Introduction to transcendental numbers

Caroline Braun

October 2021

1 Lindemann-Weierstrauss theorem

Theorem (Lindemann-Weierstrauss): Let $\alpha_1, ..., \alpha_n$ be distinct algebraic numbers. Then

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

for algebraic $\beta_1, ..., \beta_n$ if and only if $\beta_j = 0$ for every $1 \leq j \leq n$, in other words $e^{\alpha_1}, ..., e^{\alpha_n}$ are linearly independent over $\overline{\mathbb{Q}}$.

Proof: We are going to do a proof by contradiction. So let's assume, there exist $\beta_1, ..., \beta_n$ algebraic not equal 0, such that

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

To make the proof easier, we are going to do two simplifications. But first, we need to introduce some definitions:

Definition 1: Given a separable extension K' of K, a **Galois closure** E is the smallest Galois extension such that $E \supset K' \supset K$.

Remark: $E \mid \mathbb{Q}$ is a Galois extension if an only if $\mathbb{Q}$ is the fixed field of $Gal(E \mid \mathbb{Q})$

Definition 2: Let α be an algebraic element over a field K. The **conjugate elements** of α are the roots of the minimal polynomial over of α.

Now, we are ready to have a look at the two simplifications:

Claim 1: We can choose all the β_j to be (rational) integers.

Proof: The goal is to construct a new expression with coefficients in $\mathbb{Z}$, such that the new coefficients all equal 0 if an only if the initial coefficients are all 0. We define F=$\mathbb{Q}(\beta_1, ..., \beta_n)$ and let E be the Galois closure of F. Set $G := Gal(E \mid \mathbb{Q})$.
Consider

$$\prod_{\sigma \in G} (\sigma(\beta_1)e^{\alpha_1} + ... + \sigma(\beta_n)e^{\alpha_n})$$

This expression still equals 0, since it contains the initial equation. By expanding the expression, each coefficient is symmetric in a set of Galois conjugates and therefore fixed by G. Given that E is a Galois extension, the fixed field are exactly the rational numbers and thus the coefficients are rational. Finally, we can multiply the expression by a common multiple of all the denominators. By looking at terms of the form $e^{\alpha_i}e^{\alpha_i}...e^{\alpha_i}$ for $1 \leq i \leq n$, we note that the coefficient in front only involves β_i and images of β_i under σs. Since every σ sends 0 to itself, we can conclude that our initial β has to be 0. $\square$

Claim 2: We may assume that $\alpha_1, ..., \alpha_n$ form a complete set of Galois conjugates, even more that our expression is of the form

$$\beta_1 e^{\alpha_{1,1}} + \beta_1 e^{\alpha_{1,2}} + ... + \beta_1 e^{\alpha_{1,m_1}} + \beta_2 e^{\alpha_{2,1}} + ... + \beta_2 e^{\alpha_{2,m_2}} + ... + \beta_n e^{\alpha_{n,1}} + ... + \beta_n e^{\alpha_{n,m_n}}$$

where $\alpha_{i,1}...\alpha_{i,m_i}$ form a complete set of Galois conjugates for $1 \leq i \leq n$.

Proof: Since all the α's are algebraic, there exists a polynomial having $\alpha_1, ...\alpha_n$ as roots. Denote by $\alpha_{n+1}, ..., \alpha_N$ the remaining roots of the polynomial and we define $\beta_{n+1} = ... = \beta_N = 0$. Then, we consider the product

$$\prod_{\sigma \in S_N} (\beta_1 e^{\alpha_{\sigma(1)}} + ... + \beta_N e^{\alpha_{\sigma(N)}})$$

By expanding the product, we get a sum of terms of the form

$$e^{h_1\alpha_1 + ... + h_N\alpha_N}$$

where $h_1 + ... + h_N = N!$. The set of all such exponents form a complete set of Galois conjugates, since we made sure of this by putting all possible combinations of all possible conjugates. We note that

$$\prod_{\sigma \in S_N} (\beta_1 e^{\alpha_{\sigma(1)}} + ... + \beta_N e^{\alpha_{\sigma(N)}}) = \prod_{\sigma \in S_N} (\beta_1 e^{\alpha_{\theta(\sigma(1))}} + ... + \beta_N e^{\alpha_{\theta(\sigma(N))}})$$

for $\theta \in S_N$. Therefore, the terms $e^{h_1\alpha_1 + ... + h_N\alpha_N}$ and $e^{h_1\sigma(\alpha_1) + ... + h_N\sigma(\alpha_N)}$ for $\sigma \in S_N$ have the same coefficient in front and hence we can conclude that the expression is of the desired form.The only way that all the coefficients of this expanded form are zero is if the original coefficients were all zero. To see this, we can consider from each factor the non-zero term with the largest exponent in the lexicographical order on $\mathbb{C}$. Since all the $\alpha_i's$ are distinct, there is only one term with this largest exponent and it has a non-zero coefficient by construction which is a string of $\beta_i's$. Furthermore, each β_i occurs in this product since our product was over all elements of S_N. To make this more understandable, we are doing an example:
We define $\alpha_1 = \sqrt{2}$ and $\alpha_2 = \sqrt{3}$. In this example, it will be the term $e^{k\sqrt{2}+l\sqrt{3}}$ for some k and l with coefficient $\beta_1^a\beta_2^b$ for some $a, b > 0$. For example the term $\beta_1 e^{\sqrt{2}} + \beta_2 e^{\sqrt{3}}$ will contribute $\beta_2 e^{\sqrt{3}}$ or $\beta_1 e^{\sqrt{2}} + \beta_2 e^{-\sqrt{2}}$ will contribute $\beta_1 e^{\sqrt{2}}$

to get the term $\beta_1^a \beta_2^b e^{k\sqrt{2}+l\sqrt{3}}$. $\square$

In this proof, we want to work with algebraic integers, but the $\alpha_1, ..., \alpha_n$ are a priori any algebraic number.

Definition 3: α is an **algebraic integer** if its minimal monic polynomial over $\mathbb{Q}$ is in $\mathbb{Z}$[x].

Remark 1: The set of algebraic integers is closed under addition and multiplication.

Remark 2: The only algebraic integers in $\mathbb{Q}$ are the integers.

Remark 3: If α is an algebraic number and l is the leading coefficient in its minimal polynomial (with coprime integer coefficients), then $l\alpha$ is an algebraic integer.

Now, we are ready to continue with the main part of the proof.

First, we need to define the integral:

$$I(u, f) = \int_0^u e^{u-t} f(t)\, dt = e^u \sum_{l \geq 0} f^{(l)}(0) - \sum_{l \geq 0} f^{(l)}(u)$$

where f is a polynomial. Thus, $I(u, f)$ is a finite sum.

Then, for every 1≤ j≤n we define:

$$f_j(x) = \frac{A^{np}(x - \alpha_1)^p ... (x - \alpha_n)^p}{(x - \alpha_j)}$$

where A is a large integer such that $A\alpha_1, ..., A\alpha_n$ are algebraic integers. The remark implies that $f_j(x)$ has algebraic integer coefficients, since the coefficients of the expanded version only contain sums and products of the $A\alpha_i$'s.

Define now

$$J_j = \sum_{k=1}^{n} \beta_k I(\alpha_k, f_j)$$

Our goal is now to find conflicting upper and lower bounds for $|J_1 ... J_n|$, which would contradict our assumption. Therefore, we are going to proceed in two steps.

In the first step, we are going to show that each J_j is an algebraic integer divisible by $(p-1)!$ but not by $p!$. In the second step, we want to show that $J_1 ... J_n \in \mathbb{Z}$.

Claim 3: Each J_j is an algebraic integer divisible by $(p-1)!$ but not by $p!$.

Proof: By setting $I(\alpha_k, f_j)$ into J_j, we get:

$$\sum_{k=1}^{n} \beta_k (e^{\alpha_k} \sum_{l\geq 0} f_j^{(l)}(0) - \sum_{l\geq 0} f_j^{(l)}(\alpha_k)) = -\sum_{k=1}^{n} \beta_k \sum_{l\geq 0} f_j^{(l)}(\alpha_k)$$

where the second equality follows from the fact that $\sum_{k=1}^{n} \beta_k e^{\alpha_k} = 0$

Now, we are going to compute the derivatives of f_j. We distinguish between the case where j≠k and j=k:

If $j \neq k$:

$$f_j^{(l)}(\alpha_k) = \begin{cases} 0 & l \leq p-1 \\ \equiv 0 (mod p!) & l \geq p \end{cases} .$$

If $j = k$:

$$f_j^{(l)}(\alpha_k) = \begin{cases} 0 & l \leq p-2 \\ A^{np}(p-1)! \prod_{i=1}^{n} (\alpha_k - \alpha_i)^p & l = p-1 \\ \equiv 0 (mod p!) & l \geq p \end{cases}$$

From this computation follows that each J_j is an algebraic integer divisible by $(p-1)!$, but not by $p!$.

Claim 4: $J_1 ... J_n \in \mathbb{Z}$

Proof: Using the simplification from Claim 2, we get:

$$J_j = -\sum_{k=1}^{n} \beta_k \sum_{t=1}^{m_k} \sum_{l\geq 0} f_j^{(l)}(\alpha_{k,t})$$

By construction, the two interior sums are symmetric in the $\alpha_{k,t}$'s, where the $\alpha_{k,t}$'s are a complete set of Galois conjugates. Therefore, they are fixed by the Galois Group and hence contained in the rational numbers. Since every J_j is an algebraic integer, we can conclude $J_j \in \mathbb{Z}$ for $1 \leq j \leq n$. Hence, the product $J_1 ... J_n$ is a rational integer.

Finally, we can say that $J_1 ... J_n$ is divisible by $((p-1)!)^n$ but not by $p!$. Hence, we obtain:

$$|J_1 ... J_n| \geq ((p-1)!)^n$$

On the other hand, we have that:

$$|I(\alpha_k, f_j)| \leq |\alpha_k| e^{|\alpha_k|} g_j(|\alpha_k|)$$

where g_j is the polynomial obtained from f_j by replacing each coefficient with its absolute value. Thus, we obtain:

$$|J_i| \leq \sum_{k=1}^{n} |\alpha_k \beta_k| e^{\alpha_k} g_j(|\alpha_k|) \leq c_i^p$$

, where c_i is an integer independent of p. Finally, we get:

$$|J_1 ... J_n| \leq C^p$$

where $C = \prod_{k=1}^{n} c_k$ So, we have obtained two conflicting lower bounds, since the factorial grows faster then the exponential. $\square$

2 Application of Lindemann-Weierstrauss theorem:

Claim: π is transcendental.

Proof: In this proof, we are going to use the Lindemann-Weierstrauss theorem. So let's assume that π is an algebraic number. Since the algebraic numbers form a field, they are closed under multiplication. Therefore, πi is also algebraic. Then, we get:

$$e^{\pi i} + e^0 = -1 + 1 = 0$$

But this an contradiction to the linear independence of $e^{\pi i}$ and e^0. So, π is transcendental.

3 Irrationality of $\mathbf{e}^n$

Claim: For every $n \in \mathbb{N}$, e^n is irrational

Proof: Let $f \in \mathbb{Z}[x]$. We define:

$$I(u, f) = \int_0^u e^{u-t} f(t)\, dt = e^u \sum_{j \geq 0} f^{(j)}(0) - \sum_{j \geq 0} f^{(j)}(u)$$

Since f is a polynomial, I(u,f) is a finite sum. We are going to do a proof by contradiction.
So, let's assume that e^n is rational. The goal is to find conflicting upper and lower bounds. For the upper bound, we find:

$$|I(n, f)| \leq e^n \max_{x \in [0,n]} |f(x)| \cdot n$$

, which grows like C^{degf} in f
In the next step, we try to find a conflicting lower bound.For that, we define:

$$f(x) := x^{p-1}(x - n)^p$$

where p is a large prime number.
Now, we compute the j'th derivative of f, evaluated at 0 and at n:

$$f^{(j)}(0) = \begin{cases} 0 & j \leq p-2 \\ (p-1)!(-n)^p & j = p-1 \\ \equiv 0(mod p!) & j \geq p \end{cases}$$

and

$$f^{(j)}(n) = \begin{cases} 0 & j \leq p-1 \\ \equiv 0(mod p!) & j \geq p \end{cases}$$

We assume that p is large compared to n and the denominator of e^n. Then, $I(n, f)$ is divisible by $(p-1)!$, but not by $p!$. This implies that:

$$|I(n, f)| \geq (p-1)!$$

which is a contradiction since a factorial grows faster then a polynomial.

So, e^n is irrational. $\square$