ISSN 0027-1322, Moscow University Mathematics Bulletin, 2021, Vol. 76, No. 6, pp. 239–243. © Allerton Press, Inc., 2021.
Russian Text © The Author(s), 2021, published in Vestnik Moskovskogo Universiteta, Seriya 1: Matematika, Mekhanika, 2021, No. 6, pp. 3–7.

Lindemann—Weierstrass Theorem

Yu. V. Nesterenko*

Chair of Number Theory, Faculty of Mechanics and Mathematics, Lomonosov Moscow State University, Moscow, Russia

Received September 11, 2020

Abstract—We discuss issues of algebraic independence for values of the function e^z at algebraic points. The most general result of this kind was established at the end of the 19th century and is called the Lindemann—Weierstrass theorem. This is historically the first theorem on the algebraic independence of numbers and it can be proved now in various ways. Below we propose one more way to prove it.

DOI: 10.3103/S0027132221060073

Keywords: *algebraic independence, criterion of linear independence, saddle point method, exponential function*

In 1873 Ch. Hermite [1, vol. 3, pp. 150—181] proved that the number e is transcendental, that is, he proved that e cannot be a root of some polynomial with integer coefficients. In 1882 F. Lindemann [2] introduced multiple new ideas in the considerations of Hermite and proved that the number π is transcendental, thus solving the prominent problem of squaring the circle. In fact, Lindemann established a substantially more general assertion: for any algebraic number $a \neq 0$ the value of e^a is transcendental. This assertion also implies that the natural logarithms of algebraic numbers different from 0 and 1 are transcendental and, in particular, that $\pi = i^{-1}\ln(-1)$ is transcendental, as well as that the values of the trigonometric functions are transcendental.

Lindemann formulated an even more general theorem without proving it (see Theorem 2 below), noting that it can be proved using the same ideas.

Theorem 1 (Lindemann—Weierstrass theorem). *If algebraic numbers $\theta_1, \ldots, \theta_r$ are linearly independent over the field $\mathbb{Q}$, then the values of the exponential function $e^{\theta_1}, \ldots, e^{\theta_r}$ are algebraically independent over $\mathbb{Q}$.*

An equivalent formulation is given by

Theorem 2 (Lindemann—Weierstrass theorem). *If $\alpha_0, \alpha_1, \ldots, \alpha_m, m \geq 1$ are different algebraic numbers, then*

$$e^{\alpha_0}, e^{\alpha_1}, \ldots, e^{\alpha_m} \tag{1}$$

are linearly independent over the field of all algebraic numbers.

The proof of the second theorem was published by K. Weierstrass in 1885 [3]. Today, this theorem is referred to as the Lindemann—Weierstrass theorem.

1. SUFFICIENT CONDITION OF LINEAR INDEPENDENCE OF NUMBERS

Suppose that $\mathbf{K}$ is a finite extension of the field of rational numbers of order ν. For the lower bound of the number of numbers linearly independent over the field $\mathbf{K}$ in a given set, we can use the following proposition.

*E-mail: nester@mi-ras.ru

Proposition 1. *Suppose that τ is a positive number and $\sigma(t)$ is a function determined for all positive values of t, monotonously increasing beginning from some point, and unbounded such that*

$$\lim_{t\to\infty}\frac{\sigma(t+1)}{\sigma(t)}=1.$$

Suppose that $\overline{\omega}=(\omega_1,\ldots,\omega_m)\in\mathbb{C}^m\setminus\{0\}$ and $L_N(\overline{x})$ is a sequence of linear forms with integer coefficients from the field $\mathbf{K}$ satisfying the conditions

$$\ln\overline{|L_N|}\le\sigma(N),\ N\ge N_0,\qquad \lim_{N\to\infty}\frac{\ln|L_N(\overline{\omega})|}{\sigma(N)}=-\tau.$$

Then, among the numbers $\omega_1,\ldots,\omega_m$ there are at least $\dfrac{\tau}{\nu}$ numbers linearly independent over $\mathbf{K}$.

This statement is a weakened variant of the corollary proved in work [4]. The statement in the case $\mathbf{K}=\mathbb{Q}$ was proved in work [5]. In particular, it was used by T. Rivoal (see [6]) for proving the infinite dimension of the linear space over $\mathbb{Q}$ generated by the values of the Riemann zeta function $\zeta(3),\zeta(5),\zeta(7),\ldots$. In this work we use his variant for proving the Lindemann–Weierstrass theorem, which allows in our proof avoiding the structure of the complete system of linearly independent linear forms of the numbers at consideration (see papers by Siegel [7] and Mahler [8, 9]).

2. ANALYTICAL STRUCTURE

The material exposed in this section is based on the works by Mahler (see, e.g., [8, 9]), which in his turn used the Hermite integral identity providing the Hermite–Padé approximation of second kind.

Suppose that m different complex numbers $\alpha_1,\ldots,\alpha_m$ and an integer nonnegative number n are given. We set

$$N=m(n+1)-1,\qquad Q(x)=\prod_{k=1}^{m}(x-\alpha_k)^{n+1}.$$

Then, as was first proved by Hermite in 1893 [1, vol. 4, pp. 357–377], the following identity is valid:

$$R(z)=\frac{1}{2\pi i}\int_C\frac{e^{z\zeta}d\zeta}{(\zeta-\alpha_1)^{n+1}\ldots(\zeta-\alpha_m)^{n+1}}=\sum_{k=1}^{m}P_k(z)e^{\alpha_k z},\tag{2}$$

where C is a circle containing all points $\alpha_1,\ldots,\alpha_m$. For each $k, 0\le k\le m$, the coefficient $P_k(z)$ is a polynomial of z of order n:

$$P_k(z)=\sum_{j=0}^{n}a_{kj}\frac{z^{n-j}}{(n-j)!},\qquad a_{kj}=\sum_{\mathbf{l}}\prod_{\substack{i=1\\ i\ne k}}^{m}\frac{(-1)^{l_i}(n+l_i)!}{n!l_i!}(\alpha_k-\alpha_i)^{-1-n-l_i},\tag{3}$$

where the summation is carried out over all sets of integer nonnegative numbers $l_1,\ldots,l_{k-1},l_{k+1},\ldots,l_m$, the sum of which is equal to j.

Proposition 2. *Suppose that $\alpha_1,\ldots,\alpha_m$ are arbitrary algebraic numbers.*

(1) If *q is the smallest natural number such that $q(\alpha_i-\alpha_j)^{-1}\in\mathbb{Z}_{\mathbf{K}},\ 1\le i<j\le m$, then*

$$n!q^NP_k(1)\in\mathbb{Z}_{\mathbf{K}},\qquad\overline{|P_k(1)|}\le(2M+1)^N,\tag{4}$$

where $M=\max\limits_{1\le i<j\le m}\overline{|\alpha_i-\alpha_j|}^{\,-1}$.

(2) *As $n\longrightarrow\infty$, the following asymptotic formula is valid*:

$$R_n(1)=(2\pi)^{-1/2}e^{m^{-1}(\alpha_1+\ldots+\alpha_m)}N^{-N-1/2}e^N(1+o(1)),$$

where $N=m(n+1)-1$.

We assign $\overline{\omega}=(e^{\alpha_1},\ldots,e^{\alpha_m})$ and $L_n(\overline{\omega})=n!q^NR(1)$.

Corollary 1. *The value $L_n(\overline{\omega})$ defined above is a linear form of coordinates ω_j of the vector $\overline{\omega}$. The coefficients L_n belong to $\mathbb{Z}_{\mathbf{K}}$, and*

$$\ln \overline{|L_n|} \le \sigma(n) = n \ln n + cn, \qquad \lim_{n \longrightarrow \infty} \frac{\ln |L_n(\overline{\omega})|}{\sigma(n)} = 1 - m,$$

where the constant c depends only on the numbers $\alpha_1, \ldots, \alpha_m$.

Proof of Proposition 2. The right-hand side of identity (2) is a sum of residues of the function under the integral sign in the left-hand side of (2) at the points $\alpha_1, \ldots, \alpha_m$.

Embedding (4) immediately follows from the representation (3) if we take into account

$$\sum_{\substack{i=1 \\ i \ne k}}^{m} (n + 1 + l_i) = N - n + j \le N.$$

To prove inequality (4), we estimate the coefficients of the polynomial $P_k(z)$. Identity (2) implies the representation

$$a_{kj} = \frac{1}{2\pi i} \int_{C_k} \frac{(\zeta - \alpha_k)^{n+1} d\zeta}{Q(\zeta)(\zeta - \alpha_k)^{j+1}},$$

where C_k is the circle $|\zeta - \alpha_k| = \dfrac{1}{2M}$. Considering that the following inequality is true on the circle C_k for $i \ne k$:

$$|\zeta - \alpha_i| \ge |\alpha_k - \alpha_i| - |\zeta - \alpha_k| \ge \frac{1}{M} - \frac{1}{2M} = \frac{1}{2M},$$

we obtain the estimate

$$|a_{kj}| \le (2M)^{N-n+j}.$$

The same estimate is valid for the conjugates of the number a_{kj}, because from (2) it follows that for them there exists the same integral representation as for a_{kj} but with a replacement of the integrand function $\dfrac{(\zeta - \alpha_k)^{n+1}}{Q(\zeta)(\zeta - \alpha_k)^{j+1}}$ by the conjugate one. Now, from (3) we find

$$\overline{|P_k(1)|} \le \sum_{j=0}^{n} \overline{|a_{kj}|} \frac{1}{(n-j)!} \le \sum_{j=0}^{n} \frac{(2M)^{N-n+j}}{(n-j)!} \le (2M)^N \big(1 + \frac{1}{2M}\big)^N,$$

which proves inequality (4).

The proof of the second part of Proposition 2 uses the saddle point method, and we are grateful to A.Yu. Popov suggesting the variant of considerations given here.

For a sufficiently large n we set the radius of circle C to be $N = m(n+1) - 1$. Then, for $z = Ne^{i\varphi}$ we have $dz = Nie^{i\varphi} d\varphi$ such that

$$I_n = \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{Ne^{i\varphi}} (Ne^{i\varphi})^{-N} a_n(\varphi) d\varphi,$$

where $a_n(\varphi) = \prod_{j=1}^{m} \left(1 - \alpha_j N^{-1} e^{-i\varphi}\right)^{-n-1}$. For a sufficiently large n we obtain

$$a_n(\varphi) = \exp\left(e^{-i\varphi} \sum_{j=1}^{m} \frac{\alpha_j}{m} + O(n^{-1}) \right), \tag{5}$$

where the constant in $O(.)$ depends only on α_j, m and is independent of φ.

The representation $I_n = N^{-N} e^N F_n$ is valid, where

$$F_n = \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{N(e^{i\varphi} - 1 - i\varphi)} a_n(\varphi) d\varphi.$$

Denote $\lambda_n = \dfrac{\ln n}{\sqrt{n}}$ and

$$G_n = \frac{1}{2\pi}\int_{-\lambda_n}^{\lambda_n} e^{N(e^{i\varphi}-1-i\varphi)}a_n(\varphi)d\varphi.$$

Then, due to the inequality,

$$\Re(e^{i\varphi}-1-i\varphi) = \cos\varphi - 1 \le \begin{cases} -\frac{\varphi^2}{\pi}, & \text{if } |\varphi| \le \frac{\pi}{2}; \\ -1, & \text{if } \frac{\pi}{2} \le |\varphi| \le \pi, \end{cases}$$

for $\dfrac{\pi}{2} \ge |\varphi| \ge \lambda_n$ we have

$$\Re\left(e^{i\varphi}-1-i\varphi\right) \le -\frac{\ln^2 n}{\pi n},$$

so that, using (5) and the latter inequality, we obtain

$$|F_n - G_n| \le \exp\left(-\frac{m}{3}\ln^2 n\right).$$

For $|\varphi| \le \lambda_n$ we have

$$N\left(e^{i\varphi}-1-i\varphi\right) = N\left(-\frac{\varphi^2}{2} + O(\varphi^3)\right) = -\frac{N\varphi^2}{2} + O(n^{-\frac{1}{2}}\ln^3 n),$$

and, therefore,

$$e^{N\left(e^{i\varphi}-1-i\varphi\right)} = e^{-\frac{N\varphi^2}{2}}\left(1 + O(n^{-\frac{1}{2}}\ln^3 n)\right).$$

In addition to that, from (5) we find

$$a_n(\varphi) = \exp\left(\sum_{j=1}^{m}\frac{\alpha_j}{m}\right) + O(n^{-\frac{1}{2}}\ln n);$$

hence,

$$\begin{aligned} G_n &= \frac{1}{2\pi}\int_{-\lambda_n}^{\lambda_n} e^{-\frac{N\varphi^2}{2}}a_n(\varphi)d\varphi\left(1 + O(n^{-\frac{1}{2}}\ln^3 n)\right) \\ &= \frac{1}{2\pi}\exp\left(\sum_{j=1}^{m}\frac{\alpha_j}{m}\right)\int_{-\lambda_n}^{\lambda_n} e^{-\frac{N\varphi^2}{2}}d\varphi\left(1 + O(n^{-\frac{1}{2}}\ln^3 n)\right) \\ &= \frac{1}{2\pi}\exp\left(\sum_{j=1}^{m}\frac{\alpha_j}{m}\right)N^{-\frac{1}{2}}\int_{-\lambda_n N^{\frac{1}{2}}}^{\lambda_n N^{\frac{1}{2}}} e^{-\frac{t^2}{2}}dt\left(1 + O(n^{-\frac{1}{2}}\ln^3 n)\right) \\ &= \frac{1}{2\pi}\exp\left(\sum_{j=1}^{m}\frac{\alpha_j}{m}\right)N^{-\frac{1}{2}}\int_{-\infty}^{\infty} e^{-\frac{t^2}{2}}dt(1 + o(1)). \end{aligned}$$

Thus, $G_n = (2\pi N)^{-\frac{1}{2}}\exp\left(\sum_{j=1}^{m}\dfrac{\alpha_j}{m}\right)(1 + o(1))$, which leads to the desired statement.

3. PROOF OF THE LINDEMANN–WEISERSTRASS THEOREM

Apparently, Siegel was first (see [7]) who used the considerations related with the Veronese mapping in the theory of transcendental numbers to reduce the problems on algebraic independence of numbers to the problems of linear independence (see the formulations of Theorems 1 and 2). We now use his idea.

In the denotations of Theorem 1, we suppose that numbers (1) are algebraically dependent over the field of all algebraic numbers. Then, there exists a polynomial A of r of the variables $T_1, \ldots, T_r$, $A \neq 0$, with integer algebraic coefficients such that $A(e^{\theta_1}, \ldots, e^{\theta_r}) = 0$. By symbol $\mathbf{K}$ we denote the field generated over $\mathbb{Q}$ by algebraic numbers $\theta_1, \ldots, \theta_r$ and coefficients of the polynomial A. Suppose also that $\nu = [\mathbf{K} : \mathbb{Q}]$ and d is the power of the polynomial A by totality of all its variables. We choose and fix a sufficiently large natural number $h > d$ such that the inequality is valid:

$$(h+1)(h+2)\cdot \ldots \cdot (h+r) > \left(1 - \frac{1}{\nu}\right)(h+d+1)(h+d+2)\cdot \ldots \cdot (h+d+r). \tag{6}$$

This can be done, because the polynomials of h appearing in the left- and right-hand sides of this inequality have the same powers and positive leading coefficients, and the leading coefficient of the left polynomial is larger than the leading coefficient of the right polynomial.

Suppose that $\omega_1, \ldots, \omega_m$ are the numbers of type $u_1\theta_1 + \ldots + u_r\theta_r$ ordered in a certain way, where $(u_1, \ldots, u_r)$ are all sets of integer nonnegative numbers with the condition $u_1 + \ldots + u_r \leq h + d$. Because $\theta_1, \ldots, \theta_r$ are linearly independent over the field $\mathbb{Q}$, all numbers $\omega_1, \ldots, \omega_m$ are different and $m = \binom{h+d+r}{r}$.

Consider the polynomials

$$B_{\overline{v}}(T_1, \ldots, T_r) = T_1^{v_1} \ldots T_r^{v_r} A(T_1, \ldots, T_r)$$

of variables $T_1, \ldots, T_r$, where $\overline{v} = (v_1, \ldots, v_r)$ ranges over all vectors with integer nonnegative coordinates satisfying the inequality $v_1 + \ldots + v_r \leq h$. These polynomials have the degree at most $h + d$ by totality of variables $T_1, \ldots, T_r$ and different leading monomials. Therefore, considered to be the linear forms of the products of powers $T_1^{u_1} \ldots T_r^{u_r}$ with conditions $u_1 + \ldots + u_r \leq h + d$, they are linearly independent over $\mathbf{K}$. The number of such polynomials is $s = \binom{h+r}{r}$, and each of them yields the linear relation $B_{\overline{v}}(e^{\theta_1}, \ldots, e^{\theta_r}) = 0$ between the numbers $\omega_1, \ldots, \omega_m$ over the field $\mathbf{K}$. Hence, among the numbers $\omega_1, \ldots, \omega_m$ there are at most $m - s$ linearly independent numbers over $\mathbf{K}$. Comparing this estimate with Corollary 1 and Proposition 1, we obtain the inequatlity $m - s \geq \dfrac{m}{\nu}$, which contradicts (6). This contradiction completes the proof of the Lindemann–Weierstrass theorem.

CONFLICT OF INTEREST

The author declares that he has no conflicts of interest.

REFERENCES

1. Ch. Hermite, *Oeuvres de Charles Hermite* (Gauthier–Villars, Paris, 1912).
2. F. Lindemann, "Ueber die Zahl π," Math. Ann. **20**, 213–225 (1882). https://doi.org/10.1007/BF01446522
3. K. Weierstrass, "Zu Lindemann's Abhandlung: 'Über die Ludolph'sche Zahl,"' (Sitzungsber. Preuss. Akad. Wiss., 1885), pp. 1067–1085.
4. E. V. Bedulev, "On the linear independence of numbers over number fields," Math. Notes **64**, 440–449 (1998). https://doi.org/10.1007/BF02314624
5. Yu. V. Nesterenko, "On linear independence of numbers," Vestn. Mosk. Univ., Ser. 1: Mat., Mekh., No. 1, 46–49 (1985).
6. T. Rivoal, "La fonction zeta de Riemann prend une infinite de valeurs irrationnelles aux entiers impairs," C. R. Acad. Sci. A **331**, 267–270 (2000). https://doi.org/10.1016/S0764-4442(00)01624-4
7. C. L. Siegel, "Uber einige Anwendungen diophantischer Approximationen," Abh. Preuss. Akad. Wiss. Phys.-math. Kl., 1929, No. 1.
8. K. Mahler, "Zur Approximation der Exponentialfunktion und des Logarithmus. Teil I," J. Reine Angew. Math. **166**, 118–136 (1931). https://doi.org/10.1515/crll.1932.166.118
9. "Zur Approximation der Exponentialfunktion und des Logarithmus. Teil II," J. Reine Angew. Math. **166**, 137–150 (1931). https://doi.org/10.1515/crll.1932.166.137

Translated by E. Oborin