

Teorema de Hermite-Lindemann

Leonardo Guarnieri

15 de julho de 2016

1 Introdução

Provar a transcendentalidade de um número não é simples. Prova disso são diversos problemas em aberto tais como a transcendentalidade de $\pi^{\sqrt{2}}$ e $\pi + e$. Um teorema que nos permite achar uma classe boa de números transcendentais é certamente importante. Provaremos o Teorema de Hermite-Lindemann (ou Teorema de Lindemann-Weierstrass) aqui e ao final mostraremos que esse teorema nos permite provar a transcendentalidade de diversos números, entre eles π e e , como simples corolários. Além disso, ele nos ajuda a encontrar transcendentais em funções relacionadas com e , tais como $\sin$ e $\cos$.

2 Lemas e notações importantes

Utilizaremos as seguintes notações:

Dada $g \in \mathbb{C}[x]$, digamos $g(x) = \sum_{i=1}^n a_i x^i$, denotamos $g^{Abs}(x) = \sum_{i=1}^n |a_i| x^i$.

Claramente, $|g(x)| \leq g^{Abs}(|x|)$.

Dada $f \in \mathbb{R}[x]$ de grau m , denotamos $I_f(t) = \int_0^t e^{t-x} f(x) dx = e^t \sum_{j=0}^m f^{(j)}(0) - \sum_{j=0}^m f^{(j)}(t)$.

O lema a seguir é um resultado importante que vem da definição de I_f .

Lema 1. *Seja $f \in \mathbb{R}[x]$ de grau m . Então*

$$I_f(t) = \int_0^t e^{t-x} f(x) dx = e^t \sum_{j=0}^m f^{(j)}(0) - \sum_{j=0}^m f^{(j)}(t)$$

Dem. *Faremos indução sobre m . Caso $m = 0$, seja $f(x) = c$, $c \in \mathbb{R}$.*

$$\begin{aligned} I_f(t) &= \int_0^t e^{t-x} c \, dx = c \int_0^t \frac{e^t}{e^x} dx = ce^t \int_0^t \frac{dx}{e^x} = ce^t [-e^{-x}]_0^t = \\ &= -ce^t e^{-t} + ce^t = e^t c - c = e^t \sum_{j=0}^0 f^{(j)}(0) - \sum_{j=0}^0 f^{(j)}(t) \end{aligned}$$

Agora supondo que vale para toda g com $\partial g = m$ fixo, seja $\partial f = m + 1$, e note que $\partial f' = m$, portanto:

$$\begin{aligned}
I_f(t) &= \int_0^t e^{t-x} f(x) dx = e^t [-f(x)e^{-x}]_0^t - \int_0^t e^{-x} f'(x) dx = \\
&= e^t (f(0) - f(t)e^{-t}) + \sum_{j=0}^m f^{(j+1)}(0) - \sum_{j=0}^m f^{(j+1)}(t) = \\
&= e^t (f(0) - f(t)e^{-t}) + \sum_{j=1}^{m+1} f^{(j)}(0) - \sum_{j=1}^{m+1} f^{(j)}(t) = \\
&= e^t f(0) - f(t) + \sum_{j=1}^{m+1} f^{(j)}(0) - \sum_{j=1}^{m+1} f^{(j)}(t) = \\
&= \sum_{j=0}^{m+1} f^{(j)}(0) - \sum_{j=0}^{m+1} f^{(j)}(t)
\end{aligned}$$

O lema a seguir nos mostra uma forma de obter um polinômio de coeficientes racionais a partir de números algébricos. Veremos na seção 2 que esse lema irá reduzir o caso geral ao caso em que determinados coeficientes são inteiros.

Lema 2. *Seja $\{A_i\}_{i=1}^N$ o conjunto de todas as raízes de um polinômio com coeficientes racionais, $0 < n \leq N$ e α_i algébrico para $i \in I_n$. Então*

$$f(x_1, \dots, x_n) = \prod_{\sigma \in S_N} \sum_{i=1}^n A_{\sigma(i)} x_i$$

tem coeficientes racionais.

O lema a seguir é um resultado já conhecido sobre números algébricos.

Lema 3. *Seja $\{A_i\}_{i=1}^n$ uma família de números algébricos. Então existe l algébrico tal que $\{lA_i\}_{i=1}^n$ são raízes de um polinômio mônico $p \in \mathbb{Z}[x]$.*

Finalmente, iremos mostrar propriedades importantes sobre a derivada de funções de uma certa forma.

Lema 4. *Considere $\{\alpha_i\}_{i=1}^n$ algébricos e $\gamma_i(x) = \frac{\prod_{k=1}^n (x - \alpha_k)^p}{x - \alpha_i}$, p primo. Então:*

$$\gamma_i^{(j)}(\alpha_l) = 0, \text{ se } j < p - 1.$$

$$\gamma_i^{(j)}(\alpha_l) = 0, \text{ se } j = p - 1 \text{ e } k \neq i$$

$$\gamma_i^{(j)}(\alpha_l) = (p - 1)! \prod_{\substack{l=1 \\ l \neq i}}^n (\alpha_i - \alpha_l)^p, \text{ se } j = p - 1 \text{ e } k = i$$

$$p! |\gamma_i^{(j)}(\alpha_l)|, \text{ se } j > p - 1.$$

Dem. Lembrando do cálculo que a n -ésima derivada de $\prod f_i$ pode ser obtida somando todos os termos da forma $\prod f_i^{(n_i)}$ onde a soma dos n_i é n . Nesse caso, se $j < p - 1$, nenhum dos termos de $\text{gamma}_i^{(j)}$ some, e aplicando o resultado em qualquer raiz zera todos eles.

Se $j = p - 1$, apenas $(x - \alpha_i)^{p-1}$ some, e apenas quando todas as $p - 1$ derivadas forem tomadas sobre esse fator. Daí, se $l \neq i$, todos os termos zeram e se $l = i$, o único termo que sobra é $(p - 1)! \prod_{\substack{l=1 \\ l \neq i}}^n (\alpha_i - \alpha_l)^p$.

Caso $j > p - 1$, para algum $(x - \alpha_l)^p$ sumir sem zerar o termo, precisamos derivar esse fator exatamente p vezes, e nesse caso, sobra um coeficiente $p!K$, e o termo é múltiplo de $p!$. No caso de sumir $(x - \alpha_i)^{p-1}$, derivamos esse fator $p-1$ vezes, e derivamos algum outro fator pelo menos uma vez, também sobrando um coeficiente da forma $p!K$. Daí, todos os termos da soma são múltiplos de $p!$, e a soma também o é.

3 O Teorema de Hermite-Lindemann

Teorema de Hermite-Lindemann. Sejam $A_1, \dots, A_n, \alpha_1, \dots, \alpha_n$ algébricos, com $\alpha_i \neq \alpha_j$ se $i \neq j$ tais que $\sum_{i=1}^n A_i e^{\alpha_i} = 0$. Então $A_1 = \dots = A_n = 0$.

Separaremos a demonstração em três casos. O primeiro provará o teorema sob uma hipótese conveniente. O segundo ira usar uma hipótese mais fraca e o terceiro será o caso geral, sempre fazendo um caso cair no anterior. Em todos os casos, estaremos supondo por absurdo que algum dos A_i é não nulo.

Caso 1: Inicialmente, suponha que $A_i \in \mathbb{Z}$ e os α_i formam um conjunto completo de conjugados com $A_i = A_j$ se α_i e α_j são conjugados. Podemos reordenar os termos da soma de forma que existam $0 < n_1 < n_2, \dots, n_r < n$ com $\{\alpha_{n_t}, \alpha_{n_t+1}, \dots, \alpha_{n_{t+1}}\}$ formam um conjunto completo de conjugados e $A_{n_t} = A_{n_t+1} = \dots = A_{n_{t+1}}$, para $t \in I_r$. Tome l tal que lA_i e $l\alpha_i$ sejam todos inteiros algébricos, p primo arbitrário e dado $i \in I_n$ considere a seguinte função:

$$f_i(x) = l^{np} \frac{\prod_{k=1}^n (x - \alpha_k)^p}{x - \alpha_i} = l \prod_{k=1}^n \frac{(lx - l\alpha_k)^p}{lx - l\alpha_k}.$$

Note que $f_i \in \mathbb{R}[x]$ e tem grau $np-1$. Além disso, $f_i^{(j)}(\alpha_k)$ é inteiro algébrico. Denote I_{f_i} por I_i , e $J_i = \sum_{k=1}^n A_k I_i(\alpha_k)$. Disso temos:

$$\begin{aligned}
J_i &= \sum_{k=1}^n A_k I_i(\alpha_k) = \sum_{k=1}^n \left(A_k e^{\alpha_k} \sum_{j=0}^{np-1} f_i^{(j)}(0) \right) - \sum_{k=1}^n \left(A_k \sum_{j=0}^{np-1} f_i^{(j)}(\alpha_k) \right) \\
&= \left(\sum_{j=0}^{np-1} f_i^{(j)}(0) \right) \left(\sum_{k=1}^n A_k e^{\alpha_k} \right) - \sum_{k=1}^n \sum_{j=0}^{np-1} (A_k f_i^{(j)}(\alpha_k))
\end{aligned}$$

Mas por hipótese, $\sum_{k=1}^n (A_k e^{\alpha_k}) = 0$, logo

$$J_i = - \sum_{k=1}^n \sum_{j=0}^{np-1} (A_k f_i^{(j)}(\alpha_k)) \quad (1)$$

Temos que para algum p suficientemente grande, temos (Lema 4) que $f_i^{(j)}(\alpha_k)$ $J_i \neq 0$ é divisível por $p!$, exceto se $j = p-1$ e $k = i$. Disso, J_i é inteiro algébrico divisível por $(p-1)!$, mas não por $p!$. É possível ver que J_i racional, mas J_i é inteiro algébrico, logo J_i é inteiro. Temos $\prod_{k=1}^n J_k$ é um inteiro divisível por

$((p-1)!)^n$, e portanto $\left| \prod_{k=1}^n J_k \right| \geq ((p-1)!)^n$.

Agora, mostraremos que $|\alpha_k| e^{|\alpha_k|} F_i(|\alpha_k|) \geq |I_i(\alpha_k)|$, onde $F_i = (f_i)^{Abs}$. De fato

$$|I_i(\alpha_k)| = \left| \int_0^{\alpha_k} e^{\alpha_k - x} f_i(x) dx \right| \leq \int_0^{\alpha_k} |e^{\alpha_k - x}| |f_i(x)| dx$$

Mas $|e^{\alpha_k - x}| |f_i(x)| \leq e^{|\alpha_k|} F_i(|x|)$, logo

$$\int_0^{\alpha_k} |e^{\alpha_k - x}| |f_i(x)| dx \leq |\alpha_k| e^{|\alpha_k|} F_i(|x|)$$

Mas para p primo suficientemente grande, $(p-1)! > b^p$ para todo b e para c suficientemente grande, $\sum_{k=1}^n |A_k| |\alpha_k| e^{|\alpha_k|} F_i(|\alpha_k|) \leq c^p < (p-1)!$. Disso, temos as seguintes desigualdades:

$$((p-1)!)^n \leq \left| \prod_{k=1}^n J_k \right| < \prod_{k=1}^n (p-1)! = ((p-1)!)^n$$

Isso é uma contradição, logo temos que a suposição de que algum dos coeficientes são não nulos é falsa, provando esse caso do teorema.

Caso 2: Agora, suponha apenas que $A_i \in \mathbb{Z}$. Seja $p = I(\mathbb{Q}, \{\alpha_i\}_{i=1}^n)$ tal que $\{\alpha_i\}_{i=1}^n$ sejam raízes de p e sejam $\{\alpha_i\}_{i=n+1}^N$ suas outras raízes. Defina $A_i =$

$0, \forall i \in \{n+1, \dots, N\}$. Como $\sum_{i=1}^n A_i e^{\alpha_i} = 0$, temos que $\prod_{\sigma \in S_n} \left(\sum_{i=1}^n A_i e^{\alpha_{\sigma(i)}} \right) = 0$. Como todos os A_i são inteiros, esse produto pode ser expandido como uma soma de termos da forma $B e^{h_1 \alpha_1 + \dots + h_N \alpha_N}$ onde B e h_i são inteiros para todo $i \in I_N$ e $\sum_{i=1}^N h_i = N!$. Considere o conjunto de todos os números da forma $\sum_{i=1}^N h_i \alpha_i$ onde $\sum_{i=1}^N h_i = N!$. Temos que esse conjunto é um conjunto completo de conjugados, pois

$$\sum_{i=1}^N h_i \alpha_{\sigma(i)} = \sum_{i=1}^N h_{\sigma^{-1}(i)} \alpha_i, \quad \sum_{i=1}^N h_{\sigma^{-1}(i)} = N!$$

e que os coeficientes de termos conjugados são iguais. Do caso anterior, temos que cada um desses coeficientes é 0, e logo cada A_i também o é.

Caso 3: Para o caso geral, tome $p \in \mathbb{Q}[x]$ tal que $\{\alpha_i\}_{i=1}^n$ sejam raízes de p e sejam $\{\alpha_i\}_{i=n+1}^N$ suas outras raízes. Como $\sum_{i=1}^n A_i e^{\alpha_i} = 0$, temos que

$\prod_{\sigma \in S_n} \left(\sum_{i=1}^n A_{\sigma(i)} e^{\alpha_i} \right) = 0$ ⁽¹⁾. Além disso, do Lema 2, sabemos que os coeficientes de $\prod_{\sigma \in S_n} \sum_{i=1}^n A_{\sigma(i)} x_i$ são racionais. Substituindo x_i por e^{α_i} , obtemos que $\prod_{\sigma \in S_n} \left(\sum_{i=1}^n A_{\sigma(i)} e^{\alpha_i} \right) = \sum_{i=1}^{n'} B_i e^{\beta_i}$, onde cada B_i é racional e cada β_i é uma soma de alguns α_i , podendo ocorrer repetições, logo cada β_i é racional. Multiplicando os dois lados de (1) pelo denominador comum, obtemos uma expressão similar, mas com coeficientes inteiros, logo, do caso anterior, $B_i = 0$ e portanto $A_i = 0$.

4 Corolários

Como já mencionado, uma das grandes importâncias desse teorema é o fato de que ele nos permite demonstrar a transcendência de diversos números. Vejamos alguns exemplos.

Corolário 1. *e é transcendente.*

Dem. Seja $p(x) = \sum_{i=1}^n a_i x^i \in \mathbb{Q}[x]$, com $a_n \neq 0$. Pelo teorema de Hermite-Lindemann, $p(e) \neq 0$. Como p foi arbitrário, e é transcendente.

Corolário 2. *Se $x \neq 0$ é algébrico, então e^x é transcendente.*

Dem. Seja $p(x) = \sum_{i=1}^n a_i x^i \in \mathbb{Q}[x]$, com $a_n \neq 0$. Pelo teorema de Hermite-Lindemann, $p(e^x) \neq 0$. Como p foi arbitrário, e^x é transcendente.

Corolário 3. *π é transcendente.*

Dem. Suponha que π seja algébrico. Então πi também o é. Pelo teorema de Hermite-Lindemann, $e^{\pi i} + 1 \neq 0$, o que contradiz a equação de Euler, logo π é transcendente.

Corolário 4. Se $x \neq 0$ é algébrico, então $\sin(x)$, $\cos(x)$, $\sinh(x)$ e $\cosh(x)$ são transcendentos.

Dem. Suponha $\sin(x)$ algébrico. Pelo teorema de Hermite-Lindemann,

$$\frac{e^{ix}}{2} - \frac{e^{-ix}}{2} - \sin(x) \neq 0.$$

Mas isso é uma contradição, logo $\sin(x)$ é transcendente. Análogo para as outras funções.

Corolário 5. Se $x \neq 1$ é algébrico, então $\ln(x)$ é transcendente.

Dem. Suponha que $\ln(x)$ seja algébrico. Pelo teorema de Hermite-Lindemann, $e^{\ln(x)} - x \neq 0$, o que é uma contradição, logo $\ln(x)$ é transcendente.