Números transcendentes

TRABAJO DE FIN DE GRADO

Curso 2024/2025

FACULTAD DE CIENCIAS MATEMÁTICAS

Doble grado en Ingeniería Informática y Matemáticas

Autor

Daniel González Arbelo

Tutores

José Manuel Gamboa Mutuberría

Juan Ramón Delgado Pérez

José Francisco Fernando Galván

Madrid, 30 de junio de 2025

Resumen. El objetivo de este trabajo es presentar algunos de los principales resultados sobre números transcendentes (sobre los números racionales) desde el inicio de su estudio hasta la resolución del séptimo problema de Hilbert. En primer lugar presentamos la prueba de Cantor acerca de la existencia de una cantidad no numerable de números reales transcendentes y la transcendencia de los números irracionales que se aproximan bien mediante números racionales; en particular el número de Liouville, el primer número cuya transcendencia fue probada. En el segundo capítulo probamos los Teoremas de Hermite y Lindemann, que muestran la transcendencia de e y π, respectivamente. Adicionalmente, empleamos la transcendencia de π para probar la existencia de infinitos automorfismos del cuerpo $\mathbb{C}$ de los números complejos. En el tercer capítulo demostramos el Teorema de Lindemann-Weierstrass, que muestra que las exponenciales de números algebraicos distintos son linealmente independientes en el cierre algebraico de $\mathbb{Q}$. Finalmente demostramos el Teorema de Gelfond-Schneider en el último capítulo, que da respuesta al séptimo problema de Hilbert.

Abstract. The aim of this paper is to present some of the main results on transcendental numbers (over rational numbers) from the beginning of their study to the resolution of Hilbert's Seventh Problem. First, we present Cantor's proof of the existence of an uncountable number of transcendental real numbers and the transcendence of irrational numbers that are well approximated by rational numbers; in particular, Liouville's number, the first number whose transcendence was proven. In the second chapter, we prove Hermite's and Lindemann's theorems, which show the transcendence of e and π, respectively. Additionally, we use the transcendence of π to prove the existence of infinite automorphisms of the complex number field $\mathbb{C}$. In the third chapter, we prove the Lindemann-Weierstrass Theorem, which shows that the exponentials of different algebraic numbers are linearly independent in the algebraic closure of $\mathbb{Q}$. Finally, in the last chapter, we prove the Gelfond-Schneider Theorem, which answers Hilbert's Seventh Problem.

Contenido

Introducción

Motivación

Un número complejo z se dice *algebraico* si existe un polinomio no nulo $f \in \mathbb{Q}[\mathtt{t}]$ tal que $f(z) = 0$. En caso contrario, se dice que z es *transcendente.* Aunque el conocimiento actual sobre los números transcendentes sigue siendo limitado en comparación con otros conjuntos numéricos, se han alcanzado avances significativos desde el siglo XVIII.

El primero que se interesó por tales números fue Euler, quien en 1748 conjeturó (véase [E]) que dados dos números racionales positivos $r \neq 1$ y s, el cociente $\ln s / \ln r$ es racional o transcendente. Fue Liouville (véase [Li]) quien en la década de 1840 se percató de que los números algebraicos irracionales no pueden ser muy bien aproximados por números racionales. Por ello, si un número irracional puede ser muy bien aproximado por números racionales, debe ser transcendente. Esto le permitió exhibir el primer número transcendente, llamado *número de Liouville*: el número

$$\ell := \sum_{m=1}^{\infty} 10^{-m!}.$$

En 1874, Cantor [C1] obtuvo una prueba de la existencia de infinitos números reales transcendentes sin exhibir ninguno. En dicha demostración probó que los números reales algebraicos constituyen un conjunto numerable. Como $\mathbb{R}$ es no numerable, el conjunto formado por los números reales transcendentes es, de hecho, no numerable. Esto nos dice que el conjunto de los números algebraicos es realmente limitado, por lo que un conocimiento más profundo acerca de los números transcendentes es de gran interés de cara a comprender mejor el conjunto de los números reales. Además, en 1891 Cantor [C2] obtuvo un procedimiento constructivo para encontrar, dada una sucesión contenida en un intervalo $I \subseteq \mathbb{R}$, (por ejemplo, la de los números algebraicos pertenecientes a dicho intervalo) un elemento de I que no pertenece a la sucesión, cuya demostración se explica en detalle en [G].

Tiempo más tarde, se logró probar la transcendencia de los números e, demostrada por Charles Hermite en 1873, y π, demostrada por Ferdinand von Lindemann en 1882 (véase [B]). Estos fueron los primeros números cuya transcendencia fue probada sin ser números construidos con dicho propósito. Hilbert [Hi] y Hurwitz [H] simplificaron ambas pruebas en sendos artículos publicados en *Math. Annalen* en 1893. Además, empleando cualquier número transcendente (como haremos con π) se puede probar que el grupo de automorfismos del cuerpo $\mathbb{C}$ de los números complejos es infinito.

Tan solo dos años más tarde de la demostración de la transcendencia de π, Karl Weierstrass [W] demostró un resultado que Lindemann había conjeturado previamente. Hoy se conoce este resultado como Teorema de Lindemann-Weierstrass, que afirma que dados números algebraicos $\alpha_1, \ldots, \alpha_n$ distintos y números algebraicos $\beta_1, \ldots, \beta_n$ no todos nulos, entonces

$$\sum_{i=1}^{n} \beta_i e^{\alpha_i} \neq 0.$$

Veremos que de aquí se deduce que $\gamma := \beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n}$, con $\alpha_i \neq 0, i = 1, \ldots, n$, es transcendente. En particular, si $\alpha \in \mathbb{C} \setminus \{0\}$ es un número algebraico, entonces e^α es transcendente.

En el año 1900, David Hilbert fue invitado al Segundo Congreso Internacional de Matemáticos en París, en el cual propuso una lista de 10 problemas, que se extendió a 23 problemas en una versión posterior. El séptimo de estos problemas involucra números transcendentes. En él conjeturó que dados números complejos algebraicos α y β tales que $\alpha \notin \{0, 1\}$ y β no es racional, entonces cualquier valor (la exponenciación compleja es multivaluada) de α^β es transcendente. Este resultado fue probado originalmente por Alexander Gelfond y de nuevo, de forma independiente, por Theodor Schneider en 1934 (véase [T]).

En este trabajo estudiaremos todos los resultados enunciados hasta este punto. Por supuesto, este trabajo no recoge todo lo que se conoce acerca de los números transcendentes. Por ejemplo, Serge Lang demostró en 1966 que si ℓ_1, ℓ_2 y ℓ_3 son números reales $\mathbb{Q}$-linealmente independientes y β_1 y β_2 también lo son, entonces alguno de los seis números $e^{\ell_i \beta_j}$ es transcendente (véase [SL]).

En particular, tomando $\ell_1 := 1$, $\ell_2 := \gamma$ un número transcendente, $\ell_3 := \gamma^2$ y eligiendo un número algebraico α distinto de 0 y 1, los números $\beta_1 := \ln \alpha$ y $\beta_2 := \gamma \ln \alpha$ están en las hipótesis del resultado de Lang, por lo que alguno de los números

$$e^{\ell_1 \beta_1} = \alpha, \quad e^{\ell_1 \beta_2} = \alpha^\gamma = e^{\ell_2 \beta_1}, \quad e^{\ell_2 \beta_2} = \alpha^{\gamma^2} = e^{\ell_3 \beta_1} \text{ y } e^{\ell_3 \beta_2} = \alpha^{\gamma^3}$$

son $\overline{\mathbb{Q}}$-linealmente independientes. Como α es algebraico, concluimos que alguno de los tres números α^γ, α^{γ^2} y α^{γ^3} es transcendente.

Otro resultado de similar naturaleza fue obtenido de modo independiente por Brownawell y Waldschmidt (véase [Br]), del que se deduce que bien e^e o bien e^{e^2} es transcendente.

Al igual que los resultados que acabamos de señalar, hemos dejado fuera de este trabajo, por su dificultad, un celebrado resultado debido a Baker y conjeturado por Gelfond (véase [B]), que afirma que si $\alpha_1, \ldots, \alpha_n$ son números algebraicos no nulos cuyos logaritmos $\{\ln \alpha_1, \ldots, \ln \alpha_n\}$ son $\mathbb{Q}$-linealmente independientes, entonces $\{1, \ln \alpha_1, \ldots, \ln \alpha_n\}$ son $\overline{\mathbb{Q}}$-linealmente independientes.

Hay multitud de conjeturas acerca de la transcendencia de ciertos números. Una que consideramos relevante se debe a Schanuel y supone una generalización del Teorema de Lindemann-Weierstrass. Esta conjetura afirma que si $z_1, \ldots, z_n$ son números complejos $\mathbb{Q}$-linealmente independientes, entonces el grado de transcendencia de la extensión de cuerpos $\mathbb{Q}(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n})|\mathbb{Q}$ es mayor o igual que n. Otra conjetura importante es la denominada *Conjetura de las cuatro exponenciales,* que afirma que si $\{x_1, x_2\}$ e $\{y_1, y_2\}$ son dos pares de números complejos tales que cada uno de los pares es $\mathbb{Q}$-linealmente independiente, entonces alguno de los siguientes cuatro números es transcendente: $e^{x_1 y_1}$, $e^{x_1 y_2}$, $e^{x_2 y_1}$ y $e^{x_2 y_2}$. Ambas conjeturas se pueden consultar en [SL].

Objetivos y plan de trabajo

El objetivo de este trabajo es comprender el desarrollo de los principales resultados en el campo de los números transcendentes desde los primeros desarrollos en el siglo XVIII hasta la resolución del séptimo problema de Hilbert por parte de Gelfond y Schneider.

En el primer capítulo veremos la demostración de Cantor de la existencia de infinitos números transcendentes y veremos que los números irracionales algebraicos no se aproximan bien mediante números racionales, con lo que demostraremos que el *número de Liouville* es transcendente. El segundo capítulo lo dedicaremos a probar la transcendencia de los números e y π (basándonos en las demostraciones de Hilbert [Hi] y Hurwitz [H]), así como la existencia de infinitos automorfismos del cuerpo $\mathbb{C}$ de los números complejos. El tercer capítulo consistirá en probar el Teorema de Lindemann-Weierstrass. En la exposición hemos seguido el artículo de Popescu [P]. Finalmente,

en el cuarto capítulo demostraremos el Teorema de Gelfond-Schneider, para el que hemos seguido el libro de Tubbs [T].

Debemos mencionar que hemos encontrado dificultades para completar todos los detalles de algunas de las pruebas en [P] y [T], y para solventarlas nos hemos ayudado del libro de Niven [N].

Cabe destacar que el Teorema de Lindemann-Weierstrass implica de forma directa la transcendencia de e (tomando $\alpha := 1$) y la de π (pues $e^{\pi \mathtt{i}} = -1$ es algebraico, por lo que $\pi \mathtt{i}$ es transcendente). No obstante, expondremos todos los resultados en el orden en que fueron descubiertos, por ser respetuosos con el desarrollo histórico del tema, y porque las técnicas involucradas en la prueba del Teorema de Lindemann-Weierstrass suponen un refinamiento de las empleadas en la prueba de la transcendencia de e y π, en las cuales pondremos especial énfasis.

CAPÍTULO I

Existencia y construcción de algunos números transcendentes

Comenzamos presentando la controvertida (en su época) demostración de Cantor de la existencia de una cantidad no numerable de números reales transcendentes, sin encontrar ninguno. Antes recordamos la definición de número algebraico y de número transcendente.

I.1. Existencia de números transcendentes

Definición I.1.1 Sea $E|K$ una extensión de cuerpos.

(1) Se dice que un elemento $a \in E$ es *algebraico sobre* K si existe un polinomio no nulo $f \in K[\mathtt{t}]$ tal que $f(a) = 0$. En caso contrario, se dice que a es *transcendente sobre* K.

(2) Se dice que un número complejo a es *algebraico* si es algebraico sobre $\mathbb{Q}$. En caso contrario, se dice que a es *transcendente.*

Teorema I.1.2 (Cantor) *Existen infinitos números reales transcendentes.*

Demostración. Consideremos el cierre algebraico de $\mathbb{Q}$ en $\mathbb{R}$, esto es, el cuerpo

$$\overline{\mathbb{Q}}_{\mathbb{R}} := \{a \in \mathbb{R} : \ a \text{ es algebraico sobre } \mathbb{Q}\}.$$

Como $\mathbb{R} = \overline{\mathbb{Q}}_{\mathbb{R}} \sqcup (\mathbb{R} \setminus \overline{\mathbb{Q}}_{\mathbb{R}})$ no es numerable, para demostrar $\mathbb{R} \setminus \overline{\mathbb{Q}}_{\mathbb{R}}$ es infinito no numerable es suficiente probar que $\overline{\mathbb{Q}}_{\mathbb{R}}$ es numerable.

Observamos que para cada entero $d \geq 0$ el conjunto $\mathbb{Q}_d[\mathtt{t}]$ formado por los polinomios con coeficientes en $\mathbb{Q}$ de grado menor o igual que d es numerable, pues $\mathbb{Q}$ es numerable, el producto finito de conjuntos numerables es numerable y la aplicación

$$\mathbb{Q}_d[\mathtt{t}] \to \mathbb{Q}^{d+1}, \ \sum_{k=0}^{d} a_k \mathtt{t}^k \mapsto (a_0, \ldots, a_d)$$

es biyectiva. Para cada elemento $a \in \overline{\mathbb{Q}}_{\mathbb{R}}$ denotamos $P_{\mathbb{Q},a}$ el polinomio mínimo de a sobre $\mathbb{Q}$. Como cada polinomio no nulo en $\mathbb{Q}[\mathtt{t}]$ tiene tantas raíces distintas como grado, las fibras de la aplicación

$$\overline{\mathbb{Q}}_{\mathbb{R}} \to \mathbb{Q}[\mathtt{t}], \ a \mapsto P_{\mathbb{Q},a}$$

son finitas, lo que, junto a la numerabilidad de $\mathbb{Q}[\mathtt{t}]$, prueba que $\overline{\mathbb{Q}}_{\mathbb{R}}$ es numerable. □

I.2. Construcción de números transcendentes

Nuestro siguiente objetivo es exponer un procedimiento debido a Liouville para construir números transcendentes. La clave la proporciona el siguiente lema, que pone de manifiesto que los números irracionales algebraicos no se pueden aproximar muy bien mediante números racionales.

Lema I.2.1 *Sean $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ un número algebraico y $n := [\mathbb{Q}(\alpha) : \mathbb{Q}]$ el grado de la extensión de cuerpos $\mathbb{Q}(\alpha)|\mathbb{Q}$. Entonces, existe un número real positivo c tal que para todo par de enteros positivos a y b se cumple*

$$\left|\alpha - \frac{a}{b}\right| > \frac{c}{b^n}.$$

Demostración. Para aquellas fracciones $r := \frac{a}{b} \in \mathbb{Q}$ tales que $|\alpha - r| \geq 1$ basta elegir cualquier $c < 1$. Es, por tanto, suficiente encontrar un número real c que satisfaga la desigualdad del enunciado para todas las fracciones r tales que $|\alpha - r| < 1$.

Como $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, multiplicando los coeficientes del polinomio mínimo de α sobre $\mathbb{Q}$ por el mínimo común múltiplo de los denominadores de dichos coeficientes se obtiene un polinomio $f \in \mathbb{Z}[\mathtt{t}]$ de grado n e irreducible en $\mathbb{Q}[\mathtt{t}]$ tal que $f(\alpha) = 0$. En particular, como $n > 1$ y f es irreducible en $\mathbb{Q}[\mathtt{t}]$, no tiene raíces racionales, luego $f(r) \neq 0$. Por el Teorema del valor medio, existe un número real ζ_r en el intervalo de extremos α y r tal que

$$-f(r) = f(\alpha) - f(r) = f'(\zeta_r) \cdot (\alpha - r),$$

donde f' es la derivada de la función polinómica inducida por el polinomio f. Como $f(r) \neq 0$, también $f'(\zeta_r) \neq 0$. Despejando se tiene,

$$|\alpha - r| = \frac{|f(r)|}{|f'(\zeta_r)|}.$$

Además, $|\alpha - \zeta_r| \leq |\alpha - r| < 1$, luego $\zeta_r \in [\alpha - 1, \alpha + 1] := I_\alpha$.

Como f' es una función continua, el intervalo I_α es compacto y $f'(\zeta_r) \neq 0$, existe

$$C := 1 + \text{máx}\,\{|f'(u)| : u \in I_\alpha\} > 1,$$

y, por tanto, $c := \frac{1}{C} < 1$. Este es el número real que buscamos. En efecto, por un lado

$$|\alpha - r| = \frac{|f(r)|}{|f'(\zeta_r)|} > \frac{|f(r)|}{C} = c \cdot |f(r)|,$$

y, por otro,

$$|b^n \cdot f(r)| = \left|b^n \cdot f\left(\frac{a}{b}\right)\right|$$

es un entero positivo, pues $f \in \mathbb{Z}[\mathtt{t}]$ tiene grado n, luego $|f(r)| \geq \frac{1}{b^n}$. Finalmente,

$$|\alpha - r| > c \cdot |f(r)| \geq \frac{c}{b^n}.$$

□

La primera aplicación del lema anterior proporciona el primer número cuya transcendencia se supo demostrar y que recibe el nombre de *número de Liouville*, por ser demostrado por este en 1844.

Teorema I.2.2 (Liouville) *El número $\ell := \sum_{m=1}^{\infty} 10^{-m!}$, denominado* de Liouville, *es transcendente.*

Demostración. Suponemos por reducción al absurdo que ℓ es algebraico y distinguimos dos casos, según que ℓ sea o no un número racional.

Caso 1. Suponemos que $\ell \in \mathbb{R} \setminus \mathbb{Q}$. Entonces $n := [\mathbb{Q}(\ell) : \mathbb{Q}] > 1$ y existe, por el Lema I.2.1, un número real $c > 0$ tal que $|\ell - \frac{a}{b}| > \frac{c}{b^n}$ para cualesquiera números enteros positivos a y b. Como $\mathbb{R}$

es un cuerpo arquimediano existe un entero $j > 0$ tal que $cb^{j-n} > 1$, donde $b := 10^{j!}$. El número $a := b \cdot \sum_{m=1}^{j} 10^{-m!}$ es entero, y por tanto,

$$\left|\ell - \frac{a}{b}\right| > \frac{c}{b^n} > \frac{b^{n-j}}{b^n} = b^{-j}. \tag{I.2.1}$$

Sin embargo, al operar resulta

$$\begin{aligned}\left|\ell - \frac{a}{b}\right| &= \Big|\sum_{m=1}^{\infty} 10^{-m!} - \sum_{m=1}^{j} 10^{-m!}\Big| = \sum_{m=j+1}^{\infty} 10^{-m!} < 10^{-(j+1)!} \cdot \sum_{k=0}^{\infty} 10^{-k} \\ &= \frac{10^{-(j+1)!}}{1 - 1/10} = \frac{10 \cdot 10^{-(j+1)!}}{9} < 10 \cdot 10^{-(j+1)!} = 10 \cdot \left(10^{j!}\right)^{-(j+1)} = 10 \cdot b^{-(j+1)} < b^{-j},\end{aligned}$$

lo que contradice la desigualdad (I.2.1).

Obsérvese que el cálculo anterior es válido no solo para el exponente j elegido, sino también para todos los enteros mayores que él.

Caso 2. Suponemos que $\ell \in \mathbb{Q}$. En consecuencia, existen números enteros u, v tales que $\ell := \frac{u}{v}$. Con las notaciones del caso anterior, para todo entero j suficientemente grande,

$$\frac{a}{b} = \sum_{m=1}^{j} 10^{-m!} < \sum_{m=1}^{\infty} 10^{-m!} = \ell = \frac{u}{v}.$$

Por tanto, $bu - av$ es un entero positivo, luego $bu - av \geq 1$ y, según acabamos de ver,

$$b^{-j} > \left|\ell - \frac{a}{b}\right| = \ell - \frac{a}{b} = \frac{u}{v} - \frac{a}{b} = \frac{bu - av}{bv} \geq \frac{1}{bv},$$

o sea, $v > b^{j-1}$ para $j \in \mathbb{Z}$ suficientemente grande, que es imposible. □

Con esto hemos pasado de saber de la existencia de infinitos números transcendentes sin conocer ninguno a finalmente conocer un primer ejemplo. No obstante, este número fue construido precisamente con este propósito. Siendo el conjunto de los números transcendentes de cardinal no numerable, es razonable pensar que debería resultar viable encontrar ejemplos más simples de este tipo de números. En el siguiente capítulo veremos precisamente la transcendencia de dos números mucho más conocidos: e y π.

CAPÍTULO II

Transcendencia de e y π

Como adelantamos en el capítulo anterior, este capítulo se dedica a demostrar la transcendencia de los números e y π, que fueron los primeros números cuya transcendencia fue demostrada sin estar construidos con tal propósito. Como mencionamos en la introducción, estos dos resultados pueden obtenerse como consecuencia inmediata del Teorema de Lindemann-Weierstrass, que demostraremos más adelante. No obstante, nos interesa ser respetuosos con el desarrollo histórico de estos resultados. Además, pondremos especial énfasis en la estructura de las demostraciones principales, pues a pesar de su complejidad, cada una se puede entender mejor como un refinamiento de las anteriores.

II.1. Transcendencia de e

En esta sección demostraremos la transcendencia de e, demostrada originalmente por Charles Hermite (véase [B]) en 1873.

Comenzamos demostrando tres lemas auxiliares elementales. Denotaremos $f^{(k)}$ la k-ésima derivada de un polinomio f.

Lema II.1.1 *Sea $\phi : \mathbb{Z} \to \mathbb{Z}$ una función tal que $\lim_{n\to+\infty} \phi(n) = 0$. Entonces, existe un entero positivo n_0 tal que $\phi(n) = 0$ para cada $n > n_0$.*

Demostración. Dado $\varepsilon := \frac{1}{2}$, existe $n_0 \in \mathbb{Z}^+$ tal que $|\phi(n)| < \varepsilon$ para cada $n > n_0$. Así, $|\phi(n)|$ es un entero no negativo y menor que $\frac{1}{2}$ para cada $n \geq n_0$, luego ha de ser nulo, esto es, $\phi(n) = 0$ para cada $n > n_0$. □

Lema II.1.2 (Fórmula de Leibniz) *Sean $f, g \in \mathbb{C}[\mathtt{t}]$. Entonces, la derivada de orden n del producto fg cumple la igualdad*

$$(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(n-k)} g^{(k)}.$$

Demostración. El caso $n = 1$ es inmediato, y si admitimos la fórmula para n tenemos,

$$(fg)^{(n+1)} = \big((fg)'\big)^{(n)} = (f'g + fg')^{(n)} = (f'g)^{(n)} + (fg')^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(n+1-k)} g^{(k)}$$

$$+\sum_{k=0}^{n}\binom{n}{k}f^{(n-k)}g^{(k+1)}=\sum_{k=0}^{n}\binom{n}{k}f^{(n+1-k)}g^{(k)}+\sum_{k=1}^{n+1}\binom{n}{k-1}f^{(n+1-k)}g^{(k)}$$
$$=f^{(n+1)}g+\sum_{k=1}^{n}\left(\binom{n}{k}+\binom{n}{k-1}\right)f^{(n+1-k)}g^{(k)}+fg^{(n+1)}$$
$$=\sum_{k=0}^{n+1}\binom{n+1}{k}f^{(n+1-k)}g^{(k)}.$$

□

Como adelantamos en el inicio del capítulo, la estructura de varias de las demostraciones principales de este texto son similares entre sí. En estas demostraciones, uno de los principales pasos consiste en dar con cierto sumatorio dependiente de un primo p arbitrariamente grande y ver que dicho sumatorio no es nulo, lo cual se conseguirá demostrando que todos los sumandos excepto uno son divisibles entre cierto primo p.

Con este objetivo, el siguiente lema es de gran utilidad.

Lema II.1.3 *Sean m un entero positivo, p un número primo, $s := mp + p - 1$ y el polinomio de grado s*

$$f_p(\mathtt{t}) := \frac{\mathtt{t}^{p-1}\cdot(\mathtt{t}-1)^p\cdot(\mathtt{t}-2)^p\cdots(\mathtt{t}-m)^p}{(p-1)!}\in\mathbb{Q}[\mathtt{t}].$$

Entonces, dados índices i, j tales que $0 \le i \le s$ y $0 \le j \le m$, se cumple que $f_p^{(i)}(j) \in p\mathbb{Z}$ si $(i,j) \neq (p-1,0)$, mientras que $f_p^{(p-1)}(0) = (-1)^{pm}\cdot(m!)^p$.

Demostración. Escribimos $(p-1)!\cdot f_p = q_1\cdot q_2$ donde $q_1, q_2 \in \mathbb{Z}[\mathtt{t}]$ son los polinomios

$$q_1(\mathtt{t}) := \mathtt{t}^{p-1} \quad \text{y} \quad q_2(\mathtt{t}) := \prod_{j=1}^{m}(\mathtt{t}-j)^p.$$

Nótese que $q_1^{(k)}(0) = (p-1)!$ si $k = p-1$, mientras que $q_1^{(k)}(0) = 0$ si $k \neq p-1$. Por la Fórmula de Leibniz se tiene, para cada entero i no negativo,

$$(q_1\cdot q_2)^{(i)} = \sum_{k=0}^{i}\binom{i}{k}q_1^{(k)}\cdot q_2^{(i-k)}. \tag{II.1.1}$$

Calculamos las derivadas $f_p^{(i)}(0)$. Para $0 \le i < p-1$ se deduce de (II.1.1) que $(q_1\cdot q_2)^{(i)}(0) = 0$, luego $f_p^{(i)}(0) = 0$, mientras que si $i \ge p-1$

$$(q_1\cdot q_2)^{(i)}(0) = \binom{i}{p-1}\cdot q_1^{(p-1)}(0)\cdot q_2^{(i-(p-1))}(0) = (p-1)!\cdot\binom{i}{p-1}\cdot q_2^{(i-(p-1))}(0). \tag{II.1.2}$$

En particular, para $i := p-1$ resulta

$$(p-1)!\cdot f_p^{(p-1)}(0) = (q_1\cdot q_2)^{(p-1)}(0) = (p-1)!\cdot q_2(0) = (p-1)!\cdot(-1)^{pm}\cdot(m!)^p$$

y, simplificando, $f_p^{(p-1)}(0) = (-1)^{pm}\cdot(m!)^p$. Por otro lado, si $i > p-1$,

$$(p-1)!\cdot f^{(i)}(0) = (q_1\cdot q_2)^{(i)}(0) = (p-1)!\cdot\binom{i}{p-1}\cdot q_2^{(i-(p-1))}(0),$$

esto es,

$$f^{(i)}(0) = \binom{i}{p-1} \cdot q_2^{(i-(p-1))}(0).$$

Escribimos el polinomio q_2 como

$$q_2(\mathtt{t}) = \cdots + c\mathtt{t}^{i-(p-1)} + \cdots,$$

donde $c \in \mathbb{Z}$ y solo hemos resaltado el monomio que tiene interés al calcular la derivada $q_2^{(i-(p-1))}(0)$. De hecho

$$q_2^{(i-(p-1))}(0) = c \cdot (i-(p-1))!,$$

lo que muestra que si $i > p-1$,

$$f_p^{(i)}(0) = c \cdot \binom{i}{p-1} \cdot (i-(p-1))! = \frac{c \cdot i!}{(p-1)!} = c \cdot \prod_{\ell=p}^{i} \ell \in p\mathbb{Z}.$$

De este modo hemos terminado el cálculo en lo que respecta al valor en 0 de las derivadas de f_p y pasamos a calcular $f_p^{(i)}(j)$ para $1 \leq j \leq m$. Escribimos $(p-1)! \cdot f_p = g_1 \cdot g_2$, donde $g_1, g_2 \in \mathbb{Z}[\mathtt{t}]$ están definidos mediante

$$g_1(\mathtt{t}) := (\mathtt{t}-j)^p \quad \text{y} \quad g_2(\mathtt{t}) := \mathtt{t}^{p-1} \cdot \prod_{k=1,\ k\neq j}^{m} (\mathtt{t}-k)^p.$$

Como la única derivada no nula de g_1 en $\mathtt{t} := j$ es $g_1^{(p)}(j) = p!$, aplicando de nuevo la Fórmula de Leibniz se tiene, para $0 \leq i \leq s$,

$$\begin{aligned}(p-1)! \cdot f_p^{(i)}(j) = (g_1 g_2)^{(i)}(j) &= \sum_{k=0}^{i} \binom{i}{k} \cdot g_1^{(k)}(j) \cdot g_2^{(i-k)}(j) \\ &= \begin{cases} 0 & \text{si } i < p, \\ p! \cdot \binom{i}{p} g_2^{(i-p)}(j) & \text{si } p \leq i \leq s. \end{cases}\end{aligned}$$

Dividiendo ambos miembros por $(p-1)!$ resulta finalmente,

$$f_p^{(i)}(j) = \begin{cases} 0 & \text{si } i < p, \\ p \cdot \binom{i}{p} \cdot g_2^{(i-p)}(j) \in p\mathbb{Z} & \text{si } p \leq i \leq s, \end{cases}$$

y esto demuestra la afirmación del enunciado. □

Estamos en condiciones de demostrar el resultado fundamental de esta sección. Nos interesa comprender bien esta demostración, pues entender su estructura facilitará la comprensión de futuras demostraciones más complicadas.

Teorema II.1.4 (Hermite) *El número e es transcendente.*

Demostración. En caso contrario, quitando denominadores en el polinomio mínimo de e sobre $\mathbb{Q}$, se obtiene un polinomio

$$\mathtt{p}(\mathtt{t}) := a_m \mathtt{t}^m + a_{m-1}\mathtt{t}^{m-1} + \cdots + a_1\mathtt{t} + a_0 \in \mathbb{Z}[\mathtt{t}]$$

tal que $a_0 a_m \neq 0$ y $\mathtt{p}(e) = 0$. Sea $p > m^{m+1} + 1$ un número primo, y consideremos el polinomio de grado $s := mp + p - 1$

$$f_p(\mathtt{t}) := \frac{\mathtt{t}^{p-1} \cdot (\mathtt{t}-1)^p \cdot (\mathtt{t}-2)^p \cdots (\mathtt{t}-m)^p}{(p-1)!} \in \mathbb{Q}[\mathtt{t}].$$

Con todo esto, la demostración se resume en los siguientes pasos:

(H.1) Para cada p primo, veremos que $S_p := \sum_{j=0}^{m} a_j e^j \int_0^j e^{-t} f_p(t)dt$ es un número entero dependiente de p.

(H.2) Veremos que el valor absoluto de S_p tiende a 0 a medida que p tiende a ∞. Empleando el Lema II.1.1, S_p será nulo a partir de cierto número primo.

(H.3) No obstante, obtendremos que a partir de cierto primo q_0, S_p no será divisible por $p > q_0$, y por tanto no nulo. Esto contradice el punto anterior.

Pasamos a probar cada una de estas afirmaciones.

(H.1) Nótese que para cada número real t en el intervalo abierto $(0, m)$ y cada entero no negativo $j < m$ se cumple que $|t - j| < m$, luego

$$|f_p(t)| \leq \frac{m^{p-1} \cdot m^{pm}}{(p-1)!} = \frac{m^s}{(p-1)!} \quad \text{para } 0 < t < m. \tag{II.1.3}$$

También tiene grado s el polinomio $g_p := f_p + f_p' + \cdots + f_p^{(s)} \in \mathbb{Q}[\mathtt{t}]$ y, como la derivada $f_p^{(s+1)}$ es el polinomio idénticamente nulo, $g_p' = g_p - f_p$. Definimos la función de clase infinito

$$h_p : \mathbb{R} \to \mathbb{R},\ t \mapsto e^{-t} g_p(t),$$

cuya derivada cumple

$$h_p'(t) = -e^{-t} g_p(t) + e^{-t} g_p'(t) = -e^{-t}\big(g_p(t) - g_p'(t)\big) = -e^{-t} f_p(t),$$

y por tanto, para $0 \leq j \leq m$ se tiene,

$$a_j \int_0^j e^{-t} f_p(t)dt = -a_j \int_0^j h_p'(t)dt = a_j\big(h_p(0) - h_p(j)\big) = a_j\big(g_p(0) - e^{-j} g_p(j)\big).$$

Multiplicamos ambos miembros por e^j y sumamos. Puesto que $\mathtt{p}(e) = 0$, del Lema II.1.3 se deduce

$$\begin{aligned} S_p = \sum_{j=0}^{m} a_j e^j \int_0^j e^{-t} f_p(t)dt &= g_p(0) \cdot \sum_{j=0}^{m} a_j e^j - \sum_{j=0}^{m} a_j g_p(j) = g_p(0) \cdot \mathtt{p}(e) - \sum_{j=0}^{m} a_j g_p(j) \\ &= -\sum_{j=0}^{m} a_j g_p(j) = -\sum_{j=0}^{m} \sum_{i=0}^{s} a_j f_p^{(i)}(j) = -\big(a_0(-1)^{pm} \cdot (m!)^p + pk(p)\big) \end{aligned}$$

para cierto entero $k(p)$. Así, el miembro de la derecha de esta igualdad es un número entero que depende de p luego también es entero el miembro de la izquierda.

(H.2) Ahora, por (II.1.3),

$$\begin{aligned} 0 \leq \lim_{p\to+\infty} |S_p| &\leq \lim_{p\to+\infty} \left| \sum_{j=0}^{m} a_j e^j \int_0^j e^{-t} f_p(t)dt \right| \leq \sum_{j=0}^{m} |a_j e^j| \cdot \left(\lim_{p\to+\infty} \int_0^j |f_p(t)|dt \right) \\ &\leq \sum_{j=0}^{m} |a_j e^j| \cdot \left(\lim_{p\to+\infty} \frac{j \cdot m^s}{(p-1)!} \right) \leq \sum_{j=0}^{m} |a_j e^j| \cdot \left(\lim_{p\to+\infty} \frac{m^{s+1}}{(p-1)!} \right) \\ &= \sum_{j=0}^{m} |a_j e^j| \cdot \left(\lim_{p\to+\infty} \frac{m^{p\cdot(m+1)}}{(p-1)!} \right) = 0, \end{aligned}$$

puesto que

$$\lim_{p\to+\infty} \frac{m^{p(m+1)}}{(p-1)!} = 0.$$

Para probar esto último, sea $n := m^{m+1} < p-1$. Entonces,

$$\lim_{p\to+\infty} \frac{m^{p\cdot(m+1)}}{(p-1)!} = \lim_{p\to+\infty} \frac{n^p}{(p-1)!} = \lim_{p\to+\infty} \left(\frac{n^{n+1}}{n!} \cdot \frac{n}{n+1} \cdots \frac{n}{p-2} \cdot \frac{n}{p-1} \right)$$
$$\leq \lim_{p\to+\infty} \frac{n^{n+2}}{n!} \cdot \frac{1}{p-1} = 0,$$

pues $\frac{n}{k} \leq 1$ para $n+1 \leq k \leq p-2$, y $\frac{n^{n+2}}{n!}$ no depende de p. Así,

$$\lim_{p\to+\infty} \left(a_0(-1)^{pm} \cdot (m!)^p + pk(p) \right) = \lim_{p\to+\infty} \left(\sum_{j=0}^{m} a_j e^j \int_0^j e^{-t} f_p(t) dt \right) = 0,$$

y se deduce del Lema II.1.1 que existe $q_0 > m^{m+1} + 1$ tal que

$$a_0(-1)^{qm} \cdot (m!)^q + q \cdot k(q) = 0 \quad \text{para cada primo} \quad q > q_0.$$

(H.3) Sin embargo, eligiendo $q > a_0$ esto es falso, pues $q \cdot k(q) \in q\mathbb{Z}$ mientras que $a_0(-1)^{qm} \cdot (m!)^q$ no es múltiplo de q.

Por tanto, la suposición de que e tiene polinomio mínimo era falsa, lo cual concluye la demostración. □

II.2. Transcendencia de π

Nuestro siguiente objetivo es demostrar la transcendencia de π, que fue demostrada originalmente por Ferdinand von Lindemann (véase [B]) en 1882. A pesar del notable salto en dificultad, la demostración de este resultado tiene una estructura similar a la última de la sección anterior.

Una vez más necesitamos un lema auxiliar. De forma similar a lo que explicamos para introducir el Lema II.1.3, en la demostración del Teorema de Lindemann (y posteriormente en una versión débil del Teorema de Lindemann-Weierstrass), vamos a buscar cierto sumatorio para el que daremos con una cota inferior y otra superior, ambas dependientes de p. Con ellas, llegaremos a contradicción viendo que la cota inferior crece más rápidamente que la cota superior.

Con este fin, el siguiente resultado será fundamental. La segunda de las afirmaciones será útil para encontrar cotas inferiores, mientras que la tercera será útil para encontrar cotas superiores.

Lema II.2.1 *Para cada $\omega \in \mathbb{C} \setminus \{0\}$ y cada $f(\mathtt{t}) := \sum_{k=0}^{n} a_k \mathtt{t}^k \in \mathbb{C}[\mathtt{t}]$, denotamos*

$$\mathcal{J}_f(\omega) := \int_{S_\omega} e^{\omega - z} f(z) dz,$$

donde S_ω es el segmento del plano complejo de extremos 0 y ω así orientado. Entonces,

(1) *Para cada entero $k \geq 1$ se cumple*

$$\int e^{-z} z^k dz = -e^{-z} \left(k! + \sum_{j=0}^{k-1} \frac{k!}{(k-j)!} z^{k-j} \right).$$

(2)

$$\mathcal{J}_f(\omega) = e^{\omega} \cdot \sum_{k=0}^{n} f^{(k)}(0) - \sum_{k=0}^{n} f^{(k)}(\omega).$$

(3) Si denotamos $\widehat{f}(\mathtt{t}) := \sum_{k=0}^{n} |a_j| \mathtt{t}^k \in \mathbb{R}[\mathtt{t}]$, se tiene $|\mathcal{J}_f(\omega)| \leq |\omega| \cdot e^{|\omega|} \cdot \widehat{f}(|\omega|)$.

Demostración. (1) Probamos la igualdad por inducción sobre k. Para $k = 1$,

$$\int e^{-z} z dz = -\int z d(e^{-z}) = -\left(z e^{-z} - \int e^{-z} dz \right) = -e^{-z}(1+z).$$

Supongamos probado el resultado para $k-1$. Integrando por partes,

$$\begin{aligned}\int e^{-z} z^k dx &= \int z^k d(-e^{-z}) = -e^{-z} z^k + k \int e^{-z} z^{k-1} dz \\ &= -e^{-z} \left(z^k + k \cdot \left((k-1)! + \sum_{j=0}^{k-2} \frac{(k-1)!}{(k-1-j)!} z^{k-1-j} \right) \right).\end{aligned}$$

Si en la última igualdad denotamos $\ell := 1 + j$ resulta

$$\int e^{-z} z^k dz = -e^{-z} \left(z^k + k! + \sum_{\ell=1}^{k-1} \frac{k!}{(k-\ell)!} z^{k-\ell} \right) = -e^{-z} \left(k! + \sum_{\ell=0}^{k-1} \frac{k!}{(k-\ell)!} z^{k-\ell} \right).$$

(2) La fórmula obtenida en el apartado anterior es también válida para $k = 0$ si interpretamos $\frac{0! z^0}{0!} = 1$, pues $\int e^{-z} dz = -e^{-z}$. Así,

$$\begin{aligned}\mathcal{J}_f(\omega) &= e^{\omega} \int_{S_\omega} e^{-z} f(z) dz = e^{\omega} \cdot \sum_{k=0}^{n} a_k \int_{S_\omega} e^{-z} z^k dz \\ &= e^{\omega} \cdot \sum_{k=0}^{n} a_k \left[-e^{-z} \left(k! + \sum_{j=0}^{k-1} \frac{k!}{(k-j)!} z^{k-j} \right) \right]_{z=0}^{z=\omega} \\ &= e^{\omega} \cdot \sum_{k=0}^{n} a_k \cdot k! - \sum_{k=0}^{n} a_k \cdot \left(k! + \sum_{j=0}^{k-1} \frac{a_k \cdot k!}{(k-j)!} \omega^{k-j} \right) = e^{\omega} \cdot \sum_{k=0}^{n} f^{(k)}(0) - \sum_{k=0}^{n} f^{(k)}(\omega).\end{aligned}$$

(3) Por la desigualdad triangular, y puesto que el módulo de la integral es menor o igual que la integral del módulo, de la definición se desprende que

$$|\mathcal{J}_f(\omega)| \leq \int_{S_\omega} |e^{\omega - z}| \cdot |f(z)| dz \leq \int_{S_\omega} |e^{\omega - z}| \cdot \sum_{k=0}^{n} |a_k| \cdot |z|^k dz. \tag{II.2.4}$$

En la última integral $z \in S_\omega$, y entre los puntos de este segmento el de mayor módulo es ω. Además, si $\omega - z = r \cdot (\cos\theta + \mathtt{i} \operatorname{sen}\theta)$ con $r \geq 0$ se tiene, por ser la exponencial real una función creciente y $|\omega - z| \leq |\omega|$ para cada $z \in S_\omega$,

$$|e^{\omega - z}| = |e^{r \cdot (\cos\theta + \mathtt{i} \operatorname{sen}\theta)}| = |e^{r\cos\theta} \cdot e^{\mathtt{i} r \operatorname{sen}\theta}| = e^{r\cos\theta} \leq e^r = e^{|\omega - z|} \leq e^{|\omega|}.$$

Sustituyendo en (II.2.4) las desigualdades $|z| \leq |\omega|$ y $|e^{\omega - z}| \leq e^{|\omega|}$, y puesto que la longitud del segmento S_ω es $|\omega|$, resulta finalmente

$$|\mathcal{J}_f(\omega)| \leq \int_{S_\omega} e^{|\omega|} \cdot \sum_{k=0}^{n} |a_k| \cdot |\omega|^k dz = \int_{S_\omega} e^{|\omega|} \cdot \widehat{f}(|\omega|) dz = |\omega| \cdot e^{|\omega|} \cdot \widehat{f}(|\omega|).$$

□

Con esto, ya podemos probar el resultado principal.

Teorema II.2.2 (Lindemann) *El número π es transcendente.*

Demostración. Denotemos $\mathtt{i} := \sqrt{-1}$, que es algebraico por ser raíz del polinomio $\mathtt{t}^2+1$. Razonamos por reducción al absurdo. Si π fuese algebraico también lo sería $\mathtt{i}\pi$. Sean m el grado del polinomio mínimo $g := P_{\mathbb{Q},\pi\mathtt{i}}$ de $\pi\mathtt{i}$ sobre $\mathbb{Q}$ y sean $\theta_1, \ldots, \theta_m \in \mathbb{C}$ las raíces complejas de g. Denotamos $\theta_1 := \pi\mathtt{i}$.

Con esto, la estructura de la demostración es la siguiente:

(L.1) Denotando $\phi_\varepsilon := \varepsilon_1\theta_1 + \cdots + \varepsilon_m\theta_m, \varepsilon := (\varepsilon_1, \ldots, \varepsilon_m) \in \Lambda := \{0,1\}^m$ y tomando $\omega_1, \ldots, \omega_n \in \mathbb{C}$ aquellos $\phi_\varepsilon \neq 0$, veremos que $2^m - n + \sum_{i=1}^n e^{\omega_i} = 0$.

(L.2) Tomando el polinomio $f_p(\mathtt{t}) := b^{np}\mathtt{t}^{p-1}(\mathtt{t}-\omega_1)^p \cdots (\mathtt{t}-\omega_n)^p$, veremos que este pertenece a $\mathbb{Z}[\mathtt{t}]$ a partir de cierto p primo suficientemente grande.

(L.3) Definiendo $\mathcal{J}_p := \sum_{j=1}^n \mathcal{J}_{f_p}(\omega_j)$, obtendremos la cota inferior $(p-1)! \leq |\mathcal{J}_p|$.

(L.4) Obtendremos también la cota superior $|\mathcal{J}_p| \leq K^2K^{p-1}$ para cierto entero $K \geq 2$.

(L.5) Finalmente veremos que $\lim_{p\to\infty} \frac{K^2K^{p-1}}{(p-1)!} = 0$, con lo que llegamos a contradicción.

Pasamos ahora a demostrar cada una de estas afirmaciones.

(L.1) Llamando b al mínimo común múltiplo de los denominadores de los coeficientes de g, el producto bg es un polinomio con coeficientes enteros, de grado mínimo entre los que tienen a θ_1 por raíz y no son nulos. Si

$$b \cdot g(\mathtt{t}) := b\mathtt{t}^m + \sum_{j=0}^{m-1} b_j\mathtt{t}^j \in \mathbb{Z}[\mathtt{t}]$$

existen números enteros a_j tales que $(b\theta_k)^m + \sum_{j=0}^{m-1} a_j(b\theta_k)^j = b^m g(\theta_k) = 0$.

Existe por tanto un polinomio mónico $h(\mathtt{t}) := \mathtt{t}^m + \sum_{j=0}^{m-1} a_j\mathtt{t}^j \in \mathbb{Z}[\mathtt{t}]$ tal que $h(b\theta_k) = 0$ para $1 \leq k \leq m$. Como $e^{\pi\mathtt{i}} + 1 = 0$, resulta que

$$(1+e^{\theta_1}) \cdots (1+e^{\theta_m}) = 0.$$

Desarrollando mediante la propiedad distributiva el miembro de la izquierda y, como $1 = e^0$ y

$$e^{\varepsilon_1\theta_1+\cdots+\varepsilon_m\theta_m} = e^{\varepsilon_1\theta_1} \cdots e^{\varepsilon_m\theta_m} \text{ para todo } \varepsilon := (\varepsilon_1, \ldots, \varepsilon_m) \in \Lambda := \{0,1\}^m,$$

se obtiene una suma de 2^m sumandos

$$\sum_{\varepsilon\in\Lambda} e^{\phi_\varepsilon} = (1+e^{\theta_1}) \cdots (1+e^{\theta_m}) = 0,$$

donde $\phi_\varepsilon := \varepsilon_1\theta_1 + \cdots + \varepsilon_m\theta_m$. Sea q el número de m-uplas $\varepsilon \in \Lambda$ tales que $\phi_\varepsilon = 0$. Nótese que tanto q como $n := 2^m - q$ son positivos, pues $\phi_\varepsilon = 0$ para $\varepsilon := (0, \ldots, 0)$, mientras que $\phi_\varepsilon = \theta_1 \neq 0$ para $\varepsilon := (1, 0, \ldots, 0)$. Renombramos $\omega_1, \ldots, \omega_n \in \mathbb{C}$ aquellos $\phi_\varepsilon \neq 0$, por lo que

$$\sum_{\varepsilon\in\Lambda} e^{\phi_\varepsilon} = q + e^{\omega_1} + \cdots + e^{\omega_n} = \sum_{\phi_\varepsilon=0} e^{\phi_\varepsilon} + e^{\omega_1} + \cdots + e^{\omega_n} = 0. \tag{II.2.5}$$

(L.2) Vamos a demostrar que si $p \in \mathbb{Z}$ es un número primo suficientemente grande los coeficientes del polinomio

$$f_p(\mathtt{t}) := b^{np}\mathtt{t}^{p-1}(\mathtt{t}-\omega_1)^p \cdots (\mathtt{t}-\omega_n)^p$$

son números enteros. Denotando $\omega_{n+1} = \cdots = \omega_{2^m} = 0$ a aquellas sumas ϕ_ε que son nulas, basta probar que el polinomio

$$\Phi(\mathtt{t}) := \prod_{j=1}^{2^m} (\mathtt{t}-\omega_j) = \mathtt{t}^q \cdot \prod_{j=1}^{n} (\mathtt{t}-\omega_j)^p \tag{II.2.6}$$

tiene coeficientes racionales y que el denominador de cada uno de sus coeficientes es b^n. El miembro de la izquierda de (II.2.6) es un polinomio simétrico, con coeficientes en $\mathbb{Z}$, respecto de $\omega_1, \ldots, \omega_{2^m}$, luego también es simétrico respecto de $\theta_1, \ldots, \theta_m$. Se deduce del Teorema Fundamental de los polinomios simétricos (puede encontrarse su enunciado completo en [EA]) que los coeficientes de Φ son el resultado de evaluar las formas simétricas elementales en los coeficientes del polinomio $g(\mathtt{t}) = (\mathtt{t}-\theta_1)\cdots(\mathtt{t}-\theta_m)$. Como los coeficientes de este último polinomio son números racionales cuyo denominador es b, queda probado que $f_p \in \mathbb{Z}[\mathtt{t}]$ para p suficientemente grande. Además, dividiendo por $\mathtt{t}^{p-1}$, se deduce que también

$$g_p(\mathtt{t}) := b^{np}(\mathtt{t}-\omega_1)^p \cdots (\mathtt{t}-\omega_n)^p \in \mathbb{Z}[\mathtt{t}].$$

(L.3) Como $\deg(f_p) := np+p-1 = r$, con las notaciones del Lema II.2.1 y, utilizando su apartado (2) y la igualdad (II.2.5) se tiene

$$\begin{aligned} \mathcal{J}_p &:= \sum_{j=1}^{n} \mathcal{J}_{f_p}(\omega_j) = \sum_{j=1}^{n} \int_{S_{\omega_j}} e^{\omega_j - z} f_p(z)dz \\ &= \sum_{j=1}^{n} \left(e^{\omega_j} \sum_{k=0}^{r} f_p^{(k)}(0) - \sum_{k=0}^{r} f_p^{(k)}(\omega_j) \right) = -q \cdot \sum_{k=0}^{r} f_p^{(k)}(0) - \sum_{k=0}^{r}\sum_{j=1}^{n} f_p^{(k)}(\omega_j). \end{aligned} \tag{II.2.7}$$

Nuestro siguiente objetivo es comprobar que $(p-1)! \leq |\mathcal{J}_p|$ si elegimos p suficientemente grande. Para ello probaremos que $\mathcal{J}_p$ es un múltiplo entero y no nulo de $(p-1)!$.

Comenzamos viendo que el sumatorio

$$\sum_{k=0}^{r}\sum_{j=1}^{n} f_p^{(k)}(\omega_j)$$

en (II.2.7) es múltiplo de $p!$, para lo que basta comprobar que lo es cada sumando $\sum_{j=1}^{n} f_p^{(k)}(\omega_j)$. Ahora bien,

$$f_p(\mathtt{t}) = \mathtt{t}^{p-1} \prod_{j=1}^{n} (b\mathtt{t} - b\omega_j)^p,$$

luego $\sum_{j=1}^{n} f_p^{(k)}(\omega_j) \in \mathbb{Z}[\mathtt{t}]$ es un polinomio simétrico respecto de $b\omega_1, \ldots, b\omega_n$, y por tanto es un polinomio con coeficientes enteros simétrico respecto de los 2^m números $b\omega_1, \ldots, b\omega_{2^m}$.

Se desprende del Teorema Fundamental de los polinomios simétricos que $\sum_{j=1}^{n} f_p^{(k)}(\omega_j)$ es un número entero, pues $f_p \in \mathbb{Z}[\mathtt{t}]$. Veamos que es múltiplo de $p!$.

Nótese que $f_p^{(k)}(\omega_j) = 0$ si $k < p$ puesto que ω_j es raíz de multiplicidad p de f_p. Por otro lado, sea $k \geq p$ y escribimos $f_p(\mathtt{t}) := (\mathtt{t}-\omega_j)^p \psi_j(\mathtt{t})$. Al aplicar la Fórmula de Leibniz, y como la única derivada no nula de $(\mathtt{t}-\omega_j)^p$ en ω_j es la de orden p y vale $p!$, la suma $\sum_{j=1}^{n} f_p^{(k)}(\omega_j)$ es un múltiplo entero de $p!$. En cuanto al primer sumando en el miembro de la derecha de (II.2.7), como 0 es raíz de multiplicidad $p-1$ de f_p, resulta que $f_p^{(k)}(0) = 0$ si $k < p-1$. Además, si escribimos $f_p(\mathtt{t}) = b^{np}\mathtt{t}^{p-1}h_p(\mathtt{t})^p$, donde

$$h_p(\mathtt{t}) := (\mathtt{t}-\omega_1)\cdots(\mathtt{t}-\omega_n),$$

se deduce de la Fórmula de Leibniz que $f_p^{(k)}(0)$ es un múltiplo entero de $p!$ si $k \geq p$, mientras que la derivada de orden $p-1$ es

$$\begin{aligned} f_p^{(p-1)}(0) = b^{np}(p-1)! \cdot h_p^p(0) &= b^{np}(p-1)!(-1)^{np}(\omega_1 \cdots \omega_n)^p \\ &= (p-1)! \cdot g_p(0) \in (p-1)!\mathbb{Z}. \end{aligned}$$

Por tanto $\mathcal{J}_p$ es múltiplo de $(p-1)!$, pues hemos probado que todos los sumandos que aparecen en la expresión (II.2.7) son multiplos de $(p-1)!$. Para probar que $\mathcal{J}_p$ no es nulo demostraremos que, eligiendo p adecuadamente, $\mathcal{J}_p$ no es múltiplo de p. Como hemos probado que la suma

$$\sum_{k=0}^{r} f_p^{(k)}(\omega_j) \in p\mathbb{Z},$$

se trata de elegir p de modo que el sumando $q \cdot \sum_{k=0}^{r} f_p^{(k)}(0)$ no sea múltiplo de p.

Nótese que $q \in \mathbb{Z}$ no depende de p y, eligiendo $p > q$, aseguramos que $q \notin p\mathbb{Z}$, luego basta elegir p suficientemente grande para que $\sum_{k=0}^{r} f_p^{(k)}(0) \notin p\mathbb{Z}$. Pero

$$\sum_{k \neq p-1} f_p^{(k)}(0) \in p\mathbb{Z},$$

así que necesitamos que $(p-1)! \cdot g_p(0) = f_p^{(p-1)}(0) \notin p\mathbb{Z}$, y para ello es suficiente que

$$g_p(0) = (-1)^{np}(b\omega_1 \cdots b\omega_n)^p \notin p\mathbb{Z}.$$

Basta pues tomar p suficientemente grande, ya que $b\omega_1 \cdots b\omega_n$ es un número que se conoce antes de elegir p.

(L.4) Por último, con las notaciones de II.2.1 (3), $\mathcal{J}_{f_p}(\omega_j) \leq |\omega_j| \cdot e^{|\omega_j|} \cdot \widehat{f}_p(|\omega_j|)$ para $1 \leq j \leq n$, y sumando,

$$(p-1)! \leq |\mathcal{J}_p| \leq \sum_{j=1}^{n} |\mathcal{J}_{f_p}(\omega_j)| \leq \sum_{j=1}^{n} |\omega_j| \cdot e^{|\omega_j|} \cdot \widehat{f}_p(|\omega_j|) \leq K^{p+1} = K^2 \cdot K^{p-1},$$

para cierto entero $K \geq 2$ y todo primo p suficientemente grande.

(L.5) Esto es falso, ya que

$$\lim_{n\to\infty} \left\{ \frac{K^{2n}}{(2n)!} \right\} = 0.$$

En efecto, para cada $n \in \mathbb{N}$ con $K^3 < n$,

$$0 \leq \frac{K^{2n}}{(2n)!} = \frac{(K \overset{n)}{\cdots} K) \cdot (K \overset{n)}{\cdots} K)}{(1 \cdots n) \cdot (n+1) \cdots 2n} \leq K^n \cdot \left(\frac{K}{n}\right)^n = \left(\frac{K^2}{n}\right)^n < \frac{1}{K^n},$$

y $\lim_{n\to\infty} \left\{ \frac{1}{K^n} \right\} = 0$.

Por tanto, esta contradicción implica que no existe polinomio mínimo de $\pi\mathtt{i}$, con lo que este número es transcendente, por lo que π también. □

Corolario II.2.3 *De entre los dos números $e+\pi$ y $e\pi$ al menos uno es transcendente.*

Demostración. En efecto, supongamos, por reducción al absurdo, que $e+\pi$ y $e\pi$ fuesen algebraicos. Esto implica que la extensión de cuerpos $\mathbb{Q}(e+\pi, e\pi)|\mathbb{Q}$ es finita. Pero

$$(\mathtt{t} - e) \cdot (\mathtt{t} - \pi) = \mathtt{t}^2 - (e+\pi)\mathtt{t} + e\pi,$$

luego e y π son algebraicos sobre $\mathbb{Q}(e+\pi, e\pi)$, así que también la extensión $\mathbb{Q}(e,\pi)|\mathbb{Q}(e+\pi, e\pi)$ es finita. Por la transitividad del grado la extensión $\mathbb{Q}(e,\pi)|\mathbb{Q}$ es finita, lo que implica que tanto e como π son algebraicos, y esto es falso. □

Observaciones II.2.4 (1) Se sospecha que tanto $e+\pi$ como $e\pi$ son transcendentes pero hoy en día esto es una conjetura. Tampoco se conoce si π^e es o no transcendente.

(2) La aplicación $\exp : \overline{\mathbb{Q}}_{\mathbb{C}} \to \mathbb{C}$, $z \mapsto e^z$ es inyectiva. En efecto, en caso contrario existirían $\alpha, \beta \in \overline{\mathbb{Q}}_{\mathbb{C}}$ distintos tales que $e^\alpha = e^\beta$, luego $e^{\alpha-\beta} = 1$. Existiría por tanto un entero no nulo k tal que $\alpha - \beta = 2k\pi\mathtt{i}$, por lo que

$$\pi = \frac{2k\mathtt{i}}{\alpha - \beta}$$

sería un número algebraico, por ser cociente de números algebraicos, lo que es falso.

II.3. Aplicación

En esta sección empleamos la transcendencia de π para probar la infinitud del grupo de automorfismos del cuerpo $\mathbb{C}$ de los números complejos. Cabe mencionar que no es imprescindible que empleemos la transcendencia del número π. Podríamos usar el número e o incluso ℓ, pues lo único que nos importa es conocer su transcendencia.

Comenzamos recordando la noción de cuerpo algebraicamente cerrado.

Proposición II.3.1 *Sea E un cuerpo. Las condiciones siguientes son equivalentes.*

(1) *Todo polinomio $f \in E[\mathtt{t}]$ de grado ≥ 1 tiene alguna raíz en E.*

(2) *Todo polinomio $f \in E[\mathtt{t}]$ de grado ≥ 1 factoriza en $E[\mathtt{t}]$ como producto de factores de grado 1.*

(3) *Existe un subcuerpo $K \subset E$ tal que la extensión $E|K$ es algebraica y cada $f \in K[\mathtt{t}]$ de grado ≥ 1 factoriza en $E[\mathtt{t}]$ como producto de factores de grado 1.*

(4) *El cuerpo E no admite extensiones algebraicas no triviales.*

Demostración. (1) $\Longrightarrow$ (2) Argumentamos por inducción sobre $n := \deg(f)$. Si $n = 1$ nada hay que probar. Si $n > 1$, sea $\alpha_1 \in E$ raíz de f. Entonces $f(\mathtt{t}) = (\mathtt{t} - \alpha_1) \cdot g(\mathtt{t})$ para cierto polinomio $g \in E[\mathtt{t}]$ de grado $n-1$ y, por la hipótesis de inducción, existen $a, \alpha_2, \ldots, \alpha_n \in E$ tales que

$$g(\mathtt{t}) = a \cdot \prod_{i=2}^{n} (\mathtt{t} - \alpha_i).$$

Entonces,

$$f(\mathtt{t}) = (\mathtt{t} - \alpha_1) \cdot g(\mathtt{t}) = a \cdot \prod_{i=1}^{n} (\mathtt{t} - \alpha_i).$$

Para la implicación (2) $\Longrightarrow$ (3) basta elegir $K := E$.

(3) $\Longrightarrow$ (4) Sean $L|E$ una extensión algebraica y $u \in L$. Como $L|E$ y $E|K$ son extensiones algebraicas también $L|K$ lo es, así que u es algebraico sobre K. Por hipótesis, el polinomio mínimo $P_{K,u} \in K[\mathtt{t}]$ de u sobre K factoriza en $E[\mathtt{t}]$ como producto de factores de grado 1. En consecuencia, $\mathtt{t} - u \in E[\mathtt{t}]$, o sea $u \in E$, por lo que $E = L$.

(4) $\Longrightarrow$ (1) Sea $f \in E[\mathtt{t}]$ con $\deg(f) \geq 1$. Sea $h \in E[\mathtt{t}]$ un factor irreducible de f en $E[\mathtt{t}]$. Escribimos

$$h(\mathtt{t}) := \sum_{j=0}^{d} b_j \mathtt{t}^j$$

y denotamos $\mathfrak{m} := hE[\mathtt{t}]$ el ideal maximal de $E[\mathtt{t}]$ generado por h. El cociente $F := E[\mathtt{t}]/\mathfrak{m}$ es un cuerpo que contiene una copia de E vía el homomorfismo de cuerpos

$$\mathtt{j} : E \hookrightarrow F,\ x \mapsto x + \mathfrak{m}.$$

De hecho la extensión $F|E$ es finita, luego algebraica, así que, por hipótesis, $F = E$. Además, $u := \mathtt{t} + \mathtt{m} \in E$ es raíz de h, luego de f, porque

$$h(u) = \sum_{j=0}^{d} b_j u^j = \sum_{j=0}^{d} b_j (\mathtt{t} + \mathtt{m})^j = \left(\sum_{j=0}^{d} b_j \mathtt{t}^j \right) + \mathtt{m} = h + \mathtt{m} = 0_F.$$

□

Definición II.3.2 Se dice que un cuerpo E es *algebraicamente cerrado* si cumple alguna de las condiciones en la Proposición II.3.1, y por tanto todas.

Ejemplos II.3.3 (1) El cuerpo $\mathbb{C}$ de los números complejos es, por el Teorema Fundamental del Álgebra, un cuerpo algebraicamente cerrado, pues cumple la condición (1) en la Proposición II.3.1.

(2) Sea L es un subcuerpo de $\mathbb{C}$. Dados $x, y \in \mathbb{C} \setminus \{0\}$ algebraicos sobre L la extensión $L(x, y)|L$ es finita, luego también es finita la subextensión $L(x - y, xy^{-1})|L$, así que tanto $x - y$ como xy^{-1} son algebraicos. Por tanto el conjunto,

$$\overline{L}_{\mathbb{C}} := \{a \in \mathbb{C} : \ a \text{ es algebraico sobre } L\}$$

es un cuerpo y, por su propia definición, la extensión $\overline{L}_{\mathbb{C}}|L$ es algebraica. De hecho $\overline{L}_{\mathbb{C}}$, que se denomina *cierre algebraico de L en $\mathbb{C}$,* es un cuerpo algebraicamente cerrado porque cumple la condición (3) en la Proposición II.3.1. En efecto, para cada $f \in L[\mathtt{t}]$ de grado ≥ 1 existen, por el Teorema Fundamental del Álgebra, $a \in L$ y $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ tales que

$$f(\mathtt{t}) = a \cdot \prod_{i=1}^{n} (\mathtt{t} - \alpha_i).$$

Como $f \in L[\mathtt{t}]$ cada α_i es algebraico sobre L, luego pertenece a $\overline{L}_{\mathbb{C}}$, es decir, cada uno de los factores $\mathtt{t} - \alpha_i \in \overline{L}_{\mathbb{C}}[\mathtt{t}]$.

(3) En particular, tomando $L := \mathbb{Q}$, resulta que el cuerpo

$$\overline{\mathbb{Q}}_{\mathbb{C}} := \{a \in \mathbb{C} : \ a \text{ es algebraico}\}$$

de los números algebraicos es un cuerpo algebraicamente cerrado.

Necesitaremos también dos resultados de extensión de homomorfismos de cuerpos.

Lema II.3.4 *Sea $\phi : K_1 \to K_2$ un homomorfismo entre los cuerpos K_1 y K_2.*

(1) *La aplicación*

$$\Phi : K_1[\mathtt{t}] \to K_2[\mathtt{t}], \ f(\mathtt{t}) := \sum_{j=0}^{m} b_j \mathtt{t}^j \mapsto \Phi(f)(\mathtt{t}) := \sum_{j=0}^{m} \phi(b_j) \mathtt{t}^j$$

es un homomorfismo de anillos. Además, si ϕ es isomorfismo también lo es Φ.

(2) *Supongamos que $\phi : K_1 \to K_2$ es isomorfismo. Sean $L_1|K_1$ y $L_2|K_2$ extensiones de cuerpos y $\alpha_1 \in L_1$ y $\alpha_2 \in L_2$ elementos algebraicos sobre K_1 y K_2 respectivamente. Denotemos $f_i := P_{K_i, \alpha_i}$ el polinomio mínimo de α_i sobre K_i, para $i = 1, 2$. Las siguientes afirmaciones son equivalentes:*

(2.1) *Existe un isomorfismo $\psi : K_1(\alpha_1) \to K_2(\alpha_2)$ con $\psi|_{K_1} = \phi$ y $\psi(\alpha_1) = \alpha_2$.*

(2.2) *El homomorfismo Φ del apartado* (1) *cumple la igualdad $f_2 = \Phi(f_1)$.*

Demostración. (1) Es inmediato que Φ es homomorfismo y, si ϕ es sobreyectivo, entonces Φ también lo es. Además, si ϕ es inyectivo, Φ también, porque si $f(\mathtt{t}) := \sum_{j=0}^{m} b_j \mathtt{t}^j \in \ker \Phi$, entonces $\phi(b_j) = 0$ para $0 \leq j \leq m$. Como ϕ es inyectivo se tiene $b_j = 0$ para cada $0 \leq j \leq m$, luego $f = 0$.

(2) Veamos que (2.1) implica (2.2). Sea $f_1(\mathtt{t}) := \mathtt{t}^n + \sum_{k=0}^{n-1} a_k \mathtt{t}^k$, que cumple $f_1(\alpha_1) = 0$. Se tiene entonces

$$0 = \psi(0) = \psi(f_1(\alpha_1)) = \psi\left(\alpha_1^n + \sum_{k=0}^{n-1} a_k \alpha_1^k\right) = \alpha_2^n + \sum_{k=0}^{n-1} \phi(a_k)\alpha_2^k = \Phi(f_1)(\alpha_2).$$

Como f_1 es irreducible en $K_1[\mathtt{t}]$ y Φ es isomorfismo, $\Phi(f_1) \in K_2[\mathtt{t}]$ es un polinomio mónico e irreducible que se anula en α_2, luego $\Phi(f_1) = f_2$. Probamos ahora que (2.2) implica (2.1). Para $i = 1, 2$ existe un isomorfismo

$$\varphi_i : K_i(\alpha_i) \to \frac{K_i[\mathtt{t}]}{f_i \cdot K_i[\mathtt{t}]},\ \alpha_i \mapsto \mathtt{t} + f_i \cdot K_i[\mathtt{t}]$$

tal que $\varphi_i(a) = a + f_i \cdot K_i[\mathtt{t}]$ para cada $a \in K_i$. Además, el isomorfismo Φ del apartado (1) induce, puesto que $\Phi(f_1) = f_2$, un isomorfismo

$$\Psi : \frac{K_1[\mathtt{t}]}{f_1 \cdot K_1[\mathtt{t}]} \to \frac{K_2[\mathtt{t}]}{f_2 \cdot K_2[\mathtt{t}]},$$

que cumple $\Psi(\mathtt{t} + f_1 \cdot K_i[\mathtt{t}]) = \mathtt{t} + f_2 \cdot K_i[\mathtt{t}]$. Nótese que para cada $a \in K_1$

$$\Psi(a + f_1 \cdot K_i[\mathtt{t}]) = \Phi(a) + f_2 \cdot K_i[\mathtt{t}] = \phi(a) + f_2 \cdot K_i[\mathtt{t}].$$

Obtenemos así un isomorfismo $\psi = \varphi_2^{-1} \circ \Psi \circ \varphi_1 : K_1(\alpha_1) \to K_2(\alpha_2)$ que cumple

$$\psi(\alpha_1) = (\varphi_2^{-1} \circ \Psi)\big(\mathtt{t} + f_1 \cdot K_i[\mathtt{t}]\big) = \varphi_2^{-1}\big(\mathtt{t} + f_2 \cdot K_i[\mathtt{t}]\big) = \alpha_2,$$

y para cada $a \in K_1$ se tiene

$$\psi(a) = (\varphi_2^{-1} \circ \Psi)(a + f_1 \cdot K_i[\mathtt{t}]) = \varphi_2^{-1}(\phi(a) + f_2 \cdot K_i[\mathtt{t}]) = \phi(a),$$

es decir, $\psi|_{K_1} = \phi$. □

Lema II.3.5 *Sea $\mathtt{j} : K_1 \to K_2$ un homomorfismo de cuerpos de modo que K_2 es algebraicamente cerrado, y sea $L|K_1$ una extensión algebraica. Entonces, existe un homomorfismo $\psi : L \to K_2$ tal que $\psi|_{K_1} = \mathtt{j}$.*

Demostración. Sea Σ el conjunto de todos los pares (F, φ), donde $F|K_1$ es una subextensión de $L|K_1$ y $\varphi : F \to K_2$ es un homomorfismo tal que $\varphi|_{K_1} = \mathtt{j}$. El conjunto Σ es no vacío ya que $(K_1, \mathtt{j}) \in \Sigma$, y definimos en Σ la relación de orden:

$$(F_1, \varphi_1) \preceq (F_2, \varphi_2) \text{ si } F_1 \subset F_2 \text{ y } \varphi_2|_{F_1} = \varphi_1.$$

Vamos a probar que Σ admite algún elemento maximal respecto de este orden, para lo que basta comprobar que satisface la hipótesis del Lema de Zorn, es decir, que todo subconjunto totalmente ordenado $\mathcal{C} := \{(F_i, \varphi_i)\}_{i \in I}$ de Σ está acotado superiormente.

Por ser $\mathcal{C}$ totalmente ordenado, la unión $F := \bigcup_{i \in I} F_i$ es un cuerpo y $F|K_1$ es subextensión de $L|K_1$ por serlo cada $F_i|K_1$. Además, la aplicación

$$\varphi : F \to K_2,\ x \mapsto \varphi_i(x) \text{ si } x \in F_i$$

está bien definida pues, si $x \in F_i \cap F_j$ podemos suponer, por ser $\mathcal{C}$ un subconjunto totalmente ordenado, que $(F_i, \varphi_i) \preceq (F_j, \varphi_j)$, y así $\varphi_i(x) = \varphi_j(x)$.

De hecho φ es homomorfismo, pues dados $x, y \in F$ existen $i, j \in I$ tales que $x \in F_i$ e $y \in F_j$ y de nuevo podemos suponer que $(F_i, \varphi_i) \preceq (F_j, \varphi_j)$. Por tanto,

$$\begin{aligned} \varphi(x+y) = \varphi_j(x+y) = \varphi_j(x) + \varphi_j(y) = \varphi(x) + \varphi(y) \\ \& \quad \varphi(xy) = \varphi_j(xy) = \varphi_j(x)\varphi_j(y) = \varphi(x)\varphi(y). \end{aligned}$$

Nótese que $\varphi|_{K_1} = \mathtt{j}$, luego el par $(F, \varphi) \in \Sigma$ y $(F_i, \varphi_i) \preceq (F, \varphi)$ para cada $i \in I$, luego $(F, \varphi) \in \Sigma$ es cota superior de $\mathcal{C}$. Por el Lema de Zorn, Σ tiene un elemento maximal (E, ψ), y basta probar que $E = L$. Desde luego $E|K_1$ es subextensión de $L|K_1$, y si $E \subsetneq L$ existe $\alpha \in L \setminus E$. Este elemento es algebraico sobre K_1, luego es algebraico sobre E, y si denotamos

$$f_1(\mathtt{t}) := P_{E,\alpha} = \mathtt{t}^m + \sum_{k=0}^{m-1} a_k \mathtt{t}^k$$

definimos $f_2(\mathtt{t}) := \mathtt{t}^m + \sum_{k=0}^{m-1} \psi(a_k)\mathtt{t}^k \in K_2[\mathtt{t}]$, que tiene alguna raíz $\beta \in K_2$ por ser este cuerpo algebraicamente cerrado. Entonces, por el Lema II.3.4, existe un homomorfismo $\widehat{\psi} : E(\alpha) \to K_2$ tal que $\widehat{\psi}(\alpha) = \beta$ y $\widehat{\psi}|_E = \psi$, luego $(E(\alpha), \widehat{\psi}) \in \Sigma$ y $(E, \psi) \prec (E(\alpha), \widehat{\psi})$, en contra de la maximalidad de (E, ψ) en Σ. Por tanto, $L = E$, como queríamos. □

Antes de enunciar y demostrar el principal resultado de esta sección necesitamos el siguiente lema.

Lema II.3.6 *Sean K un cuerpo de característica cero y $\mathtt{j} : \mathbb{Q} \to K$ un homomorfismo de cuerpos. Entonces $\varphi(x) = x$ para cada $x \in \mathbb{Q}$.*

Demostración. Como $\mathtt{j}(1) = 1$, se tiene $\mathtt{j}(n) = n$ para cada entero positivo n pues si suponemos por inducción que $\mathtt{j}(n-1) = n-1$, entonces

$$\mathtt{j}(n) = \mathtt{j}((n-1)+1) = \mathtt{j}(n-1) + \mathtt{j}(1) = (n-1) + 1 = n.$$

Además $\mathtt{j}(0) = 0$ y si $m \in \mathbb{Z}$ es negativo su opuesto $n := -m$ es positivo, y

$$0 = \mathtt{j}(0) = \mathtt{j}(m+n) = \mathtt{j}(m) + \mathtt{j}(n) = \mathtt{j}(m) + n,$$

así que $\mathtt{j}(m) = -n = m$. Finalmente, para todo número racional $q := \frac{m}{n}$, donde $m, n \in \mathbb{Z}$ y $n \neq 0$ se tiene

$$m = \mathtt{j}(m) = \mathtt{j}(qn) = \mathtt{j}(q) \cdot \mathtt{j}(n) = \mathtt{j}(q) \cdot n$$

luego $\mathtt{j}(q) = \frac{m}{n} = q$. □

Ya estamos en condiciones de probar que el cuerpo $\mathbb{C}$ de los números complejos admite infinitos automorfismos. La siguiente proposición proporciona, además, información extra.

Proposición II.3.7 (1) *Sean E un subcuerpo de $\mathbb{C}$ y φ un automorfismo de E. Entonces existe un automorfismo σ de $\mathbb{C}$ tal que $\sigma|_E = \varphi$.*

(2) *El cuerpo $\mathbb{C}$ de los números complejos admite infinitos automorfismos.*

(3) *Sea σ un automorfismo de $\mathbb{C}$ distinto de la identidad y la conjugación. Entonces la función $\sigma : \mathbb{C} \to \mathbb{C}$ no es continua.*

Demostración. (1) Consideremos la familia Σ formada por todos los pares (L,ψ) tales que L es un subcuerpo de $\mathbb{C}$ que contiene a E y ψ es un automorfismo de L tal que $\psi|_E = \varphi$. Como $(E,\varphi) \in \Sigma$ esta familia no es vacía y la ordenamos mediante: $(E_1,\varphi_1) \preceq (E_2,\varphi_2)$ si $E_1 \subset E_2$ y $\varphi_2|_{E_1} = \varphi_1$. Comprobamos que Σ tiene elementos maximales, para lo que aplicamos el Lema de Zorn. Consideremos una cadena $\mathcal{C} := \{(E_i,\varphi_i) : i \in I\} \subset \Sigma$, esto es, un subconjunto de Σ totalmente ordenado. Entonces $F := \bigcup_{i\in I} E_i$ es un subcuerpo de $\mathbb{C}$ que contiene a E, pues dados dos elementos $x, y \in F$ tales que $y \neq 0$ existe, por ser $\mathcal{C}$ una cadena, un índice $i \in I$ tal que $x, y \in E_i$. Como éste es un cuerpo resulta que $x - y$, $xy^{-1} \in E_i \subset F$.

La aplicación $\varphi : F \to F$ que transforma $x \in F$ en $\varphi_i(x) \in E_i \subset F$ si $x \in E_i$ está bien definida, porque si $x \in E_i \cap E_j$ podemos suponer que $E_i \subset E_j$ y, por ser $\mathcal{C}$ cadena, $\varphi_j|_{E_i} = \varphi_i$, así que $\varphi_j(x) = \varphi_i(x)$. De hecho φ es homomorfismo de cuerpos, luego inyectivo. En efecto, dados $x, y \in F$ existen $i, j \in I$ tales que $x \in E_i$ e $y \in E_j$. Como $\mathcal{C}$ es una cadena podemos suponer que $E_i \subset E_j$, luego $x, y, x+y, xy \in E_j$, así que

$$\varphi(x+y) = \varphi_j(x+y) = \varphi_j(x) + \varphi_j(y) = \varphi(x) + \varphi(y) \quad \text{y}$$

$$\varphi(x\cdot y) = \varphi_j(x\cdot y) = \varphi_j(x)\cdot\varphi_j(y) = \varphi(x)\cdot\varphi(y).$$

Por último, φ es sobreyectiva, y en consecuencia es automorfismo de F, pues dado $y \in F$ existe $i \in I$ tal que $y \in E_i = \varphi_i(E_i) = \varphi(E_i) \subset \varphi(F)$.

Hemos probado que $(F,\varphi) \in \Sigma$ y, por la construcción, cada $(E_i,\varphi_i) \preceq (F,\varphi)$, luego este último par es una cota superior de la cadena $\mathcal{C}$. Esto implica, por el Lema de Zorn, que Σ posee algún elemento maximal, que denotamos (L,ψ), y todo se reduce a probar que $L = \mathbb{C}$. En caso contrario existe $u \in \mathbb{C} \setminus L$ y distinguimos dos casos, según que u sea transcendente o algebraico sobre L.

En el primer caso observamos que la aplicación

$$\widehat{\psi} : L[\mathtt{t}] \to L[\mathtt{t}],\ \sum_{k=0}^{d} a_k \mathtt{t}^k \to \sum_{k=0}^{d} \psi(a_k)\mathtt{t}^k$$

es un isomorfismo del anillo $L[\mathtt{t}]$ en sí mismo que induce por ello un automorfismo de su cuerpo de fracciones que denotamos también

$$\widehat{\psi} : L(\mathtt{t}) \to L(\mathtt{t}),\ \frac{f}{g} \mapsto \frac{\widehat{\psi}(f)}{\widehat{\psi}(g)}.$$

Obsérvese que $\widehat{\psi}|_L = \psi$. Sea $\tau : L(u) \to L(\mathtt{t})$ el homomorfismo cuya restricción a L es la identidad y transforma u en $\mathtt{t}$, que evidentemente es un isomorfismo de cuerpos (véase [EAL]). La composición

$$\sigma := \tau^{-1} \circ \widehat{\psi} \circ \tau : L(u) \to L(u)$$

es un automorfismo de $L(u)$ y $\sigma|_L = \psi$. Por tanto, $(L(u),\sigma) \in \Sigma$ y $(L,\psi) \prec (L(u),\sigma)$, lo que contradice la maximalidad de (L,ψ).

Por tanto u debe ser algebraico sobre L y denotamos $\overline{L}_{\mathbb{C}}$ el cierre algebraico de L en $\mathbb{C}$ que, según hemos visto en el Ejemplo II.3.3, es algebraicamente cerrado. Aplicando el Lema II.3.5 al homomorfismo $\mathtt{j} \circ \psi : L \to \overline{L}_{\mathbb{C}}$, donde $\mathtt{j} : L \hookrightarrow \overline{L}_{\mathbb{C}}$ es la inclusión, se deduce que existe un automorfismo $\sigma : \overline{L}_{\mathbb{C}} \to \overline{L}_{\mathbb{C}}$ tal que $\sigma|_L = \psi$. De este modo $(\overline{L}_{\mathbb{C}},\sigma) \in \Sigma$ y de hecho $(L,\psi) \prec (\overline{L}_{\mathbb{C}},\sigma)$, ya que $L \subsetneq \overline{L}_{\mathbb{C}}$ pues $u \in \overline{L}_{\mathbb{C}} \setminus L$. Esto contradice de nuevo la maximalidad de (L,ψ) en Σ, así que $L = \mathbb{C}$ como queríamos demostrar.

(2) Para cada $n \in \mathbb{Z}$ sea $u_n := n + \pi \in \mathbb{C}$, que es transcendente por serlo π, y denotemos $E := \mathbb{Q}(\pi) \subset \mathbb{C}$. Vamos a aplicar el apartado anterior al automorfismo $\varphi_n : E \to E$ cuya restricción a $\mathbb{Q}$ es la identidad y transforma π en u_n. Este automorfismo es la composición del isomorfismo

$\mathtt{j}_n : E \to \mathbb{Q}(\mathtt{t})$ que transforma π en $\mathtt{t}$ y el isomorfismo $\rho_n : \mathbb{Q}(\mathtt{t}) \to E$ que transforma $\mathtt{t}$ en u_n, cuya existencia se deduce de que el homomorfismo de anillos

$$\mathrm{ev}_{u_n} : \mathbb{Q}[\mathtt{t}] \to \mathbb{Q}[u_n],\ g(\mathtt{t}) \to g(u_n)$$

es inyectivo, por lo que es un isomorfismo entre $\mathbb{Q}[\mathtt{t}]$ y $\mathbb{Q}[u_n]$, que en consecuencia se extiende a un isomorfismo entre los cuerpos de fracciones:

$$\mathbb{Q}(\mathtt{t}) \to \mathbb{Q}(u_n),\ \frac{f(\mathtt{t})}{g(\mathtt{t})} \mapsto \frac{f(u_n)}{g(u_n)}.$$

Por el apartado (1), para cada entero n existe $\sigma_n \in \mathrm{Aut}(\mathbb{C})$ tal que $\sigma_n|_E = \varphi_n$ y, en particular, $\sigma_n \neq \sigma_m$ para $n \neq m$ ya que

$$\sigma_n(\pi) = \varphi_n(\pi) = u_n \neq u_m = \varphi_m(\pi) = \sigma_m(\pi).$$

En conclusión, $\{\sigma_n : n \in \mathbb{Z}\}$ es una familia infinita de automorfismos de $\mathbb{C}$.

(3) Sea $\mathtt{i} := \sqrt{-1}$. Obsérvese que $\sigma(\mathtt{i}) \in \{\mathtt{i}, -\mathtt{i}\}$ ya que

$$-1 = -\sigma(1) = \sigma(-1) = \sigma(\mathtt{i}^2) = (\sigma(\mathtt{i}))^2,$$

o lo que es igual, $\sigma(\mathtt{i})$ es raíz del polinomio $\mathtt{t}^2 + 1$, es decir, $\sigma(\mathtt{i}) \in \{\mathtt{i}, -\mathtt{i}\}$. Por ello, para cada número complejo $z := x + y\mathtt{i} \in \mathbb{C}$, donde $x, y \in \mathbb{R}$, se cumple que $\sigma(z) = \sigma(x) \pm \sigma(y)\mathtt{i}$. Por hipótesis σ no es ni la identidad ni la conjugación, luego existe $z \in \mathbb{C}$ tal que $\sigma(z) \notin \{z, \overline{z}\}$, y por ello existe $r \in \mathbb{R}$ tal que $\sigma(r) \neq r$. Como $\mathbb{Q}$ es denso en $\mathbb{R}$ existe una sucesión de números racionales $\{q_n\}_{n\in\mathbb{N}}$ que converge a r y, sin embargo, como $\sigma|_{\mathbb{Q}}$ es la identidad según hemos probado en el Lema II.3.6,

$$\lim_{n\to\infty} \{\sigma(q_n)\} = \lim_{n\to\infty} \{q_n\} = r \neq \sigma(r) = \sigma\Big(\lim_{n\to\infty} \{q_n\}\Big),$$

lo que demuestra que la función σ no es continua en el punto r. □

Observación II.3.8 Que el cuerpo $\mathbb{R}$ sea ordenado hace que sea mucho menos flexible que $\mathbb{C}$. Comprobemos que su único automorfismo $\mathtt{j} : \mathbb{R} \to \mathbb{R}$ es la identidad. En efecto, en caso contrario existiría $x \in \mathbb{R}$ tal que $\mathtt{j}(x) \neq x$ y, cambiando x por $-x$ si es necesario, podemos suponer que $x < \mathtt{j}(x)$. Tomamos $q \in \mathbb{Q}$ tal que $x < q < \mathtt{j}(x)$. Así $q - x > 0$, luego existe $y \in \mathbb{R}$ tal que $q - x = y^2$ y, por lo probado en el Lema II.3.6,

$$q = \mathtt{j}(q) = \mathtt{j}(x) + \mathtt{j}(y^2) = \mathtt{j}(x) + (\mathtt{j}(y))^2 \geq \mathtt{j}(x),$$

que es una contradicción.

CAPÍTULO III

Teorema de Lindemann-Weierstrass

El resultado principal que probaremos en este capítulo es el Teorema de Lindemann-Weierstrass, que afirma que las exponenciales de números algebraicos no nulos y distintos dos a dos son linealmente independientes en el cierre algebraico de $\mathbb{Q}$. Una consecuencia inmediata de esto será que la exponencial de cualquier número algebraico no nulo es transcendente. Así, pasamos de conocer esencialmente tres números transcendentes a conocer infinitos.

Además, con esto último daremos inmediatamente con varias familias nuevas de números transcendentes a través de funciones relacionadas con la exponencial, como logaritmos y funciones trigonométricas de números algebraicos.

III.1. $\mathbb{Q}$-independencia lineal de ciertas exponenciales

Comenzamos esta sección enunciando y probando algunos resultados que necesitaremos más adelante.

Proposición III.1.1 *Para cada $h \in \mathbb{Z}[\mathtt{t}]$ y cada entero $m \geq 0$ se cumple que $h^{(m)} \in m! \cdot \mathbb{Z}[\mathtt{t}]$.*

Demostración. Escribimos

$$h(\mathtt{t}) := \sum_{k=0}^{n} a_{n-k}\mathtt{t}^{n-k},$$

y al derivar m veces resulta

$$h^{(m)}(\mathtt{t}) := \sum_{k=0}^{n-m} \frac{(n-k)!}{(n-k-m)!} \cdot a_{n-k}\mathtt{t}^{n-k} = m! \cdot \sum_{k=0}^{n-m} \binom{n-k}{n-k-m} \cdot a_{n-k}\mathtt{t}^{n-k} \in m! \cdot \mathbb{Z}[\mathtt{t}].$$

□

Proposición III.1.2 *Sean B un anillo conmutativo y unitario y A un subanillo suyo. Sea $f \in A[\mathtt{t}]$ de grado $n > 0$ cuyo coeficiente director es c y que factoriza en $B[\mathtt{t}]$ como producto de factores de grado 1. Sean $\beta_1, \ldots, \beta_n \in B$ las raíces de f, no necesariamente distintas. Entonces, para cada polinomio simétrico $p \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ se cumple que $p(c\beta_1, \ldots, c\beta_n) \in A$.*

Demostración. Sean $\mathtt{s}_1, \ldots, \mathtt{s}_n$ las formas simétricas elementales en las variables $\mathtt{x}_1, \ldots, \mathtt{x}_n$. Por el Teorema Fundamental de los polinomios simétricos, existe $q \in A[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ tal que

$$p(\mathtt{x}_1, \ldots, \mathtt{x}_n) = q(\mathtt{s}_1, \ldots, \mathtt{s}_n).$$

Por otro lado,

$$f(\mathtt{t}) := \sum_{m=0}^{n} a_m\mathtt{t}^m = c\prod_{k=1}^{n}(\mathtt{t} - \beta_k).$$

Multiplicando ambos miembros de esta igualdad por c^{n-1} resulta

$$\sum_{m=0}^{n} a_m c^{n-m-1}(c\mathtt{t})^m = \prod_{k=1}^{n}(c\mathtt{t} - c\beta_k).$$

Las Fórmulas de Cardano-Viéte dicen

$$\prod_{k=1}^{n}(\mathtt{t} - \mathtt{x}_k) = \sum_{m=0}^{n}(-1)^{n-m}\mathtt{s}_{n-m}\mathtt{t}^m$$

y, en consecuencia,

$$\sum_{m=0}^{n} a_m c^{n-m-1}(c\mathtt{t})^m = \prod_{k=1}^{n}(c\mathtt{t} - c\beta_k) = \sum_{m=0}^{n}(-1)^{n-m}\mathtt{s}_{n-m}(c\beta_1, \ldots, c\beta_n)(c\mathtt{t})^m.$$

Por tanto,

$$\mathtt{s}_{n-m}(c\beta_1, \ldots, c\beta_k) = (-1)^{n-m}a_m c^{n-m-1} \in A, m = 0, \ldots, n$$

y por ello,

$$p(c\beta_1, \ldots, c\beta_n) = q(\mathtt{s}_1(c\beta_1, \ldots, c\beta_n), \ldots, \mathtt{s}_n(c\beta_1, \ldots, c\beta_n)) \in A.$$

□

El siguiente resultado es el primero en el que tratamos la independencia de ciertas exponenciales. Aunque no sea el resultado principal del capítulo, sí que conlleva la demostración más extensa, cuya estructura es, una vez más, similar a las de los Teoremas de Hermite y Lindemann. Afortunadamente, esto simplificará mucho la prueba de los resultados siguientes.

Proposición III.1.3 *Sean $f_1, \ldots, f_n \in \mathbb{Z}[\mathtt{t}]$ distintos entre sí. Para cada $i = 1, \ldots, n$ sean $\alpha_{i1}, \ldots, \alpha_{im_i}$ todas las raíces en $\mathbb{C}$ del polinomio f_i. Sean $c_1, \ldots, c_n \in \mathbb{Z}$ tales que*

$$\sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} e^{\alpha_{ij}} = 0.$$

Entonces, $c_1 = \cdots = c_n = 0$.

Demostración. Supongamos que existen enteros $c_1, \ldots, c_n$ no todos nulos cumpliendo la igualdad del enunciado. Podemos suponer que $c_1 \neq 0$. Las raíces del producto $f_1 \cdots f_n$ son los números α_{ij} y definimos el polinomio, simétrico en las variables $\mathtt{x}_{ij}$,

$$\phi(\mathtt{x}_{11}, \ldots, \mathtt{x}_{nm_n}, \mathtt{t}) := \prod_{i=1}^{n}\prod_{j=1}^{m_i}(\mathtt{t} - \mathtt{x}_{ij}) \in \mathbb{Z}[\mathtt{x}_{11}, \ldots, \mathtt{x}_{nm_n}, \mathtt{t}],$$

cuyo grado en la variable $\mathtt{t}$ es

$$\deg(\phi) = \sum_{i=1}^{n} m_i.$$

Sea b_i el coeficiente director de f_i. Como $b := b_1 \cdots b_n$ es el coeficiente director del producto $f_1 \cdots f_n$ se deduce de la Proposición III.1.2 que

$$\phi(b\alpha_{11}, \ldots, b\alpha_{1m_1}, \ldots, b\alpha_{n1}, \ldots, b\alpha_{nm_n}, \mathtt{t}) \in \mathbb{Z}[\mathtt{t}].$$

Con esta definición, la estructura de la demostración es la siguiente:

(I.1) Vamos a dar con un polinomio f_p de forma que $J_p := \sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} \mathcal{J}_{f_p}(\alpha_{ij})$ será un número entero para cualquier p primo.

(I.2) Veremos que para p suficientemente grande se cumple $(p-1)! \leq |J_p|$.

(I.3) Daremos con una cota superior de la forma $|J_p| \leq ac^p$, con a y c positivos.

(I.4) Juntando los dos últimos hechos llegamos a contradicción, pues $\lim_{p\to\infty} \frac{c^p}{(p-1)!} = 0$.

Pasamos ahora a ver cada uno de estos pasos.

(I.1) Sea p un número primo, de momento arbitrario, y consideremos el polinomio

$$g_p(\mathtt{t}) := \sum_{i=1}^{n} \sum_{j=1}^{n_i} \frac{\phi(b\alpha_{11}, \ldots, b\alpha_{1m_1}, \ldots, b\alpha_{n1}, \ldots, b\alpha_{nm_n}, \mathtt{t})^p}{\mathtt{t} - b\alpha_{ij}}.$$

Nótese que cada producto $b\alpha_{ij}$ es un cero de g_p de multiplicidad $p-1$ por ser raíz de multiplicidad p del numerador. El grado de g_p es

$$m := \deg(g_p) = p\deg(\phi) - 1 = p \cdot \sum_{i=1}^{n} m_i - 1 = Mp - 1 \leq Mp, \quad \text{donde} \quad M := \sum_{i=1}^{n} m_i,$$

y coincide con el grado de $f_p(\mathtt{t}) := g_p(b\mathtt{t})$. Consideremos la función

$$\mathcal{J}_{f_p} : \mathbb{C} \to \mathbb{C},\ \omega \mapsto \int_{S_\omega} e^{\omega - z} f_p(z) dz,$$

donde S_ω es el segmento que une los puntos 0 y ω de $\mathbb{C}$ así orientado.

Ahora, vamos a demostrar que para cada p primo el número

$$J_p := \sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} \mathcal{J}_{f_p}(\alpha_{ij})$$

es entero. Empleando la igualdad

$$\mathcal{J}_{f_p}(z) = e^z \cdot \sum_{k=0}^{m} f^{(k)}(0) - \sum_{k=0}^{m} f^{(k)}(z)$$

que vimos en II.2.1 (2) se tiene

$$\begin{aligned} J_p &= \sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} \left(e^{\alpha_{ij}} \sum_{k=0}^{m} f_p^{(k)}(0) - \sum_{k=0}^{m} f_p^{(k)}(\alpha_{ij}) \right) \\ &= \left(\sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} e^{\alpha_{ij}} \right) \cdot \sum_{k=0}^{m} f_p^{(k)}(0) - \sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} \sum_{k=0}^{m} f_p^{(k)}(\alpha_{ij}) \\ &= -\sum_{k=0}^{m} \sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} f_p^{(k)}(\alpha_{ij}). \end{aligned}$$

Nótese que cada $f_p^{(k)}(\alpha_{ij}) = 0$ si $k < p-1$ por ser α_{ij} raíz de multiplicidad $p-1$ de f_p. Por tanto,

$$J_p = -\sum_{k=p-1}^{m} \sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} f_p^{(k)}(\alpha_{ij}). \tag{III.1.1}$$

Para demostrar que J_p es un número entero es suficiente probar que lo es cada $\sum_{j=1}^{m_i} f_p^{(k)}(\alpha_{ij})$. Para cada $i = 1, \ldots, n$ y cada entero positivo k el polinomio

$$\psi_{ki} := \sum_{j=1}^{m_i} g_p^{(k)}(\mathtt{x}_j)$$

es simétrico, y se deduce de la Proposición III.1.2 que cada $\psi_{ki}(b\alpha_{i1}, \ldots, b\alpha_{im_i}) \in \mathbb{Z}$, ya que $\alpha_{i1}, \ldots, \alpha_{im_i}$ son las raíces del polinomio bf_i/b_i, cuyo coeficiente director es b. Como $f_p(\mathtt{t}) = g_p(b\mathtt{t})$ concluimos que

$$\sum_{j=1}^{m_i} f_p^{(k)}(\alpha_{ij}) = b^k \cdot \sum_{j=1}^{m_i} g_p^{(k)}(b\alpha_{ij}) = b^k \cdot \psi_{ki}(b\alpha_{i1}, \ldots, b\alpha_{im_i}) \in \mathbb{Z},$$

y así queda probado que $J_p \in \mathbb{Z}$.

(I.2) Vamos a demostrar que $(p-1)! \leq |J_p|$ para p suficientemente grande.

Se deduce directamente de la Proposición III.1.1 que $(p-1)!$ divide a J_p y a la suma

$$\sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} f_p^{(p-1)}(\alpha_{ij}).$$

De lo primero se desprende que para probar que $(p-1)! \leq |J_p|$ es suficiente ver que J_p es no nulo para p suficientemente grande. Nótese que de la igualdad (III.1.1) se sigue que

$$J_p + \sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} f_p^{(p-1)}(\alpha_{ij}) = -\sum_{k=p}^{m} \sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} f_p^{(k)}(\alpha_{ij})$$

por lo que

$$p! \text{ divide a } J_p + \sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} f_p^{(p-1)}(\alpha_{ij}).$$

Vamos a demostrar que

$$p \nmid \sum_{i=1}^{n} c_i \sum_{j=1}^{m_i} f_p^{(p-1)}(\alpha_{ij}). \tag{III.1.2}$$

Hecho esto, se tendrá que $p! \nmid J_p$ luego, en particular, $J_p \neq 0$, y habremos acabado. Introducimos los polinomios auxiliares

$$h_{ij}(\mathtt{t}) := \frac{f_p(\mathtt{t})}{(\mathtt{t} - \alpha_{ij})^{p-1}}, \text{ que cumplen } \; f_p(\mathtt{t}) = h_{ij}(\mathtt{t}) \cdot (\mathtt{t} - \alpha_{ij})^{p-1},$$

y aplicamos a esta igualdad la Fórmula de Leibniz II.1.2, que nos proporciona

$$f_p^{(p-1)}(\mathtt{t}) = \sum_{k=0}^{p-1} \binom{p-1}{k} \cdot \frac{(p-1)!}{(p-1-k)!} \cdot (\mathtt{t} - \alpha_{ij})^{p-1-k} \cdot h_{ij}^{(p-1-k)}(\mathtt{t}).$$

Evaluando en $z := \alpha_{ij}$ solo el sumando $k := p-1$ es no nulo, así que

$$f_p^{(p-1)}(\alpha_{ij}) = (p-1)! \cdot h_{ij}(\alpha_{ij}).$$

Como

$$h_{ij}(\alpha_{ij}) = b^m \cdot \prod_{r=1}^{n} \prod_{\substack{s=1 \\ (r,s) \neq (i,j)}}^{m_r} (\alpha_{ij} - \alpha_{rs})^p, \tag{III.1.3}$$

para asegurar que se cumple (III.1.2) es suficiente elegir p de modo que

$$p > \text{máx}\left\{|c_1|,\dots,|c_n|,\ |b|,\ |b|\cdot\prod_{r=1}^{n}\prod_{\substack{s=1\\(r,s)\neq(i,j)}}^{m_r}|\alpha_{ij}-\alpha_{rs}|\right\},$$

con lo que obtenemos que $(p-1)!\leq|J_p|$ con p suficientemente grande.

(I.3) Buscamos una cota superior de J_p. Para ello emplearemos el Lema II.2.1 (3). Definimos

$$\rho := \text{máx}\,\{|c_1|,\dots,|c_n|\},\quad a := \rho\cdot\sum_{i=1}^{n}\sum_{j=1}^{m_i}e^{|\alpha_{ij}|}\ \text{ y}$$

$$c := 2b^M\cdot\text{máx}\left\{i=1,\dots,n,\ j=1,\dots,m_i,\ |\alpha_{ij}|\cdot\prod_{r=1}^{n}\prod_{\substack{s=1\\(r,s)\neq(i,j)}}^{m_r}(|\alpha_{ij}|+|\alpha_{rs}|)\right\},$$

que son constantes que no dependen del primo p. Se tiene, en virtud de (III.1.3), y puesto que $m\leq Mp$,

$$\begin{aligned}
|J_p| &\leq \sum_{i=1}^{n}|c_i|\sum_{j=1}^{m_i}|\mathcal{J}_{f_p}(\alpha_{ij})| \leq \rho\cdot\sum_{i=1}^{n}\sum_{j=1}^{m_i}|\alpha_{ij}|e^{|\alpha_{ij}|}\widehat{f}_p(|\alpha_{ij}|)\\
&\leq \rho\cdot\sum_{i=1}^{n}\sum_{j=1}^{m_i}|\alpha_{ij}|e^{|\alpha_{ij}|}(|\alpha_{ij}|+|\alpha_{ij}|)^{p-1}\widehat{h}_p(|\alpha_{ij}|)\\
&\leq 2^{p-1}\rho\cdot\sum_{i=1}^{n}\sum_{j=1}^{m_i}e^{|\alpha_{ij}|}b^m|\alpha_{ij}|^p\cdot\prod_{r=1}^{n}\prod_{\substack{s=1\\(r,s)\neq(i,j)}}^{m_r}(|\alpha_{ij}+\alpha_{rs}|)^p\\
&\leq \rho\cdot\sum_{i=1}^{n}\sum_{j=1}^{m_i}e^{|\alpha_{ij}|}\left(2b^M\cdot|\alpha_{ij}|\cdot\prod_{r=1}^{n}\prod_{\substack{s=1\\(r,s)\neq(i,j)}}^{m_r}(|\alpha_{ij}|+|\alpha_{rs}|)\right)^p \leq ac^p.
\end{aligned}$$

(I.4) En los pasos (I.2) e (I.3) hemos probado que $(p-1)!\leq|J_p|\leq ac^p$ para todo primo p suficientemente grande, lo que en particular implica que

$$0=\lim_{p\to\infty}\left\{\frac{c^p}{(p-1)!}\right\}\geq\frac{1}{a},$$

que es una contradicción.

Así, concluimos que los valores $c_1,\dots,c_n$ han de ser todos nulos, lo que completa la prueba. □

Presentamos a continuación una forma débil del Teorema de Lindemann-Weierstrass.

Teorema III.1.4 *Sean $\alpha_1,\dots,\alpha_n$ números algebraicos distintos y $c_1,\dots,c_n\in\mathbb{Z}$ tales que*

$$\sum_{i=1}^{n}c_ie^{\alpha_i}=0.$$

Entonces, $c_1=\cdots=c_n=0$.

Demostración.

Como cada α_i es algebraico existen polinomios $f_1, \dots, f_n \in \mathbb{Z}[\mathtt{t}]$ irreducibles en $\mathbb{Z}[\mathtt{t}]$ tales que $f(\alpha_i) = 0$ para $i = 1, \dots, n$. Factorizamos cada f_i en $\mathbb{C}[\mathtt{t}]$ como producto de factores de grado 1:

$$f_i(\mathtt{t}) := b_i \prod_{j=1}^{m_i} (\mathtt{t} - \alpha_{ij}), \text{ donde } \alpha_{i1} = \alpha_i.$$

Escribimos la igualdad del enunciado como

$$\sum_{i=1}^{n} \sum_{j=1}^{m_i} c_{ij} e^{\alpha_{ij}} = 0, \text{ donde } c_{i1} = c_i \text{ y } c_{ij} = 0 \text{ para } j = 2, \dots, m_i. \tag{III.1.4}$$

Efectuamos un cambio de notación. Escribimos

$$\alpha_{1j} := \gamma_j, \quad \alpha_{2j} := \gamma_{m_1+j}, \dots, \alpha_{i+1j} = \gamma_{m_1+\cdots+m_i+j},$$

$$c_{1j} := \eta_j, \quad c_{2j} := \eta_{m_1+j}, \dots, c_{i+1j} = \eta_{m_1+\cdots+m_i+j},$$

de modo que, denotando $m := m_1 + \cdots + m_n$, la igualdad (III.1.4) se reescribe

$$\sum_{k=1}^{m} \eta_k e^{\gamma_k} = 0. \tag{III.1.5}$$

Sea $\mathcal{S}_m := \{\sigma_1, \dots, \sigma_{m!}\}$ el grupo de permutaciones de m elementos y definimos el polinomio simétrico en m indeterminadas

$$\phi(\mathtt{x}_1, \dots, \mathtt{x}_m) := \prod_{\sigma \in \mathcal{S}_m} \sum_{k=1}^{m} \eta_k \mathtt{x}_{\sigma(k)} = \prod_{i=1}^{m!} \sum_{k=1}^{m} \eta_k \mathtt{x}_{\sigma_i(k)} \in \mathbb{Z}[\mathtt{x}_1, \dots, \mathtt{x}_m].$$

Nótese que para $\sigma_1 := \mathrm{id}$ se obtiene el factor $\sum_{k=1}^{m} \eta_k \mathtt{x}_k$ que, por (III.1.5), se anula al evaluar $\mathtt{x}_k := e^{\gamma_k}$, luego efectuando el producto y evaluando en $\mathtt{x}_k := e^{\gamma_k}$ resulta

$$\phi(e^{\gamma_1}, \dots, e^{\gamma_m}) = 0. \tag{III.1.6}$$

□

Sea $S := \left\{\mathtt{k} = (k_1, \dots, k_{m!}) \in \mathbb{N}^{m!} : 1 \le k_j \le m, \forall j = 1, \dots, m!\right\} = \{1, \dots, m\} \times \overset{m!}{\cdots} \times \{1, \dots, m\}$. Para desarrollar la expresión de $\phi(\mathtt{x}_1, \dots, \mathtt{x}_m)$ basta con aplicar la propiedad distributiva, generando una suma de productos donde cada producto se genera eligiendo de cada sumando $\sum_{k=1}^{m} \eta_k \mathtt{x}_{\sigma_i(k)}$ un término $\eta_k \mathtt{x}_{\sigma_i(k_i)}$ para cierto k_i. De esta forma

$$\phi(\mathtt{x}_1, \dots, \mathtt{x}_m) = \sum_{\substack{\mathtt{k} \in S \\ \mathtt{k} = (k_1, \dots, k_{m!})}} \eta_{k_1} \cdots \eta_{k_{m!}} \mathtt{x}_{\sigma_1(k_1)} \cdots \mathtt{x}_{\sigma_{m!}(k_{m!})} \tag{III.1.7}$$

por lo que, a partir de (III.1.6) tenemos que

$$0 = \phi(e^{\gamma_1}, \dots, e^{\gamma_m}) = \sum_{\substack{\mathtt{k} \in S \\ \mathtt{k} = (k_1, \dots, k_{m!})}} \eta_{k_1} \cdots \eta_{k_{m!}} e^{\gamma_{\sigma_1(k_1)} + \cdots + \gamma_{\sigma_{m!}(k_{m!})}}. \tag{III.1.8}$$

Como ϕ es simétrico, el coeficiente que acompaña a $\mathtt{x}_{\sigma_1(k_1)} \cdots \mathtt{x}_{\sigma_{m!}(k_{m!})}$ es el mismo que acompaña a $\mathtt{x}_{\sigma(\sigma_1(k_1))} \cdots \mathtt{x}_{\sigma(\sigma_{m!}(k_{m!}))}$ para cualquier $\sigma \in \mathcal{S}_m$. Por tanto, en base a (III.1.8) podemos expresar

$$0 = \sum_{\substack{\mathtt{k} \in S \\ \mathtt{k} = (k_1, \dots, k_{m!}) \\ k_1 \le k_2 \le \cdots \le k_{m!}}} d_{k_1, \dots, k_{m!}} \eta_{k_1} \cdots \eta_{k_{m!}} \sum_{\sigma \in \mathcal{S}_m} e^{\gamma_{\sigma(\sigma_1(k_1))} + \cdots + \gamma_{\sigma(\sigma_{m!}(k_{m!}))}} \tag{III.1.9}$$

donde $d_{k_1,\dots,k_{m!}}$ es una constante > 0 dependiente del número de apariciones de valores distintos de $e^{\gamma_{\sigma(\sigma_1(k_1))}+\cdots+\gamma_{\sigma(\sigma_{m!}(k_{m!}))}}$ según σ, aunque dicho valor no es relevante para la discusión.

Veamos ahora que fijada cualquier tupla $\mathtt{k} = (k_1, \dots, k_{m!}) \in S$ con $k_1 \leq \cdots \leq k_{m!}$ el exponente $\sum_{i=1}^{m!} \gamma_{\sigma(\sigma_i(k_i))}$ en la expresión (III.1.8) es raíz de un mismo polinomio en $\mathbb{Z}[\mathtt{t}]$. En efecto, denotemos $b := b_1 \cdots b_m$. Es claro que el polinomio

$$\psi_{k_1,\dots,k_{m!}} := \prod_{\sigma\in\mathcal{S}_m} (b\mathtt{t} - \sum_{i=1}^{m!} \mathtt{x}_{\sigma(\sigma_i(k_i))}) \in \mathbb{Z}[\mathtt{x}_1, \dots, \mathtt{x}_m][\mathtt{t}]$$

es simétrico en las variables $\mathtt{x}_1, \dots, \mathtt{x}_m$. Luego, por la Proposición III.1.2,

$$b^{m!} \cdot \prod_{\sigma\in\mathcal{S}_m} (\mathtt{t} - \sum_{i=1}^{m!} \gamma_{\sigma(\sigma_i(k_i))}) = \psi(b\gamma_1, \dots, b\gamma_m)(\mathtt{t}) \in \mathbb{Z}[\mathtt{t}],$$

ya que $\gamma_1, \dots, \gamma_m$ son las raíces del producto $f_1 \cdots f_n$, que es un polinomio cuyo coeficiente principal es b. En consecuencia, para cada $\mathtt{k} = (k_1, \dots, k_{m!}) \in S$ con $k_1 \leq \cdots \leq k_{m!}$ los valores $\sum_{i=1}^{m!} \gamma_{\sigma(\sigma_i(k_i))}$ con $\sigma \in \mathcal{S}_m$ son raíces del polinomio

$$\overline{f}_{k_1,\dots,k_{m!}}(\mathtt{t}) := b^{m!} \cdot \prod_{\substack{\mathtt{k}\in S \\ \mathtt{k}=(k_1,\dots,k_{m!})}} (\mathtt{t} - \sum_{i=1}^{m!} \gamma_{\sigma(\sigma_i(k_i))}).$$

Juntando este hecho con (III.1.9), se deduce de la Proposición III.1.3 que $\eta_{m_1} \cdots \eta_{k_{m!}} = 0$ para toda tupla $(k_1, \dots, k_{m!}) \in S$ tal que $k_1 \leq \cdots \leq k_{m!}$. En particular, tomando $\mathtt{k} = (i, \dots, i)$ se deduce que $\eta_i = 0$ para cualquier $i = 1, \dots, m$. Como, $c_1 = \eta_1$ y $c_{i+1} = \eta_{m_1+\cdots+m_i+1}$, esto concluye la demostración.

III.2. Demostración del Teorema de Lindemann-Weierstrass

Enunciamos a continuación el teorema que da nombre a esta sección y al capítulo.

Teorema III.2.1 (Lindemann-Weierstrass) *Sean $\alpha_1, \dots, \alpha_n$ números algebraicos distintos y $\beta_1, \dots, \beta_n$ números algebraicos no todos nulos. Entonces,*

$$\sum_{i=1}^{n} \beta_i e^{\alpha_i} \neq 0.$$

Demostración. Supongamos, por reducción al absurdo, que

$$\sum_{i=1}^{n} \beta_i e^{\alpha_i} = 0.$$

Eliminando todos los β_i nulos podemos suponer que todos son no nulos. Para cada $i = 1, \dots, n$ sea $f_i \in \mathbb{Z}[\mathtt{t}]$ un polinomio irreducible en $\mathbb{Z}[\mathtt{t}]$ que tiene a β_i por raíz. Factorizamos f_i en $\mathbb{C}[\mathtt{t}]$:

$$f_i := b_i \prod_{j=1}^{m_i} (\mathtt{t} - \beta_{ij}), \text{ donde } \beta_{i1} = \beta_i \text{ y cada } \beta_{ij} \in \mathbb{C}.$$

Definimos

$$M := \{1, \dots, m_1\} \times \cdots \times \{1, \dots, m_n\}$$

y denotamos cada uno de sus elementos por $\delta := (\delta_1, \ldots, \delta_n) \in M$. Entonces el polinomio

$$\phi(\mathtt{x}_1, \ldots, \mathtt{x}_n) := \prod_{\delta \in M} \sum_{k=1}^{n} \mathtt{x}_{k,\delta_k} \cdot \mathtt{x}_k \in \mathbb{Z}[\mathtt{x}_{11}, \ldots, \mathtt{x}_{n,m_n}][\mathtt{x}_1, \ldots, \mathtt{x}_n]$$

es simétrico en las nuevas variables $\mathtt{x}_{11}, \ldots, \mathtt{x}_{n,m_n}$ luego, si denotamos $b := b_1 \cdots b_n$, se deduce de la Proposición III.1.2, que el polinomio

$$\psi(\mathtt{x}_1, \ldots, \mathtt{x}_n) := \phi(\mathtt{x}_1, \ldots, \mathtt{x}_n)(b\beta_{11}, \ldots, b\beta_{1m1}, \ldots, b\beta_{n1}, \ldots, b\beta_{nm_n}) \in \mathbb{Z}[\mathtt{x}_1, \ldots, \mathtt{x}_n].$$

Evaluando en $\mathtt{x}_i := e^{\alpha_i}$ obtenemos una expresión de la forma

$$\psi(e^{\alpha_1}, \ldots, e^{\alpha_n}) = \sum_{k_1 + \cdots + k_n = m_1 \cdots m_n} c_{k_1,\ldots,k_n} e^{k_1\alpha_1 + \cdots + k_n\alpha_n},$$

donde cada $c_{k_1,\ldots,k_n} \in \mathbb{Z}$. Además, como el polinomio

$$\varphi(\mathtt{x}_{11}, \ldots, \mathtt{x}_{n1}, \mathtt{x}_1, \ldots, \mathtt{x}_n) := \sum_{k=1}^{n} \mathtt{x}_{k1}\mathtt{x}_k$$

divide a ϕ y

$$\varphi(\beta_{11}, \ldots, \beta_{n1}, e^{\alpha_1}, \ldots, e^{\alpha_n}) = \sum_{k=1}^{n} \beta_k e^{\alpha_k} = 0,$$

se deduce que $\psi(e^{\alpha_1}, \ldots, e^{\alpha_n}) = 0$, es decir,

$$\sum_{k_1 + \cdots + k_n = m_1 \cdots m_n} c_{k_1,\ldots,k_n} e^{k_1\alpha_1 + \cdots + k_n\alpha_n} = 0.$$

Esto implica, por el Teorema III.1.4, que cada $c_{k_1,\ldots,k_n} = 0$, que es falso pues si $m := m_1 \cdots m_n$ el coeficiente $c_{m,0,\ldots,0}$ es no nulo por ser producto de todos los β_{ij} no nulos. □

Corolario III.2.2 *Dados números algebraicos $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ linealmente independientes sobre $\mathbb{Q}$, los números $e^{\alpha_1}, \ldots, e^{\alpha_n}$ son algebraicamente independientes sobre $\mathbb{Q}$.*

Demostración. Denotemos $\omega_k := e^{\alpha_k}$ para $1 \leq k \leq n$ y suponemos, por reducción al absurdo, que $\omega_1, \ldots, \omega_n$ son algebraicamente dependientes sobre $\mathbb{Q}$. Sin pérdida de generalidad podemos suponer que ω_n es algebraico sobre $\mathbb{Q}(\omega_1, \ldots, \omega_{n-1})$ luego, quitando denominadores, existen polinomios no todos nulos $g_0, \ldots, g_m \in \mathbb{Q}[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$, tales que

$$g_m(\omega_1, \ldots, \omega_{n-1})\omega_n^m + g_{m-1}(\omega_1, \ldots, \omega_{n-1})\omega_n^{m-1} + \cdots + g_0(\omega_1, \ldots, \omega_{n-1}) = 0. \tag{III.2.10}$$

Escribimos

$$g_k := \sum_{0 \leq j_\ell \leq d_{k,\ell}} a_{j_1,\ldots,j_{n-1},k} \mathtt{x}_1^{j_1} \cdots \mathtt{x}_{n-1}^{j_{n-1}},$$

donde cada $a_{j_1,\ldots,j_{n-1},k} \in \mathbb{Q}$, y evaluamos dichos polinomios en $\mathtt{x}_\ell := \omega_\ell = e^{\alpha_\ell}$. Así la igualdad (III.2.10) se reescribe

$$\sum_{0 \leq j_\ell \leq d_{m,\ell}} a_{j_1,\ldots,j_{n-1},m}(e^{\alpha_1})^{j_1} \cdots (e^{\alpha_{n-1}})^{j_{n-1}} e^{m\alpha_n} + \cdots$$
$$+ \sum_{0 \leq j_\ell \leq d_{0,\ell}} a_{j_1,\ldots,j_{n-1},0}(e^{\alpha_1})^{j_1} \cdots (e^{\alpha_{n-1}})^{j_{n-1}} = 0.$$

En consecuencia,

$$\sum_{0\le j_\ell\le d_{m,\ell}} a_{j_1,\dots,j_{n-1},\ell} e^{j_1\alpha_1+\cdots+j_{n-1}\alpha_{n-1}+m\alpha_n}+\cdots \\ +\sum_{0\le j_\ell\le d_{0,\ell}} a_{j_1,\dots,j_{n-1},0} e^{j_1\alpha_1+\cdots+j_{n-1}\alpha_{n-1}}=0.$$

Por ser $\alpha_1,\dots,\alpha_n$ linealmente independientes sobre $\mathbb{Q}$ los exponentes

$$\{j_1\alpha_1+\cdots+j_{n-1}\alpha_{n-1}+k\alpha_n:\ 0\le k\le m,\ 0\le j_\ell\le d_{k,\ell}\}$$

son distintos dos a dos. Entonces, por el Teorema de Lindemann-Weierstrass, cada coeficiente $a_{j_1,\dots,j_{n-1},k}=0$, luego $g_0=0,\dots,g_m=0$, y esto es falso. □

Ejemplos III.2.3 (1) Sean $n\ge 1$ y $\alpha_1,\dots,\alpha_n,c_1,\dots,c_n$ números algebraicos no nulos tales que $\alpha_i\ne\alpha_j$ si $i\ne j$. Entonces el número $\gamma:=c_1e^{\alpha_1}+\cdots+c_ne^{\alpha_n}$ es transcendente. En efecto, en caso contrario $c_0:=-\gamma$ es algebraico y se tiene

$$c_0e^0+c_1e^{\alpha_1}+\cdots+c_ne^{\alpha_n}=0,$$

los números $0=\alpha_0,\ \alpha_1,\dots,\alpha_n$ son distintos dos a dos y $c_0,\dots,c_n$ son números algebraicos no todos nulos. Esto contradice el Teorema de Lindemann-Weierstrass.

(2) En particular, si $\alpha\in\mathbb{C}\setminus\{0\}$ es un número algebraico, entonces e^α es transcendente.

De esto se deducen los Teoremas II.1.4 y II.2.2 de Hermite y Lindemann, respectivamente. En efecto, como $\alpha:=1\in\mathbb{C}\setminus\{0\}$ es algebraico, $e=e^\alpha$ es transcendente. Además, si π fuese algebraico también lo sería $\pi\mathtt{i}\ne 0$, por lo que $-1=e^{\pi\mathtt{i}}$ sería transcendente, y esto es falso.

(3) Si $\beta\in\mathbb{R}\setminus\{1\}$ es un número real positivo y algebraico, entonces su logaritmo neperiano $\alpha:=\ln\beta$ es transcendente. En efecto, en caso contrario, y puesto que $\alpha\ne 0$, se deduce de (2) que $\beta=e^\alpha$ es transcendente, en contra de la hipótesis.

(4) Si $\alpha\in\mathbb{R}\setminus\{0\}$ es un número algebraico, entonces $\operatorname{sen}\alpha$, $\cos\alpha$ y $\operatorname{tg}\alpha$ son números transcendentes. En efecto, para el seno y el coseno basta emplear el apartado (1), ya que

$$\operatorname{sen}\alpha=\left(\frac{1}{2\mathtt{i}}\right)e^{\mathtt{i}\alpha}-\left(\frac{1}{2\mathtt{i}}\right)e^{-\mathtt{i}\alpha}\ \text{ y }\ \cos\alpha=\left(\frac{1}{2}\right)e^{\mathtt{i}\alpha}+\left(\frac{1}{2}\right)e^{-\mathtt{i}\alpha}.$$

En cuanto a la tangente, observamos que

$$\operatorname{tg}\alpha=\frac{\operatorname{sen}\alpha}{\cos\alpha}=\frac{(e^{-\mathtt{i}\alpha}-e^{\mathtt{i}\alpha})\mathtt{i}}{e^{\mathtt{i}\alpha}+e^{-\mathtt{i}\alpha}}$$

y, quitando denominadores, resulta $e^{\mathtt{i}\alpha}\operatorname{tg}\alpha+e^{-\mathtt{i}\alpha}\operatorname{tg}\alpha=\mathtt{i}e^{-\mathtt{i}\alpha}-\mathtt{i}e^{\mathtt{i}\alpha}$, o sea,

$$(\operatorname{tg}\alpha+\mathtt{i})e^{\mathtt{i}\alpha}+(\operatorname{tg}\alpha-\mathtt{i})e^{-\mathtt{i}\alpha}=0.$$

Si $\operatorname{tg}\alpha$ fuese algebraico también lo serían los números

$$c_1:=\operatorname{tg}\alpha+\mathtt{i}\ \text{ y }\ c_2:=\operatorname{tg}\alpha-\mathtt{i},$$

que son distintos. También son algebraicos $\alpha_1:=\mathtt{i}\alpha$ y $\alpha_2:=-\mathtt{i}\alpha$ y, sin embargo, $c_1e^{\alpha_1}+c_2e^{\alpha_2}=0$, lo que contradice el Teorema de Lindemann-Weierstrass.

(5) Para cada número algebraico $\alpha\in\mathbb{R}\setminus\{0\}$ los números $\operatorname{senh}\alpha$, $\cosh\alpha$ y $\operatorname{tgh}\alpha$ son transcendentes.

Para el seno y el coseno hiperbólico basta aplicar el apartado (1), ya que

$$\operatorname{senh}\alpha = \left(\frac{1}{2}\right)e^{\alpha} - \left(\frac{1}{2}\right)e^{-\alpha} \text{ y } \cosh\alpha = \left(\frac{1}{2}\right)e^{\alpha} + \left(\frac{1}{2}\right)e^{-\alpha}.$$

Supongamos que

$$\operatorname{tgh}\alpha = \frac{e^{\alpha} - e^{-\alpha}}{e^{\alpha} + e^{-\alpha}}$$

es algebraico. Quitando denominadores,

$$(\operatorname{tgh}\alpha - 1)e^{\alpha} + (\operatorname{tgh}\alpha + 1)e^{-\alpha} = 0,$$

luego $\alpha_1 := \alpha$ y $\alpha_2 := -\alpha$ son números algebraicos distintos, $c_1 := \operatorname{tgh}\alpha - 1$ y $c_2 := \operatorname{tgh}\alpha + 1$ son algebraicos, no son ambos nulos, pero $c_1e^{\alpha_1} + c_2e^{\alpha_2} = 0$, lo que contradice el Teorema de Lindemann-Weierstrass.

(6) Una generalización del Teorema de Lindemann-Weierstrass, que a día de hoy es solo una conjetura, se debe a Schanuel y afirma que dados números complejos $\mathbb{Q}$-linealmente independientes $z_1, \ldots, z_n$ el grado de transcendencia de la extensión de cuerpos $\mathbb{Q}(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n})|\mathbb{Q}$ es mayor o igual que n. Uno se puede dar cuenta de que el caso de $n = 1$ es cierto, precisamente por el Teorema de Lindemann-Weierstrass.

(7) Existen varios números de los que se ignora si son transcendentes (en muchos casos incluso si son irracionales), aunque se sospecha que lo son. Además, aunque haya muchos números que no sabemos si son transcendentes o no, afortunadamente sabemos de casos donde la transcendencia de distintos números no es independiente, y obtener información de uno nos puede aportar a su vez información de los otros:

(7.1) Los números: $e\pi$, $e + \pi$, $\pi - e$, π/e, π^{π}, e^{e}, e^{e^2}, π^{e}, $\pi^{\sqrt{2}}$, e^{π^2}.

(7.2) La *constante γ de Euler-Mascheroni*, definida como

$$\gamma := \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \ln n\right),$$

así como la *constante δ de Gompertz*, definida como $\delta := \mathcal{G}_0(1)$, donde

$$\mathcal{G}_{\alpha}(z) := z^{-\alpha}\int_0^{\infty}(t+z)^{\alpha-1}e^{-t}dt.$$

Afortunadamente, la transcendencia de estos dos valores (que no se sabe ni si son irracionales) no son cuestiones independientes, pues se sabe que al menos uno de estos dos valores ha de ser transcendente (más generalmente, uno de los valores $\gamma + \ln(z)$ o $\mathcal{G}_0(z)$ es transcendente para cualquier $z \notin (-\infty, 0]$ algebraico, véase [R]). Así, probar que uno de los dos es algebraico implicaría que el otro no lo es. En cualquier caso, puede ser que ambos sean transcendentes, así que probar la transcendencia de uno no aportaría información sobre el otro.

(7.3) La *constante de Catalan*, que aparece en el contexto de las integrales elípticas y está definida como

$$G := \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)^2}.$$

De hecho, de forma más general no se sabe la transcendencia (ni la irracionalidad) de $\beta(2n)$ para cualquier n natural, donde β es la *función beta de Dirichlet*, definida como

$$\beta(s) := \sum_{k=0}^{\infty}\frac{(-1)^k}{(2k+1)^s}.$$

Véase que $G = \beta(2)$. Sin embargo, sí se sabe que $\beta(2n+1)$ es múltiplo de π^{2n+1} (y, por tanto, transcendente) para todo n natural (véase [RZ]).

(7.4) Los valores de $\zeta(2n+1)$ con $n \geq 1$, donde ζ es la *función zeta de Riemann*, definida como

$$\zeta(s) := \sum_{k=1}^{\infty} \frac{1}{k^s}.$$

De hecho, de todos estos valores, $\zeta(3)$, conocido como *constante de Apéry*, es el único que se sabe que es irracional. Sin embargo, se conoce que $\zeta(2n)$ es múltiplo de π (y, por tanto, transcendente) para cualquier n natural (véase [W]).

(7.5) Como se mencionó en la introducción, un caso más general de números cuya transcendencia no es independiente es que, para cualquier $\eta \in \mathbb{C} \setminus \{0\}$, alguno de los valores e^{η}, e^{η^2} o e^{η^3} debe ser transcendente (véase [Br]).

CAPÍTULO IV

Teorema de Gelfond-Schneider

Dedicamos este último capítulo al Teorema de Gelfond-Schneider, que fue probado originalmente por Alexander Gelfond y de nuevo de forma independiente por Theodor Schneider en 1934, y que afirma que dados α algebraico y distinto de 0 y 1, y β algebraico no racional, entonces cualquier valor de α^β es transcendente. Con este último resultado se resolvió el séptimo problema de Hilbert, y da lugar a que conozcamos muchos más números transcendentes que los que se conocían hasta entonces.

Cabe mencionar que, puesto que $\alpha^\beta = e^{\beta \ln(\alpha)}$, y dado que hemos visto previamente que $\ln(\alpha)$ es transcendente, el Teorema de Lindemann-Weierstrass no es suficiente para probar este resultado.

IV.1. Cuatro lemas preparatorios

La demostración que presentamos del Teorema de Gelfond-Schneider se apoya en cuatro lemas auxiliares a cuya prueba dedicamos la primera sección del capítulo. Antes recordamos las notaciones que emplearemos.

Notación IV.1.1 Sean R un número real positivo. Denotaremos

$$\overline{D}_R := \{z \in \mathbb{C} : |z| \leq R\}, \quad D_R := \{z \in \mathbb{C} : |z| < R\} \text{ y } \Gamma_R := \overline{D}_R \setminus D_R.$$

Para cada función continua $f : \Gamma_R \to \mathbb{C}$ denotamos

$$|f|_R := \max\{|f(z)| : z \in \Gamma_R\}.$$

Lema IV.1.2 *Sean $a_1(\mathtt{t}), \ldots, a_n(\mathtt{t}) \in \mathbb{R}[\mathtt{t}]$ polinomios no nulos con $\deg(a_i) := d_i$ para cada $i = 1, \ldots, n$. Sean $\omega_1, \ldots, \omega_n$ números reales distintos dos a dos. Entonces la función*

$$F : \mathbb{R} \to \mathbb{R},\ t \mapsto \sum_{j=1}^{n} a_j(t) e^{\omega_j t}$$

tiene a lo sumo $d_1 + \cdots + d_n + n - 1$ ceros, contados con multiplicidad.

Demostración. Multiplicando por $e^{-\omega_n t}$, que no tiene ceros, obtenemos una función con los mismos ceros que la dada y cuyo último sumando es $a_n(t)$. Dicho de otro modo, podemos suponer que $\omega_n = 0$ y $\omega_j \neq 0$ para cada $j \neq n$. Argumentamos por inducción sobre $k = k(F) := d_1 + \cdots + d_n + n$, y se trata de probar que F tiene, a lo sumo, $k(F) - 1$ ceros.

Si $k(F) = 1$ entonces $n = 1$ y $d_1 = 0$, es decir $a_1 \in \mathbb{C}\setminus\{0\}$ es constante y la función $F(t) = a_1 e^{\omega_1 t}$ carece de ceros. Como en este caso

$$d_1 + \cdots + d_n + n - 1 = d_1 + 1 - 1 = 0,$$

se cumple el enunciado. Sea $\ell \geq 2$ de modo que el lema se cumple siempre que $k < \ell$, y supongamos ahora que $k = \ell$. Sea N el número de ceros de la función F. Por el Teorema de Rolle la derivada

$F'(\mathtt{t})$ tiene al menos $N-1$ ceros y se escribe, por ser $\omega_n = 0$, y denotando $b_j(\mathtt{t}) := a_j'(\mathtt{t}) + a_j(\mathtt{t})\omega_j$,

$$F'(t) = \sum_{j=1}^{n-1}(a_j'(t) + a_j(t)\omega_j)e^{\omega_j t} + a_n'(t) = \sum_{j=1}^{n-1} b_j(t)e^{\omega_j t} + a_n'(t). \tag{IV.1.1}$$

Si $d_n = 0$ entonces $a_n'(t) = 0$, por lo que $F'(t)$ tiene $n-1$ sumandos y, como $d_n = 0$,

$$k(F') = \deg(b_1) + \cdots + \deg(b_{n-1}) + (n-1) = d_1 + \cdots + d_{n-1} + d_n + (n-1) = k(F) - 1.$$

Por la hipótesis de inducción, en este caso F' tiene, a lo sumo, $k(F') - 1 = k(F) - 2$ ceros.

Si $d_n \neq 0$ entonces, por (IV.1.1), $F'(t)$ tiene n sumandos, pero el grado de a_n' es $d_n - 1$ y, de nuevo,

$$k(F') = \deg(b_1) + \cdots + \deg(b_{n-1}) + \deg(a_n') + n = d_1 + \cdots + d_{n-1} + (d_n - 1) + n = k(F) - 1.$$

Por hipótesis de inducción en este caso F' tiene, a lo sumo, $k(F') - 1 = k(F) - 2$ ceros.

Por tanto, en ambos casos, $N - 1 \leq k(F) - 2$, luego $N \leq k(F) - 1$, como queríamos probar. □

Recordamos a continuación una versión del Teorema del módulo máximo de las funciones holomorfas definidas en un disco abierto y que no demostraremos.

Lema IV.1.3 *Sean R un número real positivo y $f : \overline{D}_R \to \mathbb{C}$ una función continua cuya restricción al disco abierto D_R es holomorfa. Entonces,*

$$|f(z)| \leq |f|_R \quad \textit{para todo } z \in \overline{D}_R.$$

El lema anterior es útil en la demostración del siguiente

Lema IV.1.4 *Sean r y R dos números reales tales que $1 \leq r \leq R$, y $f_1, \ldots, f_\ell$ funciones continuas, $f_i : \overline{D}_R \to \mathbb{C}$, tales que cada restricción $f_i|D_R$ es holomorfa. Sean $\zeta_1, \ldots, \zeta_\ell$ tales que $|\zeta_j| \leq r$ para $j = 1, \ldots, \ell$. Entonces, el determinante*

$$\Delta := \det \begin{pmatrix} f_1(\zeta_1) & \cdots & f_\ell(\zeta_1) \\ \vdots & \ddots & \vdots \\ f_1(\zeta_\ell) & \cdots & f_\ell(\zeta_\ell) \end{pmatrix}$$

cumple la desigualdad

$$\Delta \leq \left(\frac{R}{r}\right)^{-\ell(\ell-1)/2} \cdot \ell! \cdot \prod_{j=1}^{\ell} |f_j|_R.$$

Demostración. Consideremos las funciones continuas $g_{ij} : \overline{D}_{R/r} \to \mathbb{C}$, $z \mapsto f_j(\zeta_i z)$, $i, j = 1, \ldots, \ell$, cuyas restricciones al disco abierto $D_{R/r}$ son holomorfas. Por ello también es continua la función

$$h : \overline{D}_{R/r} \to \mathbb{C}, z \mapsto \det(g_{ij}(z)),$$

y su restricción al disco abierto $D_{R/r}$ es holomorfa. Sea $m := \ell(\ell-1)/2$. Como cada $g_{ij}|_{D_{R/r}}$ es holomorfa escribimos su desarrollo en serie

$$g_{ij}(z) = \sum_{k=0}^{m-1} b_k(j)\zeta_i^k z^k + z^m h_{ij}(z),$$

donde cada $b_k(j) \in \mathbb{C}$, las funciones $h_{ij} : \overline{D}_{R/r} \to \mathbb{C}$ son continuas y sus restricciones al disco abierto $D_{R/r}$ son holomorfas. Como el determinante es una forma multilineal existe una función continua $g : \overline{D}_{R/r} \to \mathbb{C}$ cuya restricción al disco abierto $D_{R/r}$ es holomorfa y tal que $h(z) = z^m g(z) + r(z)$ para cada $z \in \overline{D}_{R/r}$, donde $r(z)$ es suma de términos de la forma

$$z^{n_1+\cdots+n_\ell} \det(\zeta_i^{n_j}),$$

y los exponentes n_j son enteros no negativos. Obsérvese que el determinante $\det(\zeta_i^{n_j})$ es nulo si y sólo dos de los exponentes n_j coinciden. Por ello, los términos no nulos de esta forma cumplen

$$n_1 + \cdots + n_\ell \geq 0 + 1 + \cdots + (\ell - 1) = \frac{\ell(\ell-1)}{2} = m.$$

Por tanto todos los sumandos de $r(z)$ son múltiplos de z^m y, como $z^m g(z)$ también lo es, deducimos que el cociente

$$\psi : \overline{D}_{R/r} \to \mathbb{C},\ z \mapsto \frac{h(z)}{z^m}$$

es una función continua y su restricción al disco abierto $D_{R/r}$ es una función holomorfa. Se deduce del Lema IV.1.3 que

$$\left|\frac{h(\omega)}{\omega^m}\right| = |\psi(\omega)| \leq |\psi|_{R/r} = \left(\frac{r}{R}\right)^m \cdot |h|_{R/r} \ \text{ para todo } \omega \in \overline{D}_{R/r}. \tag{IV.1.2}$$

Nótese que para cada $z \in \Gamma_{R/r}$ se tiene $|\zeta_i z| \leq R$. Como el determinante de una matriz cuadrada de orden ℓ tiene $\ell!$ sumandos, y para $z \in \overline{D}_{R/r}$ cada $|g_{ij}(z)| = |f_j(\zeta_i z)| \leq |f_j|_R$, resulta

$$|h|_{R/r} \leq \ell! \cdot \prod_{j=1}^{\ell} |f_j|_R.$$

Ahora bien, $\Delta = h(1)$ y $1 \leq R/r \leq R$, por lo que empleando la desigualdad (IV.1.2) obtenemos

$$|\Delta| = |h(1)| = \left|\frac{h(1)}{1^m}\right| \leq \left(\frac{r}{R}\right)^m \cdot |h|_{R/r} \leq \left(\frac{r}{R}\right)^m \cdot \ell! \cdot \prod_{j=1}^{\ell} |f_j|_R = \left(\frac{R}{r}\right)^{-\ell(\ell-1)/2} \cdot \ell! \cdot \prod_{j=1}^{\ell} |f_j|_R.$$

□

Antes de presentar el último de los lemas de esta sección recordamos la noción de entero algebraico y una de sus propiedades básicas.

Definición IV.1.5 Se dice que un número complejo ω es un *entero algebraico* si existe un polinomio mónico e irreducible $\mathtt{p} \in \mathbb{Z}[\mathtt{t}]$ tal que $\mathtt{p}(\omega) = 0$. Es muy fácil comprobar que tal polinomio es único. De hecho es el polinomio mínimo de ω sobre $\mathbb{Q}$. Se llaman *conjugados* de ω a las raíces complejas de $\mathtt{p}$ (incluida ella misma).

Observación IV.1.6 En la definición anterior, la irreducibilidad de $\mathtt{p}$ es superflua. Si $\mathtt{p}$ fuese reducible, elegimos un factor irreducible $\mathtt{q}$ de $\mathtt{p}$ en $\mathbb{Z}[\mathtt{t}]$ tal que $\mathtt{q}(\omega) = 0$ y escribimos $\mathtt{p} := \mathtt{q} \cdot \mathtt{r}$ para cierto polinomio $\mathtt{r} \in \mathbb{Z}[\mathtt{t}]$. Sean a y b, respectivamente, los coeficientes directores de $\mathtt{q}$ y $\mathtt{r}$. Como $\mathtt{p}$ es mónico, $1 = ab$ luego $a = \pm 1$ y, cambiando $\mathtt{q}$ por $-\mathtt{q}$ si es preciso, se obtiene un polinomio mónico, irreducible en $\mathbb{Z}[\mathtt{t}]$ que tiene a ω por raíz.

Observaciones IV.1.7 (1) Emplearemos un resultado muy conocido; el conjunto formado por los enteros algebraicos constituye un anillo conmutativo y unitario con la suma y producto heredados de $\mathbb{C}$.

(2) Sea $\alpha \in \mathbb{C}$ un entero algebraico. Entonces el módulo de alguno de sus conjugados es mayor o igual que 1.

En efecto sea $P \in \mathbb{Z}[\mathtt{t}]$ un polinomio irreducible tal que $P(\omega) = 0$. Escribimos

$$P(\mathtt{t}) := \mathtt{t}^d + a_1\mathtt{t}^{d-1} + \cdots + a_{d-1}\mathtt{t} + a_d = \prod_{z\in\Omega}(\mathtt{t} - z),$$

donde Ω es el conjunto formado por los conjugados de ω. Como P es irreducible, el entero a_d es no nulo, luego

$$1 \leq |a_d| = |P(0)| = \prod_{z\in\Omega} |z|,$$

por lo que $|z| \geq 1$ para algún $z \in \Omega$.

(3) Sea $\alpha \in \mathbb{C}$ algebraico. Entonces existe un entero $c_0 \neq 0$ tal que $c_0\alpha$ es un entero algebraico. En efecto, sea

$$Q(\mathtt{t}) := b_0\mathtt{t}^d + b_1\mathtt{t}^{d-1} + \cdots + b_{d-1}\mathtt{t} + b_d \in \mathbb{Q}[\mathtt{t}]$$

un polinomio no nulo en $\mathbb{Q}[\mathtt{t}]$ que tiene a α por raíz. Escribimos cada $b_k := c_k/r$ conde $c_k, r \in \mathbb{Z}$ y $r \neq 0$, por lo que

$$c_0\alpha^d + c_1\alpha^{d-1} + \cdots + c_{d-1}\alpha + c_d = 0.$$

Multiplicando esta igualdad por c_0^{d-1} resulta

$$(c_0\alpha)^d + c_1(c_0\alpha)^{d-1} + \cdots + c_{d-1}c_0^{d-2}(c_0\alpha) + c_dc_0^{d-1} = 0,$$

luego $c_0\alpha$ es raíz del polinomio mónico

$$\mathtt{t}^d + c_1\mathtt{t}^{d-1} + \cdots + c_{d-1}c_0^{d-2}\mathtt{t} + c_dc_0^{d-1} \in \mathbb{Z}[\mathtt{t}],$$

luego se deduce de la Observación IV.1.6 que $c_0\alpha$ es un entero algebraico.

Lema IV.1.8 *Sea ℓ un entero positivo y para cada $i, j = 1, \ldots, \ell$ sea α_{ij} un número complejo algebraico sobre $\mathbb{Q}$. Supongamos que $\Delta := \det(\alpha_{ij}) \neq 0$ y que existe $c \in \mathbb{Z}$ tal que cada producto $c\alpha_{ij}$ es un entero algebraico. Entonces, el valor absoluto de alguno de los conjugados de Δ es mayor o igual que $c^{-\ell}$.*

Demostración. Nótese que $c^\ell\Delta = \det(c\alpha_{ij})$ es un entero algebraico por serlo cada $c\alpha_{ij}$. Se deduce de la Observación IV.1.7 (2) que alguno de los conjugados de $c^\ell\Delta$ es mayor o igual que 1. Como los conjugados de $c^\ell\Delta$ son los productos de c^ℓ por los conjugados de Δ existe un conjugado Δ' de Δ tal que $|c^\ell\Delta'| \geq 1$, es decir, $|\Delta'| \geq c^{-\ell}$. □

IV.2. Demostración del Teorema de Gelfond-Schneider

Estamos ya en condiciones de probar el resultado principal de este capítulo. Cabe adelantar que la siguiente demostración es la más complicada del texto, pues aparte de ser la más larga, en este caso la estructura no es similar a la de las demostraciones de los anteriores resultados principales.

Teorema IV.2.1 *Sean α y β números complejos algebraicos tales que $\alpha \notin \{0, 1\}$ y β no es racional. Entonces cualquier valor de α^β es transcendente.*

Demostración. Nótese que se emplea la expresión *cualquier valor de* α^β porque el logaritmo complejo es una función multivaluada. De hecho, por simplicidad, y para evitar ambigüedades, nosotros demostraremos solo el caso en que $\alpha > 1$ y β son números reales. Probaremos que si α^β es algebraico, o lo que es lo mismo, si $e^{\beta \ln \alpha}$ es algebraico, donde estamos tomando el valor real de $\ln \alpha$, entonces β es racional.

La estrategia consiste en encontrar dos pares distintos de números enteros (s_1, s_2) y (s_1', s_2') tales que

$$s_1 + s_2\beta = s_1' + s_2'\beta.$$

Hecho esto, al despejar se obtiene

$$\beta = \frac{s_1 - s_1'}{s_2' - s_2} \in \mathbb{Q}.$$

Paso 1. Sea S un entero suficientemente grande, que elegiremos más adelante, y definimos

$$L_0 := \lfloor S \ln S \rfloor, \quad L_1 := \left\lfloor \frac{S}{2 \ln S} \right\rfloor, \quad c := \ln(\ln S) \ \text{ y } \ L := (L_0 + 1)(L_1 + 1).$$

Se cumplen las siguientes desigualdades:

$$cL_0 \cdot \ln S \leq L; \quad cL_1 S \leq L \ \text{ y } \ L \leq S^2. \tag{IV.2.3}$$

Para que se cumpla la primera es suficiente que $c \cdot \ln S \leq L_1 + 1$, para lo que basta que

$$c \cdot \ln S \leq \frac{S}{2 \ln S}, \ \text{ es decir, } \ 2 \ln(\ln S) \cdot (\ln S)^2 \leq S.$$

Para esto es suficiente con que $(\ln S)^3 \leq S$, lo que se cumple si $S >> 0$.

Para que se cumpla la segunda es suficiente que $c \cdot S \leq L_0 + 1$, para lo que basta que

$$c \cdot S \leq S \cdot \ln S, \ \text{ es decir, } \ \ln(\ln S) \leq \ln S, \ \text{ o sea, } \ \ln S \leq S,$$

lo que sucede siempre que $S > 0$.

Por último, la tercera desigualdad se cumple si y solo si $(L_0 + 1) \cdot (L_1 + 1) \leq S^2$, para lo que es suficiente que

$$(S \ln S + 1) \cdot \left(\frac{S}{2 \ln S} + 1 \right) \leq S^2, \ \text{ es decir, } \ \frac{S^2}{2} + S \ln S + \frac{S}{2 \ln S} + 1 \leq S^2,$$

o lo que es lo mismo,

$$S \left(\ln S + \frac{1}{2 \ln S} \right) + 1 \leq \frac{S^2}{2}.$$

Como elegiremos $S > 3$, para que se cumpla la desigualdad anterior basta con que

$$S \cdot (\ln S + 1) \leq \frac{S^2}{2}, \ \text{ o lo que es lo mismo, } \ \ln S + 1 \leq \frac{S}{2},$$

y esta desigualdad la cumple cualquier entero positivo S. Por tanto, basta elegir S suficientemente grande para que se cumplan las tres desigualdades (IV.2.3).

Paso 2. Con las notaciones anteriores consideremos una reordenación cualquiera $(s_1(i), s_2(i))$ de los S^2 pares de números enteros (s_1, s_2) donde $1 \leq s_1, s_2 \leq S$. Consideremos también una reordenación cualquiera $(u(j), v(j))$ con $1 \leq j \leq L$ de los pares de números enteros (u, v) donde $0 \leq u \leq L_0$ y $0 \leq v \leq L_1$.

Definimos la matriz $\mathcal{M}$ de tamaño $S^2 \times L$ dada por

$$\mathcal{M} := \Big(\big(s_1(i) + s_2(i)\beta\big)^{u(j)} \cdot \big(\alpha^{s_1(i)+s_2(i)\beta}\big)^{v(j)} \Big).$$

Paso 3. Ahora, supongamos la existencia de un menor de orden L de la matriz $\mathcal{M}$, y denotemos con Δ su determinante. Con esto, la estructura de la demostración es la siguiente:

(GS.1) Emplearemos el Lema IV.1.4 para obtener una cota superior B_1 de $|\Delta|$.

(GS.2) Emplearemos el Lema IV.1.8 para obtener, si $\Delta \neq 0$, una cota inferior B_2 de $|\Delta|$ con $B_2 > B_1$.

(GS.3) De (GS.2) se desprende que $|\Delta| = 0$, luego $\operatorname{rg}(\mathcal{M}) < L$.

(GS.4) Existe, por tanto, una combinación nula y no trivial de las columnas de $\mathcal{M}$, a partir de la cual construiremos una función F como la del Lema IV.1.2 con menos de L raíces y que cumple

$$F\big(s_1(i) + s_2(i)\beta\big) = 0 \quad \text{para} \quad 1 \leq i \leq L.$$

(GS.5) Se deduce de (GS.4) que existen índices distintos i y k tales que $s_1(i) + s_2(i)\beta = s_1(k) + s_2(k)\beta$, lo que implica que

$$\beta = \frac{s_1(k) - s_1(i)}{s_2(i) - s_2(k)} \in \mathbb{Q},$$

como queríamos demostrar.

Pasamos a probar cada una de las afirmaciones anteriores.

(GS.1) Para $1 \leq i, j \leq L$ definimos la función holomorfa

$$f_j : \mathbb{C} \to \mathbb{C},\ z \mapsto z^{u(j)} \cdot \alpha^{v(j)z} = z^{u(j)} \cdot e^{v(j)z \ln \alpha}$$

y suponiendo, sin pérdida de generalidad, que el menor ocupa las L primeras filas de $\mathcal{M}$, definimos los números $\zeta_i := s_1(i) + s_2(i)\beta$. Nótese que f_j es holomorfa porque $u(j)$ es un entero no negativo. De hecho f_j es una función bien definida porque $\alpha^{v(j)z} = e^{v(j)z \ln \alpha}$ y $\alpha > 1$ es un número real.

Recordemos que para cada par de números complejos z_1 y z_2 se cumple que

$$|e^{z_1 z_2}| = e^{\operatorname{Re}(z_1 z_2)} \leq e^{|z_1 z_2|} = e^{|z_1| \cdot |z_2|}.$$

En consecuencia, para todo número real positivo R se cumple que $|f_j|_R \leq R^{u(j)} \cdot e^{v(j) \cdot R \cdot |\ln \alpha|}$. Aplicamos ahora el Lema IV.1.3 con $r := S(1 + |\beta|)$ y $R := e^2 r$. Se tiene entonces,

$$|\Delta| \leq \left(\frac{R}{r}\right)^{-L(L-1)/2} \cdot L! \prod_{j=1}^{L} |f_j|_R = \big(e^2\big)^{-L(L-1)/2} \cdot L! \prod_{j=1}^{L} |f_j|_R$$

por lo que

$$\begin{aligned} \ln |\Delta| &\leq -\frac{L(L+1)}{2} \cdot \ln e^2 + \ln L! + L \cdot \max\{\ln |f_j|_R : 1 \leq j \leq L\} \\ &= -L(L+1) + (\ln 1 + \ln 2 + \cdots + \ln L) \\ &\quad + L \cdot \max\{u(j) \ln R + v(j) \cdot R \cdot |\ln \alpha| : 1 \leq j \leq L\} \\ &\leq -L(L+1) + L \cdot \ln L + L \cdot L_0 \cdot \ln R + L \cdot L_1 \cdot R \cdot |\ln \alpha|. \end{aligned} \tag{IV.2.4}$$

Eligiendo S suficientemente grande se obtiene

$$\ln |\Delta| \leq -L^2 + c_1(L \cdot L_0 \cdot \ln S + L \cdot L_1 \cdot S)$$

para cierta constante c_1 independiente de la constante $c := \ln(\ln S)$ elegida en el Paso 1. Por tanto, eligiendo S de forma que $c \geq 4c_1$ resulta, empleando las desigualdades (IV.2.3),

$$\ln|\Delta| \leq -L^2 + \frac{L}{4}(c \cdot L_0 \ln S + c \cdot L_1 \cdot S) \leq -L^2 + \frac{2L^2}{4} = -\frac{L^2}{2}. \tag{IV.2.5}$$

(GS.2) Supongamos que $\Delta \neq 0$. Como tanto α como β y α^β son números algebraicos, se desprende de la Observación IV.1.7 que existe un entero positivo ρ_1 tal que $\rho_1\alpha$, $\rho_1\beta$ y $\rho_1\alpha^\beta$ son enteros algebraicos. Por ello, $\rho := \rho_1^{L_0+2S\cdot L_1}$ cumple que el producto de ρ por cada coeficiente de la matriz $\mathcal{M}$ es un entero algebraico. En particular, el producto de ρ por cada coeficiente de los que aparecen en la submatriz cuyo determinante es Δ es un entero algebraico. Se deduce del Lema IV.1.8 que el valor absoluto de alguno de los conjugados de Δ es mayor o igual que ρ^{-L}.

De hecho probaremos más adelante que existe una constante c_2 independiente de c tal que

$$\ln|\Delta| \geq -c_2 \cdot (L \cdot L_0 \ln S + S \cdot L \cdot L_1). \tag{IV.2.6}$$

(GS.3) En particular, tomando $c \geq 8c_2$ y empleando las desigualdades (IV.2.3) resulta

$$\ln|\Delta| \geq \frac{-c \cdot L}{8}(L \cdot L_0 \ln S + S \cdot L \cdot L_1) \geq \frac{L}{8}(-c \cdot L_0 \ln S - c \cdot S \cdot L_1) \geq \frac{L}{8}(-L - L) = \frac{-L^2}{4}.$$

Se desprende entonces de (IV.2.5) y (IV.2.6) que

$$\frac{-L^2}{4} \leq \ln|\Delta| \leq \frac{-L^2}{2},$$

lo cual es absurdo, ya que $L \neq 0$. Esto demuestra que $\Delta = 0$ y, por tanto, las columnas de la matriz $(f_j(\zeta_i))$ son $\mathbb{R}$-linealmente dependientes.

(GS.4) Existen por tanto números reales $b_1, \ldots, b_L$ no todos nulos tales que

$$\sum_{j=1}^{L} b_j f_j(\zeta_i) = 0 \quad \text{para} \quad 1 \leq i \leq L.$$

(GS.5) Ordenamos los pares (u, v), donde $0 \leq u \leq L_0$ y $0 \leq v \leq L_1$ poniendo $(u_1, v_1) \preceq (u_2, v_2)$ si $v_1 < v_2$ o $v_1 = v_2$ y $u_1 \leq u_2$. Así, si ponemos $\zeta_i := s_1(i) + s_2(i)\beta$ resulta

$$\sum_{v=0}^{L_1}\sum_{u=0}^{L_0} b_{(L_0+1)v+u+1}\zeta_i^u \cdot \alpha^{v\zeta_i} = 0 \quad \text{para} \quad 1 \leq i \leq L.$$

Pero podemos escribir

$$\sum_{v=0}^{L_1}\sum_{u=0}^{L_0} b_{(L_0+1)v+u+1}\zeta_i^u \cdot \alpha^{v\zeta_i} = \sum_{v=0}^{L_1} a_v(\zeta_i)e^{w_v\zeta_i},$$

donde

$$a_v(\mathtt{t}) := \sum_{u=0}^{L_0} b_{(L_0+1)v+u+1}\mathtt{t}^u \in \mathbb{R}[\mathtt{t}] \quad \text{y} \quad w_v := v\ln\alpha.$$

En consecuencia, cada uno de los L valores ζ_i es un cero de la función

$$F(\mathtt{t}) := \sum_{v=0}^{L_1} a_v(t)e^{w_v\mathtt{t}}.$$

Como cada el polinomio $a_v(\mathtt{t})$ es no nulo ya que algún coeficiente b_j es distinto de cero, y su grado es a lo sumo L_0, se deduce del Lema IV.1.2 que el número de ceros, contados con multiplicidad, de la función F es, a lo sumo,

$$L_0 \cdot (L_1 + 1) + (L_1 + 1) - 1 = (L_0 + 1) \cdot (L_1 + 1) - 1 = L - 1 < L,$$

luego dos de los L valores ζ_i y $\zeta_{i'}$ deben coincidir, o sea, existen índices distintos i e i' tales que

$$s_1(i) + s_2(i)\beta = s_1(i') + s_2(i')\beta,$$

así que

$$\beta = \frac{s_1(i') - s_1(i)}{s_2(i) - s_2(i')} \in \mathbb{Q},$$

lo que completa la prueba.

Por tanto es la desigualdad (IV.2.6) lo único que nos falta probar. Recordemos que vimos en (GS.2) que existe un entero positivo ρ_1 que solo depende de α y β tal que $\rho := \rho_1^{L_0+2S\cdot L_1} \in \mathbb{Z}$ cumple que $\rho^L\Delta$ es un entero algebraico.

Sea $K := \mathbb{Q}(\alpha, \beta, \alpha^\beta)$, que es una extensión algebraica de $\mathbb{Q}$. Por el Teorema del elemento primitivo, existe $u \in \mathbb{C}$ tal que $K = \mathbb{Q}(u)$. Sean $\{u_1, \ldots, u_N\}$ las raíces del polinomio mínimo de u, que son todas distintas por ser el cuerpo de coeficientes un cuerpo de característica 0. Así, todo homomorfismo (inmersión) de K en $\mathbb{C}$ viene determinado por la imagen de u, que debe ser una de estas N raíces, por lo que se definen en general como

$$\sigma_k : K = \mathbb{Q}(u) \to \mathbb{C}; a_0 + a_1 u + ... + a_{N_1} u^{N-1} \mapsto a_0 + a_1 u_k + ... + a_{N_1} u_k^{N-1}.$$

Así, sean $\sigma_k : K \hookrightarrow \mathbb{C}$, con $k = 1, \ldots, N$ para cierto entero positivo N, las inmersiones de K en $\mathbb{C}$.

Los conjugados de cada elemento $\gamma \in K$ son las imágenes $\sigma_1(\gamma), \ldots, \sigma_N(\gamma)$. Por tanto, si denotamos $\|\gamma\|$ el máximo de los valores absolutos de los conjugados de γ se tiene, para cada $\omega_1, \omega_2 \in K$:

$$\begin{aligned}\|\omega_1 + \omega_2\| &= \text{máx}\,\{|\sigma_k(\omega_1 + \omega_2)| : k = 1, \ldots, N\} = \text{máx}\,\{|\sigma_k(\omega_1) + \sigma_k(\omega_2)| : k = 1, \ldots, N\} \\ &\leq \text{máx}\,\{|\sigma_k(\omega_1)| + |\sigma_k(\omega_2)| : k = 1, \ldots, N\} \leq \text{máx}\,\{|\sigma_k(\omega_1)| : k = 1, \ldots, N\} \\ &+ \text{máx}\,\{|\sigma_k(\omega_2)| : k = 1, \ldots, N\} = \|\omega_1\| + \|\omega_2\|.\end{aligned}$$

Además,

$$\begin{aligned}\|\omega_1 \cdot \omega_2\| &= \text{máx}\,\{|\sigma_k(\omega_1 \cdot \omega_2)| : k = 1, \ldots, N\} = \text{máx}\,\{|\sigma_k(\omega_1) \cdot \sigma_k(\omega_2)| : k = 1, \ldots, N\} \\ &\leq \text{máx}\,\{|\sigma_k(\omega_1)| : k = 1, \ldots, N\} \cdot \text{máx}\,\{|\sigma_k(\omega_2)| : k = 1, \ldots, N\} = \|\omega_1\| \cdot \|\omega_2\|.\end{aligned}$$

Por otro lado, si $q \in \mathbb{Q}$ se tiene $\sigma_k(q \cdot \gamma) = q \cdot \sigma_k(\gamma)$ para $k = 1, \ldots, N$, lo que implica que

$$\|q \cdot \omega\| = |q| \cdot \|\omega\| \quad \text{para cada} \quad \gamma \in K.$$

Se tiene entonces, desarrollando el determinante Δ, que no es sino una suma de productos cuyos factores son sumas de enteros y de productos de números enteros por α, β o α^β,

$$\|\rho^L \cdot \Delta\| = \rho^L \cdot \|\Delta\| \leq \rho^L \cdot L! \cdot S^{L_0 L}(1 + \|\beta\|)^{L_0 L} \cdot (1 + \|\alpha\|)^{SL_1 L} \cdot (1 + \|\alpha^\beta\|)^{SL_1 L}. \qquad \text{(IV.2.7)}$$

Hemos tomado la precaución de escribir $1 + \|\beta\|$, $1 + \|\alpha\|$ y $1 + \|\alpha^\beta\|$ en lugar de $\|\beta\|$, $\|\alpha\|$ y $\|\alpha^\beta\|$ como corresponde al desarrollo del determinante, pues tal vez $\|\beta\|$, $\|\alpha\|$ o $\|\alpha^\beta\|$ pueden ser menores que 1.

Como $\rho^L\Delta \in K$ es un entero algebraico, es raíz de un polinomio mónico $g \in \mathbb{Z}[\mathtt{t}]$ cuyo grado denotamos $\deg(g) := D$. El valor absoluto del producto de las raíces de g es menor o igual que

$|\rho^L \cdot \Delta| \cdot \|\rho^L \cdot \Delta\|^{D-1}$, y dicho producto es $\pm g(0)$, cuyo valor absoluto es mayor o igual que 1 por ser un entero no nulo. En consecuencia, empleando la desigualdad (IV.2.7),

$$|\rho^L \cdot \Delta| \geq \frac{|g(0)|}{\|\rho^L \cdot \Delta\|^{D-1}} \geq \rho^{-(D-1)L} \cdot (L!)^{-D} \cdot S^{-DL_0L} \cdot (1 + \|\beta\|)^{-DL_0L} \cdot (\|\alpha\| \cdot \|\alpha^\beta\| + 1)^{-DSL_1L}.$$

En consecuencia, tomando logaritmos,

$$\ln|\Delta| \geq -DL\ln\rho - DL\ln L - DL_0L\ln S - DL_0L\ln(1 + \|\beta\|) - DSL_1L\ln(\|\alpha\| \cdot \|\alpha^\beta\| + 1),$$

lo que prueba la desigualdad (IV.2.6) y, con ello, el teorema. □

Corolario IV.2.2 (1) Sean α y γ números algebraicos no nulos tales que $\alpha \neq 1$. Entonces, el cociente $\beta := \ln\gamma/\ln\alpha$ es, o bien un número racional o bien un número transcendente.

(2) Sean α_1, α_2 números algebraicos no nulos tales que $\ln\alpha_1$ y $\ln\alpha_2$ son $\mathbb{Q}$-linealmente independientes. Entonces, $\ln\alpha_1$ y $\ln\alpha_2$ son $\overline{\mathbb{Q}}$-linealmente independientes.

(3) Sean $\ell \neq 0$ y $\beta \in \mathbb{C}\setminus\mathbb{Q}$. Entonces, al menos uno de los tres números e^ℓ, β y $e^{\beta\ell}$ es transcendente.

Demostración. (1) Nótese que

$$\gamma = e^{\ln\gamma} = e^{\beta\cdot\ln\alpha} = \alpha^\beta.$$

Supongamos que β es algebraico no racional. Como también lo es $\alpha \notin \{0,1\}$ se desprende del Teorema de Gelfond-Schneider que $\alpha^\beta = \gamma$ es transcendente, contra lo supuesto.

(2) Supongamos que existen números algebraicos no nulos β_1 y β_2 tales que $\beta_1\cdot\ln\alpha_1 - \beta_2\cdot\ln\alpha_2 = 0$. Como $\ln\alpha_1$ y $\ln\alpha_2$ son $\mathbb{Q}$-algebraicamente independientes, en particular son no nulos. Como también son no nulos β_1 y β_2 podemos dividir, de modo que

$$\frac{\ln\alpha_1}{\ln\alpha_2} = \frac{\beta_2}{\beta_1} \text{ es algebraico.}$$

Si $\beta_2/\beta_1 := q \in \mathbb{Q}$ entonces $q\cdot\ln\alpha_1 - \ln\alpha_2 = 0$, lo que contradice la $\mathbb{Q}$-independencia lineal de $\ln\alpha_1$ y $\ln\alpha_2$. Por tanto β_2/β_1 no es racional y se desprende del apartado (1) que β_2/β_1 es transcendente, que es falso por ser β_1 y β_2 números algebraicos.

(3) Supongamos que $\alpha := e^\ell$ y β son algebraicos. Como $\alpha \neq 0, 1$ y β no es racional, se deduce del Teorema de Gelfond-Schneider que $e^{\beta\ell} = \alpha^\beta$ es transcendente. □

Ejemplos IV.2.3 (1) Los números $2^{\sqrt{2}}$ y $\sqrt{2}^{\sqrt{2}}$ son transcendentes porque tanto 2 como $\sqrt{2}$ son algebraicos distintos de 0 y 1 y $\sqrt{2}$ no es racional.

(2) Sean $\mathtt{i} := \sqrt{-1}$, que es algebraico y no racional y α un número algebraico distinto de 0 y 1. Por el Teorema de Gelfond-Schneider $\alpha^{\mathtt{i}}$ es transcendente. En particular, si $a \in \mathbb{Q}\setminus\{0,1\}$ y m y n son enteros positivos, tomando $\alpha := \sqrt[m]{a^n}$ se deduce que $\sqrt[m]{a^{\mathtt{i}n}}$ es transcendente.

(3) Sean a y b números reales positivos y algebraicos con $a \neq 1$. Entonces $\log_a b$ es, o bien racional o bien transcendente. En efecto, si $\log_a b$ no es racional y sí es algebraico se desprende del Teorema de Gelfond-Schneider que $a^{\log_a b}$ es transcendente. Esto es falso ya que

$$a^{\log_a b} = e^{(\ln b)} = b \text{ es algebraico.}$$

(4) El número e^π, conocido como *constante de Gelfond* es transcendente. En efecto, en caso contrario, como es distinto de 0 y 1 e $\mathtt{i}$ es algebraico y no racional, se deduce del Teorema de Gelfond-Schneider que $-1 = e^{\pi\mathtt{i}}$ es transcendente, lo que es falso. Nótese que

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

así que se puede aplicar directamente el Teorema de Gelfond-Schneider pues -1 es algebraico distinto de 0 y 1 e $\mathtt{i}$ es algebraico.

(5) También es transcendente $e^{-\pi/2}$ pues en caso contrario su inverso $e^{\pi/2}$ sería algebraico, luego también sería algebraico su cuadrado, que es e^{π} y acabamos de probar que es transcendente. Nótese que

$$e^{-\pi/2} = \left(e^{\pi\mathtt{i}/2}\right)^{\mathtt{i}} = \left(\cos\left(\frac{\pi}{2}\right) + \mathtt{i}\,\mathrm{sen}\left(\frac{\pi}{2}\right)\right)^{\mathtt{i}} = \mathtt{i}^{\mathtt{i}}.$$

Bibliografía

[B] A. Baker: *Transcendental number theory.* Cambridge University Press, 1975. ISBN 978–0–521–20461–3.

[C1] G. Cantor: *Uber eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen.* J. Reine Angew. Math. **77**, 1874, 258–262. ISSN 0075–4102; 1435–5345/e.

[C2] G. Cantor: *Uber eine elementare Frage der Mannigfaltigkeitslehre.* Jahresbericht der Deutschen Mathematiker-Vereinigung **1**, 1891, 75–78. ISSN 0012–0456; 1869–7135.

[E] L. Euler: *Introduction to Analysis of the Infinite.* Springer, Berlin, Heidelberg, New York, 1988. ISBN 978–0–387–96824–7.

[G] R. Gray: *George Cantor and Transcendental Numbers.* American Math. Monthly, **101** no.9, 1994, 819–832. ISSN 0002–9890.

[Li] J. Liouville: *Mémoires et communications.* Comptes rendus de l'Académie des Sciences **18** 1844, 883–885.

[N] I. Niven: *Irrational numbers.* The Carus Mathematical Monographs **11**. John Wiley and Sons, Inc., 1956, 153 pp. ISBN 978–0–88385–011–4.

[P] S.A. Popescu: *A simple and self-contained proof for the Lindemann-Weierstrass theorem.* arXiv:2306.14352v2, 2023.

[T] R. Tubbs: *Hilbert's Seventh Problem.* HJBA Lecture Notes in Mathematics. Springer. 2016. ISSN 2509–8063.

[RZ] T. Rivoal y W. Zudilin: *Diophantine properties of numbers related to Catalan's constant.* Mathematische Annalen. 2003. ISSN 1432–1807.

[Br] W. Dale Brownawell: *The algebraic independence of certain numbers related by the exponential function.* Journal of Number Theory, 1974. ISSN 0022–314X.

[R] T. Rivoal: *On the arithmetic nature of the values of the gamma function, Euler's constant, and Gompertz's constant.* Michigan Mathematical Journal, 2012. ISSN 0026–2285, 1945–2365.

[W] M. Waldschmidt: *Transcendence of Periods: The State of the Art.* Pure and Applied Mathematics Quarterly, 2006. ISSN 15588599, 15588602.

[SL] S. Lang: *Introduction to transcendental numbers.* Addison-Wesley Pub. Co,, 1966. ISBN 0–201–04176–6 978–0–201–04176–7.

[H] A. Hurwitz: *Beweis der Transcendenz der Zahl e.* Mathematische Annalen, 1893. ISSN 0025–5831; 1432–1807/e.

[Hi] D. Hilbert: *Ueber die Transcendenz der Zahlen e und ...* Mathematische Annalen, 1893. ISSN 0025–5831; 1432–1807/e.

[KW] K. Weierstrass: *Zu Lindemann's Abhandlung. "Über die Ludolph'sche Zahl".* Sitzungsberichte der Königlich Preussischen Akademie der Wissen-schaften zu Berlin, 1885. DOI https://doi.org/10.1017/CBO9781139567817.017.

[EAL] J. F. Fernando Galván y J. M. Gamboa: *Ecuaciones Algebraicas: Extensiones de Cuerpos y Teoría de Galois.* Editorial Sanz y Torres, S.L., 2ª edición, 2017. ISBN 978–84–19947–96–3.

[EA] J. F. Fernando Galván y J. M. Gamboa: *Estructuras Algebraicas: Divisibilidad en Anillos Conmutativos.* Editorial Sanz y Torres, S.L., 2ª edición, 2017. ISBN 978–84–16466–53–5.