Pro Mathematica: Vol. IV, Nos. 7-8, 1990

IRRACIONALIDAD Y TRASCENDENCIA DE e Y π

José TOLA*

Las demostraciones de la trascendencia de los números e y π constituyen hechos importantes de la historia de las Matemáticas que se deben a ***Charles Hermite*** *(1872) y* ***Ferdinand Lindemann*** *(1882) respectivamente. En particular, la demostración de* ***Lindemann*** *dejó definitivamente establecido que es imposible construir un cuadrado cuya área sea* ***exactamente*** *igual a la de un círculo dado. Quedó así resuelto en sentido negativo el clásico problema de los geómetras griegos que se conoce con el nombre de* ***cuadratura del círculo.*** *En la creencia de que esas demostraciones serán de interés para los lectores de*

* Profesor Principal de la PUCP

***Pro-Mathematica** se exponen en este artículo las demostraciones de la trascendencia de e y π en la forma, más sencilla que las originales, que se deben a **David Hilbert** . Para mayor ilustración se dan, además, las pruebas, considerablemente más simples, de la irracionalidad de los mencionados números.*

§ 1. Introducción

Es un hecho bien conocido que e y Π son números trascendentes, es decir que no son raíces de ninguna ecuación algebraica

$$a_0 + a_1x + \ldots + a_nx^n = 0$$

en que los coeficientes $a_o, a_1, \ldots, a_n$ son números enteros. Las demostraciones han sido muy difundidas y no es dificil hallarlas en la literatura matemática, particularmente en otros idiomas. No obstante, considero de interés darla a conocer mejor en nuestro medio.

En parte, la importancia de la trascendencia de π está en el hecho, importante en la historia de las Matemáticas, de que puso punto final, después de muchos siglos, a los innumerables y estériles intentos de llevar a cabo, con sólo la ayuda de la regla y el compás, la construcción de un cuadrado cuya área fuera *exactamente* igual a la de un círculo de radio dado, problema que, con el nombre de *cuadratura del círculo*, se remonta a la antigüedad clásica.

El problema de la cuadratura del círculo se reduce, dado un segmento cuya longitud se toma por unidad, a construir con sólo la ayuda de la regla y el compás otro segmento cuya longitud sea exactamente igual a π. Desde luego, es preciso entender claramente que esta construcción debe concebirse en un sentido ideal, en que los medios empleados sean absolutamente perfectos y en que el resultado no esté afectado por error alguno.

Ahora bien, dado el segmento de longitud unidad, todos los números *construíbles* con la regla y el compás son aquellos y sólo aquellos que pertenecen a una extensión $\mathbb{F}_n$ del campo $\mathbb{F}_o$ de los números racionales, tal que existe una sucesión de campos $\mathbb{F}_o, \mathbb{F}_1, \ldots, \mathbb{F}_n$ que tiene la propiedad de que cada campo $\mathbb{F}_i$ $(i = 1, \ldots, n)$ resulta del precedente $\mathbb{F}_{i-1}$ por adjunción a éste de un número $\sqrt{k}$, donde k pertenece al campo $\mathbb{F}_{i-1}$ pero $\sqrt{k}$ no; es decir que $\mathbb{F}_i$ está formado por todos los números de la forma $a + b\sqrt{k}$ donde a y b pertenecen a $\mathbb{F}_{i-1}$.

Cada número construíble es *algebraico*, es decir que es raíz de una ecuación algebraica con coeficientes enteros.[1]

Por tanto, para comprobar que π no es construible con la regla y el compás basta probar que no es un número algebraico, es decir que es *trascendente*.

La historia de la demostración de la trascendencia de π está estrechamente li-

---

(1) Richard Courant y Herbert Robbins, What is Mathematics?, Oxford University Press (1941), pág. 133.

gada a la de la trascedencia de e, la base de los logaritmos neperianos :

Johann Heinrich Lambert (1728–1777) demostró en 1764 que π es un número irracional, con lo cual quedó demostrado que el problema de la cuadratura del círculo no puede ser resuelto con sólo el auxilio de la regla.

En 1872 *Charles Hermite* (*1822-1905*) [2] logró demostrar que e es trascendente, a cuyo fin se valió de un polinomio obtenido con ayuda de reducidas de fracciones contínuas que había utilizado Lambert. Finalmente, en 1882, *Ferdinand Lindemann (1852-1939*) [2] demostró, mediante una modificación de la demostración de Hermite, que π es también trascendente. Posteriormente, varios matemáticos, y entre ellos los más grandes de su tiempo como Karl Weierstrass (*1815-1897*) y *David Hilbert* (*1862-1943*), dieron variantes y modificaciones de las demostraciones originales.

Las demostraciones de la trascendencia de e y π que se dan aquí se deben a David

Hilbert [3]. *Naturalmente demuestran al mismo tiempo que esos números son irracionales. No obstante, para mayor ilustración y por ser muy sencillo, probaremos previamente la irracionalidad de e y π, aún cuando eso no es requerido para la demostración de su trascendencia.*

I. IRRACIONALIDAD Y TRASCENDENCIA DE *e*.

§ 2. Irracionalidad de *e*

e es igual a la suma de la serie $\sum_{n=0}^{\infty} \frac{1}{n!}$, en donde, en particular, $0! = 1$ por definición.

Si e fuera racional, podríamos suponer que $e = \frac{p}{q}$ donde p y q son enteros primos entre sí. Demostraremos que esta suposición conduce a una contradicción. En efecto, de ella se deduce que

$$0 < \frac{p}{q} - \left(1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{q!}\right) = \sum_{n=q+1}^{\infty} \frac{1}{n!} \quad \textbf{(1)}$$

Ahora bien, podemos escribir

$$\sum_{n=q+1}^{\infty} \frac{1}{n!} = \frac{1}{q!} \left(\frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \ldots \right)$$

$$< \frac{1}{q!} \left(\frac{1}{q+1} + \frac{1}{(q+1)^2} + \ldots \right) =$$

$$= \frac{1}{q!} \frac{\frac{1}{q+1}}{1 - \frac{1}{q+1}} = \frac{1}{q!} \frac{1}{q} .$$

Luego, de **(1)** se deduce que

$$0 < q! \left(\frac{p}{q} - 2 - \frac{1}{2!} - \ldots - \frac{1}{q!} \right) < \frac{1}{q} .$$

Esta desigualdad es imposible pues en tanto el término de enmedio es un número entero positivo, $\frac{1}{q}$ es menor que 1. Por consiguiente e es irracional.

§ 3. Trascendencia de e.

Para demostrar que e es un número trascendente es necesario probar que no es raíz de una ecuación

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0$$

en que $a_o \neq 0$ y a_o, a_1, $a_1, \ldots, a_n$ son números *enteros*. Con tal fin bastará entonces con demostrar que una relación de la forma

$$a_o + a_1 e + a_2 e^2 + \ldots + a_n e^n = 0 \qquad \textbf{(1)}$$

conduce a una contradicción.

La idea de la demostración es la siguiente: determinaremos los números *enteros* M, M_1, M_2, ... , M_n tales que se cumplen las relaciones

$$e = \frac{M_1 + \varepsilon_1}{M}, \quad e^2 = \frac{M_2 + \varepsilon_2}{M}, \ldots, \quad e^n = \frac{M_n + \varepsilon_n}{M}, \qquad \textbf{(2)}$$

donde ε_1/M, $\varepsilon_2/M, \ldots, \varepsilon_n/M$ son números positivos muy pequeños. Valiéndonos de las expresiones **(2)** de las potencias de e la relación **(1)** que suponemos cumplida toma la forma

$$[a_o M + a_1 M_1 + a_2 M_2 + \ldots + a_n M_n] + [a_1 \varepsilon_1 + a_2 \varepsilon_2 + \ldots + a_n \varepsilon_n] = 0 . \qquad \textbf{(3)}$$

La primera expresión entre corchetes es un entero. En el curso de la demostración probaremos que no es nulo. En lo que respecta a la expresión encerrada en el segundo par de corchetes, podremos establecer que puede hacerse menor que la unidad.

Resultará así una contradicción porque es imposible que un entero aumentado en un número menor que 1 resulte igual a cero. De esa manera quedará demostrado que la relación (1) es imposible, y por tanto, que e es trascendente.

En el curso de la demostración que sigue haremos uso del teorema según el cual si un entero no es divisible por un cierto número no puede ser igual a cero, por cuanto cero es divisible por cualquier número dado. Mostraremos entonces que los números $M_1, \ldots, M_n$ *son divisibles por un cierto número primo* p, pero que $a_o M$ *no es divisible por dicho número*. Resultará así que $a_o M + a_1 M + \ldots + a_n M_n$ *no es divisible por* p *y por tanto es diferente de cero.*

La ayuda más importante que tendremos es la de la *integral de Hermite*

$$M = \int_0^\infty \frac{z^{p-1}[(z-1)(z-2)\ldots(z-n)]^p\ e^{-z}}{(p-1)!}dz, \quad \textbf{(4)}$$

donde n es el grado de la ecuación **(1)** y p es un número *impar primo* que después vamos a determinar. Si el intervalo de integración lo dividimos en dos partes por el número ν, podremos definir los números M_ν y ε_ν, $(\nu = 1,\ldots,n)$ mediante las fórmulas

$$M_\nu = e^\nu \int_\nu^\infty \frac{z^{p-1}[(z-1)(z-2)\ldots(z-n)]^p\ e^{-z}}{(p-1)!}dz, \quad \textbf{(5)}$$

y

$$\varepsilon_\nu = e^\nu \int_0^\nu \frac{z^{p-1}[(z-1)(z-2)\ldots(z-n)]^p\ e^{-z}}{(p-1)!}dz, \quad \textbf{(6)}$$

De las fórmulas **(4)**, **(5)** y **(6)** se deduce la ecuación

$$e^\nu = \frac{M_\nu + \varepsilon_\nu}{M}$$

que para $\nu = 1,2,\ldots,n$, da las relaciones **(2)**.

Podemos entrar ahora a detallar la demostración.

1. Comencemos por recordar la fórmula mediante la cual se define la función gama :

$$\Gamma(\rho) = \int_0^\infty z^{\rho-1}\, e^{-z}\, dz.^{(1)}$$

Esta fórmula la vamos a necesitar únicamente para valores enteros y positivos de ρ. Esto supuesto, y que $\rho > 1$, se obtiene integrando por partes

$$\Gamma(\rho) = \int_0^\infty z^{\rho-1}e^{-z}dz = [-z^{\rho-1}e^{-z}]_o^\infty +$$

$$+ \int_0^\infty (\rho-1)z^{\rho-2}e^{-z}dz =$$

---

(1) Ver, por ejemplo, Tola, Análisis II, Lima (1971), pág. 235.

$$= (\rho-1)\int_0^\infty z^{\rho-2}e^{-z}dz = (\rho-1)\Gamma(\rho-1) =$$

$$= (\rho-1)(\rho-2)\ \Gamma(\rho-2) =$$

$$= (\rho-1)(\rho-2)(\rho-3)\ \dots\ 2.1\ \Gamma(1)\ .$$

y puesto que

$$\Gamma(1) = \int_0^\infty e^{-z}dz = 1\ .$$

resulta

$$\Gamma(\rho) = \int_0^\infty z^{\rho-1}e^{-z}dz = (\rho-1)! \qquad \textbf{(7)}$$

Por consiguiente $\Gamma(\rho)$ aumenta rápidamente cuando el entero ρ crece.

2. La fórmula que acabamos de obtener nos permitirá calcular con facilidad la integral de Hermite. Con ese fin nos valdremos de la fórmula para elevar a una potencia

un polinomio [1], y tendremos el siguiente polinomio en potencias de z :

$$[(z-1)(z-2)\ldots(z-n)]^p = [z^n+\ldots+(-1)^n n!]^p=$$
$$= z^{np}+-\ldots(-1)^n(n!)^p, \qquad \textbf{(8)}$$

en donde hemos escrito únicamente los términos en la mayor y en la menor potencia de z, y hemos tenido en cuenta nuestra suposición de que p es un número impar, y por tanto se tiene que $(-1)^{np} = [(-1)^p]^n = (-1)^n$. Se sabe además que todos los coeficientes del polinomio obtenido en **(8)** son enteros. La integral de Hermite es entonces dada por

---

(1) La fórmula para elevar a potencia un polinomio es

$$(a_1+a_2+\ldots+a_p)^m$$
$$= \sum \frac{m!}{\alpha_1!\alpha_1!\ldots\alpha_p!}\, a_1^{\alpha_1} a_2^{\alpha_2}\ldots a_p^{\alpha_p}.$$

donde la suma se extiende a todos los conjuntos $\{\alpha_1,\alpha_2,\ldots,\alpha_p\}$ de números enteros postivos o nulos tales que $\alpha_1 + \alpha_2+\ldots+\alpha_p = m$, y los coeficientes son números enteros. (Weber, Lehrbuch der Algebra, I, pág. 53).

$$M = \frac{(-1)^n (n!)^p}{(p-1)!} \int_0^\infty z^{p-1} e^{-z} dz +$$

$$\sum_{\rho=p+1}^{np+p} \frac{C_\rho}{(p-1)!} \int_0^\infty z^{\rho-1} e^{-z} dz,$$

donde los C_ρ son constantes enteras. Las integrales de la ecuación precedente pueden ser calculadas mediante la fórmula **(7)** y se obtiene

$$M = (-1)^n (n!)^p + \sum_{\rho=p+1}^{np+p} C_\rho \frac{(\rho-1)!}{(p-1)!} .$$

El índice de sumación ρ es siempre mayor que p. Por tanto la expresión $(\rho-1)!/(p-1)!$ es un número entero que tiene a p como factor, de manera que puede sacarse en factor común a p en la sumatoria y resulta

$$M = (-1)^n (n!)^p + p[C_{p+1} + C_{p+2}(p+1) + C_{p+3}(p+2) \ldots].$$

El número M no será divisible por p si no lo es el primer término del segundo miembro para lo cual, dado que p es primo, *basta que sea $p > n$*, lo que es posible porque los números primos son infinitos. Podemos suponer por tanto que $(-1)^n (n!)^p$, y por consiguiente M, no es divisible por el número primo p. También podemos escoger a p de manera que el término a_o de **(1)**, que es diferente de cero, no sea divisible por p, para lo cual basta que sea $p > |a_o|$, lo que es siempre posible. De la manera dicha *queda probado que $a_o M$ no es divisible por p*, que es uno de los hechos que nos proponíamos establecer.

3. Vamos a probar ahora que los números M_ν definidos por **(5)** son todos divisibles por p. Si en dicha ecuación introducimos el factor e^ν dentro del signo integral y hacemos el cambio de la variable z por la variable $\zeta = z-\nu$, que varía entre 0 e ∞ cuando varía entre ν e ∞, se obtiene

$$M_\nu = \int_0^\infty \frac{1}{(p-1)} \Big[(\zeta+\nu)^{p-1} [(\zeta+\nu-1)(\zeta+\nu-2)\dots$$

$$\dots(\zeta+\nu-n)]^p \, e^{-\zeta} \Big] d\zeta$$

Si se llevan a cabo las multiplicaciones del numerador se obtiene un polinomio en ζ en que el término de menor grado es en ζ^p y el de mayor grado es en $\zeta^{(n+1)p-1}$, y cuyos coeficientes son números enteros. La integral del numerador será entonces una combinación lineal de las integrales

$$\int_0^\infty \zeta^p e^{-\zeta} d\zeta, \quad \int_0^\infty \zeta^{p+1} e^{-\zeta} d\zeta, \ldots, \quad \int_0^\infty \zeta^{(n+1)p-1} e^{-z} d\zeta,$$

con coeficientes enteros. Puesto que dichas integrales, según **(7)**, son iguales a $p!$, $(p+1)!$,..., $[(n+1)p-1]!$, la integral del numerador será igual a $p!$ multiplicado por un número entero A_ν, de manera que

$$M_\nu = \frac{p!\ A_\nu}{(p-1)!} = p\ A_\nu. \qquad (\nu = 1,2,\ldots,n),$$

lo cual prueba, como ya habíamos anunciado que $M_1,\ldots,M_n$ *son números enteros divisibles por* p. Este resultado y el hecho ya probado de que $a_o M$ no es divisible por p, permite deducir que $a_o M + a_1 M_1 + \ldots + a_n M_n$ *no es divisible por* p *y por tanto es diferente de cero.*

4. Vamos a tratar ahora acerca de una nueva parte de la demostración que se refiere a la suma $a_1\varepsilon_1+\ldots+ a_n\varepsilon_n$ donde los ε_ν son dados por las fórmulas **(6)**. Vamos a probar que estos números pueden suponerse arbitrariamente pequeños. Para ese fin haremos uso del hecho de que p puede ser elegido tan grande como se quiera, pues las condiciones que hasta ahora hemos impuesto a p son la de ser un número primo mayor que n y que $|a_o|$ y que, por lo demás, puede ser arbitrariamente grande.

Designemos por G y g_ν a los máximos de los valores absolutos de $z(z-1)\ldots(z-n)$ y $(z-1)(z-2)\ldots(z-n)e^{-z+\nu}$, respectivamente, para z en el intervalo (o,n), es decir que

$$\left.\begin{aligned} &|z(z-1)\ldots(z-n)|\leq G \\ &|(z-1)(z-2)\ldots(z-n)e^{-z+\nu}|\leq g_\nu \end{aligned}\right\} \begin{array}{l}\text{para}\\ o \leq z \leq n\ .\end{array}$$

Puesto que $\nu \leq n$, se tiene para $\nu = 1,\ldots,n$,

$$|\varepsilon_\nu| \leq \int_0^\nu \left| \frac{z^{p-1}[(z-1)(z-2)\ldots(z-n)]^p e^{-z+\nu}}{(p-1)!} \right| dz$$

$$\leq \int_0^\nu \frac{G^{p-1} g_\nu}{(p-1)!} \, dz \quad ,$$

o sea

$$|\varepsilon_\nu| \leq \frac{G^{p-1} g_\nu \,.\, \nu}{(p-1)!} \qquad \textbf{(9)}$$

Ahora bien, G, g_ν y ν son números constantes independientes de p, y es claro que la fracción $G^{p-1}/(p-1)!$ es tan pequeña como se quiera si p se elige suficientemente grande.

Luego,

$$|a_1\varepsilon_1 + a_2\varepsilon_2 + \ldots + a_n\varepsilon_n| \leq |a_1||\varepsilon_1| + |a_2||\varepsilon_2| +$$

$$\ldots + |a_n||\varepsilon_n| \leq (|a_1|g_1 + |a_2|2g_2 +$$

$$\ldots + |a_n|ng_n) \, \frac{G^{p-1}}{(p-1)!} \; .$$

Puesto que el valor de la expresión entre paréntesis es independiente de p, resulta de aquí que si p es suficientemente grande la suma $|a_1\varepsilon_1+\ldots+a_n\varepsilon_n|$ es tan pequeña como se quiera y, en particular, menor que la unidad.

Con esto hemos dado término a la demostración, que fue descrita al comienzo, de que una relación de la forma **(1)** en que a_o es diferente de cero y $a_1,\ldots,a_n$ son enteros, conduce a una contradicción, y por consiguiente el número e no es algebraico. Es por tanto trascendente.

II. IRRACIONALIDAD Y TRASCENDENCIA DE π

§ 4. Irracionalidad de π

En la demostración que sigue[1] desempeña un papel importante la función

$$f(x) = \frac{x^n(1-x)^n}{n!} \qquad \textbf{(1)}$$

donde n es un número entero.

---

(1) Niven, Bull. of the Am. Math. Soc., 53 (1947) pág.209).

Designemos por $D^k f$ a la k-ésima derivada de f. Para calcularla podemos emplear la conocida fórmula de *Leibnitz* de la derivada de un producto de dos funciones[1]:

$$D^k(gh) = \sum_{j=0}^{k} \binom{k}{j} D^j g . D^{k-j} h .$$

donde $D^o g = g$ y $D^o h = h$.

Se tiene por tanto

$$D^k f = \frac{1}{n!} \sum_{j=0}^{k} \binom{k}{j} D^j g \; D^{k-j} h$$

donde $g(x) = x^n$ y $h(x) = (1-x)^n$. Por consiguiente, puesto que

$$D^j g(o) = \begin{cases} 0 & \text{si} \quad j < n \\ n! & \text{si} \quad j = n \\ 0 & \text{si} \quad j > n \end{cases} \qquad \text{y}$$

$$D^l h(o) = (-1)^l \frac{n!}{(n-l)!} ,$$

(1) R. Courant, Differential and Integral Calculus, Blackie and Son Limited, vol. I, (1942) pág. 202.

se tiene

$$D^k f(0) = 0 \quad \text{si} \quad k < n$$

y

$$D^k f(0) = \frac{1}{n!} \binom{k}{n} n!\, D^{k-n} h(0) \quad \text{si } k \geq n. \quad \textbf{(2)}$$

Además, se deduce de **(1)** que $f(1-x) = f(x)$, y por tanto, para $k = 0,1,2,...$ es $D^k f(1-x) = (-1)^k D^k f(x)$. En particular

$$D^k f(1) = (-1)^k D^k f(0). \qquad \textbf{(3)}$$

Puesto que tanto los coeficientes binomiales como $D^{k-n} h(0)$ son enteros, resulta de **(2)** y **(3)** que *$D^k f(0)$ y $D^k f(1)$, para $k = 0,1,2,...,$ son números enteros.*

2. Es claro que si probamos que π^2 no es racional tampoco lo será π. Demostraremos pues que si se supone que

$$\pi^2 = \frac{p}{q} \qquad \textbf{(4)}$$

donde p/q es una fracción irreducible se llega a una contradicción. Con este fin nos valdremos de la función f antes considerada, y supondremos que se cumple **(4)**.

Sea la función

$$F(x) = q^n\{\pi^{2n}f(x) - \pi^{2n-2}D^2f(x) + \\ + \pi^{2n-4}D^4f(x) - \dots + \\ \pi^2(-1)^{n-1}D^{2n-2}f(x)+(-1)^nD^{2n}f(x)\}. \quad \textbf{(5)}$$

En virtud de lo demostrado en la parte 1 y de **(4)**,

$$F(0) \text{ y } F(1) \text{ son números enteros} \quad \textbf{(6)}$$

Teniendo en cuenta que, por ser $f(x)$ un polinomio de grado $2n$, sus derivadas de órdenes mayores que $2n$ son nulas, podemos obtener las derivadas primera y segunda de $F(x)$ en la forma

$$F'(x)= q^n\{\pi^{2n}Df(x)-\pi^{2n-2}D^3f(x)+\pi^{2n-4}D^5f(x)- \\ -\dots+\pi^2(-1)^{n-1}D^{2n-1}f(x)\}$$

$$F''(x) = q^n\{\pi^{2n}D^2f(x)-\pi^{2n-2}D^4f(x)+ \\ \pi^{2n-4}D^6f(x)-\dots+\pi^2(-1)^{n-1}D^{2n}f(x)\};$$

de donde se deduce haciendo uso de **(5)**,

$$F''(x)+\pi^2F(x) = q^n\pi^{2n+2}f(x) = p^n\pi^2f(x) \quad \textbf{(7)}$$

Ahora bien, puede observarse que

$$(F'(x)\mathrm{sen}\ \pi x-\pi F(x)\cos\ \pi x)' = \pi F'(x)\cos\ \pi x+$$
$$F''(x)\mathrm{sen}\ \pi x+\pi^2 F(x)\mathrm{sen}\ \pi x-\pi F'(x)\cos\ \pi x =$$
$$F''(x)\mathrm{sen}\ \pi x+\pi^2 F(x)\mathrm{sen}\ \pi x\ .$$

La ecuación **(7)** nos permite escribir entonces

$$(F'(x)\mathrm{sen}\ \pi x-\pi F(x)\cos\ \pi x)'= p^n\pi^2 f(x)\mathrm{sen}\ \pi x \qquad \textbf{(8)}$$

Se deduce de aquí que

$$p^n\pi^2 \int_0^1 f(x)\mathrm{sen}\ \pi x.dx = (F'(x)\mathrm{sen}\ \pi x -$$
$$- \pi F(x)\cos\ \pi x)\Big|_0^1 - \pi F(1)+\pi F(0),$$

o sea

$$\pi p^n \int_0^1 f(x)\mathrm{sen}\ \pi x.dx = F(1)+F(0). \qquad \textbf{(9)}$$

Puesto que, según **(6)**, el segundo miembro es entero, también lo será el primer miembro cualquiera que sea el número *n*. Bastará entonces con probar que *n* puede ser elegido de modo que el primer miembro de **(9)** sea un número *positivo* estrictamente menor que 1, para que **(9)** sea una relación absurda, y por consiguiente la fórmula **(4)** implique una contradicción. Lograremos ese propósito si suponemos que n es tal que $\frac{2p^n}{n!} < 1$, lo que es posible porque $\lim_{n\to\infty} \frac{p^n}{n!} = 0$

En efecto, debido a que $x(1-x) = x-x^2$ es positivo y menor que 1 para $0 < x < 1$, en este intervalo se cumple que

$$0 < f(x) < \frac{1}{n!}$$

y por consiguiente

$$0 < \pi p^n \int_0^1 f(x) \operatorname{sen} \pi x . dx < \pi \frac{p^n}{n!} \int_0^1 \operatorname{sen} \pi x . dx$$

$$= \frac{2p^n}{n!} < 1 \ ;$$

es decir que el primer miembro de **(9)** es positivo y menor que 1 y por tanto, como hemos señalado, esa ecuación es absurda y la suposición **(4)** implica una contradicción. π es por consiguiente un número irracional.

§ 5. Trascendencia de π

5.1 Definiciones y proposiciones preliminares

La demostración de la trascendencia del número π que vamos a exponer aquí se debe a *Hilbert* como ya hemos señalado, y requiere recordar algunas definiciones y proposiciones algebraicas que damos a continuación.

Se llama *función racional* de las variables $x_1, x_2, \ldots, x_n$ a una función que es definida por un cociente de la forma

$$f(x_1, x_2, \ldots, x_n) = \frac{\sum\limits_{\alpha} c_\alpha \, x_1^{\alpha_1} \, x_2^{\alpha_2} \ldots \, x_n^{\alpha_n}}{\sum\limits_{\alpha} c'_\alpha \, x_1^{\alpha_1} \, x_2^{\alpha_2} \ldots \, x_n^{\alpha_n}},$$

donde las sumas se extienden a todos los conjuntos

$$\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$$

de n números enteros positivos o nulos, y en que los coeficientes c_α y c'_α son números complejos, un número finito de los cuales, a lo sumo, es diferente de cero; pero sin que el denominador se reduzca a cero. Si la expresión que define a f se reduce al numerador

$$f(x_1,\ldots,x_n) = \sum_{\alpha} c_\alpha \, x_1^{\alpha_1} \, x_2^{\alpha_2} \ldots x_n^{\alpha_n} ,$$

se llama *función racional entera* de $x_1,x_2,\ldots,x_n$ o *polinomio* en $x_1,x_2,\ldots,x_n$. De lo contrario se llama *función racional fraccionaria*.

Se dice que la función $f(x_1,\ldots,x_n)$ es *simétrica* si su valor no cambia cuando se realiza una permutación cualquiera de los valores que se atribuya a las variables, es decir si se cumple que

$$f(a_1,\ldots,a_n) = f(a_{\sigma(1)},\ldots,a_{\sigma(n)}),$$

cualesquiera que sean los números $a_1,\ldots,a_n$ del dominio en que la función es definida y la permutación σ de los subíndices $1,2,\ldots,n$. Las funciones racionales enteras que son simétricas se denominan en forma abreviada *polinomios simétricos* en las variables $x_1, \ldots, x_n$.

Atención especial merecen los polinomios evidentemente simétricos

$$s_1 = x_1 + x_2 + \ldots + x_n$$
$$s_2 = x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n$$
$$s_3 = x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_n = x_1x_2 \ldots x_n \text{ ,}$$
[1]

los cuales se llaman *funciones simétricas elementales* de las variables $x_1, \ldots, x_n$.

Consideremos ahora la ecuación algebraica de grado n

$$a_o + a_1x + \ldots + a_{n-1}x^{n-1} + x^n = 0 , \qquad \textbf{(1)}$$

cuyos coeficientes son números complejos, y en que el coeficiente de x^n es *1*, razón

---

(1) Observar que cada término $x_{j_1} x_{j_2} \ldots x_{j_p}$ de s_p es tal que $j_1 < j_2 < \ldots < j_p$

por la cual diremos que la ecuación es *mónica*. Si $\alpha_1,\alpha_2,\ldots,\alpha_n$ son las raíces de la ecuación, es sabido que se cumple la identidad

$$a_o+ a_1x +\ldots+ a_{n-1}x^{n-1}+ x^n = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n),$$

de donde se deduce que

$$-a_{n-1}= \alpha_1+ \alpha_2+\ldots+ \alpha_n$$

$$a_{n-2}= \alpha_1\alpha_2+ \alpha_1\alpha_3+\ldots+ \alpha_1\alpha_n+ \alpha_2\alpha_3+\ldots+ + \alpha_{n-1}\alpha_n$$

$$-a_{n-3}= \alpha_1\alpha_2\alpha_3+ \alpha_1\alpha_2\alpha_4+\ldots+ \alpha_{n-2}\alpha_{n-1}\alpha_n$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(-1)^n a_o = \alpha_1\alpha_2 \ldots \alpha_n .$$

Puede reconocerse de inmediato que los segundos miembros de las ecuaciones anteriores son la funciones simétricas elementales de las raíces de la ecuación y se cumple por tanto que *las funciones simétricas elementales* $s_1,s_2,\ldots,s_n$ *de las raíces de una ecuación mónica son iguales a los coeficientes de la ecuación con sus propios signos o con signos contrarios, de acuerdo* *con la fórmula*

$$s_p = (-1)^p a_{n-p}\ , \qquad (p = 1,2,\ldots,n).$$

La siguiente proposición, que luego vamos a utilizar, es consecuencia del teorema fundamental de la teoría de las funciones simétricas[1]

Teorema 1.

a) Cada polinomio simétrico P de las variables $x_1,x_2,\ldots,x_n$ es igual a un polinomio Q en las funciones simétricas elementales $s_1,\ldots,s_n$ de dichas variables y en los coeficientes de P; y los coeficientes de Q son números enteros.

b) Si todos los coeficientes de P son números *racionales*, Q es un polinomio en las funciones simétricas elementales de las variables y sus coeficientes son *racionales*.

c) Si todos los coeficientes de P son números *enteros*, Q es un polinomio en las

---

(1) Ver por ejemplo, Van der Warden, Moderne Algebra I, Springer (1937).

funciones simétricas elementales de las variables y sus coeficientes son *enteros*.

Las observaciones hechas precedentemente acerca de la ecuación mónica **(1)** da lugar a la siguiente consecuencia del teorema anterior.

Teorema 2.

a) Cada polinomio simétrico P en las raíces $\alpha_1,\dots,\alpha_n$ de la ecuación mónica **(1)** es igual a un polinomio Q en los coeficientes $a_o,a_1,\dots,a_{n-1}$ de la ecuación y en los coeficientes de P; y los coeficientes de Q son enteros.

b) Si todos los coeficientes de P y los de la ecuación **(1)** son números *racionales*, P es igual a un número *racional*.

c) Si todos los coeficientes de P y los de la ecuación **(1)** son números *enteros*, P es igual a un número *entero*.

Si la ecuación que se considera no es mónica, y si $a_n\neq o$ es el coeficiente de x^n, lo expresado anteriormente se cumple sustituyendo a los coeficientes $a_o, a_1, \ldots, a_n$ por los números $\frac{a_o}{a_n}, \frac{a_1}{a_n}, \ldots, \frac{a_{n-1}}{a_n}$.

Por último, recordaremos los siguientes conceptos acerca de los *números algebraicos*[1]:

Un número complejo se llama *algebraico* si es una raíz de una ecuación algebraica con coeficientes enteros, o bien, equivalentemente, de una ecuación *mónica* con coeficientes racionales.

Un número algebraico se llama *entero algebraico* si es raíz de una ecuación *mónica* con coeficientes enteros racionales. *En adelante mantendremos la denominación de enteros para los números enteros racionales :*

La suma, la diferencia, el producto y el cociente, de números algebraicos (con divisor diferente de cero en el último ca-

(1) L.W.Reid, The Elements of the Theory of Algebraic Numbers, The Macmillan Co. (1910).

so) son números algebraicos; y la suma, la diferencia y el producto de números enteros algebraicos son también enteros algebraicos.

En el anexo se ha reunido una información complementaria acerca de los números algebraicos; en particular, se da la demostración de las proposiciones enunciadas anteriormente.

5.2 Demostración de la trascendencia de π

De la ecuación

$$e^{z} = e^{x+iy} = e^{x}(cos\ y + i\ sen\ x)$$

mediante la cual se define a la función exponencial de la variable compleja 2, resulta la relación

$$1 + e^{i\pi} = 0 \qquad \textbf{(2)}$$

La trascendencia de e, que ya fue demostrada, asegura que no puede existir una ecuación de la forma

$$a_{o} + a_{1}e + \ldots a_{n}e^{n} = 0$$

donde $a_o \neq o$ y $a_o, a_1, \ldots, a_n$ son números enteros racionales.

Lindemann demostró en 1882 que tampoco es posible que se cumpla una relación de la forma

$$a_o + a_1 e^{b_1} + a_2 e^{b_2} + \ldots + a_n e^{b_n} = o \qquad \textbf{(3)}$$

en que los números a_j y b_j $(j = o, 1, \ldots, n)$ sean *algebraicos*. Ahora bien, la unidad imaginaria i es un número algebraico por cuanto es raíz de la ecuación $1 + x^2 = o$. Luego, si π fuera algebraico también lo sería $i\pi$, y no podría cumplir la ecuación **(2)** en virtud del teorema de *Lindemann*. Resulta así que π es trascendente.

Aquí no vamos a demostrar el teorema general de *Lindemann* sino un caso particular. La demostración de *Hilbert* que vamos a exponer es una modificación de la que fue dada para demostrar la trascendencia de e .

Comenzamos pues suponiendo, contrariamente a lo que queremos probar, que π es algebraico, es decir que es raíz de una ecuación algebraica con coeficientes *enteros*. Según lo dicho $i\pi$ satisfaría también a una ecuación de la misma clase, cuyas raíces ($i\pi$ entre ellas) vamos a designar por $\alpha_1,\alpha_2,\ldots,\alpha_n$. A causa de **(2)** se cumple entonces la relación

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

que puede escribirse en la forma

$$\left.\begin{array}{l}(1+e^{\alpha_1}+e^{\alpha_2}+\ldots+e^{\alpha_n})+(e^{\alpha_1+\alpha_2}+e^{\alpha_1+\alpha_3}+\ldots \\ +e^{\alpha_{n-1}+\alpha_n})+\ldots+(e^{\alpha_1+\alpha_2+\alpha_3}+e^{\alpha_1+\alpha_2+\alpha_4}+\ldots \\ +e^{\alpha_{n-2}+\alpha_{n-1}+\alpha_n})+\ldots+(e^{\alpha_1+\alpha_2+\ldots+\alpha_n})=0\end{array}\right\}\textbf{(4)}$$

Puede ocurrir que algunos de los exponentes de esta ecuación sean nulos. Cada vez que eso ocurra uno de los términos se reducirá a *1*. Si los sumamos con el *1* que ya aparece en el primer término resultará un número racional entero positivo a_o. Los demás exponentes, todos ellos diferentes de cero, los designamos por $\beta_1, \beta_2, \ldots, \beta_N$, y por tanto **(4)** puede escribirse en la forma

$$a_o + e^{\beta_1} + e^{\beta_2} + \ldots + e^{\beta_N} = 0, \quad (a_o \text{ entero} > 0) \quad \textbf{(5)}$$

Podemos probar que los números $\beta_1, \beta_2, \ldots, \beta_N$ son las raíces de una ecuación algebraica con coeficientes enteros racionales. En efecto, a partir de la ecuación cuyas raíces son $\alpha_1, \alpha_2, \ldots, \alpha_n$ podemos construir otra ecuación con coeficientes enteros cuyas raíces son las sumas de dos términos $\alpha_1 + \alpha_2$, $\alpha_1 + \alpha_3, \ldots, \alpha_{n-1} + \alpha_n$[1].

---

(1) Los coeficientes de la ecuación mónica de grado $n(n-1)/2$

$$(x-(\alpha_1+\alpha_2))(x-(\alpha_1+\alpha_3))\ldots(x-(\alpha_{n-1}+\alpha_n)),$$

cuyas raíces son los números $\alpha_i+\alpha_j$, donde $i,j = 1,2,\ldots,n$, e $i<j$, son funciones simétricas de los α_k y por tanto son funciones racionales enteras de los coeficientes del polinomio mónico cuyas raíces son $\alpha_1, \alpha_2, \ldots, \alpha_n$, y por consiguiente son números racionales. Luego, los números $\alpha_i + \alpha_j$ son raices de una ecuación algebraica con coeficientes enteros.

Semejantemente, a partir de la ecuación cuyas raíces son estos últimos números podemos construir otra, también con coeficientes enteros, cuyas raíces son las sumas de tres términos $\alpha_1+\alpha_2+\alpha_3, \alpha_1+\alpha_2+\alpha_4, \ldots, \alpha_{n-2}+\alpha_{n-1}+\alpha_n$; y así sucesivamente. Por último, $\alpha_1+\alpha_2+\ldots+\alpha_n$ que es el coeficiente de mayor grado de la ecuación mónica, cuyas raíces son $\alpha_1, \alpha_2, \ldots, \alpha_n$, es un número racional y satisface por tanto a una ecuación *lineal* de coeficientes enteros. Multiplicando todas las ecuaciones así obtenidas se obtendrá una ecuación de coeficientes enteros algunas de cuyas raíces pueden ser nulas, y cuyas restantes raíces son $\beta_1, \beta_2, \ldots, \beta_N$. Si la dividimos por la potencia de la incógnita cuyo exponente es igual al número de raíces nulas, resultará una ecuación de grado N cuyas raíces son los N números $\beta_1, \beta_2, \ldots, \beta_N$:

$$b_o+b_1z+b_2z^2+\ldots+b_Nz^N = 0, \ (b_o, b_N \neq 0 \ ; \ b_i \text{ entero para } i = 0, 1, \ldots, N). \qquad (6)$$

Resumiendo: si se supone que π es algebraico tendrá que cumplirse la ecuación **(5)** en donde los exponentes $\beta_1, \beta_2, \ldots, \beta_N$ son raices de una ecuación **(6)**. Si demostramos que de **(5)** y **(6)** resulta una contradicción quedará probado que π es un número trascendente. Podemos decir en consecuencia que para demostrar que π es trascendente basta probar la siguiente proposición que es un caso particular del teorema de *Lindemann : Si* $\beta_1, \beta_2, \ldots, \beta_N$ *son las raíces de una ecuación* **(6)**, *no es posible que se cumpla la relación* **(5)**.

La demostración se hará siguiendo pasos semejantes a los de la demostración de la trascendencia de e, de la que difiere en aspectos muy importantes. Tal como entonces pudimos obtener expresiones apropiadas de las potencias enteras de e, ahora las obtendremos para las potencias de e que figuran en la ecuación **(5)**. Ellas serán

$$e^{\beta_1} = \frac{M_1 + \varepsilon_1}{M}, \quad e^{\beta_2} = \frac{M_2 + \varepsilon_2}{M}, \ldots,$$

$$e^{\beta_N} = \frac{M_N + \varepsilon_N}{M}, \qquad (7)$$

en donde, como probaremos luego, M será un entero y los números $\varepsilon_1,\ldots,\varepsilon_N$, que ahora podrán ser complejos, serán tan pequeños como se quiera en valor absoluto; pero en que, a diferencia de lo que tuvo lugar en el caso de e, la suma $\sum_{\nu} M_{\nu}$, y no cada uno de los números M_{ν}, será un entero divisible por un cierto número primo p[1].

Sustituyendo en **(5)** los valores **(7)** se obtiene

$$[a_o M+M_1+M_2+\ldots+M_N]+[\varepsilon_1+\varepsilon_2+\ldots+\varepsilon_N]= 0 \qquad \textbf{(8)}$$

En el curso de la demostración probaremos que $a_o M$, y por tanto la primera expresión entre corchetes, es un entero no divisible por un número primo p, y es por consiguiente un entero diferente de cero. Probaremos también que basta elegir al número primo p suficientemente grande, para que la suma $\varepsilon_1+\varepsilon_2+\ldots+\varepsilon_N$ se haga tan pequeña

(1) Como observaremos mas tarde, los números M_{ν} serán ahora enteros algebraicos, no necesariamente enteros (racionales).

como se quiera. Resultará así que **(9)** es una relación imposible, lo que probará que π es trascendente.

Procederemos ahora a exponer los detalles de la demostración que acabamos de describir.

1. Para definir al número M utilizaremos una adecuada modificación de la integral de *Hermite* que fue utilizada para demostrar la trascendencia de e. M será dado por

$$M = \int_0^\infty \frac{1}{(p-1)!} z^{p-1} \Big[(z-\beta_1)(z-\beta_2) \dots$$
$$\dots (z-\beta_N) \Big]^p e^{-z} . b_N^{(N-1)p} \, dz,$$

donde b_N es el coeficiente de z^n en **(6)**, y p es un cierto número primo que luego determinaremos. Puesto que $\beta_1, \dots, \beta_N$ son las raices de la ecuación **(6)**, puede escribirse

$$(z-\beta_1)(z-\beta_2)\dots(z-\beta_N) = \frac{1}{b_N} (b_o + b_1 z + \dots$$
$$+ b_N z^N) \qquad \textbf{(9)}$$

y por consiguiente

$$M = \int_0^\infty \frac{e^{-z} z^{p-1} dz}{(p-1)!} [b_o + b_1 z + \ldots + b_N z^N]^p .$$

$$. b_N^{(N-1)p-1} \qquad (10)$$

2. Desarrollemos ahora el integrando según las potencias de z . La menor potencia es z^{p-1} y da origen al término

$$\int_0^\infty \frac{e^{-z} z^{p-1} dz}{(p-1)!} \, b_o^p \, b_N^{(N-1)p-1} \qquad (11)$$

de la expresión de M.

La fórmula

$$\Gamma(\rho) = \int_0^\infty z^{\rho-1} e^{-z} dz = (\rho-1)! \qquad (12)$$

que da el valor de la función *gama* para ρ entero positivo permite escribir el término (11) en la forma

$$b_o^p \, b_N^{(N-1)p-1} .$$

Los demás términos del integrando de la expresión de M contienen a z elevado a la potencia p o mayores que p, de manera que sus integrales son de la forma

$$\frac{K_q}{(p-1)!} \int_0^{\infty} e^{-z} z^{q-1} dz, \qquad (q-1 \geq p),$$

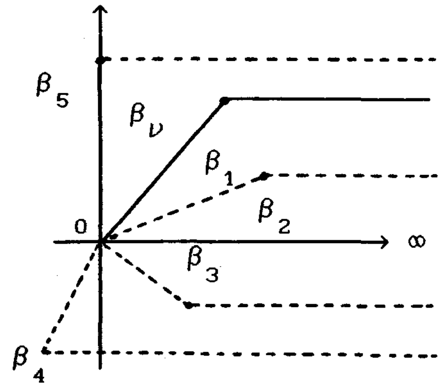
donde k_q es un entero. En virtud de **(12)** esos términos tienen valores

$$K_q \frac{(q-1)!}{(p-1)!} = K_q . p \ldots (q-1), \qquad (q-1 \geq p),$$

de manera que todos ellos son números enteros divisibles por p. Resulta así que M es la suma de $b_o\ b_N^{(N-1)p-1}$ y de un múltiplo de p. Basta con que elijamos al número primo p de modo que sea $p > |b_o|$ y $p > |b_N|$ para que $b_o\ b_N^{(N-1)p-1}$ no sea divisible por p, y por tanto, para que M tampoco sea divisible por p. Por último, puesto que a_o es un entero positivo, $a_o M$ *no será divisible por p si elegimos a p con la condición adicional* $p > a_o$.

3. Ahora vamos a determinar a los números M_ν y ε_ν de las fórmulas **(7)**. El procedimiento que fue empleado en el caso de e requiere ahora una importante modificación porque para definir esos números vamos a emplear los números β_ν como uno de los límites de integración, que pueden ser complejos (de hecho: uno de ellos es $i\pi$). Por consiguiente las integrales mediante las cuales definiremos a M_ν y ε_ν deberán considerarse sobre el plano complejo, a cuyo fin podemos observar que los integrandos son funciones analíticas uniformes de la variable compleja z, regulares salvo en el punto $z = \infty$ en que hay una singularidad esencial. Debemos por tanto fijar convenientemente el camino de integración.

Para cada valor de ν la integral que expresa el valor de M en la fórmula **(10)** puede ser elegido, como se ve en la figura de la pag. 109, formado por un segmento de recta que parte de o y llega a β_ν, y por una semirrecta paralela al eje real, que parte de β_ν, y va a ∞. Como es sabido, el valor de la integral resulta ser el mismo para todos del número ν .



La integral a lo largo del segmento $o\beta_\nu$ definirá el valor de ε_ν que, como luego veremos podrá hacerse arbitrariamente pequeño si se elige al número primo p suficientemente grande; y la integral a lo largo de la semirrecta $\beta_\nu\infty$ proporcionará el valor de M_ν . Se tiene por tanto

$$\varepsilon_\nu = e^{\beta_\nu} \int_0^{\beta_\nu} \frac{e^{-z} z^{p-1} dz}{(p-1)!} [b_o + b_1 z + \ldots + b_N z^N]^p \cdot$$

$$\cdot \; b_N^{(N-1)p-1} , \qquad (13)$$

$$M = \varepsilon^{\beta_\nu} \int_{\beta_\nu}^{\infty} \frac{e^{-z} z^{p-1} dz}{(p-1)!} [b_o + b_1 z + \ldots + b_N z^N]^p \, .$$

$$. \, b_N^{(N-1)p-1} \, , \qquad \textbf{(14)}$$

valores que es fácil observar que satisfacen a las relaciones **(7)**.

4. Trataremos ahora acerca de los ε_ν . Como se sabe, el valor de la integral de una función de variable compleja es no mayor que el producto del máximo del valor absoluto del integrando sobre el camino de integración por la longitud de éste que en este caso es $|\beta_\nu|$.

El integrando puede escribirse en la forma

$$\frac{[z(b_o + b_1 z + \ldots + b_N z^N) b_N^{N-1}]^{p-1}}{(p-1)!} (e^{-z}(b_o + b_1 z + \ldots + b_N z^N) b_N^{N-2}) .$$

Si G denota al máximo de $|z(b_o+b_1z+\ldots+ b_N z^N) b_N^{N-1}|$ en una región del plano complejo que contiene a todos los segmentos que unen a o con los β_ν, resultará que $|\varepsilon_\nu|$ se-rá no mayor que el producto de $G^{p-1}/(p-1)!$ por factores que son independientes de p. Resultará así que si se aumenta convenientemente el valor de p, lo que es siempre posible, los números ε_ν y por tanto *la suma* $\varepsilon_1+\ldots+\varepsilon_\nu$ *puede hacerse tan pequeña como se quiera*; en particular, menor que la unidad.

5. Nos ocuparemos ahora de los números M_ν.

Si reemplazamos en el integrando de la ecuación **(14)** la expresión entre corchetes por su valor deducido de **(9)** y sustituímos luego la variable z por la variable $\zeta_\nu = z-\beta_\nu$, que deberá variar entre o e ∞, se obtiene

$$M_\nu = \int_0^\infty \frac{e^{-\zeta}d\zeta}{(p-1)!} (\zeta+\beta_\nu)^{p-1}(\zeta+\beta_\nu-\beta_1)^p\ldots\zeta^p\ldots$$

$$\ldots(\zeta+\beta_\nu-\beta_N)^p b_N^{Np-1} = \int_0^\infty \frac{e^{-\zeta}d\zeta}{(p-1)!} \zeta^p \quad \Phi_\nu(\zeta), \tag{15}$$

en donde

$$\Phi_\nu(\zeta) = b_N^{Np-1}(\zeta+\beta_\nu)^{p-1}(\zeta+\beta_\nu-\beta_1)^p\ldots$$

$$\ldots(\zeta+\beta_\nu-\beta_{\nu-1})^p(\zeta+\beta_\nu-\beta_{\nu+1})^p\ldots$$

$$\ldots(\zeta+\beta_\nu-\beta_N)^p. \qquad (16)$$

Se tiene entonces que

$$\sum_{\nu=1}^{N} M_\nu = \sum_{\nu=1}^{N} \int_0^\infty \frac{e^{-\zeta}d\zeta}{(p-1)!}\,\zeta^p\,\Phi(\zeta), \qquad (17)$$

en donde

$$\Phi(\zeta) = \sum_{\nu=1}^{N} b_N^{Np-1}(\zeta+\beta_\nu)^{p-1}(\zeta+\beta_\nu-\beta_1)^p\ldots$$

$$\ldots(\zeta+\beta_\nu-\beta_{\nu-1})^p(\zeta+\beta_\nu-\beta_{\nu+1})^p\ldots$$

$$\ldots(\zeta+\beta_\nu-\beta_N)^p$$

es un polinomio en ζ, en cada uno de cuyos sumandos una de las N cantidades $\beta_1,\beta_2,\ldots,\beta_N$ juega un papel particular; pero en el conjunto de ellos ninguna de esas cantidades tiene un rol diferente del de las demás. Por esa razón, si se desarrollan las potencias y se llevan a cabo los productos de la expresión de $\Phi(\zeta)$, cada uno de los coeficientes de las potencias de ζ es una función racional entera y simétrica de β_1, $\ldots,\beta_N$ con coeficientes enteros. Ahora bien, los números $\beta_1,\ldots,\beta_N$ son todas raíces de la ecuación **(6)** cuyos coeficientes son enteros, pero que no es mónica. Por tanto el teorema **2** de la sección **5.1** nos permite establecer que los mencionados coeficientes de las potencias de ζ del polinomio $\Phi(\zeta)$ son racionales. Pero nosotros deseamos probar que esos coeficientes son *enteros*. Esto podemos lograrlo valiéndonos del factor entero b_N^{Np-1} que aparece en todos los términos de $\Phi(\zeta)$. Puede escribirse en efecto

$$\Phi(\zeta) = \sum_{\nu=1}^{N} (b_N\zeta+b_N\beta_\nu)^{p-1}(b_N\zeta+b_N\beta_\nu-b_N\beta_1)^p \ldots$$

$$\ldots(b_N\zeta+b_n\beta_\nu-b_N\beta_{\nu-1})^p(b_N\zeta-b_N\beta_\nu-b_N\beta_{\nu+1})^p$$

$$\ldots(b_N\zeta+b_N\beta_\nu-b_N\beta_N)^p.$$

Cuando se lleva a cabo el cálculo de los coeficientes de las potencias de ζ mediante la fórmula de la potencia de un polinomio se obtienen funciones enteras racionales simétricas de los productos $b_N\beta_1, b_N\beta_2, \ldots, b_N\beta_N$, con coeficientes enteros. Ahora bien, estos últimos N productos son todas las raíces de la ecuación que resulta de la ecuación **(4)** cuando se reemplaza la incógnita z por la incógnita w tal que $w = b_N$, o sea la ecuación

$$b_o + b_1\left(\frac{w}{b_N}\right) + \ldots + b_{N-1}\left(\frac{w}{b_N}\right)^{N-1} + b_N\left(\frac{w}{b_N}\right)^N = 0,$$

y también, por tanto, de la que resulta de ésta al multiplicarla por b_N^{N-1}, o sea

$$b_o b_N^{N-1} + b_1 b_N^{N-2} w + \ldots + b_{N-2} b_N w^{N-2} +$$

$$+ b_{N-1} w^{N-1} + w^N = 0, \qquad \textbf{(18)}$$

que es una ecuación mónica con coeficientes enteros. Resulta así, según el teorema **2** de la sección **5.1**, que los coeficientes del polinomio $\Phi(\zeta)$ son números enteros que denotaremos por $A_o, A_1, \ldots, A_{Np-1}$. Se tiene por consiguiente

$$\sum_{\nu=1}^{N} M_\nu = \int_0^\infty \frac{e^{-\zeta}\zeta^p d\zeta}{(p-1)!} (A_o + A_1\zeta + A_2\zeta^2 + \\ \dots + A_{Np-1}\zeta^{Np-1}),$$

y en virtud de **(12)** resulta

$$\sum_{\nu=1}^{N} M_\nu = \frac{1}{(p-1)!} (A_o p! + A_1 (p+1)! + \dots \\ + A_{Np-1}(Np)!), \qquad \textbf{(19)}$$

que prueba que $\sum_{\nu-1}^{N} M_\nu$ es un número entero divisible por p.[1]

---

(1) Cabe aquí observar que, tal como indicamos en una nota de pie de página precedente, los números M_ν son enteros algebraicos. En efecto, puesto que $b_N\beta_1, \dots, b_N\beta_N$ son todas las raíces de la ecuación mónica (18) con coeficientes enteros, dichos números son, por definición, enteros algebraicos. De (15) puede deducirse entonces, mediante la fórmula (12), que M_ν es una expresión racional entera de números algebraicos. De lo dicho al final de la sección 5.1 resulta que M_ν es un número entero algebraico.

En la parte 2 de la demostración hemos probado que $a_o M$ es un entero que no es divisible por p .

Por consiguiente la suma

$$a_o M + \sum_{\nu=1}^{N} M_\nu$$

es necesariamente un número racional entero que no es divisible por p , y por tanto es diferente de cero. Resulta así que la ecuación

$$[a_o M + \sum_{\nu=1}^{N} M_\nu] + [\sum_{\nu=1}^{N} \varepsilon_\nu] = 0 ,$$

que es la ecuación **(8)** no puede cumplirse, pues no es posible que la suma de un entero diferente de cero y de un número que es menor que la unidad pueda ser igual a cero. Esto prueba, según fue explicado al comenzar la demostración, que si se supone que π es un número algebraico, la ecuación **(2)**, que es cierta sin duda, no podría cumplirse. Luego π es un número trascendente, y como consecuencia resulta la imposibilidad de resolver el problema clásico de la cuadratura del círculo.

§ 6. ANEXO

Los Números Algebraicos

Para las definiciones de los números algebraicos y de los números enteros algebraicos remitimos al lector a la sección **5.1** .

Sea $\mathbb{Q}$ el campo de los números racionales y $\mathbb{Q}[x]$ el anillo de los polinomios en x, con coeficientes racionales.

Un polinomio $f(x) \in \mathbb{Q}[x]$ se llama *irreducible* si no es posible expresarlo como un producto de dos polinomios ninguno de los cuales sea de grado 0, es decir elementos pertenecientes a $\mathbb{Q}$.

Teorema 3.

La suma, la diferencia, el producto y el cociente (en este último caso con divisor diferente de cero) de dos números algebraicos, son números algebraicos.

Demostración.

Sean α y β dos números algebraicos. Por definición serán raíces de las repectivas ecuaciones mónicas

$$x^m + a_1 x^{m-1} + \ldots + a_m = 0 \qquad (1)$$

$$x^n + b_1 x^{n-1} + \ldots + b_n = 0 \qquad (2)$$

cuyos coeficientes son números racionales.

Sean $\alpha_o = \alpha, \alpha_1, \ldots, \alpha_{m-1}$ las raíces de **(1)** y $\beta_o = \beta, \beta_1, \ldots, \beta_{n-1}$ las raíces de **(2)**.

Consideremos la ecuación mónica

$$\prod_{i,j} (x-(\alpha_i + \beta_j)) = x^{mn} + c_1 x^{mn-1} + \ldots + c_{mn} = 0, \qquad (3)$$

donde el producto del primer miembro se extiende a todos los pares (i,j) tales que $i = 0, 1, \ldots, m-1$, $j = 0, 1, \ldots, n-1$.

Los coeficientes $c_1, c_2, \ldots, c_{mn}$ son funciones enteras simétricas de las raíces de las ecuaciones (1) y (2); son por tanto funciones racionales enteras de los coeficientes de dichas ecuaciones, es decir que son números racionales. Puesto que $\alpha + \beta = \alpha_o + \beta_o$ es una raíz de (3), será un número algebraico. De manera semejante se prueba que $\alpha-\beta$ y $\alpha\beta$ son números algebraicos. Para probar que α/β, con $\beta \neq 0$, es algebraico, puede observarse que $1/\beta$ es algebraico porque es raíz de la ecuación de coeficientes racionales

$$b_n y^n + b_{n-1} y^{n-1} + \ldots + b_1 y + 1 = 0$$

Resulta entonces que el producto $\alpha . \frac{1}{\beta} = \frac{\alpha}{\beta}$ es algebraico.■

Corolario 1.

Toda función racional de números algebraicos con coeficientes racionales, en que ningún divisor es nulo, es un número algebraico.

Demostración.

Resulta del Teorema porque todo número racional es algebraico.■

Corolario 2.

La suma, la diferencia y el producto de dos números enteros algebraicos son enteros algebraicos.

Demostración.

En este caso, los coeficientes c de la ecuación **(3)**, en el caso de la suma $\alpha + \beta$ de dos enteros algebraicos, son funciones racionales enteras de los coeficientes a y b; y puesto que estos son ahora enteros por hipótesis, los c serán también enteros. Luego $\alpha+\beta$ será un número entero algebraico. Semejantemente para $\alpha-\beta$ y $\alpha\beta$.■

La siguiente proposición no es utilizada en los parágrafos precedentes. Se incluye aquí unicamente a título de información complementaria de interés en la teoría de los números algebraicos.

Teorema 4.

Si ω es una raíz de la ecuación

$$F(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n = 0,$$

donde los coeficientes son números algebraicos, es también raíz de una ecuación con coeficientes racionales y por tanto es un número algebraico.

Demostración.

Cada uno de los números $\alpha_i (i=1,...,n)$, por cuanto es algebraico, será raíz de una ecuación mónica $\varphi_i(x) = 0$ de grado m_i con coeficientes racionales, cuyas raíces vamos a designar por

$$\alpha_i^0 = \alpha_i, \; \alpha_i', \; \alpha_i'', ..., \; \alpha_i^{(m_i-1)}.$$

Sea $m = m_1 m_2 ... m_n$, y definamos los m polinomios

$$F_j(x) = x^n + \alpha_1^{j_1} x^{n-1} + \alpha_2^{j_2} x^{n-2} + ... + \alpha_{n-1}^{j_{n-1}} x + \alpha_n^{j_n}$$

donde $j= \{j_1,...,j_n\}$, $j_k \in \{0,1,2,...,m_k-1\}$ para $k = 1,2,...,n$; de manera que

$$F_{(0,...,0)} = F(x).$$

Consideremos el polinomio

$$f(x) = \prod_j F_j(x)$$

donde el producto se extiende a todos los conjuntos j. El número ω es raíz de la ecuación

$$f(x) = 0.$$

Ahora bien, los coeficientes de $f(x)$ son evidentemente funciones racionales enteras simétricas de todas las raíces de la ecuación mónica $\varphi_1(x)\varphi_2(x)\ldots\varphi_n(x) = 0$ de coeficientes racionales; por consiguiente, según el teorema **2**, son funciones racionales de estos últimos coeficientes, y por consiguiente ellos mismos son números racionales. Puesto que ω es raíz de la ecuación $f(x) = 0$, será un número algebraico.■

Ejemplo.

Sea ω una raíz de la ecuación

$$F(x) = x^2 + \sqrt{2}\,x + \sqrt{3} = 0.$$

Tenemos ahora: $\alpha_1 = \sqrt{2}$ y $\alpha_2 = \sqrt{3}$, de modo que $\varphi_1(x) = x^2-2$ y $\varphi_2(x) = x^2-3$. Por tanto

$$\alpha_1^0 = \sqrt{2},\ \alpha_1' = -\sqrt{2},\ \alpha_2^0 = \sqrt{3},\ \alpha_2' = -\sqrt{3},$$

y

$$F_{(o,o)} = x^2 + \sqrt{2}x + \sqrt{3}$$
$$F_{(1,o)} = x^2 - \sqrt{2}x + \sqrt{3}$$
$$F_{(o,1)} = x^2 + \sqrt{2}x - \sqrt{3}$$
$$F_{(1,1)} = x^2 - \sqrt{2}x - \sqrt{3}.$$

Se tiene entonces

$$f(x) = F_{(o,o)} . F_{(1,o)} . F_{(o,1)} F_{(1,1)} =$$
$$x^8 - 4x^6 - 2x^4 - 12x^2 + 9 = 0.$$

Puesto que ω es una raíz de esta última ecuación, es un número algebraico. Puede observarse que es un entero algebraico; lo cual es consecuencia de que los coeficientes del polinomio $F(x)$ son enteros algebraicos, según resulta del siguiente corolario.

Corolario.

Si ω es raíz de la ecuación

$$F(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n = 0,$$

donde $\alpha_1, \alpha_2, \ldots, \alpha_n$ son enteros algebraicos, entonces él mismo es un entero algebraico.

Demostración.

Usando las notaciones de la demostración del teorema anterior, los coeficientes de $f(x)$ son funciones racionales enteras de los coeficientes de las ecuaciones $\varphi_i(x) = 0$, los cuales son ahora enteros racionales. Luego los coeficientes de $f(x)$ son racionales enteros y ω es un entero algebraico.■

Bibliografía.

[1] *Courant and Robbins*, What is Mathematics? Oxford University Press, (1941).

[2] *Hermite*, Comptes Rendus, vol.77(1873); págs. 18-24, 74-79, 226-233, 285-293.

[3] *Hilbert*,Mathematische Annålen,43(1893)

[4] *Lindemann*, Sitzungsberichte der Berliner Akademie. (1882), pág.679. Mathematische Annalen, 20 (1882), pág. 213.

[5] *Niven*, Bull. of the Am. Math. Soc., 53 (1947).

[6] *Reid L.W.* The Elements of the Theory of Algebraic Numbers, The Mac Millan Co. (1910).

[7] *Van der Waerden,* Moderne Algebra I, (1937).

[8] *Weber,* Lehrbuch der Algebra I, Braunschweig, Vierweg und Sohn, (1912)