7 Lindemann's Theorem

Our next result is due to Lindemann.

Theorem 18. *Let $\alpha_1, \ldots, \alpha_n$ be distinct algebraic numbers, and let $\beta_1, \ldots, \beta_n$ be non-zero algebraic numbers. Then*

$$\beta_1 e^{\alpha_1} + \beta_2 e^{\alpha_2} + \cdots + \beta_n e^{\alpha_n} \neq 0.$$

The numbers e^{α_j} above may be multi-valued. The theorem is true for any values of e^{α_j}.

Before proving Theorem 18, it is worth noting the following consequences of it.

Corollary 1. *The following numbers are transcendental:*

(i) π.

(ii) e^{α} *if* α *is a non-zero algebraic number.*

(iii) $\sin(\alpha)$, $\cos(\alpha)$, *and* $\tan(\alpha)$ *if* α *is a non-zero algebraic number.*

(iv) $\log(\alpha)$ *if* α *is an algebraic number different from 0 and 1.*

Proof of Theorem 18. Assume the theorem is false. Then

$$\beta_1 e^{\alpha_1} + \beta_2 e^{\alpha_2} + \cdots + \beta_n e^{\alpha_n} = 0. \tag{9}$$

By reordering if necessary, we may suppose that

$$|\alpha_1| = \max_{1 \leq j \leq n} \{|\alpha_j|\},$$

and we do so. Let

$$F_1(u_1, \ldots, u_n, v_1, \ldots, v_n) = u_1 v_1 + u_2 v_2 + \cdots + u_n v_n,$$

and consider

$$F_2(u_2, \ldots, u_n, v_1, \ldots, v_n) = \prod_{u_1} F_1(u_1, \ldots, u_n, v_1, \ldots, v_n),$$

where u_1 runs through the conjugates of β_1. In particular, F_2 has rational coefficients, the coefficient of the highest power of v_1 is a non-zero rational number, and

$$F_2(\beta_2, \ldots, \beta_n, e^{\alpha_1}, \ldots, e^{\alpha_n}) = 0.$$

Also, observe that F_1 and F_2 are homogeneous polynomials in the variables $v_1, \ldots, v_n$. Now, consider

$$F_3(u_3, \ldots, u_n, v_1, \ldots, v_n) = \prod_{u_2} F_2(u_2, \ldots, u_n, v_1, \ldots, v_n),$$

where u_2 runs through the conjugates of β_2. In particular, F_3 has rational coefficients, the coefficient of the highest power of v_1 is a non-zero rational number, and

$$F_3(\beta_3, \ldots, \beta_n, e^{\alpha_1}, \ldots, e^{\alpha_n}) = 0.$$

Also, F_3 is a homogeneous polynomial in $v_1, \ldots, v_n$. Continuing in this manner and clearing denominators (and combining terms), we end up with an expression of the form (9) with a possibly new value of n and with each β_j being a rational integer. We show also that the β_j are not all 0. Observe that there is an N such that F_{n+1} is a homogeneous polynomial in $v_1, \ldots, v_n$ of degree N. Each term in $F_{n+1}(e^{\alpha_1}, \ldots, e^{\alpha_n})$ is of the form $c \exp(\sum_{j=1}^{n} a_j \alpha_j)$ where the a_j are natural numbers summing to N. The coefficient of $\exp(N\alpha_1)$ is, in particular, non-zero. Moreover, the condition $|\alpha_1| = \max_{1 \le j \le n}\{|\alpha_j|\}$ implies that with a_j as before, $\sum_{j=1}^{n} a_j \alpha_j = N\alpha_1$ only if $a_1 = N$ and $a_j = 0$ otherwise (as can be shown from the triangle inequality). Therefore, we may suppose from the start that the β_j are rational integers.

We next make a similar observation about the α_j's. There is some non-zero polynomial with integer coefficients which has $\alpha_1, \ldots, \alpha_n$ all as roots. Let $\alpha_1, \ldots, \alpha_N$ (N possibly different than above) be the complete set of roots of such a polynomial. Observe that all the conjugates of each α_j appear among $\alpha_1, \ldots, \alpha_N$. Let

$$\beta_{n+1} = \beta_{n+2} = \cdots = \beta_N = 0.$$

Consider the product

$$\prod \left(\beta_1 e^{\alpha_{k_1}} + \beta_2 e^{\alpha_{k_2}} + \cdots + \beta_N e^{\alpha_{k_N}}\right)$$

where, in the product, $k_1, k_2, \ldots, k_N$ runs over all $N!$ permutations of the numbers $1, 2, \ldots, N$. Note that when expanded the product will be of the form given in (9) and will be 0. If βe^{α} denotes a term in this expanded product, then $\alpha = a_1\alpha_1 + \cdots + a_N\alpha_N$ for some non-negative integers $a_1, \ldots, a_n$ summing to $N!$. Here, β will be a rational integer (since the β_j are). Also, there will be in the expanded product all those terms of the form $\beta e^{\alpha'}$ with $\alpha' = a_1\alpha_{k_1} + \cdots + a_N\alpha_{k_N}$ where $k_1, k_2, \ldots, k_N$ is any of the $N!$ permutations of the numbers $1, 2, \ldots, N$. Note that such α' will run through a complete set of conjugates of α (and maybe more). Finally, we observe that some term βe^{α} in the expanded product is non-zero; to see this, consider the non-zero term βe^{α} in each factor of the unexpanded product with α having the largest real part and of those the one with α having the largest imaginary part - the product of these will give a term βe^{α} which is non-zero. Thus, in (9), we may suppose that there are integers $n_0 = 0 < n_1 < \cdots < n_r = n$ such that for each $t \in \{0, 1, \ldots, r-1\}$, the numbers $\alpha_{n_t+1}, \ldots, \alpha_{n_{t+1}}$ form a complete set of conjugates and

$$\beta_{n_t+1} = \cdots = \beta_{n_{t+1}}.$$

Let b be a positive integer for which $b\alpha_j$ are algebraic integers for each j. Let p be a large prime. For $i \in \{1, \ldots, n\}$, let

$$f_i(x) = b^{np}(x - \alpha_1)^p \cdots (x - \alpha_n)^p/(x - \alpha_i).$$

Finally, for $i \in \{1, \ldots, n\}$, let

$$J_i = \beta_1 I_i(\alpha_1) + \cdots + \beta_n I_i(\alpha_n)$$

where $I_i(t)$ denotes $I(t)$ in (8) of the previous notes with $f = f_i$. We will obtain a contradiction by making appropriate upper and lower bounds for $|J_1 J_2 \ldots J_n|$. From (8) and (9), we obtain that

$$J_i = -\sum_{j=0}^{m}\sum_{k=1}^{n} \beta_k f_i^{(j)}(\alpha_k)$$

where $m = np-1$. Note that $f_i^{(j)}(\alpha_k)$ is $p!$ times an algebraic integer unless $j = p-1$ and $k = i$. Also,

$$f_i^{(p-1)}(\alpha_i) = b^{np}(p-1)! \prod {}^{1\le k\le n}_{k\ne i}(\alpha_i - \alpha_k)^p = (p-1)!(F'(\alpha_i))^p$$

where

$$F(x) = \prod_{k=1}^{n}(bx - b\alpha_k) \in \mathbb{Z}[x].$$

We consider the product $J_1 \cdots J_n$. Observe that one term in the product will be

$$\prod_{i=1}^{n}\left((p-1)!(F'(\alpha_i))^p\right)$$

which is $(p-1)!$ (even $((p-1)!)^n$) times a non-zero rational integer. If p is sufficiently large, this integer is furthermore not divisible by p. Every other term can be written as $p!$ times an algebraic integer. We show that the sum of these algebraic integers is rational so that by Lemma 3 of the previous notes the remaining terms sum to a rational integer divisible by $p!$. Observe that this will follow if we can show that $J_1 \cdots J_n$ is a rational number for then the sum we seek is simply

$$\left(J_1 \cdots J_n - (p-1)!^n \prod_{i=1}^{n}(F'(\alpha_i))^p\right)/p!$$

which is clearly rational. So consider

$$J_1 \cdots J_n = (-1)^n \prod_{i=1}^{n}\left(\sum_{j=0}^{m}\sum_{k=1}^{n}\beta_k f_i^{(j)}(\alpha_k)\right).$$

It will follow that $J_1 \cdots J_n$ is a rational number if we can show that for each $t \in \{0, 1, \ldots, r-1\}$, the right-hand side is symmetric in $\alpha_{n_t+1}, \ldots, \alpha_{n_{t+1}}$. Let σ represent any permutation of $n_t + 1, \ldots, n_{t+1}$ and extend σ so that it fixes the other elements of $\{1, 2, \ldots, n\}$. Then we wish to show that

$$\prod_{i=1}^{n}\left(\sum_{j=0}^{m}\sum_{k=1}^{n}\beta_k f_{\sigma(i)}^{(j)}(\alpha_{\sigma(k)})\right) = \prod_{i=1}^{n}\left(\sum_{j=0}^{m}\sum_{k=1}^{n}\beta_k f_i^{(j)}(\alpha_k)\right).$$

Since $\sigma(i)$ runs through the numbers $1, \ldots, n$ as i does, we obtain

$$\prod_{i=1}^{n}\left(\sum_{j=0}^{m}\sum_{k=1}^{n}\beta_k f_{\sigma(i)}^{(j)}(\alpha_{\sigma(k)})\right) = \prod_{i=1}^{n}\left(\sum_{j=0}^{m}\sum_{k=1}^{n}\beta_k f_i^{(j)}(\alpha_{\sigma(k)})\right).$$

Letting $\ell = \sigma(k)$, we see that

$$\prod_{i=1}^{n}\left(\sum_{j=0}^{m}\sum_{k=1}^{n}\beta_k f_i^{(j)}(\alpha_{\sigma(k)})\right) = \prod_{i=1}^{n}\left(\sum_{j=0}^{m}\sum_{\ell=1}^{n}\beta_{\sigma^{-1}(\ell)} f_i^{(j)}(\alpha_\ell)\right).$$

The equation $\beta_{n_t+1} = \cdots = \beta_{n_{t+1}}$ and the definition of σ give

$$\prod_{i=1}^{n}\left(\sum_{j=0}^{m}\sum_{\ell=1}^{n}\beta_{\sigma^{-1}(\ell)} f_i^{(j)}(\alpha_\ell)\right) = \prod_{i=1}^{n}\left(\sum_{j=0}^{m}\sum_{\ell=1}^{n}\beta_\ell f_i^{(j)}(\alpha_\ell)\right),$$

and we deduce that $J_1 \cdots J_n$ is a rational number as desired. Therefore, $J_1 \cdots J_n$ is a rational integer divisible by $(p-1)!$ and not divisible by p. Hence,

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

We get an upper bound for the product by using an upper bound for $|I(t)|$. Thus,

$$|J_1 \cdots J_n| \leq \prod_{i=1}^{n} \left(\sum_{k=1}^{n} |\beta_k||\alpha_k| e^{|\alpha_k|} \overline{f}_i(|\alpha_k|) \right) \leq (c_1 c_2^p)^n \leq c_3 c_4^p$$

for some constants c_1, c_2, c_3, and c_4 independent of p. We obtain a contradiction when p is sufficiently large, completing the proof. $\square$