Transcendental Numbers (Rough Outline 11/11/23)

Vincent Lin

Fall 2023

Contents

Abstract

Research into transcendental numbers started with rational approximations. This paper covers preliminaries on the neccesary parts of field theory before going into the Lindemann-Weierstrass theorem, Gelfond-Schneider theorem, and Baker's theorem and concludes with a discussion of Schanuel's conjecture. This sequence of theorems are related to determining whether complex numbers are transcendental or not and is based off of the work by Baker.

Chapter 1

Preliminaries

1.1 Algebraic and Transcendental Numbers

Def An **algebraic number** is $\alpha \in \mathbb{C}$ which is the root of a nonzero polynomial in $\mathbb{Q}[x]$. A **transcendental number** is a complex number that is not algebraic.

Note We will use $\mathbb{A}$ to denote the set of algebraic numbers and we will use $\mathbb{C} \setminus \mathbb{A}$ to denote the set transcendental numbers. We will use $\mathbb{R} \setminus \mathbb{A}$ to denote the set of real transcendental numbers.

To find examples of algebraic numbers, we can take any nonzero polynomial in $\mathbb{Q}[x]$ find its roots. By definition, these roots are algebraic numbers. For example, $\sqrt{2}$ is algebraic because it is a root of $x^2 - 2$. Also, i is algebraic because it is the root of $x^2 + 1$. All rational numbers are algebraic as well. Let $\frac{p}{q} \in \mathbb{Q}$ be rational, where $p, q \in \mathbb{Z}$ and q is nonzero. Then, it is the root of $x - \frac{p}{q}$. Therefore, $\mathbb{Q} \subseteq \mathbb{A}$.

What about transcendental numbers? Do they exist?

Theorem 1.1.1 *Yes, transcendental numbers exist.*

Proof Consider the set of algebraic numbers, which we will denote by $\mathbb{A}$. This set is countable. We will show this by forming a surjection

$$\phi : \left(\mathbb{N} \times \bigcup_{n \in \mathbb{N}} \mathbb{Q}^n \right) \to \mathbb{A}\,.$$

Note that $\mathbb{N} \times \bigcup_{n \in \mathbb{N}} \mathbb{Q}^n$ is countable because it is the Cartesian product of a countable set with a countable union of countable sets. By the fundamental theorem of algebra, we know that a polynomial of degree k has k (not necessarily distinct) roots. Therefore, we can number the k roots from 1 to k for each polynomial. Thus, if we specify the nonzero rational coefficients $(a_0, \ldots, a_k)$ and an index i for $i \in [k]$ to be the i-th root of the polynomial $a_k x^k + \cdots + a_0$, we get an algebraic number. We define the map $\phi(i, (a_0, \ldots, a_k))$ to be the i-th root of $a_k x^k + \cdots + a_0$ if it exists. Otherwise, we map the input to zero. From the definition, we know that every algebraic number can be encoded this way since it is one of the roots of a nonzero rational polynomial. Thus, for all $a \in \mathbb{A}$, there must be an input x such that $\phi(x) = a$, making this a surjective map from a countable set to $\mathbb{A}$. This makes $\mathbb{A}$ countable. However, since $\mathbb{C}$ is uncountable, it cannot be the case that all complex numbers are algebraic. Thus, if a complex number is not algebraic, it must be transcendental. Furthermore, $\mathbb{R}$ is uncountable so there must be real transcendental numbers as well.

♦

If transcendental numbers exist, then can we find an example? To show that a number is algebraic, we just have to find a nonzero rational polynomial that it is a root of, evaluate that polynomial at that number, and verify that we get zero. However, checking if a number is transcendental is a very hard problem. The rest of this paper will discuss the transcendence of a large class of numbers and methods for determining the transcendence.

1.2 Fields

Before that, we will generalize the concept of transcendence to other fields. In order to do this, we will list several definitions. Let k, l be fields and let l/k be a field extension.

- $a \in l$ is **algebraic** over k if there is a nonzero polynomial $f \in k[x]$ such that $f(a) = 0$. Otherwise, a is **transcendental** over k. In other words, an algebraic number is a complex number that is algebraic over $\mathbb{Q}$ and a transcendental number is a complex number that is not algebraic over $\mathbb{Q}$.

- $X \subseteq L$ is **algebraically independent** over k if for all $a_1, \ldots, a_t$ distinct and all $f \in k[x_1, \ldots, x_t]$, $f(a_1, \ldots, a_t) = 0$ implies $f = 0$.

- If $a \in l$ is algebraic over k, the **minimal polynomial** of a over k, denoted m_a, is the unique monic irreducible polynomial which generates the kernel of the evaluation map $\phi(f) = f(a)$ for $f \in k[x]$. The **degree** of $\alpha \in k$ is the degree of the minimial polynomial m_a.

- l/k is an **algebraic extension** if every element in l is algebraic over k.

- l is **algebraically closed** if every nonconstant single variable polynomial in l has a root in l.

- An **algebraic closure** of k is an algebraic extension of k that is algebraically closed.

1.3 Liouville Numbers

Now we will start looking for our first transcendental number! First, we will start by proving a lemma.

Lemma 1.3.1 *For any nonzero polynomial $p(x)$ with a root at $x = \alpha$ of multiplicity $m > 0$, $p'(x)$ has the root α with multiplicity $m - 1$.*

Proof From the fundamental theorem of algebra, we can write $p(x)$ as $(x-\alpha)^m q(x)$ where $(x-\alpha) \nmid q(x)$. Now, taking the derivatives of both sides and using the product rule, we get

$$\begin{aligned}
p(x) &= (x-\alpha)^m q(x) \\
p'(x) &= ((x-\alpha)^m)' \, q(x) + (x-\alpha)^m q'(x) \\
&= m(x-\alpha)^{m-1} q(x) + (x-\alpha)^m q'(x) \\
&= (x-\alpha)^{m-1} \left(mq(x) + (x-\alpha)q'(x)\right)
\end{aligned}$$

Therefore, we get that $(x-\alpha)^{m-1} \mid p'(x)$ so $p'(x)$ has the root α of multiplicity at least $m-1$.

Now, we want to show that $p'(x)$ has root α with multiplicity at most $m-1$. In order to show this, we will shift the polynomial by α (all of the roots will therefore be shifted by α as well). Namely, we look at $p(x+\alpha) = x^m q(x+\alpha)$. Note that $p(x+\alpha)$ now has the root 0 with multiplicity m (it has m factors of x) and since $q(x)$ had no $x-\alpha$ factors, $q(x+\alpha)$ has no roots at zero. In other words, $x \nmid q(x+\alpha)$. Now, showing $p'(x)$ has root α with multiplicity $m-1$ is equivalent to showing $p'(x+\alpha)$ as root 0 with multiplicity $m-1$ (it has exactly $m-1$ factors of x). Thus, substituting $x+\alpha$ in $p'(x)$:

$$p'(x+\alpha) = x^{m-1} \left(mq(x+\alpha) + xq'(x+\alpha)\right)$$

We have $m-1$ factors of x from the x^{m-1} term. Therefore, we need to show the rest of the expression has no factors of x. In other words, $x \nmid (mq(x+\alpha) + xq'(x+\alpha))$, we can take the expression $(mq(x+\alpha) + xq'(x+\alpha))$ modulo x to get $mq(x+\alpha)$. Since $m > 0$ and $q(x+\alpha)$ has no factors of x, we know that x cannot divide the entire expression. Shifting back by α, we get that $x-\alpha$ cannot be a factor of $mq(x)+(x-\alpha)q'(x)$, so the multiplicity of $x-\alpha$ in $p(x)$ is at most $m-1$.

♦

Def A **Liouville number** is a real number x such that for all $n \in \mathbb{N}$, there exists integers p, q with $q > 1$ such that

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

Essentially, Liouville numbers are real numbers that can be approximately really, really closely by a sequence of rationals of the form $\left\{\frac{p_i}{q_i}\right\}$, where $q_i > 1$, and the distance between x and $\frac{p_i}{q_i}$ is nonzero, but less than $\frac{1}{(q_i)^i}$.

Theorem 1.3.2 *(Liouville's Approximation Theorem) Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be an algebraic number of degree n. Then, for any rational approximation $\frac{p}{q}$ to α, we have*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{q^n}$$

Proof Let f be the minimal polynomial of α over $\mathbb{Q}$. Note that $f'(\alpha) \neq 0$. This is because $\deg(f') < \deg(f)$ and f is the minimal polynomial. Furthermore, f is irreducible in $\mathbb{R}[x]$, so it cannot be the case that $(x - r) \mid f$ for a rational r. In other words, f has no rational roots. Now let $\frac{p}{q}$ be a rational number which we will use to approximate α and plug it into $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$.

$$\begin{aligned} f\left(\frac{p}{q}\right) &= a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_0 \\ &= \frac{C}{q^n} \end{aligned}$$

for some constant $C \neq 0$ as $\frac{p}{q}$ is not a root of f. Also, note that since we want a good approximation of α that is close to $\frac{1}{q^n}$ away, this rational must be at most distance 1 away from α.

♦

1.4 Transcendence of e and π

Lemma 1.4.1 *Let $f(x)$ be a real polynomial with degree m. Let*

$$I(t) = \int_0^t e^{t-x} f(x)dx.$$

Then,

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

where $f^{(j)}(t)$ is the j-th derivative of f with respect to x evaluated at t.

Proof Probably induction and integration by parts. I will fill this in later.

Chapter 2

Lindemann-Weierstrass Theorem

Theorem 2.0.1 *(Lindemann-Weierstrass Theorem) Suppose*

$$\alpha_1, \ldots, \alpha_n$$

are algebraic numbers that are linearly independent over $\mathbb{Q}$. *Then,*

$$e^{\alpha_1}, \ldots, e^{\alpha_n}$$

are linearly independent over the algebraic numbers. In other words, the extension field $\mathbb{Q}(e^{\alpha_1}, \ldots, e^{\alpha_n})$ *has transcendence degree* n *over* $\mathbb{Q}$.

Proof

Chapter 3

Gelfond-Schneider Theorem

3.1 Background

In this chapter, we will prove the Gelfond-Schneider Theorem. We will introduce a few definitions and lemmas to help prove this.

<u>Def</u> The square **<u>Vandermonde matrix</u>** of size n is the matrix $V = V(x_1, \ldots, x_n)$ is the $n \times n$ matrix

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

with nonzero complex elements x_i^j in the i-th row and $j+1$-th column column where $0 \leq j \leq n-1$ and $1 \leq i \leq n$.

Lemma 3.1.1 *Let $V = V(x_1, \ldots, x_n)$ be the square Vandermonde matrix of size n. Then, the determinant of the square Vandermonde matrix is*

$$\prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Therefore, the determinant vanishes if and only if $x_i = x_j$ for any $i \neq j$.

<u>Proof</u> For $1 \leq i \leq n$, let $E := \{e_i\}$ be the canonical basis for $\mathbb{C}^n$.

Let P_n be the $\mathbb{C}$-vector space of polynomials with degree less than n. Furthermore, for $1 \leq i \leq n$, let $A := \{a_i\}$ be the monomial basis for P_n where $a_i(x) = x^{i-1}$ and let $B := \{b_i\}$

be another monomial basis for P_n where $b_i(x) = \prod_{j<i}(x - x_j)$. For example,

$$\begin{aligned}
b_1 &= 1, \\
b_2 &= (x - x_1), \\
b_3 &= (x - x_1)(x - x_2), \\
&\vdots \\
b_n &= (x - x_1)(x - x_2)\dots(x - x_{n-1}).
\end{aligned}$$

Consider the linear transformation $\psi : P_n \to \mathbb{C}^n$ via $\psi(p) = (p(x_1), \dots, p(x_n))$. We can think of this as a map from $p(x)$ to a column vector of length n.

$$p \mapsto \begin{pmatrix} p(x_1) \\ p(x_2) \\ \vdots \\ p(x_n) \end{pmatrix}$$

Let V be the matrix of ψ with respect to A and E. Now, let L be the matrix of ψ with respect to B and E. Finally, let U be the change of basis matrix from B to A. Then,

$$\begin{aligned}
VU &= L \\
\det(VU) &= \det(L) \\
\det(V)\det(U) &= \det(L)
\end{aligned}$$

Now, V, the matrix of ψ with respect to A and E is

$$\begin{pmatrix} | & | & \cdots & | \\ \psi(a_1) & \psi(a_2) & \cdots & \psi(a_n) \\ | & | & \cdots & | \end{pmatrix} = \begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{pmatrix},$$

the square Vandermonde matrix of size n.

On the other hand, L, the matrix of ψ with respect to B and E is

$$\begin{aligned}
&\begin{pmatrix} | & | & \cdots & | \\ \psi(b_1) & \psi(b_2) & \cdots & \psi(b_n) \\ | & | & \cdots & | \end{pmatrix} \\
&= \begin{pmatrix} 1 & (x_1 - x_1) & \cdots & (x_1 - x_1)(x_1 - x_2)\dots(x_1 - x_{n-1}) \\ 1 & (x_2 - x_1) & \cdots & (x_2 - x_1)(x_2 - x_2)\dots(x_2 - x_{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & (x_n - x_1) & \cdots & (x_n - x_1)(x_n - x_2)\dots(x_n - x_{n-1}) \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & (x_2 - x_1) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & (x_n - x_1) & \cdots & (x_n - x_1)(x_n - x_2)\dots(x_n - x_{n-1}) \end{pmatrix}
\end{aligned}$$

Note that L is lower triangular so $\det(L)$ is the product of the entries along its diagonal, or $\prod\limits_{1\leq i<j\leq n}(x_j - x_i)$.

Finally, consider the change of basis matrix U from basis B to basis A in P_n. The columns of U records the coefficients of the b_i polynomials after expanding. Note that since the b_i are monic, the diagonal of U consists of all 1s because the (i,i)-entry of U is the coefficient of x^{i-1} (the leading coefficient) in b_i. Therefore, U is of the form

$$\begin{pmatrix} 1 & \text{blah} & \text{blah} & \cdots & \text{blah} \\ 0 & 1 & \text{blah} & \cdots & \text{blah} \\ 0 & 0 & 1 & \cdots & \text{blah} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Thus, since U is upper triangular, $\det(U)$ is the product of the 1s along the diagonal so $\det(U) = 1$.

Plugging what we know about $\det(L)$ and $\det(U)$ into $\det(V)\det(U) = \det(L)$, we get that $\det(V) = \prod\limits_{1\leq i<j\leq n}(x_j - x_i)$.

♦

Now we will introduce some concepts from complex analysis. Consider the set of complex numbers $\mathbb{C}$ as a normed space equipped with the absolute value function $|\cdot| : \mathbb{C} \to \mathbb{R}$ via $|z| = \sqrt{z\bar{z}}$, where $\bar{z}$ is the complex conjugate of z. This norm induces a metric space, so we can define the distance between x and y as $d(x,y) := |x-y|$. Furthermore, this metric space induces a topological space so we can define open sets $U \subseteq \mathbb{C}$ such that all points $z \in U$ are contained in a ball within U centered at z. In other words, for all $z \in U$, there is $\varepsilon > 0$ such that for all y where $d(z,y) < \varepsilon$, $y \in U$.

Def Let $f : \mathbb{C} \to \mathbb{C}$ be a function. The **limit** of f as $z \to z_0$ is L if and only if for all $\varepsilon > 0$, there is $\delta > 0$ such that $0 < |z - z_0| < \delta \implies |f(x) - L| < \varepsilon$. We write L as

$$\lim_{z\to z_0} f(z).$$

Def Let $U \subseteq \mathbb{C}$ be an open subset. Let $f : U \to \mathbb{C}$ be a function. The **derivative** of f at a point $z_0 \in \mathbb{C}$ is defined as

$$f'(z_0) := \lim_{z\to z_0} \frac{f(z) - f(z_0)}{z - z_0}.$$

If the derivative exists, the function is said to be **complex differentiable** or **differentiable** at z_0.

Def Let $f : \mathbb{C} \to \mathbb{C}$ be a function and let $U \subseteq \mathbb{C}$ be an open subset of $\mathbb{C}$. Then, f is **holomorphic** on U if it is complex differentiable on every point in U. Furthermore, if $U = \mathbb{C}$, then f is an **entire** function.

Theorem 3.1.2 *(Cauchy's Residue Theorem) Let $U \subseteq \mathbb{C}$ be a simply connected open set containing a finite number of points $\{a_1, \ldots, a_n\}$. Then, let U_0 be $U \setminus \{a_1, \ldots, a_n\}$. Let $f : U_0 \to \mathbb{C}$ be holomorphic on U_0. Furthermore, let γ be a closed rectifiable curve in U_0, $\operatorname{Res}(f, a_i)$ denote the residue of f at each a_k, and $I(\gamma, a_k)$ be the winding number of γ around a_k. Then,*

$$\oint_\gamma f(z)dz = 2\pi i \sum_{k=1}^{n} I(\gamma, a_k) \operatorname{Res}(f, a_k).$$

Lemma 3.1.3 *Let the functions*

$$a_1(t), \dots, a_n(t)$$

be nonzero real polynomials ($\in \mathbb{R}[t]$) *of degree*

$$d_1, \dots, d_n$$

respectively. Furthermore, let

$$w_1, \dots, w_n$$

be (pairwise) distinct real numbers. Then, counting multiplicities, the function

$$f(t) = \sum_{j=1}^{n} a_j(t) e^{w_j t}$$

has at most $n - 1 + \sum_{i=1}^{n} d_i$ *real roots.*

Proof Note that we can multiply the function $f(t)$ by $e^{-w_n t}$ and the number of roots stays the same. This is because this function is nonzero

Let $k = n + \sum_{i=1}^{n} d_i$. This means that we want to show $f(t)$ has at most $k-1$ roots. We will prove this statement using strong induction on k. For our base case $k = 1$. In this case, we know that

$$1 = n + \sum_{i=1}^{n} d_i$$

so it must be the case that $n = 1$, making $d_1 = 0$. Therefore, $a_1(t)$ is a nonzero constant polynomial so $f(t) = a_1(t)e^{w_j t} = ce^{w_j t}$ for some nonzero constant c. This is an exponential function which is either always greater than zero or always less than zero. Therefore, it has $k - 1 = 0$ roots. This completes the base case.

Now assume that $k > 1$ and that the proposition holds true for all k', where $1 \leq k' < k$. Now, consider $f'(t)$. We will try to bound the number of roots in $f'(t)$. Firstly, note that $f(t)$ is differentiable over the reals. Therefore, between any two different roots, i.e. $f(i) = f(j) = 0$, where $i \neq j$ there is a point with derivative zero from Rolle's theorem. Therefore, we know that if $f(t)$ has N roots.

Lemma 3.1.4 *Let $f(z)$ be an analytic function in the disk $D \subseteq \mathbb{C}$. Here, we define $D = \{z : |z| < d\}$ for some positive real d. Suppose f is continuous on the closure of D, $\overline{D} = \{z : |z| \leq d\}$. Furthermore, let $|f|_d = \max\limits_{z \in \overline{D}, |z| = d} f(z)$. Then, for every $z \in \overline{D}$, $|f(z)| \leq |f|_d$.*

Proof Seems very difficult. Involves Maximum Modulus Principle, proof is omitted in most texts.

Lemma 3.1.5 *something from complex analysis*

Lemma 3.1.6 *something with matrices*

3.2 Main Theorem

Theorem 3.2.1 *(Gelfond-Schneider Theorem) Let α and β be algebraic numbers such that $\alpha \notin \{0, 1\}$ and $\beta \in \mathbb{C} \setminus \mathbb{Q}$. Then, α^β is transcendental.*

3.3 Consequences

Proof We will incorporate four lemmas in this proof

Chapter 4

Baker's Theorem

Theorem 4.0.1 *(Baker's Theorem) Let* $\mathbb{L} = \left\{\lambda \in \mathbb{C} : e^{\lambda} \in \overline{\mathbb{Q}}\right\}$. *Then, if*

$$\lambda_1, \ldots, \lambda_n \in \mathbb{L}$$

are linearly independent over $\mathbb{Q}$*,*

Chapter 5

Schanuel's Conjecture

Conjecture 5.0.1 *(Schanuel's Conjecture) Suppose we have n complex numbers*

$$z_1, \ldots, z_n$$

that are linearly independent over $\mathbb{Q}$. Then, $\mathbb{Q}(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n})$ has transcendence degree at least n over $\mathbb{Q}$.

Index