TRANSCENDENTAL NUMBERS

ERAN ASSAF

1. Introduction

In this class we talk mainly about algebraic extensions, but we should not forget about our transcendental friends. Almost by definition, $t \in F(t)$ is transcendental over F, but the most intriguing cases in terms of proving transcendentality occur already over $\mathbb{Q}$. A complex number $\alpha \in \mathbb{C}$ is called **transcendental** if it is transcendental over $\mathbb{Q}$. Recall that we have shown that "most" numbers are transcendental (even in $\mathbb{R}$), but showing that some of them are indeed transcendental is very difficult. Today we will survey what is known about this problem.

The main reference for this short note is Baker, "Transcendental Number Theory".

2. Liouville Numbers

In 1844, Liouville was the first to show that certain numbers are transcendental. He introduced a class of numbers that are "almost rational", so that we can approximate them closely by sequences of rational numbers.

Definition 1. *A* **Liouville number** $x \in \mathbb{R}$ *is a number such that for any positive integer* $n \in \mathbb{Z}_{>0}$*, there exist* $p_n, q_n \in \mathbb{Z}$ *with* $q_n > 1$ *such that*

$$0 < \left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^n}.$$

Theorem 2. *Liouville numbers exist. In fact, the set of Liouville numbers is uncountable.*

Proof. The proof is actually constructive(!). Let

$$x = \sum_{k=1}^{\infty} \frac{a_k}{b^{k!}},$$

where $b \in \mathbb{Z}_{\geq 2}$, and let $\{a_k\}_{k=1}^{\infty}$ be a sequence of integers such that $a_k \in \{0, 1, 2, \ldots, b-1\}$ for all k and $a_k \neq 0$ for infinitely many k (so that the sum is not finite). It is an easy exercise in calculus to see that the sum converges to a real number $x \in \mathbb{R}$. Note that the cardinality of the set of such infinite sequences $\{a_k\}$ is the cardinality of the continuum, $c = |\mathbb{R}|$.

For any $n \in \mathbb{Z}_{>0}$ define

$$q_n = b^{n!}, \quad p_n = q_n \sum_{k=1}^{n} \frac{a_k}{b^{k!}} = \sum_{k=1}^{n} a_k b^{n!-k!} \in \mathbb{Z}.$$

Note that $q_n > 1$, since $b \geq 2$. Then, as infinitely many a_k are nonzero, and all of them are nonnegative,

$$x - \frac{p_n}{q_n} = \sum_{k=n+1}^{\infty} \frac{a_k}{b^{k!}} > 0.$$

Moreover, as $a_k < b$ for all k we have

$$\begin{aligned}\sum_{k=n+1}^{\infty} \frac{a_k}{b^{k!}} &\leq \sum_{k=n+1}^{\infty} \frac{b-1}{b^{k!}} = (b-1) \sum_{k=n+1}^{\infty} \frac{1}{b^{k!}} \\ &< (b-1) \sum_{k=(n+1)!}^{\infty} \frac{1}{b^k} = \frac{b-1}{b^{(n+1)!}} \cdot \frac{1}{1-b^{-1}} \\ &= \frac{b}{b^{(n+1)!}} \leq \frac{b^{n!}}{b^{(n+1)!}} = \frac{1}{b^{(n+1)!-n!}} = \frac{1}{b^{n \cdot n!}} = \frac{1}{q_n^n}.\end{aligned}$$

□

A special case of this construction, which is the simplest to write down in base 10 is

Definition 3. *The number* $\alpha = \sum_{n=1}^{\infty} 10^{-n!}$ *is called* **Liouville's constant**.

Liouville then proceeds to show that all Liouville numbers are transcendental.

Theorem 4. *If* $\alpha \in \mathbb{R}$ *is a root of an irreducible polynomial* $f(x) \in \mathbb{Z}[x]$ *of degree* $n > 0$*, then there is some* $C \in \mathbb{R}_{>0}$ *such that for all* $p, q \in \mathbb{Z}$ *with* $q > 0$ *either* $\alpha = \frac{p}{q}$ *or*

$$\left|\alpha - \frac{p}{q}\right| > \frac{C}{q^n}.$$

Proof. Let $M = \max_{\{x:|x-\alpha|<1\}} |f'(x)|$. Select $C \in \mathbb{R}_{>0}$ such that

$$C < \min\left(1, \frac{1}{M}\right).$$

Assume, on the contrary, that there exist $p, q \in \mathbb{Z}$ such that $q > 0$ and

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{C}{q^n} \leq C,$$

and let $r = \frac{p}{q}$. Assume $r \neq \alpha$, so that $f(r) \neq 0$. By the Mean Value Theorem, there exists x_0 between α and r such that

$$f(\alpha) - f(r) = f'(x_0)(\alpha - r).$$

Since $f(\alpha) = 0$ and $f(r) \neq 0$, it follows that $f'(x_0) \neq 0$, so that

$$|\alpha - r| = \frac{|f(\alpha) - f(r)|}{|f'(x_0)|} = \frac{|f(r)|}{|f'(x_0)|}.$$

If we write $f(x) = \sum_{i=0}^{n} c_i x^i$ with $c_i \in \mathbb{Z}$, then

$$f(r) = f\left(\frac{p}{q}\right) = \sum_{i=0}^{n} c_i \left(\frac{p}{q}\right)^i = \frac{1}{q^n} \sum_{i=0}^{n} c_i p^i q^{n-i} \in \frac{1}{q^n}\mathbb{Z},$$

so from $f(r) \neq 0$, it follows that $|f(r)| \geq \frac{1}{q^n}$.

Since $|\alpha - x_0| < |\alpha - r| < 1$, by definition of M we get $|f'(x_0)| \leq M < \frac{1}{C}$, hence

$$|\alpha - r| > \frac{C}{q^n},$$

contradicting the hypothesis. □

Corollary 5. *Liouville numbers are transcendental.*

Proof. Let $x \in \mathbb{R}$ be a Liouville number. If x is algebraic, then there exist n and $C > 0$ such that for all $p, q \in \mathbb{Z}$ with $q > 0$ one has either $x = \frac{p}{q}$ or

$$\left| x - \frac{p}{q} \right| > \frac{C}{q^n}.$$

Let r be a positive integer such that $2^{-r} \leq C$, and let $m = n + r$. Since x is a Liouville number, there exist integers $p, q \in \mathbb{Z}$ with $q > 1$ such that

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^m} = \frac{1}{q^{n+r}} \leq \frac{1}{2^r} \frac{1}{q^n} \leq \frac{C}{q^n},$$

contradiction. □

Note that Liouville found these numbers before Cantor invented the notion of countability, so it was only after that it was discovered that the algebraic numbers are countable, and the transcendental numbers are uncountable.

Great, we have constructed uncountably many transcendental numbers, but these are still not a lot. (In what sense? It is a null set in the sense of measure theory - exercise.) But we care about specific numbers, like e and π, which are not Liouville numbers (In fact, e have irrationality measure 2, and π has an irrationality measure between 2 and 7.103...).

Before we prove that π and e are transcendental, we need a couple of technical lemmata.

Lemma 6. *Let $f(x) \in \mathbb{R}[x]$ be s.t. $\deg f(x) = m$, and let*

$$I_f(s) = \int_0^s e^{s-u} f(u)\ du$$

be the contour integral taken over the line joining 0 and s. Then

$$I_f(s) = e^s \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(s).$$

Proof. By induction on m. If $m = 0$, then

$$\int_0^s e^{s-u} f(u)\ du = \int_0^1 s e^{s(1-t)} f(0)\ dt = -e^{s(1-t)} f(0)|_{t=0}^1 = e^s f(0) - f(0) = e^s f(0) - f(s),$$

establishing the base of induction. For the induction step, we use integration by parts.

$$\int_0^s e^{s-u} f(u)\ du = \int_0^1 s e^{s(1-t)} f(st)\ dt = -e^{s(1-t)} f(st)|_{t=0}^1 + \int_0^1 s e^{s(1-t)} f'(st)\ dt.$$

Since $\deg f'(x) = m-1$, by the induction hypothesis, we obtain

$$I_f(s) = e^s f(0) - f(s) + \left(e^s \sum_{j=1}^{m} f^{(j)}(0) - \sum_{j=1}^{m} f^{(j)}(s) \right) = e^s \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(s).$$

□

Lemma 7. *Let $f(x) = \sum_{i=0}^{m} a_i x^i \in \mathbb{R}[x]$, and write*

$$\overline{f}(x) = |a_i| x^i \in \mathbb{R}[x].$$

Then

$$|I_f(s)| \leq |s| e^{|s|} \overline{f}(|s|).$$

Proof. By the triangle inequality for integrals, we have

$$|I_f(s)| = \left| \int_0^1 s e^{s(1-t)} f(st)\ dt \right| \leq \int_0^1 |s| e^{|s(1-t)|} |f(st)|\ dt \leq |s| e^{|s|} |f(s)|.$$

But by the triangle inequality, one has

$$|f(s)| = \left| \sum_{i=0}^{m} a_i s^i \right| \leq \sum_{i=0}^{m} |a_i| |s|^i = \overline{f}(|s|). \quad \square$$

We now proceed, following Hermite, to prove that e is transcendental.

Theorem 8. *e is transcendental.*

Proof. Assume, on the contrary, that e is algebraic, and let $m_e(x) = \sum_{k=0}^{n} a_k x^k$ be its minimal polynomial. In particular, $a_0 \neq 0$ and $n > 0$. Let p be a large prime, and let

$$f(x) = x^{p-1}(x-1)^p \cdots (x-n)^p \in \mathbb{R}[x].$$

Consider the quantity

$$J = \sum_{k=0}^{n} a_k I_f(k).$$

From the first lemmas and $m_e(e) = 0$ we obtain

$$J = \sum_{k=0}^{n} a_k \left(e^k \sum_{j=0}^{np+p-1} f^{(j)}(0) - \sum_{j=0}^{np+p-1} f^{(j)}(k) \right) = -\sum_{k=0}^{n} \sum_{j=0}^{(n+1)p-1} a_k f^{(j)}(k).$$

As k is a root of f with multiplicity p for all $k > 0$, $f^{(j)}(k) = 0$ for all $j < p$ and all $k > 0$ and as 0 has multiplicity $p-1$, also for all $j < p-1$ if $k = 0$. It follows that for all $(k,j) \neq (0, p-1)$, $p! \mid f^{(j)}(k)$. Furthermore,

$$f^{(p-1)}(0) = (p-1)!(-1)^{np}(n!)^p,$$

whence, if $p > n$, $f^{(p-1)}(0)$ is divisible by $(p-1)!$ and not by $p!$. In particular, if $|a_0| < p$, then $a_0 f^{(p-1)}(0)$ is the unique summand not divisible by p, so that $J \neq 0$ and J is divisible

by $(p-1)!$, thus $|J| \geq (p-1)!$. However, the second lemma, together with the estimate $\overline{f}(k) \leq (2n)^{(n+1)p-1}$ (note that $\overline{f}(x) \leq x^{p-1}(x+1)^p \cdots (x+n)^p$) yields

$$|J| \leq \sum_{k=0}^{n} k a_k e^k \overline{f}(k) \leq \sum_{k=0}^{n} k a_k e^k (2n)^{(n+1)p-1} = A \cdot C^p,$$

where A, C are constants. Choosing p large enough, yields a contradiction. □

Finally, we can prove that π is transcendental.

Theorem 9. *π is transcendental.*

Proof. Assume, on the contrary, that π is algebraic, then so is $\theta = \pi i$. Let $m_\theta(x) \in \mathbb{Z}[x] = a_d x^d + \ldots$ be its minimal polynomial, scaled to have relatively prime integral coefficients with $a_d > 0$, and write $\theta = \theta_1, \ldots, \theta_d$ for its roots. From Euler's equation $e^{i\pi} = -1$, we obtain

$$(1 + e^{\theta_1})(1 + e^{\theta_2}) \cdots (1 + e^{\theta_d}) = 0.$$

Expanding the left hand side, we obtain

$$\sum_{\epsilon \in \{0,1\}^d} e^{\Theta_\epsilon} = 0, \quad \text{where } \Theta_\epsilon = \sum_{j=0}^{d} \epsilon_j \theta_j.$$

Suppose exactly n of the Θ_ϵ are nonzero, and denote them by $\alpha_1, \ldots, \alpha_n$. Then

$$2^d - n + e^{\alpha_1} + \ldots + e^{\alpha_n} = 0.$$

Let p be a large prime, and consider

$$f(x) = a_d^{np} x^{p-1} (x - \alpha_1)^p \cdots (x - \alpha_n)^p.$$

We shall compare estimates for

$$J = \sum_{k=0}^{n} I_f(\alpha_k).$$

From the first Lemma, we obtain

$$J = \sum_{k=1}^{n} \left(e^{\alpha_k} \sum_{j=0}^{(n+1)p-1} f^{(j)}(0) - \sum_{j=0}^{(n+1)p-1} f^{(j)}(\alpha_k) \right) = (n - 2^d) \sum_{j=0}^{(n+1)p-1} f^{(j)}(0) - \sum_{k=1}^{n} \sum_{j=0}^{(n+1)p-1} f^{(j)}(\alpha_k).$$

The sum over k is a symmetric polynomial in $a_d\alpha_1, \ldots, a_d\alpha_k$ with integral coefficients, hence it is an integral linear combination of elementary symmetric functions of them, and hence also of the 2^d numbers $a_d\Theta_\epsilon$, which in turn implies that they are integral linear combinations of elementary symmetric functions in the numbers $a_d\theta_1, \ldots, a_d\theta_d$, hence an integral linear combination of the coefficients of m_θ, hence a rational integer. Also, for $j < p$, $f^{(j)}(\alpha_k) = 0$, for $j \neq p-1$, $p! \mid f^{(j)}(0)$, and

$$f^{(p-1)}(0) = (p-1)!(-a_d)^{np}(\alpha_1 \cdots \alpha_n)^p$$

is divisible by $(p-1)!$, and not by $p!$, if p is sufficiently large, hence if $p > a_d$, then $|J| \geq (p-1)!$, but again

$$|J| \leq \sum_{k=1}^{n} |\alpha_k| e^{|\alpha_k|} \overline{f}(|\alpha_k|) \leq c^p$$

for some c independent of p, hence for p large enough, we get a contradiction.

□

These two theorems are a special case of the following, more general, theorem.

Theorem 10 (Lindemann-Weierstrass)**.** *Let $\alpha_1, \ldots, \alpha_n$ be distinct algebraic numbers, and let $\beta_1, \ldots, \beta_n$ nonzero algebraic numbers. Then*

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

Corollary 11. *If $\alpha_1, \ldots, \alpha_n$ are $\mathbb{Q}$-linearly independent algebraic numbers, then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are algebraically independent.*

Proof of Corollary. Assume $p(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ is such that $p(e^{\alpha_1}, \ldots, e^{\alpha_n}) = 0$. Write $p(x) = \sum_{d \in \mathbb{Z}^n_{\geq 0}} a_d x^d$ where $x^d = \prod_{k=1}^n x_k^{d_k}$. Then

$$0 = p(e^{\alpha_1}, \ldots, e^{\alpha_d}) = \sum_{d \in \mathbb{Z}^n_{\geq 0}} a_d e^{\sum_{k=1}^n d_k \alpha_k}.$$

Note that if $c \neq d \in \mathbb{Z}^n_{\geq}$, and $\sum_{k=1}^n d_k \alpha_k = \sum_{k=1}^n c_k \alpha_k$, then $\sum_{k=1}^n (c_k - d_k)\alpha_k = 0$ but by assumption this implies $c_k = d_k$ for all k. Therefore, all the exponents in the above sum are distinct. From the theorem, it follows that all the coefficients vanish, i.e. $a_d = 0$ for all d, showing that the e^{α_k} are algebraically independent. □

Corollary 12. *If $\alpha \neq 0$ is algebraic, then e^α, $\cos\alpha$, $\sin\alpha$ and $\tan\alpha$ are transcendental. If also $\alpha \neq 1$, then $\log\alpha$ is transcendental.*

Proof. The first statement is the previous corollary with $n = 1$. Then if $\cos\alpha = \frac{e^{i\alpha}+e^{-i\alpha}}{2}$ is algebraic, then $x = e^{i\alpha}$ satisfies $x + x^{-1} = 2\cos\alpha$, i.e. $x^2 - 2\cos\alpha x + 1 = 0$, so it is algebraic over $\mathbb{Q}(\cos\alpha)$, hence over $\mathbb{Q}$. But as $i\alpha \neq 0$ is algebraic, this is a contradiction. For $\sin\alpha = \frac{e^{i\alpha}-e^{-i\alpha}}{2i}$, the proof is similar. If $\tan\alpha$ is algebraic, then from $(\tan^2\alpha+1)^{-1} = \cos^2\alpha$, we obtain that $\cos\alpha$ is also algebraic. Finally, if $\alpha \notin \{0, 1\}$, then $\log\alpha \neq 0$ is algebraic, hence $\alpha = e^{\log\alpha}$ is transcendental. □

Finally, let us prove the theorem

Proof. Assume $\sum_{k=1}^n \beta_k e^{\alpha_k} = 0$. We may assume that $\beta_k \in \mathbb{Z}$ (otherwise, multiply all conjugate expressions to obtain rationals, and scale by a common denominator). Let $p(x) \in \mathbb{Z}[x]$ be a polynomial of degree N that has $\alpha_1, \ldots, \alpha_n$ as roots, and let $\alpha_{n+1}, \ldots, \alpha_N$ be its other roots. Considering the expression

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

where $\beta_{n+1} = \ldots = \beta_N = 0$, we obtain a linear combination of terms $e^{\sum_{k=1}^N h_k \alpha_k}$ where the h_k sum to $N!$, and the exponents form a complete set of conjugates. Symmetry ensures that a complete set of conjugates for such a linear expression has the same coefficient (a symmetric function of the original β_k, and by ordering $\mathbb{C}$, e.g. lexicographically, we can look at the coefficient of the exponent of highest degree, and see that it is nonzero. Let ℓ be a positive integer such that $\ell\alpha_1, \ldots, \ell\alpha_k, \ell\beta_1, \ldots, \beta_k$ are all algebraic integers, and let

$$f_i(x) = \ell^{np} \frac{(x-\alpha_1)^p \cdots (x-\alpha_n)^p}{x - \alpha_i},$$

where p is a large prime. Consider

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

where $I_i(s) = I_{f_i}(s)$ and consider estimates for the product $|J_1 \cdots J_n|$. We proceed as before. From the first Lemma

$$J_i = \sum_{k=0}^{n} \beta_k \left(e^{\alpha_k} \sum_{j=0}^{np-1} f_i^{(j)}(0) - \sum_{j=0}^{np-1} f_i^{(j)}(\alpha_k) \right) = -\sum_{k=0}^{n} \beta_k \sum_{j=0}^{np-1} f_i^{(j)}(\alpha_k),$$

and $f_i^{(j)}(\alpha_k)$ is an algebraic integer divisible by $p!$ unless $i = k$ and $j = p-1$, in which case we have

$$f_i^{(p-1)}(\alpha_i) = \ell^{np}(p-1)! \prod_{k \neq i}^{n} (\alpha_i - \alpha_k)^p,$$

so if p is large enough, it is divisible by $(p-1)!$, but not by $p!$. It follows that J_i is an algebraic integer divisible by $(p-1)!$. Further, our symmetry assumption implies that $J_1 \cdots J_n$ is a rational integer, hence a rational integer divisible by $((p-1)!)^n$, but again we can bound each term by an exponential in p, leading to a contradiction if p is large enough. □

3. SUMMARY

We have seen the definition of separable polynomials, and investigated separability. This led us to consider the Frobenius endomorphism over fields of characteristic $p > 0$, and naturally to the definition of a perfect field, which include all characteristic 0 fields and all finite fields. We have used what we learned today and in the previous lesson to show the existence and uniqueness of a finite field of size $q = p^n$.

Finally, we have seen that over a perfect field all algebraic extensions are separable, and introduced the notions of a separable and inseparable degrees of a polynomial.

We will return to this notion after learning some more Galois theory.