UMA 2022

Concurso de Monografías

Teoría de Números Trascendentes

Matías Palumbo

Licenciatura en Matemática

Universidad Nacional de Rosario

Índice

Introducción

La teoría de números trascendentes ha resultado ser una rama de la matemática increíblemente amplia e interesante, no solo por la dificultad inherente a la mayoría de las pruebas sobre trascendencia de números, sino también por la pluralidad de métodos utilizados en este tipo de demostraciones y por el gran impacto que ciertos resultados han tenido en la matemática en general.

Los primeros indicios del desarrollo de esta teoría datan del siglo XVII, cuando Leonhard Euler conjetura que ciertos números de la forma $\log_a(b)$ son trascendentes, es decir, que no son raíz de ningún polinomio no nulo a coeficientes racionales. Sin embargo, el primer resultado formal relacionado a la existencia de números trascendentes se atribuye al matemático Joseph Liouville. Liouville logró definir una clase de números irracionales (los hoy denominados números de Liouville) de manera tal que la propiedad que define a sus elementos es suficiente para garantizar su trascendencia. Concretamente, Liouville probó que si un número puede ser *muy bien aproximado* mediante fracciones, entonces debe ser trascendente. Esta noción de aproximar "muy bien" un número fue perfeccionada a lo largo del siglo XX por matemáticos tales como Axel Thue, Carl Siegel y Klaus Roth, quienes fortalecieron en cada instancia los resultados inicialmente propuestos por Liouville. En 1958, Roth fue premiado con una Medalla Fields por su trabajo en la materia.

Las conjeturas que históricamente han sido objeto de investigación en la teoría de números trascendentes refieren a la trascendencia de números omnipresentes en la matemática, tales como π y e. La trascendencia de este último fue probada por primera vez por Charles Hermite en 1873, aunque Hilbert propuso luego una prueba simplificada que presentamos en esta monografía. Ferdinand von Lindemann continuó esta línea de investigación, probando en 1882 que e^α es trascendente si α es un número algebraico no nulo. En 1885, Karl Weierstrass logró demostrar una versión generalizada de este último resultado, hoy conocida como Teorema de Lindemann-Weierstrass.

En el siglo XX también se pueden apreciar grandes avances en la materia. En 1930, Aleksandr Gelfond y Theodor Schneider probaron la trascendencia de números de la forma a^b, donde a y b son algebraicos, $a \neq 0, 1$ y $b \notin \mathbb{Q}$. Este interrogante había sido popularizado originalmente por David Hilbert, quien lo incluyó como el séptimo de los legendarios problemas de Hilbert: una lista con 23 problemas abiertos (hasta ese entonces) de la matemática, publicada por el propio Hilbert en 1900. Otro exponente moderno en la teoría de números trascendentes es Alan Baker, quien en la década del 60 demostró una generalización del Teorema de Gelfond-Schneider la cual resultó tener aplicaciones en la teoría de ecuaciones diofánticas, es decir, ecuaciones con dos o más incógnitas sobre los números enteros.

El propósito de esta monografía es introducir al lector en los principales conceptos y resultados de la teoría de números trascendentes. Sin embargo, para poder indagar en profundidad en la materia resulta necesario comprender en detalle el conjunto de los números algebraicos y sus particularidades. Por esta razón, el primer capítulo se dedica a presentar las nociones básicas de la teoría de números algebraicos.

En el segundo capítulo se estudian algunas propiedades que sirven como introducción al estudio del conjunto de números trascendentes, para luego exponer los primeros resultados formales de la teoría: los números de Liouville, sus propiedades y lo que éstas implican en materia de trascendencia.

El tercer capítulo se dedica en su totalidad a la exposición de los más notables avances en la materia, muchos de los cuales fueron mencionados en los párrafos anteriores. A grandes rasgos, éstos incluyen las pruebas de trascendencia de e y π, los teoremas de Lindemann-Weierstrass, Gelfond-Schneider y Schneider-Lang, así como también observaciones sobre las aplicaciones de algunos de estos resultados en otras áreas de la matemática.

Capítulo 1

Números Algebraicos

1. Nociones Básicas

Notamos con $\mathbb{Q}[x]$ al conjunto de todos los polinomios a coeficientes racionales, y con $\mathbb{Z}[x]$ al conjunto de los polinomios a coeficientes enteros.

Definición 1.1.1. Un número complejo α es **algebraico** si existe $P \in \mathbb{Q}[x]$, $P \neq 0$ tal que $P(\alpha) = 0$.

Un número complejo α es **trascendente** si no es algebraico. Es decir, si α no es raíz de ningún polinomio no nulo a coeficientes racionales.

La definición de número algebraico en términos de polinomios a coeficientes *enteros* es equivalente a la dada. Esto se debe a que, dado un polinomio

$$P(x) = \sum_{k=0}^{n} a_k x^k$$

a coeficientes racionales, la ecuación $P(x) = 0$ tendrá las mismas soluciones que la ecuación $kP(x) = 0$ a coeficientes enteros, donde k es el mínimo común múltiplo de los denominadores de los coeficientes.

Por conveniencia, en ocasiones utilizaremos dicha definición equivalente.

Definición 1.1.2. El **grado** de un número algebraico α se define como

$$\deg(\alpha) = \min \{\deg(P) : 0 \neq P \in \mathbb{Q}[x] \wedge P(\alpha) = 0\}.$$

Es decir, el grado de α es el mínimo grado de los polinomios no nulos de $\mathbb{Q}[x]$ de los cuales α es raíz.

Definición 1.1.3. El **polinomio mínimo** de α se define como el único polinomio $P \in \mathbb{Q}[x]$ que verifica:

1. $\deg(P) = \deg(\alpha)$.

2. El coeficiente principal de P es 1 (un polinomio de este tipo se suele llamar **mónico**).
3. $P(\alpha) = 0$.

Teorema 1.1.4. *(Buena definición) Todo número algebraico tiene un único polinomio mínimo.*

Demostración. Sean $P, Q \in \mathbb{Q}[x]$ tal que P es un polinomio mínimo de α y $Q(\alpha) = 0$. Por el algoritmo de división para polinomios, existen $D, R \in \mathbb{Q}[x]$ con $\deg(R) < \deg(P)$ tal que

$$Q(x) = D(x)P(x) + R(x).$$

Además, $Q(\alpha) = P(\alpha) = 0$ implica que $R(\alpha) = 0$, y así $R \equiv 0$ por ser P un polinomio mínimo de α. Por lo tanto, Q divide a P.

Ahora, si suponemos que Q es un polinomio mínimo de α, de lo anterior podemos concluir que P divide a Q. Entonces $P(x) = cQ(x)$ para alguna constante $c \in \mathbb{Q}$. Sin embargo, ambos polinomios son mónicos, por lo que $P(x) = Q(x)$. $\square$

Definición 1.1.5. Un número algebraico es un **entero algebraico** si su polinomio mínimo es a coeficientes enteros.

Nos encontramos en condiciones de identificar algunos números algebraicos. Los polinomios de la forma

$$x - \frac{p}{q},$$

donde p y q son enteros coprimos, tienen como solución (única) al número racional p/q, por lo que todo número racional es un número algebraico (pero no es un entero algebraico si $q \neq 1$). Es simple ver que la raíz enésima de todo número racional también es un número algebraico: podemos considerar polinomios de $\mathbb{Q}[x]$ de la forma

$$x^n - \frac{p}{q}.$$

Números como i y el número áureo $\varphi = \frac{1+\sqrt{5}}{2}$ también verifican ser algebraicos, al ser solución de los polinomios cuadráticos

$$P(x) = x^2 + 1 \qquad y \qquad Q(x) = x^2 - x + 1$$

respectivamente.

2. Polinomios Simétricos

Para explorar las propiedades más interesantes del conjunto de números algebraicos precisamos utilizar resultados de la teoría de polinomios simétricos. A continuación, se define la noción de cuerpo, los conceptos de polinomio simétrico y polinomio simétrico elemental, y se prueba el Teorema Fundamental de los Polinomios Simétricos. La demostraciones de esta sección utilizan ideas dadas por Cox [1].

Definición 1.2.6. Un **cuerpo** es una terna $(F,+,\cdot)$, donde F es un conjunto y $+, \cdot$ son funciones de $F \times F$ en F que verifican las siguientes propiedades:

1. Ambas operaciones son asociativas y conmutativas.
2. Vale la propiedad distributiva de $+$ con respecto a $\cdot$.
3. Existen $0, 1 \in F$ tales que $a + 0 = a$ y $a \cdot 1 = a$ para todo $a \in F$.
4. Para todo $a \in F$ existe $-a \in F$ tal que $a + (-a) = 0$.
5. Para todo $a \in F$ existe $a^{-1} \in F$ tal que tal que $a \cdot a^{-1} = 1$.

Observación 1.2.7. $\mathbb{Q}$ es un cuerpo con la suma y el producto usual.

Notamos por $F[x_1, \dots, x_n]$ al conjunto de polinomios en las variables $x_1, \dots, x_n$ con coeficientes en el cuerpo F.

Definición 1.2.8. Un polinomio $P \in \mathbb{Q}[x_1, \dots, x_n]$ es **simétrico** si

$$P\left(x_{\tau(1)}, \dots, x_{\tau(n)}\right) = P(x_1, \dots, x_n)$$

para cualquier permutación de n elementos τ.

Definición 1.2.9. Sean $x_1, \dots, x_n$ variables sobre un cuerpo F. Los **polinomios simétricos elementales** en $x_1, \dots, x_n$ son

$$\begin{aligned} \sigma_1 &= \sum_{i=1}^{n} x_i, \\ \sigma_2 &= \sum_{1 \leq i < j \leq n} x_i x_j, \\ &\vdots \\ \sigma_r &= \sum_{1 \leq i_1 < \ldots < i_r \leq n} x_{i_1} x_{i_2} \cdots x_{i_r}, \\ &\vdots \\ \sigma_n &= x_1 x_2 \cdots x_n. \end{aligned}$$

Evidentemente $\sigma_1, \dots, \sigma_n \in F[x_1, \dots, x_n]$. En ocasiones notamos $\sigma_i = \sigma_i(x_1, \dots, x_n)$ para $i = 1, \dots, n$.

Observación 1.2.10. Los polinomios simétricos elementales son simétricos.

Teorema 1.2.11. *Sea $P \in F[x]$ un polinomio con raíces $\alpha_1, \dots, \alpha_n$. Luego,*

$$P(x) = \prod_{i=1}^{n}(x - \alpha_i) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^r \sigma_r x^{n-r} + \cdots + (-1)^n \sigma_n,$$

donde los polinomios $\sigma_1, \dots, \sigma_n$ son los polinomios simétricos elementales en $\alpha_1, \dots, \alpha_n$.

Demostración. El teorema se deduce de expandir el producto

$$\prod_{i=1}^{n}(x - \alpha_i).$$

En general, los pasos para calcular el término asociado a x^r son:

1. Para cada uno de los n factores $x - \alpha_i$ elegimos x o α_i de manera que se haya elegido x exactamente r veces.
2. Tomamos el producto de las variables elegidas.
3. Sumamos los productos de todas las posibles elecciones de las variables.

Por ejemplo, el término independiente de P es

$$(-\alpha_1)(-\alpha_2)\cdots(-\alpha_n) = (-1)^n \alpha_1 \alpha_2 \cdots \alpha_n = (-1)^n \sigma_n.$$

□

Corolario 1.2.12. *Sea $P(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in F[x]$ de grado $n > 0$. Luego, los coeficientes a_k de P quedan expresados en términos las raíces $\alpha_1, \dots, \alpha_n$ de P de la siguiente manera:*

$$a_r = (-1)^r \sigma_r(\alpha_1, \dots, \alpha_n), \qquad r = 1, \dots, n.$$

Teorema 1.2.13. ***(Teorema Fundamental de los Polinomios Simétricos)*** *Todo polinomio simétrico de $F[x_1, \dots x_n]$ puede ser escrito de manera única como un polinomio de $F[\sigma_1, \dots, \sigma_n]$, donde $\sigma_1, \dots, \sigma_n$ son los polinomios simétricos elementales en $x_1, \dots, x_n$.*

Demostración. Ordenamos monomios de acuerdo al *orden lexicográfico graduado*: concretamente,

$$\begin{aligned} x_1^{a_1} \cdots x_n^{a_n} < x_1^{b_1} \cdots x_n^{b_n} \iff & a_1 + \cdots + a_n < b_1 + \cdots + b_n, \\ & \text{ó } a_1 + \cdots + a_n = b_1 + \cdots + b_n \\ & \quad \text{y } a_1 < b_1, \\ & \text{ó } a_1 + \cdots + a_n = b_1 + \cdots + b_n \\ & \quad \text{y } a_1 = b_1 \text{ y } a_2 < b_2, \\ & \dots \end{aligned}$$

Además, $x_1^{b_1}\cdots x_n^{b_n} > x_1^{a_1}\cdots x_n^{a_n} \iff x_1^{a_1}\cdots x_n^{a_n} < x_1^{b_1}\cdots x_n^{b_n}$. Definimos el término principal de $P \in F[x_1,\dots,x_n]$ como el término en el cual el producto de las variables es mayor respecto al orden lexicográfico graduado.

Destacamos dos consecuencias importantes de este orden:

1. Fijados $a_1,\dots,a_n$, existe una cantidad finita de monomios $x_1^{b_1}\cdots x_n^{b_n}$ tales que $x_1^{b_1}\cdots x_n^{b_n} < x_1^{a_1}\cdots x_n^{a_n}$. Esto se debe a que si $x_1^{b_1}\cdots x_n^{b_n} < x_1^{a_1}\cdots x_n^{a_n}$, entonces $N := a_1+\cdots+a_n \geq b_1+\cdots+b_n$, y así existen a los sumo $N+1$ posibles elecciones para cada b_i.

2. Si $P \in F[x_1,\dots,x_n]$ es simétrico y su término principal es $cx_1^{a_1}\cdots x_n^{a_n}$, entonces $a_1 \geq a_2 \geq \cdots \geq a_n$. Si suponemos que $a_i < a_{i+1}$ para algún $i \in \{1,\dots,n-1\}$, como P es simétrico, intercambiar las variables x_i y x_{i+1} resulta en el mismo polinomio. Además, como $cx_1^{a_1}\cdots x_n^{a_n}$ es un término de P, $cx_1^{a_1}\cdots x_{i+1}^{a_i}x_i^{a_{i+1}}\cdots x_n^{a_n}$ también lo es. Sin embargo, $cx_1^{a_1}\cdots x_n^{a_n} < cx_1^{a_1}\cdots x_{i+1}^{a_i}x_i^{a_{i+1}}\cdots x_n^{a_n}$ de acuerdo al orden lexicográfico graduado, contradiciendo el hecho de que $cx_1^{a_1}\cdots x_n^{a_n}$ es el término principal.

Probemos el teorema. Sea $P \in F[x_1,\dots,x_n]$ un polinomio simétrico no nulo con término principal $c_0x_1^{a_1}\cdots x_n^{a_n}$ (el resultado es evidente para el polinomio nulo). Definimos

$$Q_0 := \sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3}\cdots\sigma_{n-1}^{a_{n-1}-a_n}\sigma_n^{a_n},$$

donde $\sigma_1,\dots,\sigma_n$ son los polinomios simétricos elementales en $x_1,\dots,x_n$. Nótese que Q_0 está bien definido debido a la propiedad anterior ($a_i - a_j \geq 0$ para $i \leq j$). Además, el término principal de Q_0 es el producto de los términos principales de los polinomios σ_r elevados a sus respectivos exponentes. Luego, como el termino principal de σ_r es $x_1\cdots x_r$, el término principal de Q_0 es

$$x_1^{a_1-a_2}(x_1x_2)^{a_2-a_3}\cdots(x_1\cdots x_{n-1})^{a_{n-1}-a_n}(x_1\cdots x_n)^{a_n} =$$
$$x_1^{a_1-a_2+a_2-a_3+\cdots-a_n+a_n}x_2^{a_2-a_3+\cdots-a_n+a_n}\cdots x_{n-1}^{a_{n-1}-a_n+a_n}x_n^{a_n} = x_1^{a_1}\cdots x_n^{a_n}.$$

Es decir, P y c_0Q_0 tienen el mismo término principal. Por lo tanto, $P_1 := P - c_0Q_0$ tiene un término principal estrictamente menor (de acuerdo al orden lexicográfico graduado) que el término principal de P.

Repetimos el proceso anterior. Como P_1 es simétrico al serlo P y Q_0, su término principal $c_1x_1^{b_1}\cdots x_n^{b_n}$ verifica $b_1 \geq \cdots \geq b_n$. Definimos Q_1 como la expresión análoga a Q_0 en términos de los polinomios simétricos elementales de manera que P_1 y c_1Q_1 tengan el mismo término principal. Continuando de esta manera, obtenemos polinomios

$$\begin{gathered} P_0 := P, \\ P_1 = P - c_0Q_0, \\ P_2 = P - c_0Q_0 - c_1Q_1, \\ P_3 = P - c_0Q_0 - c_1Q_1 - c_2Q_2, \\ \vdots \end{gathered}$$

donde el término principal de P_i es estrictamente mayor que el de P_{i+1}. Podemos asegurar que $P_m \equiv 0$ para cierto $m \in \mathbb{N}$, ya que en caso contrario existiría una sucesión infinita de polinomios no nulos con términos principales estrictamente decrecientes, contradiciendo el hecho de que existen finitos monomios menores al término principal de P.

Por lo tanto,

$$P_m = P - \sum_{i=0}^{m-1} c_i Q_i = 0.$$

Cada polinomio Q_i es un producto de potencias de los polinomios simétricos elementales en $x_1, \ldots, x_n$, y luego

$$P = \sum_{i=0}^{m-1} c_i Q_i = \sum_{i=0}^{m-1} c_i Q_i(\sigma_1, \ldots, \sigma_n) \in F[\sigma_1, \ldots, \sigma_n].$$

La prueba de la unicidad de esta expresión de P puede encontrarse en *Teoría de Galois*, de David Cox (2012). □

3. El Cuerpo de los Números Algebraicos

A continuación probamos una de las propiedades más interesantes sobre el conjunto de números algebraicos: sus elementos forman un cuerpo. La suma y el producto de dos números algebraicos es, entonces, un número algebraico. Gracias a esto último estaremos en condiciones de probar fácilmente la naturaleza algebraica de una infinidad de números, ya que cualquier combinación lineal algebraica de números algebraicos resulta ser un número algebraico.

Teorema 1.3.14. *El conjunto de números algebraicos es un cuerpo con la suma y la multiplicación usual.*

Demostración. Debemos probar que la suma y el producto de dos números algebraicos es un número algebraico, y que el inverso de un número algebraico es también algebraico. Se sigue la prueba dada por Niven [2].

Dados α y β números algebraicos de grado m y n respectivamente, veamos que $\alpha+\beta$ es algebraico. Sea $P(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ el polinomio mínimo de α. Notemos que la igualdad $P(\alpha) = 0$ permite expresar a α^m como combinación lineal racional de $1, \alpha, \alpha^2 \ldots, \alpha^{m-1}$. Concretamente,

$$\alpha^m = -a_{m-1}\alpha^{m-1} - \cdots - a_1\alpha - a_0,$$

y por lo tanto

$$\alpha^{m+r} = -a_{m-1}\alpha^{m+r-1} - \cdots - a_1\alpha^{r+1} - a_0\alpha^r$$

para todo $n \in \mathbb{N}$. Reemplazando los términos con exponente mayor a m por la expresión de α^m podemos concluir que α^{m+r} es combinación lineal racional de $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ para todo $r \in \mathbb{N}$. Análogamente, β^{n+r} es combinación lineal racional de $1, \beta, \beta^2, \ldots, \beta^{n-1}$ para todo $r \in \mathbb{N}$.

Consideremos ahora los $mn + 1$ números

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

Expandiendo la expresión de cada número y reemplazando las potencias de α y β con exponentes mayores que m y n por sus respectivas expresiones, obtenemos que cada uno de estos $mn+1$ números es combinación lineal racional de los mn números $\alpha^j\beta^k$, con $j = 0, 1, \ldots, m-1$ y $k = 0, 1, \ldots, n-1$. Es decir, existe una matriz $A \in \mathbb{Q}^{(mn+1)\times mn}$ tal que

$$\begin{pmatrix} 1 \\ \alpha + \beta \\ (\alpha + \beta)^2 \\ \vdots \\ (\alpha + \beta)^{mn} \end{pmatrix} = A \begin{pmatrix} 1 \\ \alpha \\ \beta \\ \vdots \\ \alpha^m\beta^n \end{pmatrix}.$$

Como la matriz A tiene a lo sumo rango mn, podemos concluir que existe $k \in \{1, \ldots, mn\}$ tal que $(\alpha + \beta)^k$ puede expresarse como combinación lineal de $(\alpha + \beta)^i$, para $i = 0, 1 \ldots, mn$, $i \neq k$. Concretamente,

$$(\alpha + \beta)^k = c_{mn}(\alpha + \beta)^{mn} + \cdots + c_{k+1}(\alpha + \beta)^{k+1} + c_{k-1}(\alpha + \beta)^{k-1} + \cdots + c_0.$$

Es decir, si $c_k := -1$, $\alpha + \beta$ es raíz del polinomio (no nulo) a coeficientes racionales

$$P(x) = \sum_{i=0}^{mn} c_i x^i,$$

y por lo tanto es un número algebraico.

El razonamiento para demostrar que $\alpha\beta$ es algebraico es completamente análogo; en lugar de las potencias de $\alpha + \beta$ se deben considerar las potencias de $\alpha\beta$.

Por último, notemos que si α es un número algebraico de grado m y P es su polinomio mínimo, luego

$$\tilde{P}(x) = x^m P\left(\frac{1}{x}\right)$$

es un polinomio no nulo a coeficientes racionales, y

$$\tilde{P}\left(\frac{1}{\alpha}\right) = \frac{1}{\alpha^m} P(\alpha) = 0.$$

$\square$

Si bien destacamos la conveniencia de poder atribuirle al conjunto de números algebraicos la estructura de un cuerpo, la propiedad más fascinante se presenta a continuación. El cuerpo de los números algebraicos resulta ser **algebraicamente cerrado**. Esto es, toda raíz de un polinomio a coeficientes algebraicos es a su vez un número algebraico. En consecuencia, la **clausura algebraica** de $\mathbb{Q}$ son los números algebraicos, razón por la cual el cuerpo de los números algebraicos suele notarse por $\overline{\mathbb{Q}}$.

Como quizás el lector haya notado, los resultados de esta sección no solo tienen como propósito profundizar la comprensión de los números algebraicos. Cada estructuración, caracterización y teorema que incluya a los números algebraicos es automáticamente una herramienta en toda prueba sobre trascendencia. Como veremos más adelante en esta monografía, las pruebas en la teoría de números trascendentes son intrínsecamente complejas, por lo que es indispensable construir un arsenal de herramientas de la teoría de números algebraicos a la hora de afrontar los números trascendentes.

Probamos en primer lugar un lema dado por Niven [2], necesario para demostrar que $\mathbb{Q}$ es algebraicamente cerrado:

Lema 1.3.15. *Sean $\alpha_1, \ldots, \alpha_n$ las raíces de un polinomio*

$$P(x) = bx^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}[x].$$

Sea $Q \in \mathbb{Q}[x_1, \ldots, x_n]$ un polinomio simétrico. Luego, $Q(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$.

Demostración. Notemos que $b\alpha_1, \ldots, b\alpha_n$ son las raíces de

$$b^{n-1}P\left(\frac{x}{b}\right) = x^n + a_1x^{n-1} + ba_2x^{n-2} + \cdots + b^{n-2}a_{n-1}x + b^{n-1}a_n.$$

Como el polinomio anterior es a coeficientes enteros, por el Corolario 1.2.12 los polinomios simétricos elementales $\sigma_k(b\alpha_1, \ldots, b\alpha_n)$ son a coeficientes enteros.

Por otro lado, para cualquier polinomio simétrico elemental σ de grado r (es decir, $\sigma = \sigma_r$),

$$\sigma(b\alpha_1, \ldots, b\alpha_n) = b^r\sigma(\alpha_1, \ldots, \alpha_n),$$

ya que cada término del polinomio es el producto de r variables. Ahora, el Teorema Fundamental de los Polinomios Simétricos nos permite expresar a Q como un polinomio de $\mathbb{Q}[\sigma_1, \ldots, \sigma_n]$. Concretamente,

$$Q(x_1, \ldots, x_n) = c_0 + \sum_{k=1}^{n} c_k\sigma_k(x_1, \ldots, x_n),$$

donde $c_k \in \mathbb{Q}$ para $k = 0, 1, \ldots, n$. Por lo tanto,

$$b^nQ(\alpha_1, \ldots, \alpha_n) = b^nc_0 + \sum_{k=1}^{n} b^{n-k}c_k\sigma_k(b\alpha_1, \ldots, b\alpha_n)$$

es un número racional, y así $Q(\alpha_1, \ldots, \alpha_n)$ lo es. $\square$

Teorema 1.3.16. *Toda raíz de un polinomio $P(x)$ a coeficientes algebraicos es un número algebraico.*

Demostración. Sin pérdida de generalidad, supongamos que P es mónico. Luego $P(x) = x^n + \alpha_n x^{n-1} + \cdots + \alpha_2 x + \alpha_1$, donde $\alpha_1, \ldots, \alpha_n$ son números algebraicos. Podemos identificar a P como un polinomio a coeficientes racionales en las variables $x, \alpha_1, \ldots, \alpha_n$. Notemos por $\tilde{P}$ a dicha identificación. Es decir, $\tilde{P} \in \mathbb{Q}[x, \alpha_1, \ldots, \alpha_n]$.

Sean $\beta_1 := \alpha_1, \beta_2, \ldots, \beta_k$ las raíces del polinomio mínimo de α_1. Definimos $Q \in \mathbb{Q}[x, \alpha_2, \ldots, \alpha_n]$ de la siguiente manera:

$$Q(x, \alpha_2, \ldots, \alpha_n) = \prod_{i=1}^{k} \tilde{P}(x, \beta_i, \alpha_2, \ldots, \alpha_n).$$

Nótese que las raíces de $\tilde{P}$ son raíces de Q. Además, Q es un polinomio simétrico con respecto a $\beta_1, \ldots, \beta_n$. Más aún, expandiendo el producto en la definición de Q se puede observar que cada coeficiente de Q es un polinomio simétrico de $\mathbb{Q}[\beta_1, \ldots, \beta_n]$. Aplicando el Teorema Fundamental de los Polinomios Simétricos y el Corolario 1.2.12 obtenemos que cada uno de estos coeficientes es un número racional. Por lo tanto, podemos reescribir a Q de la siguiente manera:

$$Q(x, \alpha_2, \ldots, \alpha_n) = x^h + f_{h-1}(\alpha_2, \ldots, \alpha_n)x^{h-1} + \cdots + f_0(\alpha_2, \ldots, \alpha_n),$$

donde $f_i \in \mathbb{Q}[x, \alpha_2, \ldots, \alpha_n]$. Como los números algebraicos forman un cuerpo, cada una de las funciones f_i evaluadas en $\alpha_2, \ldots, \alpha_n$ corresponden a un número algebraico. Así, repitiendo el proceso anterior $n-1$ veces obtenemos una expresión para Q que no depende de ninguno de los números algebraicos α_i. Esto es, Q es de la forma

$$x^s + a_{s-1}x^{s-1} + \cdots + a_0,$$

donde $a_i \in \mathbb{Q}$ para $i = 0, \ldots, s-1$. Por lo tanto, toda raíz de Q es un número algebraico, y en particular todas las raíces de $\tilde{P}$ (y por ende de P) son números algebraicos. $\square$

Capítulo 2

Números Trascendentes

Quitemos el foco de los números algebraicos para comenzar a estudiar los números trascendentes en sí.

Como se advirtió en el capítulo anterior, las pruebas sobre trascendencia usualmente tienen un grado de dificultad mayor que las demostraciones que aseguran que un número dado es algebraico. Por un lado, tan solo aplicando la Definición 1.1.1 probamos la naturaleza algebraica de una infinidad de números, ya que encontrar un polinomio del cual un número dado sea raíz es lo único necesario para asegurar que dicho número es algebraico. Sin embargo, la dinámica es completamente distinta en pruebas sobre trascendencia. En estos casos se debe demostrar que el número en cuestión no es raíz de *ningún* polinomio no nulo a coeficientes racionales. Si bien veremos que es posible construir funciones que permitan deducir esto, no existe un criterio general para determinar la trascendencia de un número, ni tampoco resultados que refieran a la trascendencia de combinaciones aritméticas de números trascendentes.

Ante la ausencia de un criterio generalizado y la dificultad intrínseca a este tipo de pruebas, la gran mayoría de las demostraciones se realizan por contradicción, suponiendo que el número en cuestión es algebraico.

Para comenzar, consideremos dos resultados relativamente simples.

Teorema 2.0.1. *$\alpha = a + ib \in \mathbb{C}$ (con $a, b \in \mathbb{R}$) es un número trascendente si y sólo si $\mathfrak{Re}\,\alpha = a$ es trascendente o $\mathfrak{Im}\,\alpha = b$ es trascendente.*

Demostración. Si $\alpha = a + ib$ $(a, b \in \mathbb{R})$ es trascendente pero a y b son algebraicos, al ser $\overline{\mathbb{Q}}$ un cuerpo obtenemos que $\alpha = a + ib$ es algebraico, una clara contradicción.

Recíprocamente, supongamos sin pérdida de generalidad que a es trascendente pero que α es algebraico. En dicho caso, $\overline{\alpha}$ (el conjugado de α) también es algebraico ya que es raíz del polinomio mínimo de α, al tener dicho polinomio coeficientes racionales (y en particular, reales). Por lo tanto,

$$a = \frac{\alpha + \overline{\alpha}}{2}$$

es un número algebraico, nuevamente una contradicción. $\square$

Equivalentemente, el teorema anterior establece que un número es algebraico si y solo si sus partes real e imaginaria son números algebraicos.

Teorema 2.0.2. *Si α y β son números trascendentes, entonces $\alpha+\beta$ es trascendente o $\alpha\beta$ es trascendente.*

Demostración. Si suponemos que ambos $\alpha+\beta$ y $\alpha\beta$ son números algebraicos, el polinomio $P(x) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$ es a coeficientes algebraicos. Del Teorema 1.3.16 obtenemos que α y β son algebraicos, contradiciendo lo supuesto. $\square$

Todavía no hemos probado que existen números trascendentes. Si bien se puede intuir que este es el caso (si no existieran los números trascendentes, tampoco lo haría esta monografía), debemos de alguna forma garantizar la trascendencia de al menos un número.

Georg Cantor fue quien formalizó, con su mirada puesta en el infinito, uno de los conceptos más útiles e interesantes de la matemática: la cardinalidad de un conjunto. Probemos el siguiente resultado sobre la cardinalidad del cuerpo de los números algebraicos, para luego deducir la del conjunto de números trascendentes y así, de una vez por todas, demostrar formalmente su existencia.

Teorema 2.0.3. *$\overline{\mathbb{Q}}$ es numerable.*

Demostración. Comencemos observando que $\mathbb{Q}[x]$ es numerable. Efectivamente, para $n \in \mathbb{N}_0$ el conjunto

$$\mathbb{Q}_n[x] = \{P \in \mathbb{Q}[x] : P \text{ es de grado } n\}$$

es numerable al serlo $\mathbb{Q}$, y es claro que

$$\mathbb{Q}[x] \setminus \{0\} = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_n[x]$$

es numerable, al ser unión numerable de conjuntos numerables (el grado del polinomio nulo se define como -1).

El Teorema Fundamental del Álgebra establece que todo polinomio no nulo de $\mathbb{Q}[x]$ de grado n tiene a lo sumo n raíces complejas distintas. Por lo tanto, el conjunto

$$\overline{\mathbb{Q}} = \bigcup_{0\neq P\in\mathbb{Q}[x]} \{x : x \text{ es raíz de } P\}$$

es numerable al ser unión numerable de conjuntos finitos. $\square$

Corolario 2.0.4. *El conjunto de números trascendentes es no numerable.*

Demostración. El resultado surge del Teorema 2.0.3 y de la no numerabilidad de $\mathbb{C}$. Como $\mathbb{C}$ es unión disjunta de $\overline{\mathbb{Q}}$ y $\mathbb{C}\setminus\overline{\mathbb{Q}}$, debe haber una cantidad infinita no numerable de números trascendentes. $\square$

La teoría de la medida brinda otra herramienta útil a la hora de sacar conclusiones sobre los números trascendentes. Notemos que al ser $\overline{\mathbb{Q}}$ numerable, es un conjunto de medida nula, y luego "casi todo" número complejo es trascendente. En cierto modo, podría decirse que los números algebraicos "no ocupan espacio" en el plano complejo.

1. Números de Liouville

Los resultados de esta sección, originalmente propuestos por Joseph Liouville [3], constituyen los primeros avances formales en la teoría de números trascendentes.

Definición 2.1.5. $\alpha \in \mathbb{R}$ es un **número de Liouville** si para todo $n \in \mathbb{N}$ existe algún racional p/q, con $p, q \in \mathbb{Z}$ y $q > 1$, tal que

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

El conjunto de números de Liouville es no vacío: veamos que

$$\alpha = \sum_{n=0}^{\infty} 2^{-n!}$$

verifica la Definición 2.1.5.

Sea $n \in \mathbb{N}$. Consideremos $q = 2^{n!}$ y $p = q\sum_{k=0}^{n} 2^{-k!}$. Luego,

$$\left|\alpha - \frac{p}{q}\right| = \left|\sum_{k=n+1}^{\infty} 2^{-k!}\right| = \sum_{k=n+1}^{\infty} 2^{-k!} < \sum_{k=(n+1)!}^{\infty} 2^{-k} = 2^{-(n+1)!+1} \leq 2^{-n!n} = \frac{1}{q^n}.$$

Más generalmente, podemos probar lo siguiente: fijados un número natural $b > 1$ y una sucesión $(a_n)_{n\in\mathbb{N}}$ tal que $a_n \in \{x \in \mathbb{N}_0 : 0 \leq x \leq b-1\}$ para todo $n \in \mathbb{N}$ y $a_n \neq 0$ para infinitos n, el número

$$\alpha = \sum_{n=1}^{\infty} a_n b^{-n!}$$

es un número de Liouville.

El procedimiento es similar al anterior: dado $n \in \mathbb{N}$ definimos $q = b^{n!}$ y $p = q \sum_{k=0}^{n} a_k b^{-k!}$. Luego,

$$0 < \left| \alpha - \frac{p}{q} \right| = \sum_{k=n+1}^{\infty} a_k b^{-k!} \leq \sum_{k=n+1}^{\infty} (b-1) b^{-k!}.$$

Por otro lado,

$$\sum_{k=n+1}^{\infty} (b-1) b^{-k!} < (b-1) \sum_{k=(n+1)!}^{\infty} b^{-k} < b^{-(n+1)!+2} \leq b^{-n!n} = \frac{1}{q^n}.$$

Es decir, α verifica la Definición 2.1.5.

Teorema 2.1.6. *Todo número de Liouville es irracional.*

Demostración. Supongamos que α es un número de Liouville racional. Sean $a, b \in \mathbb{Z}$ coprimos tales que $b > 0$ y $\alpha = a/b$. Consideremos también $n \in \mathbb{N}$ tal que $2^{n-1} > b$ y $p, q \in \mathbb{Z}$ como en la Definición 2.1.5. Es decir, p y q verifican

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^n}.$$

Además,

$$0 < \left| \frac{a}{b} - \frac{p}{q} \right| = \left| \frac{aq - bp}{bq} \right|.$$

Notemos que, de la desigualdad anterior, $|aq - bp| \geq 1$. Por lo tanto,

$$\frac{1}{bq} \leq \left| \frac{aq - bp}{bq} \right| = \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^n}.$$

De estas desigualdades podemos concluir que $q^n < bq$. Entonces,

$$q^{n-1} < b < 2^{n-1}.$$

Sin embargo, la desigualdad $q^{n-1} < 2^{n-1}$ implica que $q \leq 1$, contradiciendo el hecho de que $q > 1$ de acuerdo a lo establecido en la Definición 2.1.5. Por lo tanto, α es irracional. □

Habiendo probado la irracionalidad de todo número de Liouville, es natural que surja el interrogante sobre su trascendencia. A propósito de esto, Liouville logra encontrar una condición necesaria para que un número dado sea algebraico, y por lo tanto, una condición suficiente para su trascendencia. La estrecha relación entre esta condición y la dada en la Definición 2.1.5 es la esencia del *Teorema de Liouville (sobre aproximación diofántica)*, presentado a continuación. La demostración del teorema sigue las ideas originales de Liouville, analizadas con mayor claridad por Baker [4], y la prueba del corolario subsiguiente hace uso de ideas propuestas por Oxtoby [5].

Teorema 2.1.7. *(Teorema de Liouville) Sea α un número algebraico de grado $n > 1$. Luego, existe $C > 0$ tal que para cualesquiera $p, q \in \mathbb{Z}$, con $q > 0$,*

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

Demostración. Notemos que α es irracional al ser de grado mayor que 1. Sea $P \in \mathbb{Z}[x]$ de grado n tal que $P(\alpha) = 0$, y sean $\alpha_1, \ldots, \alpha_m$ las raíces de P distintas de α. Definimos

- $M = \max\limits_{x \in [\alpha-1, \alpha+1]} |P'(x)|$,
- $C < \min \left\{ 1, \frac{1}{M}, |\alpha - \alpha_1|, \ldots, |\alpha - \alpha_m| \right\}$.

Supongamos que existen $p, q \in \mathbb{Z}$, con $q > 0$ tales que

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{C}{q^n}.$$

Luego,

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{C}{q^n} \leq C < \min \left\{ 1, \frac{1}{M}, |\alpha - \alpha_1|, \ldots, |\alpha - \alpha_m| \right\}.$$

Es decir, $p/q \in [\alpha - 1, \alpha + 1]$ y p/q no es raíz de P. Suponiendo sin pérdida de generalidad que $\alpha > p/q$, apliquemos el Teorema del Valor Medio sobre P en el intervalo $[p/q, \alpha]$. Ya que $P(\alpha) = 0 = P(p/q) - P(p/q)$, obtenemos

$$-P(p/q) = P(\alpha) - P(p/q) = (\alpha - p/q)P'(\lambda)$$

para algún $\lambda \in (p/q, \alpha)$. Además, $P'(\lambda) \neq 0$.

Por otro lado, es claro que $P(p/q) \in \mathbb{Q}$ y que el denominador de $P(p/q)$ es q^n, al ser P de grado n. Además, el numerador de $|P(p/q)|$ necesariamente es mayor o igual a 1. Por lo tanto,

$$\left| \alpha - \frac{p}{q} \right| = \frac{|P(p/q)|}{|P'(\lambda)|} \geq \frac{1}{Mq^n} > \frac{C}{q^n},$$

una contradicción a lo supuesto. $\square$

Corolario 2.1.8. *Todo número de Liouville es trascendente.*

Demostración. Supongamos que cierto número de Liouville α es algebraico. Según lo probado en el Teorema 2.1.7 existe $C > 0$ tal que cualesquiera sean $p, q \in \mathbb{Z}$ con $q > 0$, vale la desigualdad

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

donde $n = \deg(\alpha)$.

Sea $r \in \mathbb{N}$ tal que $2^{-r} \leq C$. De la Definición 2.1.5, existen $p, q \in \mathbb{Z}$, con $q > 1$ tales que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{n+r}} = \frac{1}{q^n q^r} \leq \frac{1}{q^n 2^r} \leq \frac{C}{q^n},$$

lo cual resulta en una contradicción. □

Todo número de Liouville se define de manera que pueda ser muy bien aproximado mediante números racionales. Interpretando la Definición 2.1.5, si α es un número de Liouville, para cualquier $n \in \mathbb{N}$ existe un número racional p/q a distancia menor que $1/q^n$ de α. En base a esto, lo que el Teorema de Liouville plantea es que si un número es algebraico, entonces no puede ser aproximado por racionales de esta manera.

Sin embargo, la característica más importante de los números de Liouville no refiere simplemente a la cualidad de poder ser aproximados por números racionales, sino a la "rapidez" de esta aproximación. Para poner esto último en perspectiva, consideremos el conjunto

$$\{x \in \mathbb{Q} : x^2 < 2\}.$$

Dicho conjunto tiene a $\sqrt{2}$ como supremo en $\mathbb{R}$, por lo que para cualquier $\varepsilon > 0$ existe $x \in \mathbb{Q}$ tal que $\sqrt{2} - \varepsilon \leq x < \sqrt{2}$. Es decir, podemos encontrar números racionales arbitrariamente cercanos a $\sqrt{2}$.

En el caso de un número de Liouville α, la distancia entre α y p/q (donde p y q quedan determinados por algún $n \in \mathbb{N}$) depende *exponencialmente* de q. Por esta razón, algunos de los ejemplos vistos de números de Liouville son sumas infinitas de racionales p_n/q_n tales que $1/q_n$ tiende a 0 muy rápidamente (concretamente, más rápidamente que $1/q^n$).

Destaquemos algunas propiedades que verifica el conjunto de números de Liouville. Llamemos L a dicho conjunto.

Teorema 2.1.9. *L es no numerable.*

Demostración. Sea $b \in \mathbb{N}$, $b > 1$ y

$$A = \left\{ \sum_{n=1}^{\infty} a_n b^{-n!} : \ 0 \leq a_n \leq b-1 \ \forall n \in \mathbb{N}, \ a_n \neq 0 \text{ para infinitos } n \right\}.$$

Anteriormente probamos que todo elemento de A es un número de Liouville, es decir, que $A \subseteq L$. A es no numerable, ya que cada número de A está unívocamente determinado por la sucesión a_n asociada a él, y el conjunto de este tipo de sucesiones es no numerable. La prueba de esto último se deduce directamente del argumento de diagonalización empleado originalmente por Cantor para probar la no numerabilidad de $\mathbb{R}$. □

Las ideas de la siguiente demostración se atribuyen a Oxtoby [5].

Teorema 2.1.10. *L tiene medida de Lebesgue nula.*

Demostración. Veamos que para todo $m \in \mathbb{N}$, $L \cap (-m, m)$ tiene medida de Lebesgue nula.

Para $n, q \in \mathbb{N}$, con $n > 2$ y $q > 1$, sea

$$I_{n,q} = \bigcup_{p\in\mathbb{Z}} \left(\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n} \right).$$

Nótese que $L \subseteq \bigcup_{q=2}^{\infty} I_{n,q}$, ya que L es el conjunto de números a distancia menor que $1/q^n$ de cualquier racional p/q. Por lo tanto,

$$L \cap (-m, m) \subseteq \bigcup_{q=2}^{\infty} (I_{n,q} \cap (-m, m)) \subseteq \bigcup_{q=2}^{\infty} \bigcup_{p=-mq}^{mq} \left(\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n} \right).$$

La longitud de cada uno de estos intervalos es

$$\left(\frac{p}{q} + \frac{1}{q^n} \right) - \left(\frac{p}{q} - \frac{1}{q^n} \right) = \frac{2}{q^n}.$$

Luego, teniendo en cuenta que la medida de Lebesgue λ sobre intervalos coincide con su longitud, obtenemos

$$\lambda(L \cap (-m, m)) \leq \sum_{q=2}^{\infty} \sum_{p=-mq}^{mq} \frac{2}{q^n} = \sum_{q=2}^{\infty} \frac{2}{q^n}(2mq + 1) \leq \sum_{q=2}^{\infty} \frac{4m + 2}{q^{n-1}} \leq$$

$$\leq (4m + 2) \int_1^{\infty} \frac{1}{q^{n-1}} dq = (4m + 2) \lim_{b\to\infty} \frac{b^{2-n} - 1}{2 - n} = \frac{4m + 2}{n - 2}.$$

Observando que $\frac{4m+2}{n-2} \to 0$ si $n \to \infty$ podemos concluir que $\lambda(L \cap (-m, m)) = 0$ para todo $m \in \mathbb{N}$. Por lo tanto, $\lambda(L) = 0$. □

L sirve como un ejemplo de conjuntos con la curiosa propiedad de ser no numerables y tener medida nula (calculamos la medida de L a continuación). En base a esto podemos concluir que los números de Liouville "casi no ocupan espacio" dentro del conjunto de números trascendentes, lo que a su vez da lugar a una intrigante revelación: existen (muchos) números reales trascendentes que *no* son de Liouville. La búsqueda del conocimiento en la teoría de números trascendentes recién comienza.

Corolario 2.1.11. *Existen números trascendentes que no son de Liouville.*

Demostración. Como $\overline{\mathbb{Q}}$ y L tienen medida 0 en $\mathbb{R}$, el conjunto de números reales, trascendentes y no de Liouville tiene medida positiva en $\mathbb{R}$. Por lo tanto, es no vacío, y más aún, no numerable. □

1.1. Versiones Fuertes del Teorema de Liouville

La teoría de aproximación diofántica es el área de la matemática que estudia la aproximación de números reales mediante números racionales. El Teorema de Liouville fue de gran importancia en esta línea de investigación, al ser el primer resultado que determinó una cota inferior para la aproximación de números reales algebraicos. Recordemos que según dicho teorema, para cualquier número algebraico α de grado $n > 1$ existe una constante $C(\alpha) > 0$ tal que

$$\left|\alpha - \frac{p}{q}\right| > \frac{C(\alpha)}{q^n} > C(\alpha)$$

cualesquiera sean $p, q \in \mathbb{Z}$, con $q > 0$. Efectivamente, $C(\alpha)$ es una cota inferior en la aproximación de α por racionales.

En relación al resultado probado por Liouville, surgió el interrogante sobre la existencia de cotas más estrictas en la aproximación diofántica de números algebraicos. El objetivo principal de esta búsqueda, según Gelfond [6], era encontrar un valor "óptimo" del exponente en el denominador de $C(\alpha)/q^n$. Es decir, encontrar una constante $\theta = \theta(n)$ tal que si α es un número algebraico de grado $n > 1$ y $\varepsilon > 0$, exista una constante $C(\alpha, \varepsilon) > 0$ que verifique

$$\left|\alpha - \frac{p}{q}\right| > \frac{C(\alpha, \varepsilon)}{q^{\theta+\varepsilon}}$$

para cualquier número racional p/q ($p, q \in \mathbb{Z}$, $q > 0$), y esto no se verifique si $\varepsilon \leq 0$. Notemos que encontrar una cota superior para θ consiste en probar lo anterior sin la necesidad de probar la no validez para $\varepsilon \leq 0$. De esta manera, con su espléndido teorema, Liouville demostró que dicho valor óptimo $\theta(n)$ debe ser menor o igual a n.

Observemos, además, que para encontrar una cota $\tilde{\theta}$ para θ basta con probar lo siguiente: si α es un número algebraico de grado $n > 1$ y $\varepsilon > 0$, la desigualdad

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\tilde{\theta}+\varepsilon}}$$

tiene finitas soluciones p/q, con $p, q \in \mathbb{Z}$ y $q > 0$. Habiendo probado esto, la elección de una adecuada constante $C = C(\alpha, \varepsilon)$ permite asegurar que no existen soluciones racionales p/q para la ecuación

$$\left|\alpha - \frac{p}{q}\right| < \frac{C(\alpha, \varepsilon)}{q^{\tilde{\theta}+\varepsilon}},$$

y por lo tanto la desigualdad inversa vale para todo p y q.

Veamos, además, cómo el descubrimiento de cotas más estrictas para θ implica directamente la trascendencia de una mayor cantidad de números. Tal descubrimiento podría ser formulado de manera similar al Teorema de Liouville, cambiando el exponente en el denominador de C/q^n por la respectiva cota, llamémosla $\tilde{\theta} = \tilde{\theta}(n)$. Luego, podemos considerar números con la propiedad de que para todo $n \in \mathbb{N}$ y todo $\varepsilon > 0$ existe algún racional p/q, con $p, q \in \mathbb{Z}$ y $q > 1$, tal que

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{\tilde{\theta}(n)+\varepsilon}},$$

es decir, una propiedad casi idéntica a la dada en Definición 2.1.5 con la excepción de un cambio en el exponente del lado derecho de la desigualdad. Una modificación similar en el Corolario 2.1.8 demuestra, mediante una prueba análoga, la trascendencia de esta nueva clase de números.

En base a lo anterior, es claro que los resultados sobre aproximación diofántica de números algebraicos son relevantes en la teoría de números trascendentes. Afortunadamente, durante el siglo XX diferentes matemáticos lograron fortalecer la condición originalmente propuesta por Liouville, y, si bien las demostraciones escapan el objetivo de esta monografía, se considera importante enunciar los principales resultados. El primero de ellos fue dado en 1909, cuando Axel Thue [7] probó que el exponente óptimo θ no es mayor a $n/2 + 1$:

Teorema 2.1.12. *(Teorema de Thue) Sea α un número algebraico de grado $n > 1$, y sea $\varepsilon > 0$. Luego, la desigualdad*

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

tiene finitas soluciones $p, q \in \mathbb{Z}$, con $q > 0$.

Carl Siegel [8] logró mejorar la cota propuesta por Thue, probando en 1921 que $\theta(n) \leq 2\sqrt{n}$, y en 1947 Freeman Dyson [9] demostró que $\theta(n) \leq \sqrt{2n}$. El último gran resultado en la materia es el siguiente, probado por Klaus Roth [10] en 1955. Suele llamarse Teorema de Thue-Siegel-Roth en reconocimiento de la importancia de los avances anteriores.

Teorema 2.1.13. *(Teorema de Thue-Siegel-Roth) Sea α un número irracional algebraico de grado n, y sea $\varepsilon > 0$. Luego, la desigualdad*

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

tiene finitas soluciones $p, q \in \mathbb{Z}$, con $q > 0$.

Roth logró probar que $\theta \leq 2$. Dicho valor resulta ser óptimo; puede probarse que la desigualdad deja de ser válida si $\varepsilon = 0$. Por lo tanto, $\theta = 2$. Este magnífico resultado concluye una línea de investigación abierta por más de un siglo, y fue suficiente para otorgarle a Roth la medalla Fields en 1958.

Si bien el Teorema de Thue-Siegel-Roth es el "mejor posible" en la búsqueda de exponentes de q, una conjetura propuesta por Lang fortalece este resultado reemplazando q^ε por $\ln(q)^{1+\varepsilon}$.

Conjetura. *Sea α un número irracional algebraico de grado n, y sea $\varepsilon > 0$. Luego, la desigualdad*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2 \ln(q)^{1+\varepsilon}}$$

tiene finitas soluciones $p, q \in \mathbb{Z}$, con $q > 0$.

La superioridad de esta conjetura por sobre el Teorema de Thue-Siegel-Roth radica en que

$$\frac{1}{q^{2+\varepsilon}} < \frac{1}{q^2 \ln(q)^{1+\varepsilon}}$$

si q es suficientemente grande.

Capítulo 3

Resultados Notables

En el presente capítulo se exponen los resultados más importantes en la teoría de números trascendentes. Es fundamental en una introducción a esta rama de la matemática poder dar una noción de las ideas subyacentes que tienen en común las demostraciones sobre trascendencia. A grandes rasgos, la gran mayoría de estas pruebas consisten en construir funciones auxiliares que permitan arribar a una contradicción, habiendo supuesto inicialmente que el número en cuestión es algebraico. Por ejemplo, para demostrar el principal resultado de la próxima sección, deducimos ecuaciones donde el lado izquierdo de la igualdad es un número entero pero el lado derecho puede ser arbitrariamente pequeño en valor absoluto.

1. Trascendencia de e

Si bien la trascendencia de la constante e fue probada originalmente por Charles Hermite en 1873, la demostración presentada en esta monografía es una versión simplificada ideada por Hilbert [11] posteriormente. Se incluyen algunos aspectos de la prueba en forma de lemas con el propósito de simplificar la lectura e introducir las propiedades de la función auxiliar que utilizaremos.

Lema 3.1.1. *Sea* $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$*. Para todo* $p \in \mathbb{N}$*, la integral*

$$I(p) = \int_0^\infty x^{p-1} f(x) e^{-x} dx$$

es un número entero divisible por todo entero positivo menor que p*. Más aún, si* p *es primo y* p *no divide a* a_0*, entonces* p *no divide a* $I(p)$*.*

Demostración. Recordemos que la función

$$\Gamma(t) = \int_0^\infty x^{t-1} e^{-x} dx,$$

conocida como función Gama, está bien definida para los números reales positivos, y verifica la siguiente propiedad:

$$\Gamma(t) = (t-1)\Gamma(t-1).$$

Observando además que $\Gamma(1) = 1$ obtenemos que $\Gamma(n) = (n-1)!$ para $n \in \mathbb{N}$.

Trabajando la expresión de $I(p)$,

$$\begin{aligned} I(p) &= \int_0^\infty x^{p-1} f(x) e^{-x} dx = \\ &= \int_0^\infty x^{p-1} \left(\sum_{k=0}^n a_k x^k \right) e^{-x} dx = \sum_{k=0}^n a_k \int_0^\infty x^{p+k-1} e^{-x} dx = \\ &= \sum_{k=0}^n a_k \Gamma(p+k) = \sum_{k=0}^n a_k (p+k-1)! = \\ &= a_0(p-1)! + a_1 p! + \cdots + a_n(p+n-1)!. \end{aligned}$$

Como $f \in \mathbb{Z}[x]$, la expresión del último renglón es un número entero. Además, cada término incluye a $(p-1)!$ como un factor, por lo que todo entero positivo menor a p divide a la expresión. Por otro lado, si suponemos que p es primo y $p \nmid a_0$, entonces p no divide a la expresión, ya que no divide a $a_0(p-1)!$. $\square$

Lema 3.1.2. *Sean $n, p, k \in \mathbb{N}$. Si $k \leq n$, la integral,*

$$\int_k^\infty x^{p-1} \left[(x-1)\cdots(x-n)\right]^p e^{k-x} dx$$

es un número entero divisible por todo entero positivo menor o igual que p.

Demostración. Dados $n, p, k \in \mathbb{N}$ supongamos que $k \leq n$. Aplicando el cambio de variables $u = x - k$,

$$\int_k^\infty x^{p-1} \left[(x-1)\cdots(x-n)\right]^p e^{k-x} dx = \int_0^\infty (u+k)^{p-1} \left[\prod_{j=1}^n (u+k-j) \right]^p e^{-u} du.$$

Uno de los términos del producto $\prod_{j=1}^n (u+k-j)$ es igual a u, por lo que podemos reescribir la integral en cuestión como

$$\int_0^\infty u^p f(u) e^{-u} du,$$

donde

$$f(u) = (u+k)^{p-1} \prod_{\substack{j \leq n \\ j \neq k}} (u+k-j)^p.$$

Aplicando el Lema 3.1.1, esta integral resulta ser un número entero divisible por todo entero positivo menor que $p+1$. $\square$

Teorema 3.1.3. *e es trascendente.*

Demostración. Supongamos que e es un número algebraico. Sea $P \in \mathbb{Z}[x]$ tal que

$$P(e) = a_0 + a_1 e + \cdots + a_n e^n = 0.$$

Buscamos llegar a una contradicción. Consideremos

$$I(p) = \int_0^\infty x^{p-1} f(x) e^{-x} dx,$$

donde $p \in \mathbb{N}$ es algún número primo mayor que n, y $f(x) = [(x-1)\cdots(x-n)]^p$. Multiplicando por $I(p)$ en la ecuación $P(e) = 0$ obtenemos la ecuación

$$\sum_{k=0}^{n} a_k e^k I(p) = \sum_{k=0}^{n} a_k e^k \int_0^\infty x^{p-1} f(x) e^{-x} dx = 0.$$

Descomponemos la k-ésima integral de la sumatoria ($k = 1, \ldots, n$) en dos integrales, una entre 0 y k y la otra de k en adelante, llegando a la expresión

$$a_0 I(p) + \sum_{k=1}^{n} a_k e^k \left(\int_0^k x^{p-1} f(x) e^{-x} dx + \int_k^\infty x^{p-1} f(x) e^{-x} dx \right) = P_1 + P_2 = 0,$$

donde

$$P_1 = a_0 I(p) + \sum_{k=1}^{n} a_k \int_k^\infty x^{p-1} \left[(x-1)\cdots(x-n)\right]^p e^{k-x} dx,$$

$$P_2 = \sum_{k=1}^{n} a_k e^k \int_0^k x^{p-1} \left[(x-1)\cdots(x-n)\right]^p e^{-x} dx.$$

De los lemas anteriores, $P_1 \in \mathbb{Z}$. Además, como p es primo y $p > n$, p no divide a $(-1)^n n!$, el término independiente de $f(x)$. Del Lema 3.1.1, entonces, p no divide a $I(p)$. Como P sí divide a los términos de la sumatoria presente en P_1 (por Lema 3.1.2 y ya que $f(x) \in \mathbb{Z}[x]$) podemos concluir que *p no divide a P_1*. Es decir, $P_1 \not\equiv 0 \pmod{p}$ y luego $P_1 \neq 0$.

Por otro lado, consideremos

$$Q_1 = \frac{P_1}{(p-1)!} \qquad Q_2 = \frac{P_2}{(p-1)!}.$$

Claramente, $Q_1 \neq 0$. Del Lema 3.1.1, $(p-1)!$ divide a todos los términos de P_1, por lo que $Q_1 \in \mathbb{Z}$. Veamos que si p es lo suficientemente grande, $|Q_2| < 1/2$.

De la continuidad de todo polinomio, podemos asegurar la existencia de una constante $M > 0$ que verifique

$$\prod_{k=1}^{n} |x - k| \leq M$$

para $x \in [0, n]$. Luego, trabajando el k-ésimo sumando de Q_2 (llamémoslo Q_{2_k}), con $k = 1, \ldots, n$, obtenemos

$$\begin{aligned} |Q_{2_k}| &= \frac{|a_k|e^k}{(p-1)!} \left| \int_0^k x^{p-1} \left[(x-1)\cdots(x-n)\right]^p e^{-x} dx \right| \\ &\leq \frac{|a_k|e^k}{(p-1)!} \int_0^k |x|^{p-1} \left|(x-1)\cdots(x-n)\right|^p dx \\ &\leq \frac{|a_k|e^k}{(p-1)!} \int_0^k k^{p-1} M^p dx \\ &= |a_k|e^k \frac{(kM)^p}{(p-1)!}. \end{aligned}$$

Es claro que

$$\lim_{p\to\infty} |a_k|e^k \frac{(kM)^p}{(p-1)!} = 0.$$

Entonces, para $1 \leq k \leq n$ es posible elegir números primos mayores a n (llamémoslos p_k) de manera que

$$|Q_{2_k}| \leq \frac{1}{2n}.$$

Si $p := \max\{p_1, \ldots, p_n\}$,

$$|Q_2| \leq \sum_{k=1}^{n} |Q_{2_k}| \leq \sum_{k=1}^{n} \frac{1}{2n} = \frac{1}{2}.$$

Logramos llegar a una contradicción. Notemos que $P_1 + P_2 = 0$ implica que $Q_1 + Q_2 = 0$. Sin embargo, $0 \neq Q_1 \in \mathbb{Z}$ y $|Q_2| < 1/2$. Por lo tanto, la suposición inicial de que e es algebraico no es válida. Concluimos que e es un número trascendente. $\square$

2. Teorema de Lindemann-Weierstrass

El teorema presentado a continuación fue propuesto por Lindemann en 1882 y probado rigurosamente por Weierstrass en 1885. Es considerado uno de los mayores avances en la materia.

Hacemos uso del siguiente concepto en el enunciado del teorema:

Definición 3.2.4. $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ son **algebraicamente independientes** sobre $\mathbb{Q}$ si no existe ningún polinomio no nulo $P \in \mathbb{Q}[x_1, \ldots, x_n]$ tal que $P(\alpha_1, \ldots, \alpha_n) = 0$.

Teorema 3.2.5. *(Teorema de Lindemann-Weierstrass) 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 $\mathbb{Q}$.*

Baker [4] demostró en 1990 que el siguiente teorema es una formulación equivalente del Teorema de Lindemann-Weierstrass. Presentamos una idea general de la prueba de la formulación de Baker.

Teorema 3.2.6. *Para números algebraicos distintos $\alpha_1, \dots, \alpha_n$ y para números algebraicos no nulos $\beta_1, \dots, \beta_n$, se verifica*

$$\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} \neq 0.$$

Es decir, $e^{\alpha_1}, \dots, e^{\alpha_n}$ son linealmente independientes sobre $\overline{\mathbb{Q}}$ si $\alpha_1, \dots \alpha_n$ son números algebraicos distintos.

Demostración. Dado un polinomio a coeficientes reales $f(x) = \sum_{k=0}^{m} a_k x^k$, la función auxiliar a utilizar en este caso es

$$I(t) = \int_0^t e^{t-x} f(x) dx.$$

Integrando por partes $m = \deg(f)$ veces obtenemos

$$I(t) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t),$$

y podemos acotar a $I(t)$ de la siguiente manera:

$$|I(t)| \leq \int_0^t |e^{t-x} f(x)| dx \leq |t| e^{|t|} \sum_{k=0}^{m} |a_k| |t|^k.$$

Los pasos a seguir en la demostración son los siguientes:

1. Se supone que la tesis es falsa: es decir, $\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} = 0$.
2. Se definen ciertos polinomios f_i de grado $np - 1$ para algún $p \in \mathbb{N}$, y para $i = 1, \dots, n$ se considera

$$I_i(t) = \int_0^t e^{t-x} f_i(x) dx.$$

3. Se asocia a cada polinomio f_i el número $J_i = \beta_1 I_i(\alpha_1) + \cdots + \beta_n I_i(\alpha_n)$. Luego,

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

4. Para $i = 1, \ldots, n$, se prueba que J_i es un número entero no nulo divisible por $(p-1)!$. De esta manera $J_1 J_2 \cdots J_n$ es un entero no nulo divisible por $[(p-1)!]^n$.

5. Se acota el producto $|J_1 J_2 \cdots J_n|$. De lo anterior, $|J_1 J_2 \cdots J_n| \geq (p-1)!$. Además, si $f_i(x) = \sum\limits_{k=0}^{np-1} a_{i_k} x^k$,

$$|J_i| \leq \sum_{k=1}^{n} |\beta_k| |I_i(\alpha_k)| \leq \sum_{k=1}^{n} |\beta_k \alpha_k| e^{|\alpha_k|} \left(\sum_{j=0}^{np-1} |a_{i_j}| |\alpha_k|^j \right) \leq C^p$$

para alguna constante $C \in \mathbb{R}$ cuya elección no depende de p. La contradicción surge de la desigualdad $(p-1)! \leq C^p$ y de la arbitrariedad de p; si p es suficientemente grande, la desigualdad no se verifica.

□

Claramente, la formulación de Baker implica el Teorema de Lindemann-Weierstrass: si $\alpha_1, \ldots, \alpha_n$ son números algebraicos linealmente independientes sobre $\mathbb{Q}$ y $P(x_1, \ldots, x_n) = \sum b_i x_1^{i_1} \cdots x_n^{i_n} \in \mathbb{Q}[x_1, \ldots, x_n]$ tenemos que $P(e^{\alpha_1}, \ldots, e^{\alpha_n}) = \sum b_i e^{i_1\alpha_1 + \cdots + i_n\alpha_n}$, y los exponentes de e en cada término de $P(e^{\alpha_1}, \ldots, e^{\alpha_n})$ son números algebraicos distintos. Aplicando la formulación de Baker, obtenemos que $P(e^{\alpha_1}, \ldots, e^{\alpha_n}) = 0$ si y solo si $P \equiv 0$.

Es difícil sobreestimar la importancia del Teorema de Lindemann-Weierstrass en la teoría de números trascendentes, ya que sus principales consecuencias corroboran conjeturas históricas sobre la trascendencia de números omnipresentes en la matemática. Veamos algunos de estos ejemplos destacables, analizados en detalle por Niven [2].

Teorema 3.2.7. *e^α es trascendente para todo número algebraico $\alpha \neq 0$.*

Demostración. El conjunto $\{\alpha\}$ es linealmente independiente sobre $\mathbb{Q}$. Aplicando el Teorema de Lindemann-Weierstrass, no existe $0 \neq P \in \mathbb{Q}[x]$ tal que $P(e^\alpha) = 0$. Esto es, e^α es trascendente. □

El resultado anterior es conocido como Teorema de Hermite-Lindemann. Fue probado por Lindemann en 1882 utilizando métodos originalmente propuestos por Hermite en su prueba de la trascendencia de e. Lindemann conjeturó el Teorema de Lindemann-Weierstrass como una generalización natural del Teorema de Hermite-Lindemann.

Teorema 3.2.8. *$\ln(\alpha)$ es trascendente para todo número algebraico α, con $\alpha \neq 0, 1$ (si $\ln(\alpha)$ asume más de un valor, todos los valores que asume son trascendentes).*

Demostración. Considerando algún $\beta \in \mathbb{C}$ que verifique $\ln(\alpha) = \beta$, si suponemos que β es algebraico el Teorema de Hermite-Lindemann asegura que $e^\beta = \alpha$ es trascendente, una clara contradicción. □

Teorema 3.2.9. *π es trascendente.*

Demostración. Supongamos que π es algebraico. Entonces $i\pi$ también lo es, al ser i algebraico. La contradicción se deduce de aplicar el Teorema de Hermite-Lindemann, del cual obtenemos que $e^{i\pi} = -1$ es trascendente, es decir, una contradicción. □

Teorema 3.2.10. *$\sin(\alpha)$, $\cos(\alpha)$, $\tan(\alpha)$, $\sinh(\alpha)$, $\cosh(\alpha)$ y $\tanh(\alpha)$ son trascendentes si $\alpha \neq 0$ es un número algebraico.*

Demostración. Recordemos que

$$\cos(z) = \frac{e^{iz} + e^{-iz}}{2}, \qquad \sin(z) = \frac{e^{iz} - e^{-iz}}{2i}, \qquad \tan(z) = \frac{\sin(z)}{\cos(z)},$$

$$\sinh(z) = -i\sin(iz), \qquad \cosh(z) = \cos(iz), \qquad \tanh(z) = -i\tan(iz).$$

Dado un número algebraico $\alpha \neq 0$, supongamos que $\sin(\alpha) = \beta$, $\cos(\alpha) = \gamma$ y $\tan(\alpha) = \delta$ son algebraicos. De las definiciones, obtenemos

$$\begin{aligned} e^{i\alpha} - e^{-i\alpha} - 2i\beta = e^{i\alpha} - e^{-i\alpha} - 2i\beta e^0 = 0, \\ e^{i\alpha} + e^{-i\alpha} - 2\gamma = e^{i\alpha} + e^{-i\alpha} - 2\gamma e^0 = 0, \\ (1 - i\delta)e^{i\alpha} - (1 + i\delta)e^{-i\alpha} = 0, \end{aligned}$$

tres contradicciones al Teorema de Lindemann-Weierstrass. Por lo tanto $\sin(\alpha)$, $\cos(\alpha)$ y $\tan(\alpha)$ son trascendentes.

La trascendencia de las funciones hiperbólicas se deduce directamente de esto último utilizando sus expresiones en términos de las funciones trigonométricas. Por ejemplo, si $\sinh(\alpha)$ fuera un número algebraico, $i\sinh(\alpha) = \sin(i\alpha)$ también sería algebraico, contradiciendo lo recién probado. □

Teorema 3.2.11. *Las funciones hiperbólicas inversas y trigonométricas inversas evaluadas en un número algebraico $\alpha \neq 0$ son trascendentes.*

Demostración. Sigue un razonamiento similar al Teorema 3.2.8. □

3. Cuadratura del Círculo

Una parte del legado que dejó la Antigua Grecia a la comunidad matemática mundial toma la forma de tres famosos problemas sobre construcciones geométricas. Estos son la trisección del ángulo, la duplicación del cubo y la cuadratura del círculo.

El problema de la trisección del ángulo consiste en determinar un método para dividir un ángulo dado en tres ángulos iguales, utilizando regla y compás. La duplicación del cubo refiere a construir con regla y compás un cubo cuyo volumen sea exactamente el doble al de otro cubo dado. Por último, el problema de la cuadratura del círculo consiste en construir un cuadrado cuya área sea igual a la de un círculo dado.

Sin lugar a dudas, uno de los aspectos más intrigantes de la matemática es cómo conceptos que a simple vista no tienen relación alguna, luego de una mirada más profunda dejan entrever fuertes correspondencias. La cuadratura del círculo es un maravilloso ejemplo de este hecho, ya que un resultado de la teoría de números trascendentes permitió dar la respuesta final al problema.

Antes de indagar en resultados, formalicemos la noción de "construir con regla y compás". Las construcciones permitidas surgen de los primeros tres postulados en *Los Elementos* de Euclides:

1. Existe una única línea recta que une dos puntos cualesquiera.
2. Una línea recta puede extenderse indefinidamente.
3. Dado un punto y una longitud, se puede construir un círculo centrado en el punto dado y con radio igual a la longitud dada.

Las construcciones en cuestión son, entonces, trazar una línea recta entre dos puntos, extender dicha línea recta y construir círculos de radio arbitrario.

Debemos definir, también, qué entendemos por "construir un número".

Definición 3.3.12. Un número $a \in \mathbb{R}$ es **construible** si, dada una unidad de medida, puede construirse con regla y compás un segmento de longitud a en un número finito de pasos.

Ahora, reduzcamos el problema de cuadrar un círculo a algo más concreto. Si consideramos el radio r del círculo dado como la unidad de medida, su área es de magnitud π. Por lo tanto, construir con regla y compás un cuadrado cuya área sea igual a π es equivalente a construir de la misma manera un segmento de longitud $\sqrt{\pi}$.

En 1837, Pierre Wantzel [12] busca caracterizar algebraicamente cuándo un número dado es construible. Wantzel observa que todo número construible puede asociarse a un determinado sistema de ecuaciones cuadráticas a coeficientes racionales, y en base a esto logra encontrar una condición necesaria para que un número dado sea construible con regla y compás.

Teorema 3.3.13. *(Teorema de Wantzel) Si α es un número construible, entonces es raíz de un polinomio irreducible de grado 2^n, para algún $n \in \mathbb{N}$.*

En otras palabras, Wantzel prueba que *todo número construible es algebraico*. Esto permite concluir que $\sqrt{\pi}$ no es construible, pues si lo fuera, $\sqrt{\pi}$ sería un número algebraico y consecuentemente $\pi = \sqrt{\pi}\sqrt{\pi}$ también lo sería. Por lo tanto, el problema de cuadrar el círculo con regla y compás (en finitos pasos) es imposible.

4. Teorema de Gelfond–Schneider

En el año 1900, David Hilbert publica una lista con 23 problemas de la matemática sin resolver hasta ese momento. La lista había sido construida con el propósito de atraer atención a problemas cuya resolución, según Hilbert, era clave para continuar con el desarrollo de la matemática.

Si bien algunos de los problemas ya eran reconocidos como grandes conjeturas, el renombre de Hilbert en ese entonces fue suficiente para popularizar ampliamente el listado. Hasta el día de hoy, varios de los problemas recopilados por Hilbert siguen siendo asociados a la lista publicada en 1900.

A lo largo de los años, algunos de estos problemas fueron probados formalmente, otros desmentidos, e incluso en algunos casos quedó probada la imposibilidad de encontrar una solución.

En esta sección exploramos el séptimo de los Problemas de Hilbert, un resultado sumamente importante en la teoría de números trascendentes. Su prueba es atribuida a Aleksandr Gelfond y Theodor Schneider, quienes publicaron demostraciones independientes en 1934 y 1935, respectivamente.

Teorema 3.4.14. *(Teorema de Gelfond-Schneider) Si α y β son números algebraicos tales que $\alpha \neq 0, 1$ y $\beta \notin \mathbb{Q}$, entonces cualquier valor de α^β es trascendente.*

Demostración. La demostración del teorema es considerablemente extensa, por lo que presentamos una idea general. La prueba completa puede encontrarse en *Números Irracionales*, de Ivan Niven (1956).

El procedimiento es el siguiente:

1. Se supone que algún valor particular de α^β es algebraico.
2. Se fijan números $h, m \in \mathbb{N}$, donde $m = 2h+3$, y se consideran $q, n, t \in \mathbb{N}$ (a determinar luego) tales que $q > 4m^2$, $n = q^2/2m$ (es decir, q^2 es múltiplo de $2m$) y $t = q^2 = 2mn$. q, n y t facilitarán la contradicción al final de la prueba. Se definen además $\rho_1, \dots, \rho_t$ como los números
$$(r + k\beta)\ln(\alpha), \qquad r = 1, \dots, q, \qquad k = 1, \dots, q.$$
No es necesario especificar individualmente qué valores de r y k le corresponden a cada uno de los $\rho_1, \dots, \rho_t$.
3. Se define la función compleja
$$F(z) = \sum_{j=1}^{t} \eta_j e^{z\rho_j},$$
donde $\eta_1, \dots, \eta_t$ son ciertos enteros algebraicos.
4. Se prueba que existe $1 \leq B \leq m$ y $p \in \mathbb{N}$, $p \geq n$ tal que $\zeta \neq 0$, donde
$$\zeta = \ln(\alpha)^{-p} F^{(p)}(B) = \sum_{j=1}^{t} \eta_j \ln(\alpha)^{-p} \rho_j^p e^{B\rho_j} = \sum_{j=1}^{t} \eta_j (r + k\beta)^p \alpha^{Br} \alpha^{\beta Bk}.$$
Notemos que según lo supuesto, ζ es un número algebraico.
5. Se prueba que existe una constante C independiente de n y p que verifica $|N(\zeta)| \geq C^{-p}$, donde $N(\zeta) := \zeta_1, \dots, \zeta_{\deg(\zeta)}$ es el producto de las raíces del polinomio mínimo de ζ.
6. Se busca acotar superiormente a $N(\zeta)$. Para lograr esto, se define una segunda función auxiliar
$$S(z) = p! F(z) \prod_{b=1}^{m} (z - b)^{-p} \prod_{\substack{b=1 \\ b \neq B}} (B - b)^p.$$
Expandiendo la serie de Taylor de F alrededor de B y reemplazando la expresión resultante en la definición de S se obtiene que $S(B) = F^{(p)}(B)$, y así $\zeta = \ln(\alpha)^{-p} S(B)$. Luego, integrando la función $S(z)/(z - B)$ a lo largo del círculo de radio p/q centrado en el origen y utilizando ciertas cotas para $F(z)$ dentro de esta región, logramos acotar el valor de $S(B)$ y por lo tanto el valor de $N(\zeta)$. La cota resultante es $|N(\zeta)| < \tilde{C}^p p^{-p}$, donde $\tilde{C}$ no depende de n ni de p.
7. La contradicción surge de lo siguiente:
$$C^{-p} \leq |N(\zeta)| < \tilde{C}^p p^{-p}.$$

Esta desigualdad implica que $(C\tilde{C})^{-p} < p^{-p}$, y equivalentemente que $C\tilde{C} > p$. Sin embargo, C y $\tilde{C}$ no dependen de p ni de n, y p fue elegido de manera que $p \geq n$. Por lo tanto, la desigualdad no se verifica si se elige n suficientemente grande.

$\square$

Destaquemos algunos números cuya trascendencia puede probarse directamente aplicando el Teorema de Gelfond-Schneider.

- $2^{\sqrt{2}}$ y $\sqrt{2}^{\sqrt{2}}$ son números trascendentes.
- Cualquier valor de α^i es trascendente para todo número algebraico $\alpha \neq 0, 1$. En particular, cualquier valor de $\left(a^{\frac{n}{m}}\right)^i = \sqrt[m]{a^{in}}$ es trascendente para todo $a \in \mathbb{Q}$, $a \neq 0, 1$.
- $\log_a(b)$ es trascendente si a y b son números algebraicos reales tales que $a, b > 0$ y $a \neq 1$. Si suponemos que $\log_a(b)$ es algebraico, aplicando el Teorema de Gelfond-Schneider obtenemos que

$$a^{\log_a(b)} = e^{\ln(a)\frac{\ln(b)}{\ln(a)}} = b$$

  es trascendente, una clara contradicción.
- La **constante de Gelfond** e^π es trascendente, ya que

$$e^\pi = e^{-i^2\pi} = \left(e^{i\pi}\right)^{-i} = (-1)^{-i}.$$

- El número i^i es trascendente. Notemos además que

$$i^i = \left[\cos\left(\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2}\right)\right]^i = \left(e^{\frac{i\pi}{2}}\right)^i = e^{-\frac{\pi}{2}}.$$

La hipótesis de la naturaleza algebraica de α es fundamental. Si consideramos $\alpha = \sqrt{2}^{\sqrt{2}}$, el número α^β (con β algebraico y no racional) no es trascendente en general. Por ejemplo,

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2.$$

Otro contraejemplo está dado por el número trascendente $\alpha = i^{-\sqrt{2}i}$ y el número irracional $\beta = \sqrt{2}$:

$$\alpha^\beta = \left(i^{-\sqrt{2}i}\right)^{\sqrt{2}} = \left(i^i\right)^{-2} = \left(e^{-\frac{i\pi}{2}}\right)^{-2} = e^{i\pi} = -1.$$

También es indispensable en las hipótesis que β sea algebraico: vimos anteriormente que α^β es algebraico si $1 \neq \alpha \in \mathbb{R}^+$ y $\beta = \log_\alpha(b)$ para algún $b \in \mathbb{R}^+$.

Existe una formulación equivalente del Teorema de Gelfond-Schneider:

Teorema 3.4.15. *Si α y γ son números algebraicos no nulos, con $\alpha \neq 1$, entonces*

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

es un número racional o es trascendente.

Demostración. Probemos la equivalencia de ambos teoremas.

Supongamos que se satisfacen las hipótesis del Teorema 3.4.15 pero β es un número algebraico irracional. De la definición de β resulta que $\alpha^\beta = \gamma$, y aplicando el Teorema de Gelfond-Schneider obtenemos que γ es trascendente, contradiciendo la hipótesis. Por lo tanto, el Teorema de Gelfond-Schneider implica el Teorema 3.4.15.

Recíprocamente, si α y β verifican las hipótesis de Gelfond-Schneider pero $\alpha^\beta = \gamma$ es un número algebraico, entonces

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

y por el Teorema 3.4.15, β es racional o trascendente, nuevamente contradiciendo la hipótesis. □

Notemos que, debido a la formulación equivalente dada en el Teorema 3.4.15, el Teorema de Gelfond-Schneider es esencialmente un resultado sobre la lineal independencia de logaritmos. Concretamente, establece que para cualesquiera números algebraicos no nulos $\alpha_1, \alpha_2, \beta_1, \beta_2$ tales que $\ln(\alpha_1)$ y $\ln(\alpha_2)$ son linealmente independientes sobre $\mathbb{Q}$, resulta

$$\beta_1 \ln(\alpha_1) + \beta_2 \ln(\alpha_2) \neq 0.$$

5. Teorema de Schneider-Lang

El siguiente resultado implica directamente los teoremas de Gelfond-Schneider y Hermite-Lindemann. Fue probado por Lang [13] en 1966 como un perfeccionamiento de un resultado similar atribuido a Schneider, razón por la cual es conocido como Teorema de Schneider-Lang. Si bien el resultado en sí hace uso de conceptos de la teoría de cuerpos, enunciamos una versión que puede comprenderse en su totalidad utilizando los conceptos vistos en esta monografía.

Notamos por $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ al cuerpo resultante de intersecar todos los cuerpos que contienen a $\mathbb{Q} \cup \{\alpha_1, \ldots, \alpha_n\}$. Para enunciar el teorema, precisamos además de lo siguiente:

Teorema 3.5.16. *Dados $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$, existe $\beta \in \overline{\mathbb{Q}}$ tal que*

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

Definición 3.5.17. n funciones $f_1, \ldots, f_n$ con dominio en el plano complejo son **algebraicamente independientes** sobre un cuerpo K si no existe $0 \neq P \in K[x_1, \ldots, x_n]$ tal que $P(f_1(z), \ldots, f_n(z)) = 0$ para todo z.

La demostración del Teorema 3.5.16 puede encontrarse en *Teoría de Números Algebraicos Introductoria*, de Saban Alaca y Kenneth Williams (2004).

Presentamos el teorema en cuestión:

Teorema 3.5.18. *(Teorema de Schneider-Lang) Sean $\alpha_1, \ldots, \alpha_n$ números algebraicos, y sean $f_1, \ldots, f_N$ funciones analíticas en $\mathbb{C}$ salvo quizás en un conjunto de puntos aislados, y tales que f_k' $(k = 1, \ldots, n)$ es un polinomio en las funciones $f_1, \ldots, f_N$ a coeficientes en $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Supongamos además que al menos dos de dichas funciones $f_1, \ldots, f_N$, llamémoslas f_{k_1} y f_{k_2}, son algebraicamente independientes sobre $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, y sea*

$$\rho_j = \limsup_{r \to \infty} \frac{\ln(\ln(\sup_{|z|<r} |f_{k_j}(z)|))}{\ln(r)}.$$

Luego, si β es tal que $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\beta)$, existen a lo sumo

$$m = \deg(\beta)(\rho_1 + \rho_2)$$

números complejos distintos $w_1, \ldots, w_m$ tales que $f_i(w_j) \in \mathbb{Q}(\beta)$ para cada $i = 1, \ldots, N$ y cada $j = 1, \ldots, m$.

Deduzcamos el Teorema de Hermite-Lindemann haciendo uso del Teorema de Schneider-Lang. Si suponemos que e^α es algebraico para $0 \neq \alpha \in \overline{\mathbb{Q}}$, se verifican las hipótesis del teorema en cuestión considerando $\mathbb{Q}(\alpha, e^\alpha)$, $f_1(z) = z$ y $f_2(z) = e^z$. Sin embargo, $f_1(n\alpha) = n\alpha$ y $f_2(n\alpha) = (e^\alpha)^n$ son elementos de $\mathbb{Q}(\alpha, e^\alpha)$ para todo $n \in \mathbb{N}$, contradiciendo el hecho de que esto último puede suceder sólo para finitos números.

Análogamente, para deducir el Teorema de Gelfond-Schneider suponemos que α^β es algebraico y aplicamos el Teorema de Schneider-Lang considerando $\mathbb{Q}(\alpha, \beta, \alpha^\beta)$, $f_1(z) = e^z$ y $f_2(z) = e^{\beta z}$. En este caso, $f_1(n \ln(\alpha)) = \alpha^n$ y $f_2(n \ln(\alpha)) = (\alpha^\beta)^n$ son elementos de $\mathbb{Q}(\alpha, \beta, \alpha^\beta)$ para cada $n \in \mathbb{N}$, llegando a una contradicción similar.

6. Combinaciones Lineales de Logaritmos

El teorema presentado a continuación es una generalización del Teorema de Gelfond-Schneider probada por el matemático Alan Baker [4] en 1966. Mediante dicho teorema, Baker logró demostrar la independencia algebraica sobre $\overline{\mathbb{Q}}$ de los logaritmos de n números algebraicos, dado que estos logaritmos sean linealmente independientes sobre $\mathbb{Q}$.

Teorema 3.6.19. *Si $\alpha_1, \ldots, \alpha_n$ son números algebraicos no nulos y sus logaritmos $\ln(\alpha_1), \ldots, \ln(\alpha_n)$ son linealmente independientes sobre $\mathbb{Q}$, entonces $1, \ln(\alpha_1), \ldots, \ln(\alpha_n)$ son linealmente independientes sobre $\overline{\mathbb{Q}}$.*

La demostración del Teorema 3.6.19 es, si bien considerablemente más compleja, similar a la del Teorema de Gelfond-Schneider. Consiste en suponer la existencia de números algebraicos $\beta_0, \beta_1, \ldots, \beta_n$, con al menos uno de ellos no nulo, tales que

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

La contradicción se busca proponiendo una función auxiliar compleja Φ (en este caso, Φ es una función de varias variables complejas) y encontrando cotas para los valores de Φ y sus derivadas. El paso final consiste en probar que al menos una de las desigualdades dadas por las cotas de Φ no puede verificarse bajo lo supuesto inicialmente.

En lo que respecta a la teoría de números trascendentes, el Teorema 3.6.19 tiene a los siguientes resultados como principales consecuencias.

Teorema 3.6.20. *Si $\alpha_1, \ldots, \alpha_n, \beta_0, \beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$ son tales que $\alpha_k \neq 0$ para $k = 1, \ldots, n$ y $\beta_0 \neq 0$, entonces*

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

Demostración. El resultado es trivial para $n = 0$. Supongamos que es válido para todo $n \in \mathbb{N}$ menor a cierto m.

Si $\ln(\alpha_1) \ldots, \ln(\alpha_m)$ son linealmente independientes sobre $\mathbb{Q}$, por el Teorema 3.6.19

$$\beta_0 + \beta_1 \ln(\alpha_1) + \cdots + \beta_m \ln(\alpha_m) \neq 0,$$

pues $1, \ln(\alpha_1), \ldots, \ln(\alpha_m)$ son linealmente independiente sobre $\overline{\mathbb{Q}}$ y los coeficientes no son todos nulos.

Por otro lado, si existen $\rho_1, \ldots, \rho_m$ no todos nulos (digamos, $\rho_r \neq 0$) tales que

$$\rho_1 \ln(\alpha_1) + \cdots + \rho_m \ln(\alpha_m) = 0,$$

entonces

$$\begin{gathered}
\rho_r \left(\beta_0 + \beta_1 \ln(\alpha_1) + \cdots + \beta_m \ln(\alpha_m)\right) = \\
= \rho_r \left(\beta_0 + \beta_1 \ln(\alpha_1) + \cdots + \beta_n \ln(\alpha_m)\right) - \beta_r \left(\rho_1 \ln(\alpha_1) + \cdots + \rho_m \ln(\alpha_m)\right) = \\
= \beta_0' + \beta_1' \ln(\alpha_1) + \cdots + \beta_m' \ln(\alpha_m),
\end{gathered}$$

donde $\beta_0' = \rho_r \beta_0$ y $\beta_j' = \rho_r \beta_j - \beta_r \rho_j$, para $j = 1, \ldots, m$. Además, $\beta_0' \neq 0$ y $\beta_r' = 0$. Logramos reducir la expresión al eliminar el término que incluye a α_r y β_r'. El resultado sigue de aplicar la hipótesis inductiva. $\square$

Teorema 3.6.21. *Si* $\alpha_1, \ldots, \alpha_n, \beta_0, \beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}}$ *son tales que* $\alpha_k \neq 0$ *para* $k = 1, \ldots, n$*, entonces*

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

es trascendente.

Demostración. Supongamos que $\beta_0 + \beta_1 \ln(\alpha_1) + \cdots + \beta_n \ln(\alpha_n)$ es algebraico. Luego, $-\beta_1 \ln(\alpha_1) - \cdots - \beta_n \ln(\alpha_n)$ es algebraico. Aplicando el Teorema 3.6.20 obtenemos que

$$\begin{aligned} 0 &= -\beta_0 - \beta_1 \ln(\alpha_1) - \cdots - \beta_n \ln(\alpha_n) + \beta_0 + \beta_1 \ln(\alpha_1) + \cdots + \beta_n \ln(\alpha_n) \\ &= (-\beta_1 \ln(\alpha_1) - \cdots - \beta_n \ln(\alpha_n)) + \beta_1 \ln(\alpha_1) + \cdots + \beta_n \ln(\alpha_n) \\ &\neq 0, \end{aligned}$$

una clara contradicción. □

Corolario 3.6.22. $\pi + \ln(\alpha)$ *es trascendente si* $\alpha \neq 0$ *es un número algebraico.*

Demostración. De la igualdad $e^{i\pi} = -1$ obtenemos $\pi = \frac{1}{i} \ln(-1) = -i \ln(-1)$ (recordemos que trabajamos con alguna rama de la función logaritmo en el plano complejo). Por el Teorema 3.6.21,

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

es un número trascendente. □

Teorema 3.6.23. $e^{\beta_0} \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ *es trascendente si* $\alpha_1, \ldots, \alpha_n, \beta_0, \beta_1, \ldots, \beta_n$ *son números algebraicos no nulos.*

Demostración. Si suponemos que $\alpha = e^{\beta_0} \alpha_1^{\beta_1} \cdots \alpha_n^{\beta_n}$ es algebraico, entonces

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

es un número algebraico no nulo, contradiciendo el Teorema 3.6.20. □

Corolario 3.6.24. $e^{\alpha\pi + \beta}$ *es trascendente si* α *y* β *son números algebraicos, con* $\beta \neq 0$.

Demostración. Nuevamente hacemos uso de la expresión $\pi = -i \ln(-1)$. Aplicando el Teorema 3.6.23, obtenemos que □

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

es un número trascendente.

7. El Próximo Gran Teorema

El más grande de los problemas abiertos en la teoría de números trascendentes es una conjetura que, de ser probada, generaliza la mayoría de los resultados vistos en este capítulo. Esto continúa con la narrativa usual en esta línea de investigación: luego de haber sido probada la trascendencia de e surgió el Teorema de Hermite-Lindemann, el cual después fue generalizado por el Teorema de Lindemann-Weierstrass, siendo este último un caso particular del resultado demostrado posteriormente por Baker.

La conjetura en cuestión fue propuesta originalmente por Stephen Schanuel en la década del 60, razón por la cual hoy es conocida como la Conjetura de Schanuel.

Conjetura. *(Conjetura de Schanuel) Sean $z_1, \ldots, z_n$ números complejos linealmente independientes sobre $\mathbb{Q}$. Luego, el* ***grado de trascendencia*** *de $\mathbb{Q}(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n})$ sobre $\mathbb{Q}$ es al menos n, es decir, el máximo cardinal de un subconjunto de $\mathbb{Q}(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n})$ algebraicamente independiente sobre $\mathbb{Q}$ es al menos n.*

En caso de valer la Conjetura de Schanuel, el Teorema de Lindemann-Weierstrass se deduce directamente si $z_1, \ldots, z_n$ son números algebraicos. Si se consideran $z_1, \ldots, z_n$ de manera que $e^{z_1}, \ldots, e^{z_n}$ sean algebraicos, entonces $z_i = \ln(w_i)$ para algún $w_i \in \overline{\mathbb{Q}}$ $(i = 1, \ldots, n)$, y aplicando la conjetura podríamos concluir que $\ln(w_1), \ldots, \ln(w_n)$ son algebraicamente independientes sobre $\overline{\mathbb{Q}}$. Es decir, obtendríamos una generalización del Teorema 3.6.19, al ser la independencia algebraica una condición claramente más fuerte que la lineal independencia.

Conclusiones

A lo largo de esta monografía se buscó asentar una sólida base en lo que respecta a los conceptos básicos de la teoría de números algebraicos y trascendentes, prestando particular atención a cuestiones relacionadas a la cardinalidad y medida de los conjuntos tratados, para luego explorar los grandes resultados sobre trascendencia que han ido surgiendo a lo largo de los siglos. Concretamente, se incluyó la prueba de Hilbert de la trascendencia de e como un primer ejemplo de las extensas demostraciones características de esta área de la matemática. Se enunció también el Teorema de Lindemann-Weierstrass, el cual nos permitió confirmar supuestos sobre la trascendencia de números con los que todo matemático trabaja cotidianamente. Teoremas como el de Gelfond-Schneider y Schneider-Lang fueron presentados con el objetivo de seguir indagando en los más grandes resultados en la materia. Culminamos mencionando el más notable de los problemas abiertos en la teoría de números trascendentes, la Conjetura de Schanuel.

Quizás es exagerado afirmar que nunca dejarán de aparecer resultados curiosos e intrigantes en la teoría de números trascendentes. Sin embargo, existen hechos que inequívocamente dan lugar a este pensamiento. Basta con observar que los números cuya trascendencia ha sido probada constituyen un subconjunto relativamente pequeño de los números complejos. Por ejemplo, si bien en la actualidad podemos asegurar que e^α es trascendente si α es algebraico y no nulo, no podemos llegar con certeza la misma conclusión si α en sí es un número trascendente arbitrario. Quitar la hipótesis de que ciertos números sean algebraicos en los teoremas vistos en esta monografía resulta en conjeturas tan generales que son prácticamente imposibles de abordar. Por otro lado, la mayoría de estos resultados refieren a la trascendencia de las funciones más usuales en la matemática evaluadas en números algebraicos. Se desconoce en la actualidad la trascendencia de otras funciones importantes evaluadas en ciertos números algebraicos, como por ejemplo la función zeta de Riemann $\zeta(s)$, donde $s > 1$ es un número impar.

Como reflexión personal, creo importante destacar que la teoría de números trascendentes concentra algunas de las particularidades que hacen de la matemática una disciplina increíblemente bella y fructífera.

Una de estas particularidades tiene que ver con el alcance de los resultados. Si bien los conceptos básicos son simples nociones sobre polinomios, la influencia que ciertos avances han tenido en la matemática es innegable. Como un caso particular, el Teorema de Wantzel permite transportar el mundo de los números construibles al terreno (mucho menos sinuoso) de los números algebraicos, facilitando la resolución de un problema abierto por miles de años y dando clara evidencia de la importancia que posee la trascendencia como cualidad de un número.

Otra de las particularidades, quizás más filosófica, refiere al lugar que los números trascendentes ocupan en el universo de los conceptos matemáticos. En mi opinión, el concepto de trascendencia connota misterio y complejidad; refiere a una propiedad enigmática que todavía no logramos dominar como comunidad matemática. No hemos podido (y quizás nunca podamos) alcanzar con la trascendencia lo que buscamos con cada concepto que definimos: estructurarlo y caracterizarlo completamente. Esta naturaleza intrigante y llena de potencial representa a mi parecer lo maravilloso de la matemática: sin importar cuántos teoremas sean demostrados o cuántos artículos científicos vean la luz del día, el mundo de lo desconocido y lo que aún debemos comprender es infinitamente extenso.

Bibliografía

[1] D. A. Cox. *Galois Theory*. 2.ª ed. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs, and Tracts. John Wiley & Sons, Inc., 2012. ISBN: 978-1-118-07205-9.

[2] I. Niven. *Irrational Numbers*. The Carus Mathematical Monographs. The Mathematical Association of America, 1956. ISBN: 0883850389.

[3] J. Liouville. "Mémoires et communications". En: *Comptes rendus de l'Académie des Sciences* 18 (1844), págs. 883-885, 910-911.

[4] A. Baker. *Transcendental Number Theory*. Cambridge University Press, 1975. ISBN: 0521204615.

[5] J. C. Oxtoby. *Measure and Category*. 2.ª ed. Graduate Texts in Mathematics. Springer-Verlag, 1980. ISBN: 0387905081.

[6] A. O. Gelfond. *Transcendental and Algebraic Numbers*. Dover Books on Advanced Mathematics. Dover Publications, Inc., 1960. ISBN: 0486495264.

[7] A. Thue. "Über Annäherungswerte algebraischer Zahlen". En: *Journal für die reine und angewandte Mathematik* 1909.135 (1909), págs. 284-305. DOI: `10.1515/crll.1909.135.284`.

[8] C. Siegel. "Approximation algebraischer Zahlen". En: *Mathematische Zeitschrift* 10.3-4 (1921). DOI: `10.1007/bf01211608`.

[9] F. J. Dyson. "The approximation to algebraic numbers by rationals". En: *Acta Mathematica* 79.1 (dic. de 1947), págs. 225-240. ISSN: 1871-2509. DOI: `10.1007/BF02404697`.

[10] K. F. Roth. "Rational approximations to algebraic numbers". En: *Mathematika* 2.1 (1955), págs. 1-20. DOI: `10.1112/S0025579300000644`.

[11] D. Hilbert. *Gesammelte Abhandlungen*. 1932.

[12] J. Suzuki. "A Brief History of Impossibility". En: *Mathematics Magazine* 81.1 (2008), págs. 27-38.

[13] S. Lang. *Introduction to Transcendental Numbers*. Addison-Wesley Series in Mathematics. Addison-Wesley Publishing Company, 1966. ISBN: 9780201041767.

[14] S. Alaca y K. S. Williams. "Introductory Algebraic Number Theory". En: Cambridge University Press, 2003. ISBN: 978-0-511-16494-1. URL: `www.cambridge.org/9780521832502`.