

**Definición:** Sea  $P(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ . Un número complejo  $\omega \in \mathbb{C}$  se denomina algebraico si  $P(\omega) = 0$ , es decir, si es solución de una ecuación polinómica con coeficientes enteros. Los números complejos que no son algebraicos se denominan trascendentes.

**Teorema de Liouville, 1844:** Existen números trascendentes.

**Teorema de Cantor, 1874:** El conjunto de los números algebraicos es numerable.

**Corolario de Cantor, 1874:** El conjunto de los números trascendentes es no numerable.

**Teorema de Lindemann, 1882:** El número  $\pi$  es trascendente.

**Demostración:** (Ian Stewart, 1970)

Supongamos que  $\pi$  es algebraico. Entonces,  $i\pi$  también es algebraico, es decir,  $\exists p_1(x) \in \mathbb{Z}[x]$  tal que  $p_1(i\pi) = 0$  y sean  $\alpha_1 = i\pi, \alpha_2, \dots, \alpha_n \in \mathbb{C}$  sus raíces.

Por otra parte, como  $e^{i\pi} + 1 = 0$  (fórmula de Euler), se tiene que

$$(e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \dots (e^{\alpha_n} + 1) = 0$$

y, además,  $p_2(\alpha_j + \alpha_k) = 0 \quad \forall j, k = 1, \dots, n$  para  $j \neq k$ , luego

$$p_2(\alpha_j + \alpha_k + \alpha_l) = 0 \quad \forall j, k, l = 1, \dots, n \text{ para } j \neq k \neq l$$

y como consecuencia,  $p(x) = p_1(x)p_2(x) \dots p_n(x) = 0$  es una ecuación polinómica cuyas raíces son todas las sumas que pueden hacerse con las raíces  $\alpha_k$ .

Eliminando las raíces que son cero, si las hay, obtenemos que

$$p(x) = cx^r + c_1 x^{r-1} + \dots + c_r \in \mathbb{Z}[x]$$

con  $c_r \neq 0$ , y conocemos todas sus raíces.

Llamamos  $\beta_1, \dots, \beta_r$  a estas raíces, y obtenemos que

$$e^{\beta_1} + \dots + e^{\beta_r} + e^0 + \dots + e^0 = 0$$

esto es,

$$\sum_{j=1}^r e^{\beta_j} + k = 0$$

Donde  $k \in \mathbb{N}$ , ya que siempre aparece algún 1.

Definimos ahora las funciones

$$f(x) = c^{r^{p-1}} x^{p-1} \frac{[p(x)]^p}{(p-1)!}$$

y

$$F(x) = f(x) + f'(x) + \dots + f^{(p-1)}(x)$$

Se tiene que

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

y, por tanto,

$$e^{-x} F(x) - F(0) = -\int_0^x e^{-y} f(y) dy$$

Multiplicamos la igualdad anterior por  $e^x$  y tomamos  $y = \lambda x$ :

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

Consideramos ahora  $x$  en el rango de los  $\beta_j$ , y sumamos en  $j$ . Como

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

Vamos a demostrar que el miembro de la izquierda de la igualdad es un entero distinto de cero. Por definición de  $f$ , se tiene que

$$\sum_{j=1}^r f^{(t)}(\beta_j) = 0 \text{ para } 0 < t < p$$

Cada derivada de orden  $p$  o mayor, tiene un factor  $c^{rp-1}$  y  $f^{(t)}(\beta_j)$  es un polinomio en  $\beta_j$  con  $\deg f^{(t)}(\beta_j) \leq rp - 1$ .

La suma es simétrica y dado que cada coeficiente es divisible entre  $c^{rp-1}$ , esa suma es un número entero, y al tener a  $p$  como factor se tiene que

$$\sum_{j=1}^r f^{(t)}(\beta_j) = pk_t \text{ para } t = p, \dots, p + (rp - 1)$$

Como consecuencia, el miembro de la izquierda es un número entero más  $kF(0)$ .

Se tiene que

$$\begin{aligned} f^{(t)}(0) &= 0 \text{ para } t = 0, \dots, p-2 \\ f^{(p-1)}(0) &= c^{rp-1} c_r^p \text{ con } c_r \neq 0 \\ f^{(t)}(0) &= p \in \mathbb{Z} \text{ para } t = p, p+1, \dots \end{aligned}$$

Por tanto, el miembro de la izquierda de la igualdad es un entero múltiplo de  $p + c^{rp-1} c_r^p k$ , que no es divisible por  $p$  tomando  $p > k, c, c_r$ .

Así, para valores suficientemente grandes de  $p$ , el miembro de la izquierda es un entero no nulo, pero, por otra parte,

$$\lim_{p \rightarrow +\infty} \left( -\sum_{j=1}^r \beta_j \int_0^1 e^{(1-\lambda)\beta_j} f(\lambda \beta_j) d\lambda \right) = 0$$

lo que constituye una contradicción.

C.Q.D.

### **Resultados sobre la trascendencia de números:**

**Teorema:** Si  $\alpha$  y  $\beta$  son números trascendentes, entonces al menos uno de los números  $\alpha + \beta$ ,  $\alpha\beta$  es trascendente.

**Teorema:** Si  $\alpha$  y  $\beta$  son números trascendentes, entonces al menos uno de los números  $\alpha + \beta$ ,  $\alpha\beta$  es trascendente.

**Teorema de Lindemann, 1882:** El número  $e^\alpha$  es trascendente para todo número algebraico  $\alpha \neq 0$ .

**Corolario:** Si  $\alpha \in \mathbb{C} - \{0, 1\}$  es un número algebraico, entonces  $\log \alpha$  es trascendente.

**Teorema de Lindemann-Weierstrass, 1885:** Si  $\alpha_1, \dots, \alpha_n$  son números algebraicos linealmente independientes sobre  $\mathbb{Q}$ , entonces  $e^{\alpha_1}, \dots, e^{\alpha_n}$  son algebraicamente independientes sobre  $\mathbb{Q}$ , es decir,  $[\mathbb{Q}(e^{\alpha_1}, \dots, e^{\alpha_n}) : \mathbb{Q}] = n$ .

**Corolario:**  $\alpha \in \mathbb{C} - \{0\}$  es un número algebraico, entonces  $e^\alpha$ ,  $\cos \alpha$ ,  $\sin \alpha$  y  $\operatorname{tg} \alpha$  son trascendentes.

**Teorema de Gelfond-Schneider, 1934-1935:** Si  $\alpha$  y  $\beta$  son números algebraicos  $\neq 0, 1$ , y si  $\beta \notin \mathbb{Q}$ , entonces  $\alpha^\beta$  es un número trascendente.

**Teorema:** Sea  $\alpha \in \mathbb{C}$  un número algebraico e  $i \in \mathbb{C}$  la unidad imaginaria. Entonces,  $i\alpha$  también es algebraico.

**Teorema:** Sean  $\alpha, \beta \in \mathbb{C}$  dos números algebraicos y  $P \in \mathbb{Q}[x, y]$ . Entonces,  $P(\alpha, \beta)$  es un número algebraico.

**Teorema de Thue-Siegel-Roth, 1955:** Si  $\alpha \in \mathbb{R}$  es algebraico, entonces para cada  $\varepsilon > 0$ , la inecuación  $\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\varepsilon}}$  solo tiene un número finito de soluciones racionales  $\frac{p}{q}$ .

**Corolario (Criterio de trascendencia):** Si para algún  $\varepsilon > 0$  hay infinitas soluciones racionales, el número  $\alpha \in \mathbb{R}$  es trascendente.

**Limitación del criterio de Thue-Siegel-Roth:** El conjunto de números trascendentes que pueden ser identificados por el criterio de Thue-Siegel-Roth es un conjunto de medida (de Lebesgue) nula.

**Conjetura de Schanuel, ~ 1960:** Sean  $z_1, \dots, z_n \in \mathbb{C}$  linealmente independientes sobre  $\mathbb{Q}$ . Entonces,  $[\mathbb{Q}(z_1, \dots, z_n, e^{z_1}, \dots, e^{z_n}) : \mathbb{Q}] \geq n$ .