\pi i}\int_\Lambda \frac{\phi(w)}{w^{j+1}}dw$$

onde Λ denota o círculo $|w| = 1$, orientado no sentido positivo.

Segue-se

$$|\phi_j(0)| < \frac{j!}{2\pi}\cdot e^{-XY}\cdot 2\pi \leqslant j^j e^{-XY} < e^{-h^{8n}}$$

para $0 \leqslant j \leqslant h^{8n}$ e h suficientemente grande.

□

Lema 6.2.6 *Para todos inteiros $t_1, \cdots, t_n$, não todos nulos, com valor absoluto no máximo T, temos*

$$|t_1 \log \alpha_1 + \cdots + t_n \log \alpha_n| > C^T$$

Demonstração

Seja $\tilde{a}_j$ $(1 \leqslant j \leqslant n)$ o coeficiente líder do polinômio $F_{\alpha_j,\mathbb{Q}}(x)$ ou $F_{\alpha_j^{-1},\mathbb{Q}}(x)$ (6.1) de acordo com $t_j \geqslant 0$ ou $t_j < 0$ respectivamente. Defina

$$w = \tilde{a}_1^{|t_1|} \cdots \tilde{a}_n^{|t_n|} \ (\alpha_1^{t_1} \cdots \alpha_n^{t_n} - 1)$$

Como $\tilde{a}_i\alpha_i$ ou $\tilde{a}_i\alpha_1^{-1}$ é inteiro algébrico, de acordo com $t_i \geqslant 0$ ou $t_i < 0$, então w é um inteiro algébrico e seu grau é menor ou igual a d^n e sobre todo conjugado de w, obtido pela substituição arbitrária dos conjugados de $\alpha_1, \cdots, \alpha_n$ temos:

$$\left|w^{(i)}\right| = \left|a_1^{|t_1|} \cdots a_n^{|t_n|}\right| \left|(\alpha_1^{(i_1)})^{t_1} \cdots (\alpha_n^{(i_n)})^{t_n} - 1\right| \leqslant c_{21}^{nT} 2^{nT} c_{22}^{nT} = c_{23}^T$$

onde $c_{21} = max\{\tilde{a}_1, \cdots, \tilde{a}_n\}$, $c_{22} = max\{1, \alpha_l^{(j)} \mid 1 \leqslant l \leqslant n;\ 1 \leqslant j \leqslant d\}$ e $c_{23} = (2c_{21}c_{22})^n$.

Como w é um inteiro algébrico então $N(w) = 0$ ou $N(w) \in \mathbb{Z} - \{0\}$. Consideremos os 2 casos:

Caso 1. $N(w) = 0$

Então $w = 0$ e como $\tilde{a}_1 \cdots \tilde{a}_n \neq 0$ deve-se ter $\alpha_1^{t_1} \cdots \alpha_n^{t_n} = 1$. Portanto,

$$\Upsilon = t_1 \log \alpha_1 + \cdots + t_n \log \alpha_n = 2\tilde{k}\pi i, \text{ onde } \tilde{k} \in \mathbb{Z}$$

Por hipótese do Teorema, $\log \alpha_1, \cdots, \log \alpha_n$ são linearmente independentes sobre $\mathbb{Q}$, então $\tilde{k} \neq 0$. Daí,

$$|\Upsilon| = |2\tilde{k}\pi| > C^{-T},\ C = 2\tilde{k}\pi$$

Observe que se $|\Upsilon| \geqslant 1$ então o resultado segue-se imediatamente. Podemos então supor $|\Upsilon| < 1$.

Caso 2. $N(w) \in \mathbb{Z} - \{0\}$

Seja $s \leqslant d^n$,

$$1 \leqslant |N(w)| = |w||w^{(2)}| \cdots |w^{(s)}| \leqslant |w| c_{23}^{Td^n}$$

daí

$$|w| \geqslant c_{23}^{-Td^n} \tag{6.24}$$

Sabe-se que, para todo z, $|e^z - 1| \leqslant |z|e^{|z|}$. Fazendo $z = \Upsilon$ nessa desigualdade, obtemos

$$e|\Upsilon| \geqslant e^{|\Upsilon|}|\Upsilon| \geqslant |w| \geqslant c_{23}^{-Td^n}$$

Portanto,

$$|\Upsilon| \geqslant c_{24}^{-T}, \text{ onde } c_{24} = (e \cdot c_{23})^{d^n}$$

□

Lema 6.2.7 *Sejam R, S inteiros positivos e $\sigma_0, \cdots, \sigma_{R-1}$ números complexos distintos. Defina σ como o máximo entre $1, |\sigma_0|, \cdots, |\sigma_{R-1}|$ e defina ρ como o mínimo entre 1 e $|\sigma_i - \sigma_j|$ com $0 \leqslant i < j < R$. Então, para todos r, s, inteiros, com $0 \leqslant r < R$, $0 \leqslant s < S$ existem números complexos $w_i (0 \leqslant i < RS)$ com valor absoluto no máximo $\left(\frac{8\sigma}{\rho}\right)^{RS}$ tal que o polinômio*

$$w(z) = \sum_{j=0}^{RS-1} w_j z^j$$

satisfaz $w_j(\sigma_i) = 0$ para todos i, j com $0 \leqslant i < R$, $0 \leqslant j < S$, $(i,j) \neq (r,s)$ e $w_s(\sigma_r) = 1$.

Demonstração

O polinômio pedido é dado por

$$w(z) = \left(\frac{-1}{S!}\right)\frac{1}{2\pi i}\int_{C_r}\frac{(\zeta-\sigma_r)^s\,U(z)}{(\zeta-z)U(\zeta)}d\zeta$$

onde $U(z) = \{(z-\sigma_0)\cdots(z-\sigma_{R-1})\}^S$ e C_r denota o círculo, percorrido no sentido positivo, com centro σ_r e raio suficientemente pequeno, menor que os números ρ e $|z-\sigma_r|$, para $z \neq \sigma_r$. Como o valor absoluto do integrando multiplicado por $|\zeta|$ tende à 0 quando $|\zeta| \longrightarrow \infty$, temos, pelo Teorema dos Resíduos de Cauchy,

$$w(z) = \frac{(z-\sigma_r)^s}{s!} + \frac{U(z)}{s!}\frac{1}{2\pi i}\sum_{\substack{j=0\\ j\neq r}}^{R-1}\int_{C_j}\frac{(\zeta-\sigma_r)^s}{(\zeta-z)U(\zeta)}d\zeta \tag{6.25}$$

onde c_j, como c_r acima, é um círculo centrado em σ_j e com raio suficientemente pequeno. Claramente o somatório acima sobre j é uma função racional de z, regular em $z = \sigma_r$ e, como $U(z)$ tem um zero em $z = \sigma_r$ de ordem S, então

$$U_l(\sigma_r) = 0,\ para\ 0 \leqslant l < S \tag{6.26}$$

Por (6.25),

$$\begin{aligned} w_l(z) &= \frac{s(s-1)\cdots(s-l+1)}{s!}(z-\sigma_r)^{s-l} + \\ &+ \frac{U_l(z)}{s!}\cdot\frac{1}{2\pi i}\sum_{\substack{j=0\\ j\neq r}}^{R-1}\int_{C_j}\frac{(\zeta-\sigma_r)^s}{(\zeta-z)U(\zeta)}d\zeta + \\ &+ \frac{U(z)}{s!}\cdot\frac{1}{2\pi i}\sum_{\substack{j=0\\ j\neq r}}^{R-1}\frac{d^l}{dz^l}\int_{C_j}\frac{(\zeta-\sigma_r)^s}{(\zeta-z)U(\zeta)}d\zeta \end{aligned}$$

Usando (6.26) e que $s < S$, $w_s(\sigma_r) = 1$ e $w_l(\sigma_r) = 0$ caso contrário. Seja $t = S - s - 1 \geqslant 0$. Pelo Teorema da Integral de Cauchy:

$$\begin{aligned} \frac{-1}{s!}\left[\frac{1}{t!}\frac{d^t}{d\zeta^t}\frac{(\zeta-\sigma_r)^sU(z)}{(\zeta-z)U(\zeta)}\right]_{\zeta=\sigma_r} &= \frac{-1}{s!}\left[\frac{1}{2\pi i}\int_{C_r}\frac{(\zeta-\sigma_r)^SU(z)}{(\zeta-z)U(\zeta)(\zeta-\sigma_r)^{t+1}}d\zeta\right] = \\ &= \frac{-1}{s!}\left[\frac{1}{2\pi i}\int_{C_r}\frac{(\zeta-\sigma_r)^sU(z)}{(\zeta-z)U(\zeta)}d\zeta\right] \end{aligned}$$

Portanto,

$$w(z) = \frac{-1}{s!t!}\left[\frac{d^t}{d\zeta^t}\frac{(\zeta-\sigma_r)^S U(z)}{(\zeta-z)U(\zeta)}\right]_{\zeta=\sigma_r}$$

e assim

$$w(z) = (-1)^{t-1}(s!)^{-1}U(z)\sum v(j_0,\cdots,j_{R-1})(\sigma_r - z)^{-jr-1} \tag{6.27}$$

onde o somatório é sobre todos os inteiros não negativos $j_0,\cdots,j_{R-1}$ com $j_0+\cdots+j_{R-1}=t$ e

$$v(j_0,\cdots,j_{R-1}) = \prod_{\substack{i=0\\ i\neq r}}^{R-1}\binom{S+j_i-1}{j_i}(\sigma_r-\sigma_i)^{-S-j_i}$$

Note que $1 \leqslant j_r+1 \leqslant t+1 = S-s \leqslant S$, daí $w(z)$ é um polinômio com grau no máximo $RS-1$. Entretanto vemos que $w(z)$, como $U(z)$, tem um zero em $z=\sigma_i (i\neq r)$ de ordem S e então $w_l(\sigma_i)=0$ para todo $l<S$. Para estimar o valor absoluto dos coeficientes de $w(z)$, perceba que

$$\tbinom{S+j_i-1}{j_i}(\sigma_r-\sigma_i)^{-S-j_i} \leqslant 2^{S+j_i-1}\rho^{-S-j_i}$$

e daí

$$|v(j_0,\cdots,j_{R-1})| \leqslant \left(\frac{2}{\rho}\right)^{(R-1)S+j_0+\cdots+j_{R-1}} = \left(\frac{2}{\rho}\right)^{(R-1)S+t} \leqslant \left(\frac{2}{\rho}\right)^{RS}$$

Por outro lado, os coeficientes de $(\sigma_r-z)^{-j_r-1}U(z)$ tem valores absolutos no máximo $(\sigma+1)^{RS}$ e o número de termos, N, no somatório em (6.27) é igual ao número de inteiros $j_0,\cdots,j_{R-1}$, não negativos, satisfazendo;
$j_0+\cdots+j_{R-1}=t$. Então

$$N = \tbinom{R+t-2}{t} \leqslant S^R$$

Afirmação 6.2.3 *$a(\sigma+1)^a \leqslant (4\sigma)^a$, $\forall\ a\in\mathbb{N}$, em particular*

$$S(\sigma+1)^S \leqslant (4\sigma)^S$$

Demonstração

Usando indução sobre a. Para $a = 1$ é verdade. Suponha que $k(\sigma+1)^k \leqslant (4\sigma)^k (III)$. Para $1 \leqslant k < a$, as desigualdades abaixo também são válidas:

$$(\sigma+1)^k \leqslant (4\sigma)^k \tag{6.28}$$

$$\sigma + 1 \leqslant \frac{4\sigma}{2} \tag{6.29}$$

Somando as desigualdades (6.28) e (6.29), obtemos

$$(k+1)(\sigma+1)^k \leqslant 2(4\sigma)^k$$

agora multiplicando a desigualdade acima pela desigualdade (III)

$$(k+1)(\sigma+1)^{k+1} \leqslant (4\sigma)^{k+1}$$

que garante o resultado desejado.

□

Usando as majorações anteriores e a Afirmação 6.2.3, segue-se que os coeficientes de $w(z)$ tem valores absolutos no máximo

$$S^R(\sigma+1)^{RS}\left(\frac{2}{\rho}\right)^{RS} = [S(\sigma+1)^S]^R\left(\frac{2}{\rho}\right)^{RS} \leqslant (4\sigma)^{RS}\cdot\left(\frac{2}{\rho}\right)^{RS} = \left(\frac{8\sigma}{\rho}\right)^{RS}$$

terminando assim a demonstração do lema.

□

Para finalizar a demonstração do Teorema 6.2.1, escreva $S = L + 1$ e $R = S^n$. Note que todo inteiro com $0 \leqslant i < RS$ pode ser expresso unicamente na forma

$$i = \lambda_{0i} + \lambda_{1i}S + \cdots + \lambda_{ni}S^n$$

onde $\lambda_{0i}, \cdots, \lambda_{ni}$ são inteiros entre 0 e L inclusive. Para todo $i \in \{0, \cdots, RS-1\}$, defina

$$\nu_i = \lambda_{0i},\ p_i = p(\lambda_{0i}, \cdots, \lambda_{ni}) \text{ e } \psi_i = \lambda_{0i}\log\alpha_1 + \cdots + \lambda_{ni}\log\alpha_n$$

Claramente,

$$\phi(z) = \sum_{i=0}^{RS-1} p_i z^{\nu_i} e^{\psi_i z} \tag{6.30}$$

Entretanto, pelo Lema 6.2.6,

$$|\psi_i - \psi_j| = |(\lambda_{0i} - \lambda_{0j}) \log \alpha_1 + \cdots + (\lambda_{ni} - \lambda_{nj}) \log \alpha_n| > c_{24}^{-L}$$

Em particular, exatamente R dos ψ_i são distintos, e podemos denotá-los em alguma ordem, por $\sigma_0, \cdots, \sigma_{R-1}$. Se σ, ρ são definidos como no Lema 6.2.7, então

$$\sigma \leqslant c_{25} L,\ c_{25} = \max\{1, nc_9\}$$

e

$$\rho \geqslant c_{26}^{-L},\ c_{26} = min\{1, c_{11}\}$$

Sejam t um inteiro positivo tal que $p_t \neq 0$, $s = \nu_t$ e r tal que $\psi_t = \sigma_r$ e $W(z)$, o polinômio fixado no Lema 6.2.7.

Como $W_j(\sigma_i) = 1$ para $j = \nu_t$ e $i = t$ e $W_j(\sigma_i) = 0$ caso contrário, então

$$p_t = \sum_{i=0}^{RS-1} p_i W_{\nu_i}(\psi_i)$$

e

$$W_{\nu_i}(\psi_i) = \sum_{j=0}^{RS-1} j(j-1)\cdots(j-\nu_i+1) w_j \psi_i^{j-\nu_i} \tag{6.31}$$

Por outro lado,

$$\begin{aligned} \frac{d^j}{dz^j}(z^{\nu_i} e^{\nu_i z})|_{z=0} &= \sum_{k=0}^{j} \binom{j}{k} \frac{d^k}{dz^k}(z^{\nu_i}) \cdot \frac{d^{(j-k)}}{dz^{(j-k)}}(e^{\psi_i z})|_{z=0} = \\ &= \sum_{k=0}^{j} \binom{j}{k} \nu_i(\nu_i - 1)\cdots(\nu_i - k + 1) z^{\nu_i - k} \psi_i^{j-k} e^{\psi_i z}|_{z=0} \end{aligned}$$

Observe que a expressão acima, em $z = 0$, é não nula apenas quando $\nu_i = k$. Daí,

$$\frac{d^j}{dz^j}\left(z^{\nu_i}e^{\psi_i z}\right)\Big|_{z=0} = \binom{j}{\nu_i}\nu_i!\psi_i^{j-\nu_i} = j(j-1)\cdots(j-\nu_i+1)\psi_i^{j-\nu_i}$$

Por (6.31), obtemos que

$$W_{\nu_i}(\psi_i) = \sum_{j=0}^{RS-1} w_j \left[\frac{d^j}{dz^j}(z^{\nu_i}e^{\psi_i z})\right]_{z=0}$$

Além disso, por (I)

$$\begin{aligned}\sum_{j=0}^{RS-1} w_j\phi_j(0) &= \sum_{j=0}^{RS-1} w_j \frac{d^j}{dz^j}\left(\sum_{i=0}^{RS-1} p_i z^{\nu_i}e^{\psi_i z}\right) = \\ &= \sum_{i=0}^{RS-1} p_i \sum_{j=0}^{RS-1} w_j \left[\frac{d^j}{dz^j}(z^{\nu_i}e^{\psi_i z})\right]_{z=0} = \\ &= \sum_{i=0}^{RS-1} p_i W_{\nu_i}(\psi_i) = p_t\end{aligned}$$

isto é, $p_t = \sum_{j=0}^{RS-1} w_j\phi_j(0)$.

Mas $RS \leqslant h^{2h+2}$ e pelo Lema 6.2.5; $|\phi_j(0)| < e^{-h^{8n}}$ para todo j com $0 \leqslant j \leqslant RS$. Entretanto pelo Lema 6.2.7,

$$\begin{aligned}|w_j| &\leqslant \left(\frac{8\sigma}{\rho}\right)^{RS} \leqslant (8c_{25}Lc_{26}^L)^{RS} \leqslant c_{27}^{h^{2n+2}} \cdot L^{h^{2n+2}} \cdot c_{26}^{h^{2n+4}} \leqslant \\ &\leqslant c_{27}^{h^{2n+4}} e^{h^{2n+4}} c_{26}^{h^{2n+4}} = c_{28}^{h^{2n+4}}\end{aligned}$$

onde $c_{28} = c_{27}ec_{26}$ e $c_{27} = 8c_{25}$.

Afirmação 6.2.4 *Para todo constante C, existe h suficientemente grande tal que*

$$h^{8n} > \log RS + Ch^{2n+4}$$

Demonstração

Suponha por absurdo que existe C (constante) tal que

$$h^{8n} \leqslant \log RS + Ch^{2n+4}, \text{ para todo } h > 0$$

Então

$$\begin{aligned} h^{8n} &\leqslant \log RS + Ch^{2n+4} = (n+1)\log S + Ch^{2n+4} \leqslant \\ &\leqslant (n+1)\log\left(2h^{2-\frac{1}{4n}}\right) + Ch^{2n+4} = \\ &= (n+1)\left(\log 2 + \left(2 - \frac{1}{4n}\right)\log h\right) + Ch^{2n+4} \end{aligned}$$

Como $h^{2n+4} \geqslant \log h$ e $2n+4 \leqslant 6n$ para $n \geqslant 1$,

$$h^{8n} \leqslant (n+1)(h^{6n}\log 2 + \left(2 - \frac{1}{4n}\right)h^{6n}) + Ch^{6n}$$

Daí,

$$h^{2n} \leqslant (n+1)\log 2 + (n+1)(2 - \frac{1}{4n}) + C$$

Absurdo!, pois o lado direito da desigualdade é constante e h pode ser tomado arbitrariamente grande.

□

Voltando a demonstração do teorema, observe que $|p_t| \geqslant 1$ (já que $p_t \in \mathbb{Z}$). Portanto,

$$1 \leqslant |p_t| = \left|\sum_{j=0}^{RS-1} w_j\phi_j(0)\right| \leqslant RSc_{28}^{h^{2n+4}}e^{-h^{8n}}$$

e então

$$0 \leqslant \log RS + h^{2n+4}c_{29} - h^{8n},\ c_{29} = \log c_{28}$$

Mas a desigualdade acima é impossível para h suficientemente grande (Afirmação 6.2.2). Esta contradição finaliza a demonstração do teorema.

□

6.3 Conseqüências e Aplicações

Apresentaremos agora alguns teoremas importantes que decorrem do Teorema 6.2.1.

Teorema 6.3.1 *Dados $\alpha_1, \cdots, \alpha_n$ números algébricos, não nulos, e $\beta_1, \cdots, \beta_n$ números 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 um número transcendente.

Demonstração

Basta-nos mostrar que para números algébricos $\alpha_1, \cdots, \alpha_n, \beta_0, \beta_1, \cdots, \beta_n$, com $\alpha_j \neq 0$, $1 \leqslant j \leqslant n$, temos

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \neq 0$$

Procedendo por indução vê-se que para $n = 1$ o resultado é válido. Assuma então a validade para $n < m$, onde m é um inteiro, mostraremos o resultado para $n = m$.

Se $\log \alpha_1, \cdots, \log \alpha_m$ são linearmente independentes sobre $\mathbb{Q}$, o resultado segue-se do Teorema 6.2.1. Assim, suponha que existem $\rho_1, \cdots, \rho_m$, números racionais, com $\rho_r \neq 0$ tais que

$$\rho_1 \log \alpha_1 + \cdots + \rho_m \log \alpha_m = 0$$

Entretanto,

$$\begin{aligned} \rho_r(\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_m \log \alpha_m) &= \rho_r(\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_m \log \alpha_m) - \\ &- \beta_r(\rho_1 \log \alpha_1 + \cdots + \rho_m \log \alpha_m) = \\ &= \beta'_0 + \beta'_1 \log \alpha_1 + \cdots + \beta'_m \log \alpha_m \end{aligned}$$

onde $\beta'_0 = \rho_r \beta_0$, $\beta'_j = \rho_r \beta_j - \rho_j \beta_r$ $(1 \leqslant j \leqslant m)$. Daí,

$$\rho_r(\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_m \log \alpha_m) = \beta'_0 + \beta'_1 \log \alpha_1 + \cdots + \beta'_m \log \alpha_m \quad (6.32)$$

Note que $\beta'_0 \neq 0$ e $\beta'_r = 0$, então por hipótese de indução, o lado direito de (6.32) é não nulo e como $\rho_r \neq 0$ segue-se que

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_m \log \alpha_m \neq 0$$

□

Teorema 6.3.2 *$e^{\beta_0}\alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ é transcendente para todos números algébricos $\alpha_1, \cdots, \alpha_n, \beta_0, \beta_1, \cdots, \beta_n$, não nulos.*

Demonstração

Se $\alpha_{n+1} = e^{\beta_0}\alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ é algébrico, então

$$\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n - \log \alpha_{n+1} = -\beta_0 \neq 0$$

Portanto, $\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n - \log \alpha_{n+1}$ é um número algébrico, não nulo, contrariando o Teorema 6.3.1.

□

Corolário 6.3.1 *Se $\alpha \in \mathbb{A} - \{0\}$, então $\pi + \log \alpha$ é transcendente.*

Demonstração

Como $\alpha \neq e^{-\pi}$ então $\pi + \log \alpha \neq 0$. Suponha que $\pi + \log \alpha$ é algébrico. Considere $\beta_0 = i(\pi + \log \alpha)$, $\alpha_1 = \alpha$, $\beta_1 = -i$. Pelo Teorema 6.3.2, $e^{\beta_0}\alpha_1^{\beta_1}$ é transcendente. Por outro lado,

$$e^{\beta_0}\alpha_1^{\beta_1} = e^{i(\pi + \log \alpha)}\alpha^{-i} = -1\alpha^i\alpha^{-i} = -1$$

Segue-se o resultado.

□

Exemplo 6.3.1 *Fazendo $\alpha = 1$ no corolário acima, obtemos a transcendência de π.*

Existe um teorema análogo ao Teorema 6.3.2 para caso $\beta_0 = 0$.

Teorema 6.3.3 *$\alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ é transcendente para todos números algébricos $\alpha_1, \cdots, \alpha_n$, diferentes de 0 ou 1, e todos números algébricos $\beta_1, \cdots, \beta_n$ com $1, \beta_1, \cdots, \beta_n$ linearmente independentes sobre $\mathbb{Q}$.*

Demonstração

Para a prova, é suficiente mostrar que se $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_n$ são algébricos satisfazendo as hipóteses do teorema, então

$$\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \neq 0$$

e a demonstração será feita por indução sobre n. Para $n = 1$ é trivial. Suponha que o resultado é válido para $n < m$ onde m é um inteiro positivo, devemos mostrar a validade, para $n = m$. O resultado é conseqüência imediata do Teorema 5.2.1 se $\log \alpha_1, \cdots, \log \alpha_m$ são linearmente independentes sobre $\mathbb{Q}$. Assim, podemos supor que existem racionais $\rho_1, \cdots, \rho_m$ e números β'_j como na prova do Teorema 6.3.1, com $\beta_0 = \beta'_0 = 0$.

Afirmação 6.3.1 *$\beta'_1, \cdots, \widehat{\beta'_r}, \cdots, \beta'_m$ são linearmente independentes sobre $\mathbb{Q}$.*

De fato, sejam $a_1, \cdots, \widehat{a_r}, \cdots, a_m$ números racionais. Se

$$\begin{aligned} 0 &= a_1\beta'_1 + \cdots + \widehat{a_r\beta'_r} + \cdots + a_m\beta'_m = \\ &= a_1(\rho_r\beta_1 - \rho_1\beta_r) + \cdots + \widehat{a_r\beta'_r} + \cdots + a_m(\rho_r\beta_m - \rho_m\beta_r) = \\ &= \rho_r(a_1\beta_1 + \cdots + \widehat{a_r\beta_r} + \cdots + a_m\beta_m) - \beta_r(a_1\rho_1 + \cdots + \widehat{a_r\rho_r} + \cdots + a_m\rho_m) \end{aligned}$$

Como $\beta_r = 0$ e $\rho_r \neq 0$ então $a_1 = \cdots = \widehat{a_r} = \cdots = a_m = 0$, pois $\beta_1, \cdots, \beta_m$ são linearmente independentes sobre $\mathbb{Q}$.

Basta proceder analogamente à demonstração do Teorema 6.3.1.

□

Apêndice A

Alguns Números Transcendentes

Já se passaram mais de 150 anos desde que o primeiro exemplo de número transcendente foi dado, durante esse período vários matemáticos devotaram algum tempo tentando mostrar que certos números eram ou não transcendentes. (Todos os números citados abaixo são transcendentes).

1851 LIOUVILLE, ver [5], p. 11-13.

Números da forma $\sum_{k=0}^{\infty} \frac{a_k}{10^{k!}}$, $a_k \in \{0, \cdots, 9\}$, com infinitos a_k's não nulos.

1873 HERMITE, ver [5], p. 38.

$e = 2,7182818284590452354\ldots$ a base dos logaritmos neperianos.

1882 LINDEMANN, ver [5], p. 43.

$\pi = 3,1415926535897932385\ldots$ a razão entre a circunferência e o diâmetro de um círculo.

1929 GELFOND - SCHNEIDER.

- $e^{\pi} = 23,140692632779269006\ldots$. ver [5], p. 104-110.
- $2^{\sqrt{2}} = 2,6651441426902251887\ldots$. a constante de Gelfond-Schneider, ver [5], p. 114.

1961 MAHLER, ver [5], p. 21-25.

$0,12345678910111213 14\ldots$ a constante de Champernowne.

1983 LE LIONNAIS, ver [11], p. 46.

$\Gamma\left(\frac{1}{3}\right) = 2,6789385347077476337\ldots$

1984 CHUDNOVSKY, ver [6], p. 308.

- $\Gamma\left(\frac{1}{4}\right) = 3,6256099082219083119\ldots$, conhecida como constante leminiscata.
- $\Gamma\left(\frac{1}{6}\right) = 5,5663160017802352043\ldots$

2003 SMITH - MARGOLIUS, ver [13].

$(\tan^{-1}\frac{1}{2}) \cdot \pi^{-1} = 0,14758361765043327417...$ a constante de Plouffe, mas geralmente $(\tan^{-1}(x)) \cdot \pi^{-1} \in \mathbb{T}$, onde $x \in \mathbb{Q} - \{0, \pm 1\}$.

2003 SONDOW, ver em [16]

$S = \sum_{n=1}^{\infty} \frac{1}{a_n} = 1,611114925808376736 11...$, onde $a_1 = 1$ e $a_n = n^{a_{n-1}}$ é uma seqüência recorrente conhecida como exponencial fatorial.

2007 SONDOW - MARQUES, ver em [17]

$\sqrt[3]{e}^{\sqrt[3]{e}^{\sqrt[3]{e}^{\cdot^{\cdot}}}} = 1,85718386020...$

Apêndice B

Números Algébricos da Forma T^T, $T \in \mathbb{T}$

Os próximos resultados são devidos a J. Sondow e o autor e correspondem a seção 2 do trabalho feito em [17]. Resultados semelhantes para as equações Diofantinas $x^x = y^y$, $x^y = y^x$ e $y = x^{x^y}$ podem ser vistas no mesmo trabalho.

Notação Ponha $\mathbb{R}^+ = \{x \in \mathbb{R} \,/\, x > 0\}$, $\mathbb{Q}^+ = \mathbb{Q} \cap \mathbb{R}^+$, $\mathbb{A}^+ = \mathbb{A} \cap \mathbb{R}^+$ e $\mathbb{T}^+ = \mathbb{T} \cap \mathbb{R}^+$.

Usando o Teorema 4.2.1, estudamos soluções algébricas e transcendentes da equação $x^{\,x} = y$.

Corolário B.0.2 *Seja* $A \geq e^{-1/e} = 0.69220\ldots$ (*resp.,* $A \in [e^{-1/e}, 1)$) *um número algébrico. Se* $T \geq e^{-1} = 0.36787\ldots$ (*resp.,* $T \in (0, e^{-1}]$) *satisfaz* $T^T = A$. *Então* T *é transcendente se, e somente se* $A \neq Q^Q$ *para todo* $Q \in \mathbb{Q} \cap [e^{-1}, \infty)$ (*resp.,* $Q \in \mathbb{Q} \cap (0, e^{-1}]$).

Demonstração A prova segue-se do Teorema 4.2.1 e do fato que a função x^x é injetiva sobre os intervalos $[e^{-1}, \infty)$ e $(0, e^{-1}]$.

Observação B.0.1 Se $T, Q \in (0, 1)$ estão em lados opostos do ponto e^{-1}, então pode acontecer que $T \in \mathbb{T}$, $Q \in \mathbb{Q}$, e $T^T = A = Q^Q$.

Lema B.0.1 *Se $Q \in \mathbb{Q} - \mathbb{Z}$, então $Q^Q \notin \mathbb{Q}$.*

Demonstração Suponha $(a/b)^{a/b} \in \mathbb{Q}$, onde $0 \neq a \in \mathbb{Z}$ e $b \in \mathbb{N}$, com $\mathrm{mdc}(a,b) = 1$. Deduzimos que $b^{1/b} \in \mathbb{N}$, portanto $b = 1$.

Corolário B.0.3 *Dados $A \in [e^{-1/e}, \infty)$ e $T > 0$ satisfazendo $T^T = A$. Suponha que*

(i) *$A \in \mathbb{Q} - \{n^n : n \in \mathbb{N}\}$, ou*

(ii) *$A^n \in \mathbb{A} - \mathbb{Q}$ para todo $n \in \mathbb{N}$.*

Então T é transcendente.

Demonstração (i) Lema B.0.1 implica $A \neq Q^Q$ para todo $Q \in \mathbb{Q}^+$. O resultado segue-se pelo Corolário B.0.2.
(ii) Assuma que $T \in \mathbb{A}$. Como $T^T = A \in \mathbb{A}$, O Teorema 4.2.1 implica $T \in \mathbb{Q}$, digamos $T = m/n$ com $m, n \in \mathbb{N}$. Então $A^n = T^m \in \mathbb{Q}$, uma contradição. □

Exemplo B.0.2 *Os números $0.15351\ldots = T_0 < e^{-1} < T_1 = 0.63626\ldots$ e $T_2 = 1.55961\ldots$ satisfazem*

$$T_0^{T_0} = T_1^{T_1} = 3/4, \qquad T_2^{T_2} = 2, \qquad T_0, T_1, T_2 \in \mathbb{T}.$$

Exemplo B.0.3 *Os números $0.18461\ldots = T_0 < e^{-1} < T_1 = 0.58872\ldots$ e $T_2 = 1.68644\ldots$ satisfazem*

$$T_0^{T_0} = T_1^{T_1} = \sqrt{3} - 1, \qquad T_2^{T_2} = \sqrt{2} + 1, \qquad T_0, T_1, T_2 \in \mathbb{T}.$$

Proposição B.0.1 *Dados um polinômio não constante $P(x) \in \mathbb{A}[x] \cap \mathbb{R}[x]$ que assume um valor positivo, $A_0 \in \mathbb{A} \cap \mathbb{R}$ e $Q_0, Q \in \mathbb{Q}$, com $A_0 Q_0 \neq 0$. Então o conjunto*

$$\left\{ A \mid A = P(T)^{A_0 \cdot P(T)^{Q_0} + Q} \in \mathbb{A},\ T \in \mathbb{T} \cap \mathbb{R} \right\}$$

é denso em um intervalo.

Demonstração Temos $0 < P(x) \neq 1$ sobre algum resultado $\alpha \leq x \leq \beta$. Sua imagem pela função

$$f(x) = P(x)^{A_0 \cdot P(x)^{Q_0} + Q}$$

é um intervalo $f([\alpha, \beta]) = [\gamma, \delta] \subset \mathbb{R}^+$. Evidentemente, existe $A_1 \in \mathbb{A}^+$ tal que $A_0^k A_1^n \notin \mathbb{Q}$ para todo $n, k \in \mathbb{Z}$ com $n \neq 0$ (de fato, dependendo do A_0, podemos tomar $A_1 = 1 + \sqrt{2}$ ou $A_1 = 1 + \sqrt{3}$). O conjunto $\{A \mid \gamma < A = Q_1 A_1 < \delta,\ Q_1 \in \mathbb{Q}^+\}$ é denso em $[\gamma, \delta]$, e todo elemento A é igual à $f(T)$ para algum $T = T(A) \in (\alpha, \beta)$. Mostramos que $T \in \mathbb{T}$. se não, então $P(T) \in \mathbb{A}$. ponha $Q' = A_0 \cdot P(T)^{Q_0} + Q$, então $A = P(T)^{Q'} \in \mathbb{A}$. Como $P(T) \notin \{0, 1\}$, O Teorema 4.2.1 implica $Q' \in \mathbb{Q}$, digamos $Q' = a/b$ com $a \in \mathbb{Z}$ e $b \in \mathbb{N}$. Escreva $Q_0 = c/d$, onde $c \in \mathbb{Z} - \{0\}$ e $d \in \mathbb{N}$. Usando $A_0 \neq 0$, Deduzimos que $A_0^{ad} A_1^{bc} = (Q' - Q)^{ad} \in \mathbb{Q}$. Mas isso contradiz a escolha do A_1. Portanto $T \in \mathbb{T}$. □

Por fim deixarei uma questão que motivou todo o trabalho feito em [17].

Questão. Quais condições devemos impor sobre números reais positivos R_1, R_2 para que tenhamos pelo menos um dos números $R_1^{R_2}, R_2^{R_1}$ transcendente?

Referências Bibliográficas

[1] AKHIEZER, N. I. **Elements of the theory of elliptic functions**. Providence, R.I: American Mathematical Society, 1990. 237 p.

[2] BAKER, Alan. **Transcendental number theory**. Cambridge: Cambridge University Press, 1979. 164 p.

[3] BASTOS, Gervásio Gurgel. **Notas de álgebra**. Fortaleza: Premius, 2001. 143 p.

[4] BASTOS, Gervásio Gurgel. **Tópicos de álgebra abstrata**. Fortaleza: Premius, 2003. 128 p.

[5] BURGER, Edward. TUBBS, Robert. **Making transcendence transparent**. New York: Springer, 2004. 263 p.

[6] CHUDNOVSKY, Gregory. **Contributions to the theory of transcendental numbers**. Providence, RI: Amer. Math. Soc., 1984. 450 p.

[7] DIETRICH, Verne. ROSENTHAL, Arthur. Transcendence of factorial series with periodic coefficients. **Bulletin American Mathematical Society**, 55 (1949), 954-956.

[8] ENDLER, Otto. **Teoria dos corpos**. Rio de Janeiro: IMPA, 1987. 204 p. (Monografia de Matemática; n.44).

[9] LANG, Serge. **Algebra**. Massachusetts: Addison-Wesley, 1969. 508 p.

[10] LANG, Serge. **Introduction to transcendental numbers**. Reading: Addison-Wesley, 1966. 105 p.

[11] LE LIONNAIS, François. **Les nombres remarquables**. Paris: Hermann, 1979. 158 p.

[12] LINS NETO, Alcides. **Funções de uma variável complexa**. 2. ed. Rio de Janeiro: IMPA, 1993. 468 p.

[13] MARGOLIUS, Barbara. **Plouffe's constant is transcendental**. (2003, preprint) available at http://www.lacim.uqam.ca/ plouffe/articles/plouffe.pdf.

[14] NIVEN, Ivan Morton. **Irrational numbers**. Rahway, NJ: The Mathematical Association of America, 1956. 164 p.

[15] POLLARD, Harry. **The theory of algebraic numbers**. Baltimore: The Mathematical Association of America, 1950. 141 p. (The Carus Mathematical Monographs; v.9).

[16] SONDOW, Jonathan. **Irrationality measures, irrationality bases and a theorem of Jarnik**. (2004, preprint) available at http://arxiv.org/abs/math.NT/0406300.

[17] SONDOW, Jonathan. MARQUES, Diego. **Algebraic, irrational, and transcendental solutions of some exponential equations and values of the infinite power tower functions**. (2008, preprint.)

[18] USPENSKY, James Victor. **Theory of equations**. New York: MacGraw-Hill, 1948. 353 p.