CARLETON UNIVERSITY

SCHOOL OF
MATHEMATICS AND STATISTICS

HONOURS PROJECT

TITLE: Irrational & Transcendental Numbers

AUTHOR: Sarah Zamperin

SUPERVISOR: Brandon Fodden

DATE: August 25th, 2020

# 1 Introduction

In this paper we will look at irrational and transcendental numbers. In Section 2, we discuss irrational numbers, proving that $\sqrt{2}$, $e$, and $\pi$ are irrational, among others. In Section 3, we will discuss algebraic numbers, proving that they form a field and some results that follow from that. In Section 4, we give counting arguments to show that most complex numbers are not algebraic. In Section 5, we will discuss the transcendental numbers, which are the counterpart to algebraic numbers. This section will include proofs that the Liouville constant and $e$ are transcendental. In Section 6, we will discuss consequences of the Lindemann-Weierstrass and Gelfond-Schneider Theorems, and in Section 7, we will prove the Lindemann-Weierstrass Theorem.

# 2 Irrational Numbers

We will begin by discussing irrational numbers.

**Definition 2.1.** *A* rational number *is a number that can be written in the form* $\frac{p}{q}$, *for* $p, q \in \mathbb{Z}$ *with* $q \neq 0$. *A real number is* irrational *if this is not the case.*

One of the first numbers proved to be irrational was $\sqrt{2}$.

**Theorem 2.2.** *The number* $\sqrt{2}$ *is irrational.*

*Proof.* Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{p}{q}$ for some $p, q \in \mathbb{Z}, q \neq 0$. We assume $\frac{p}{q}$ is in lowest terms. Then, $2 = \frac{p^2}{q^2}$ and so $p^2 = 2q^2$. Since $q^2 \in \mathbb{Z}$ this implies $p^2$ is even which implies $p$ is even. Thus, $p = 2r$ for some $r \in \mathbb{Z}$. Since $p^2 = 2q^2$, we have that $(2r)^2 = 2q^2$ and so, $q^2 = 2r^2$. Since $r^2 \in \mathbb{Z}$, $q^2$ is even which implies that $q$ is even. Thus, we have shown that $2 \mid p$ and $2 \mid q$. This is a contradiction since $\frac{p}{q}$ is in lowest terms. $\square$

We can now generalize this result with the following theorem.

**Theorem 2.3.** *If $n \in \mathbb{Z}$, $n \neq m^k$ for some $m \in \mathbb{Z}$, $k \in \mathbb{N}$, then any real $k^{th}$ root of $n$ is irrational.*

*Proof.* Let $n$ have a real $k^{\text{th}}$ root and suppose that the root is equal to $\frac{p}{q}$ for $p, q \in \mathbb{Z}$, $q \neq 0$. Without loss of generality, let $q > 0$. We may assume that $\frac{p}{q}$ is in lowest terms. Then, $n = \frac{p^k}{q^k}$ and so $nq^k = p^k$. Note, since $\frac{p}{q}$ is in lowest terms, we have that $\gcd(p, q) = 1$, which implies $\gcd(p^k, q^k) = 1$. Thus, $p^k \mid n$. Since $p^k$ and $q^k$ are coprime, this implies that $q^k = 1$. Hence, $n = p^k$, a contradiction. $\square$

It is easy to show that many logarithms are irrational.

**Theorem 2.4.** *For $b, n \geq 2$, if $b$ and $n$ do not share the same prime divisors, then $\log_b n$ is irrational.*

*Proof.* Suppose $\log_b n = \frac{p}{q}$ for $p, q \in \mathbb{Z}$. Then $b^{\frac{p}{q}} = n$ and so $b^p = n^q$. Thus, $b$ and $n$ share the same prime divisors, a contradiction. $\square$

Euler first showed that the number $e$ is irrational in 1737. Our proof is based on a later proof by Fourier.

**Theorem 2.5.** *$e$ is irrational.*

*Proof.* Suppose that $e = \frac{p}{q}$, where $p, q \in \mathbb{Z}, q \neq 0$. Without loss of generality, we can take $p, q$ to be positive. Note that $e = \sum_{n=0}^{\infty} \frac{1}{n!}$. Consider,

$$\begin{aligned} q!e &= q! \sum_{n=0}^{\infty} \frac{1}{n!} \\ &= q! \left( \frac{1}{0!} + \frac{1}{1!} + \cdots + \frac{1}{q!} + \frac{1}{(q+1)!} + \ldots \right) \\ &= \frac{q!}{0!} + \frac{q!}{1!} + \cdots + \frac{q!}{q!} + \frac{q!}{(q+1)!} + \ldots \end{aligned}$$

Since $e = \frac{p}{q}$ we have that $q!e = p(q-1)!$ which implies that $q!e \in \mathbb{N}$. We also have that $\frac{q!}{0!} + \frac{q!}{1!} + \cdots + \frac{q!}{q!} \in \mathbb{Z}$. Let $q!e - \left[\frac{q!}{0!} + \frac{q!}{1!} + \cdots + \frac{q!}{q!}\right] = n \in \mathbb{Z}$. Then,

$$\begin{aligned} n &= \frac{q!}{(q+1)!} + \frac{q!}{(q+2)!} + \frac{q!}{(q+3)!} + \ldots \\ &= \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \frac{1}{(q+1)(q+2)(q+3)} + \ldots \\ &< \frac{1}{q+1} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} + \ldots \\ &= \frac{1}{q+1}\left(1 + \frac{1}{q+1} + \frac{1}{(q+1)^2} + \ldots\right) \\ &= \frac{1}{q+1}\sum_{n=0}^{\infty}\frac{1}{(q+1)^n} \\ &= \frac{1}{q+1}\left(\frac{1}{1-\frac{1}{q+1}}\right) \\ &= \frac{1}{q+1}\left(\frac{q+1}{q}\right) \\ &= \frac{1}{q}. \end{aligned}$$

Thus, $n < \frac{1}{q}$, but $q \geq 1$, and so we have $0 < n < 1$, a contradiction since $n \in \mathbb{N}$. □

In 1761, Lambert proved that $\pi$ is irrational. Our proof was done much later, given in 1947 by Niven.

**Theorem 2.6.** *$\pi$ is irrational*

*Proof.* Suppose $\pi$ is rational. That is, $\pi = \frac{p}{q}$ for $p, q \in \mathbb{Z}, q \neq 0$. Without loss of generality, we can take $p, q$ to be positive. Fix $n \in \mathbb{Z}, n > 0$ and let

$$f(x) = \frac{x^n(p-qx)^n}{n!}$$

and

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x).$$

Note that $f^{(k)}(0)$ and $f^{(k)}(\pi) \in \mathbb{Z}$ for $k \in \mathbb{Z}, k > 0$. To see this, we note that $f(\pi - x) = f(x)$ and so $f^{(k)}(x) = (-1)^k f^{(k)}(\pi - x)$. For $k < n$, we have

$f^{(k)} = 0$, and so $f^{(k)}(\pi) = 0$ as well. For $k \geq n$, if a term of $f^{(k)}(x)$ has a factor that contains a positive power of $x$, then it will contribute 0 when $x = 0$. Thus, any terms that contribute to the sum when $x = 0$ must have the power of $x$ differentiated away. This will yield a constant factor of $n!$, which will cancel the $n!$ in the denominator, leaving an integer. Thus,

$$\begin{aligned}
[F'(x)\sin x - F(x)\cos x]' &= F''(x)\sin x + F'(x)\cos x - F'(x)\cos x + F(x)\sin x \\
&= F''(x)\sin x + F(x)\sin x \\
&= [F''(x) + F(x)]\sin x.
\end{aligned}$$

Since $f(x)$ is a polynomial of degree $2n$, $f^{(2n+2)}$ is the zero polynomial. Then, $F''(x) + F(x) = f(x)$, and so

$$[F'(x)\sin x - F(x)\cos x]' = f(x)\sin x.$$

Integrating this over $[0, \pi]$ yields

$$\begin{aligned}
\int_0^\pi f(x)\sin x dx &= [F'(x)\sin x - F(x)\cos x]|_0^\pi \\
&= [F'(\pi)\sin\pi - F(\pi)\cos\pi] - [F'(0)\sin 0 - F(0)\cos 0] \\
&= F(\pi) + F(0).
\end{aligned}$$

$F(\pi)$ and $F(0)$ are determined by $f^{(k)}(0)$ and $f^{(k)}(\pi)$ which are integers. This implies that $F(\pi) + F(0) \in \mathbb{Z}$. On the interval $(0, \pi)$, $f(x) > 0$ and $\sin x > 0$ implies that $f(x)\sin x > 0$ on $(0, \pi)$ and so $F(\pi) + F(0) > 0$. Then, for all $x \in (0, \pi)$, $0 < \sin x < 1$ implying that $0 < f(x)\sin x < f(x)$ on $(0, \pi)$. Note that $0 < p - qx < p$ on $(0, \pi)$ implies $(p - qx)^n < p^n$, but, $x^n < \pi^n$ on $(0, \pi)$ so, $f(x) = \frac{x^n(p-qx)^n}{n!} < \frac{\pi^n p^n}{n!}$. Thus, for all $x \in (0, \pi), 0 < f(x)\sin x < \frac{\pi^n p^n}{n!}$. Integrating over $[0, \pi]$ gives us

$$0 < \int_0^\pi f(x)\sin x dx < \int_0^\pi \frac{\pi^n p^n}{n!} dx$$

implying that $0 < F(\pi) + F(0) < \frac{\pi^{n+1}p^n}{n!}$. Then, for large enough $n$, $\frac{\pi^{n+1}p^n}{n!} < 1$, which is a contradiction since $F(\pi) + F(0) \in \mathbb{Z}$. $\square$

# 3 Algebraic Numbers

We continue by introducing the field of algebraic numbers.

**Definition 3.1.** *A complex number $\alpha$ is said to be an* algebraic number *if there exists a non-zero polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. A complex number that is not algebraic is* transcendental.

The next theorem allows us to define minimal polynomials. We will state the theorem without proof. Proofs can be found in [1] and [4].

**Theorem 3.2.** *Given an algebraic number $\alpha$, there exists a unique irreducible monic polynomial $P(x) \in \mathbb{Q}[x]$ such that $P(\alpha) = 0$. This is called the* minimal polynomial of *$\alpha$.*

We now look at the degrees of algebraic numbers.

**Definition 3.3.** *An algebraic number $\alpha$ is said to be of* degree $n$ *if its minimal polynomial $P(x)$ has degree $n$.*

**Theorem 3.4.** *Rational numbers are algebraic of degree* 1.

*Proof.* Let $\frac{p}{q} \in \mathbb{Q}$, $p, q \in \mathbb{Z}$, $q \neq 0$. Let $x = \frac{p}{q}$. Then, $qx = p \implies qx - p = 0$. Thus, $\frac{p}{q}$ is a root of a linear polynomial. That is, $\frac{p}{q}$ is algebraic of degree 1. □

The contrapositive implies that a real transcendental number must be irrational. However, some irrational numbers are algebraic.

**Theorem 3.5.** $\sqrt{2}$ *is algebraic of degree* 2.

*Proof.* Let $x = \sqrt{2}$. Then $x^2 = 2$, and so $x^2 - 2 = 0$. Thus, $f(x) = x^2 - 2 = 0$ when $x = \sqrt{2}$. We see that $x^2 - 2$ is irreducible, so $f(x)$ is the minimal polynomial of $\sqrt{2}$, hence, $\sqrt{2}$ is algebraic of degree 2. □

**Theorem 3.6.** $i$ *is algebraic of degree* 2.

*Proof.* Let $x = i$. Then $x^2 = i^2 = -1$, and so $x^2 + 1 = 0$. Thus, $f(x) = x^2 + 1 = 0$ when $x = i$. We can see that $x^2 + 1$ is irreducible and so, $i$ is algebraic of degree 2. □

**Theorem 3.7.** *The algebraic numbers form a field, which we will denote as* $\mathbb{A}$.

*Proof.* We know that algebraic numbers are a subset of $\mathbb{C}$, so it suffices to show that $\mathbb{A}$ is a subfield of $\mathbb{C}$. Let $\alpha \in \mathbb{A}$ and let $f$ be the minimal polynomial of $\alpha$. Then $\alpha$ satisfies the equation $f(x) = 0$, so, $-\alpha$ satisfies $f(-x) = 0$ and $\frac{1}{\alpha}$ satisfies $x^m f(\frac{1}{x}) = 0$ where $m$ is the degree of $f(x)$. Since each of these are polynomials, $-\alpha$ and $\alpha^{-1}$ are in $\mathbb{A}$. Now, let $\alpha, \beta \in \mathbb{A}$ where $\alpha$ is of degree $m$ and $\beta$ is of degree $n$. We will now show that $\alpha + \beta$ and $\alpha\beta$ are algebraic. Since $\alpha$ is algebraic, it satisfies the following equation,

$$\alpha^m = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + a_1\alpha + a_0 \tag{1}$$

where $a_j$ is a rational coefficient for all $j$. So we have that $\alpha^m$ is a linear combination of $1, \alpha, \ldots, \alpha^{m-1}$. Similarly, by multiplying the above equation by $\alpha$, we get $\alpha^{m+1} = a_{m-1}\alpha^m + a_{m-2}\alpha^{m-1} + a_1\alpha^2 + a_0\alpha$. We can use (1) to replace $a_{m-1}\alpha^m$ by terms of a lower degree. Using induction, we can repeat this to show that $\alpha^m, \alpha^{m+1}, \alpha^{m+2}, \ldots$ can be written as a linear combination of $1, \alpha, \ldots, \alpha^{m-1}$ with rational coefficients. In a similar way, we can see that $\beta^n, \beta^{n+1}, \beta^{n+2}, \ldots$ can be expressed a linear combinations of $1, \beta, \ldots, \beta^{n-1}$ with rational coefficients. We now consider

$$1, \alpha + \beta, (\alpha + \beta)^2, \ldots, (\alpha + \beta)^{mn}. \tag{2}$$

If we expand these and replace the $m^{\text{th}}$, $n^{\text{th}}$, and any powers higher of $\alpha$ and $\beta$ respectively with lower powers, we have that all $mn + 1$ numbers above can be written as linear combinations of the $mn$ values $\alpha^j\beta^k$ where $j = 0, 1, \ldots, m-1$ and $k = 0, 1, \ldots, n-1$. Thus, we can see that the numbers in (2) are linearly dependent over the rationals. That is,

$$c_0 + c_1(\alpha + \beta) + \cdots + c_{mn}(\alpha + \beta)^{mn} = 0$$

for $c_i$ not all zero, so, $\alpha + \beta$ is algebraic. Similarly, we can conclude that $\alpha\beta$ is algebraic. To see this, we consider the following numbers,

$$1, \alpha\beta, (\alpha\beta)^2, \ldots, (\alpha\beta)^{mn}. \tag{3}$$

Again, we can write the higher powers of $\alpha\beta$ with lower powers so that all of the $mn + 1$ values in (3) can be written as linear combinations of the $mn$ values $\alpha^j \beta^k$ where $j = 0, 1, \ldots, m - 1$ and $k = 0, 1, \ldots, n - 1$ and so, they are linearly dependent over the rationals which implies that $\alpha\beta$ is algebraic. □

From this proof we can get an interesting corollary.

**Corollary 3.8.** *The sum of an algebraic and transcendental numbers is transcendental. The product of a nonzero algebraic number and a transcendental number is transcendental.*

*Proof.* Let $a$ be an algebraic number and let $b$ be transcendental. Suppose the sum of an algebraic and transcendental numbers is algebraic. If $a + b$ is algebraic, then Theorem 3.7 implies that $a + b - a$ is also algebraic. This is a contradiction since $a + b - a = b$, a transcendental number.
Now suppose $a$ is also nonzero and the product $ab$ is algebraic. Then, by Theorem 3.7, $aba^{-1}$ is algebraic. However, $aba^{-1} = b$, a contradiction. □

We would now like to show that $\mathbb{A}$ is algebraically closed. We will require a few results to do so.

Given an algebraic number $\theta$ that satisfies a minimal polynomial of degree $n$, we have that

$$\mathbb{Q}(\alpha) = \{f(\alpha) : f \in \mathbb{Q}[x]\}$$

is a field, called an *algebraic number field* of degree $n$. If we have an element $\beta$ of $\mathbb{Q}(\theta)$, then there are unique $a_i \in \mathbb{Q}$ where

$$\beta = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}.$$

Proof of both of these facts can be found in [1].

**Lemma 3.9.** *Suppose $V$ is a finite dimensional vector space over the field $S$, and $S$ is a finite dimensional vector space over the field $F$. Then $V$ is a finite dimensional vector space over $F$.*

*Proof.* Let $V$ be finite dimensional over $S$, then there exist vectors $v_1, \ldots, v_m \in V$ that span $V$ using coefficients in S. Similarly, there exist vectors $s_1, \ldots, s_n \in S$ that span S using coefficients in F. Let $u \in V$. Then, $u = \sum_{i=1}^{m} c_i v_i$ for $c_i \in S$. Since each $c_i$ is a linear combination of the $s_j$'s, then for some $b_{ij} \in F$, we have

$$u = \sum_{i=1}^{m} \left( \sum_{j=1}^{n} b_{ij} s_j \right) v_i = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij} (s_j v_i).$$

Note that each $s_j v_i$ is a vector in $V$, thus, we have that every vector in $V$ can be written as a linear combination of finitely many vectors in $V$ using coefficients in $F$. That is, $V$ is a finite dimensional vector space over $F$. □

**Definition 3.10.** *A field $\mathbb{F}$ is* algebraically closed *if the roots of any polynomial with coefficients in $\mathbb{F}$ are in $\mathbb{F}$*

**Theorem 3.11.** *The field of algebraic numbers is algebraically closed.*

*Proof.* Let $f$ be a polynomial with algebraic coefficients. Since $\mathbb{A}$ is a field by Theorem 3.7, we can divide the polynomial by the leading coefficient to obtain a polynomial with the same roots. Thus, we may assume that $f$ is monic. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where $a_i \in \mathbb{A}$. Then each $a_i$ is a root of a polynomial of degree $m_i$ with rational coefficients. Let $S = \mathbb{Q}(a_{n-1}, \ldots, a_0)$ be the algebraic number field formed by $a_{n-1}, \ldots, a_0$. Since $S$ is the span of all products of the powers of the $a_i$ up to $m_i - 1$, then $S$ is a finite dimensional vector space over $\mathbb{Q}$. Let $\alpha$ be a root of $f$, and let

$$V = \text{span}\{1, \alpha, \ldots, \alpha^{n-1}\}$$

be a vector space over $S$. Since $S$ is a finite dimensional vector space over $\mathbb{Q}$, Lemma 3.9 implies that $V$ is a finite dimensional vector space over $\mathbb{Q}$, say of dimension $k$. Since we can reduce the exponents of the powers of $\alpha$ using the fact that $\alpha$ is a root of $f$, which yields

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0,$$

we have that $V$ contains all natural number powers of $\alpha$. Consider the set $1, \alpha, \alpha^2, \ldots, \alpha^k \in V$. Since the set contains more than $k$ vectors, it is linearly dependent over $\mathbb{Q}$. Thus, there exists $c_i \in \mathbb{Q}$ not all zero with

$$c_k\alpha^k + \cdots + c_1\alpha + c_0 = 0.$$

Hence, $\alpha$ is a root of the polynomial $c_kx^k + \cdots + c_1x + c_0$ with $c_i \in \mathbb{Q}$, and therefore $\alpha$ is algebraic. □

Finally, we conclude with a few additional results on algebraic numbers.

**Theorem 3.12.** *The $n^{th}$ root of an algebraic number is algebraic.*

*Proof.* Let $\alpha$ be algebraic. Then, for some polynomial $P(x)$, $P(x) = 0$ when $x = \alpha$. Let $Q(x) = P(x^n)$. Since $\sqrt[n]{\alpha}$ is a root of the polynomial Q, $\sqrt[n]{\alpha}$ is algebraic. □

**Theorem 3.13.** *$a + bi$ is algebraic if and only if $a$ and $b$ are algebraic.*

*Proof.* ($\Leftarrow$) Let $a$ and $b$ be algebraic. By Theorem 3.6, $i$ is algebraic and since algebraic numbers form a field (Theorem 3.7), this implies that $a + bi$ is algebraic.

($\Rightarrow$) Let $a+bi$ be algebraic. Then, there exists a polynomial $P(x) \in \mathbb{Q}[x]$ such that $P(a + bi) = 0$. Similarly, $a - bi$ is a root of $P(x)$, so $a - bi$ is algebraic. Thus, by Theorem 3.7, $(a+bi) \pm (a-bi)$ is algebraic. This implies that $2a$ and $2bi$ are also algebraic, and so, $\frac{1}{2}(2a) = a$ and $(-\frac{i}{2})(2bi) = b$ are algebraic. □

# 4 Cantor's Cardinality Arguments

We will take the following results as facts. The proofs are typically given in an introductory mathematical reasoning course.

**Fact 4.1.** *There are countably many rational numbers.*

**Fact 4.2.** *The set of real numbers is uncountable.*

**Fact 4.3.** *The set of complex numbers is uncountable.*

**Fact 4.4.** *A countable union of countable sets is countable.*

We continue by proving the countability/uncountability of some interesting sets.

**Theorem 4.5.** *The set of irrational numbers is uncountable.*

*Proof.* We know that $\mathbb{R}$ is the disjoint union of rational and irrational numbers. By Facts 4.1 and 4.2, we have that $\mathbb{R}$ is uncountable and $\mathbb{Q}$ is countable. Thus, if the irrational numbers were countable, this would imply that $\mathbb{R}$ is countable, by Fact 4.4. This is a contradiction. $\square$

**Theorem 4.6.** *The set of algebraic numbers is countably infinite.*

*Proof.* Let P be the set of monic polynomials in $\mathbb{Q}[x]$ and let $R_p$ denote the set of roots of a polynomial $p$. Then we have that $\mathbb{A} = \bigcup_{p \in P} R_p$. By definition, we can see that $R_p$ is finite, so it suffices to show that $P$ is countable. If we let $P_n$ be the set of monic polynomials of degree $n$ with rational coefficients, then $P = \bigcup_{n=1}^{\infty} P_n$. We can define the map $\mathbb{Q}^n \to P_n$ where $(a_0, a_1, \dots, a_{n-1}) \mapsto x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. One can see that this is a bijection and so we have that $P_n$ is countable since $\mathbb{Q}$ is countable. Thus, $P$ is a countable union of countable sets, so by Fact 4.4 $P$ is countable. Since we have that $P$ is countable, then $\mathbb{A}$ is comprised of a countable union of countable sets, by Fact 4.4, $\mathbb{A}$ is countable. Since $\mathbb{N} \subseteq \mathbb{A}$, $\mathbb{A}$ is also infinite. $\square$

**Theorem 4.7.** *The set of transcendental numbers is uncountable.*

*Proof.* By Definition 3.1, $\mathbb{C} = \mathbb{A} \cup \mathbb{T}$ where $\mathbb{T}$ is the set of transcendental numbers. By Theorem 4.6 and Fact 4.3, we have that $\mathbb{A}$ is countable and $\mathbb{C}$ is uncountable. Thus, by similar argument in the proof of Theorem 4.5, if $\mathbb{T}$ were countable, this would imply that $\mathbb{C}$ is countable, which is a contradiction. □

Cantor proved this in 1874, at which time only a few transcendental numbers were known.

# 5 Early Transcendental Numbers

Here we will begin to discuss early transcendental numbers. In 1853, Liouville proved the following theorem regarding approximations of algebraic numbers by rationals. This theorem allowed him to construct the transcendental number $\sum_{n=0}^{\infty} \frac{1}{10^{n!}}$, called the Liouville constant.

**Theorem 5.1.** *Given a real algebraic number $\alpha$ of degree $n > 1$, there exists a positive constant $c = c(\alpha)$ such that for all rational numbers $\frac{p}{q}$ with $\gcd(p, q) = 1, q > 0$, we have that $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^n}$.*

*Proof.* Let $\alpha$ be an algebraic number of degree $n > 1$ and let $P(x)$ be the minimal polynomial of $\alpha$. If we clear the denominators of the coefficients of $P(x)$, we have a polynomial of degree $n$ with integer coefficients that is irreducible in $\mathbb{Z}[x]$ with a positive leading coefficient. Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

be this polynomial. Then,

$$\left|f\left(\frac{p}{q}\right)\right| = \left|a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0\right|$$

$$= \left|\frac{1}{q^n}\right| |a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n|$$
$$\geq \frac{1}{q^n}.$$

We cannot have $f\left(\frac{p}{q}\right) = 0$ since $f$ is of degree at least 2 and is irreducible over $\mathbb{Q}$, and so the second factor is at least 1. If $\alpha_1, \ldots, \alpha_n$ with $\alpha = \alpha_1$ are the roots of $f$, let $M$ be the maximum of the values $|\alpha_i|$, i.e. $M = \max_{1\leq i\leq n} |\alpha_i|$. Consider the case when $\left|\frac{p}{q}\right| > 2M$. Then,

$$\begin{aligned}\left|\frac{p}{q} - \alpha\right| &\geq \left|\left|\frac{p}{q}\right| - |\alpha|\right| \\ &> 2M - |\alpha| \\ &\geq 2M - M \\ &= M \\ &\geq \frac{M}{q^n}.\end{aligned}$$

Now, if $\left|\frac{p}{q}\right| \leq 2M$, then we have,

$$\begin{aligned}\left|\alpha_i - \frac{p}{q}\right| &\leq |\alpha_i| + \left|\frac{p}{q}\right| \\ &\leq M + 2M \\ &= 3M.\end{aligned}$$

Note that $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i) = (x - \alpha_1)a_n \prod_{i=2}^{n}(x - \alpha_i)$. Then,

$$\begin{aligned}\frac{1}{q^n} &\leq \left|f\left(\frac{p}{q}\right)\right| \\ &= \left|\frac{p}{q} - \alpha_1\right| |a_n| \prod_{i=2}^{n} \left|\alpha_i - \frac{p}{q}\right|.\end{aligned}$$

This implies that

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{1}{|a_n| q^n \prod_{i=2}^{n} |\alpha_i - \frac{p}{q}|} \geq \frac{1}{|a_n| q^n (3M)^{n-1}}.$$

Thus, choosing $c(\alpha) = \min\left(M, \frac{1}{|a_n|(3M)^{n-1}}\right)$, we have that $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^n}$. $\square$

We can now show that the Liouville constant is transcendental.

**Theorem 5.2.** *The Liouville constant,* $\sum_{n=0}^{\infty} \frac{1}{10^{n!}}$ *is transcendental.*

*Proof.* Suppose not and let $\alpha = \sum_{n=0}^{\infty} \frac{1}{10^{n!}}$. Consider the rational partial sums $\frac{p_k}{q_k} := \sum_{n=0}^{k} \frac{1}{10^{n!}}$ where $10^{k!} = q_k$. Then

$$\begin{aligned}
\left|\alpha - \frac{p_k}{q_k}\right| &= \left|\sum_{n=0}^{\infty} \frac{1}{10^{n!}} - \sum_{n=0}^{k} \frac{1}{10^{n!}}\right| \\
&= \left|\sum_{n=k+1}^{\infty} \frac{1}{10^{n!}}\right| \\
&= \frac{1}{10^{(k+1)!}} + \left(\frac{1}{10^{(k+1)!}}\right)^{k+2} + \left(\frac{1}{10^{(k+1)!}}\right)^{(k+2)(k+3)} + \dots \\
&\leq \frac{1}{10^{(k+1)!}}\left(1 + \frac{1}{10^2} + \frac{1}{10^3} + \dots\right) \\
&= \left(\frac{1}{10^{(k+1)!}}\right) S,
\end{aligned}$$

where $S = 1 + \frac{1}{10^2} + \frac{1}{10^3} + \cdots = \frac{91}{90}$. Thus we have that

$$\left|\sum_{n=k+1}^{\infty} \frac{1}{10^{n!}}\right| \leq \frac{S}{q_k^{k+1}}.$$

By Theorem 5.1, we have that $\left|\alpha - \frac{p_k}{q_k}\right| \geq \frac{c(\alpha)}{q_k^n}$ which implies

$$\frac{S}{q_k^{k+1}} \geq \frac{c(\alpha)}{q_k^n}.$$

Thus, for $k$ large enough, we get a contradiction, so $\sum_{n=0}^{\infty} \frac{1}{10^{n!}}$ is transcendental. □

We now continue by showing that $e$ is transcendental which was first proved by Charles Hermite in 1873.

**Theorem 5.3.** *$e$ is transcendental.*

*Proof.* Let $f$ be a polynomial and let $k \in \mathbb{Z}, k \geq 0$. Then, using integration by parts, we have that

$$\int_0^k e^{-u} f(u)du = [-e^{-u} f(u)]\big|_0^k + \int_0^k e^{-u} f'(u)du.$$

Let

$$I(k, f) := \int_0^k e^{k-u} f(u) du.$$

Then,

$$\begin{aligned}
I(k, f) &= e^k \int_0^k e^{-u} f(u) du \\
&= e^k \left( [-e^{-u} f(u)]\Big|_0^k + \int_0^k e^{-u} f'(u) du \right) \\
&= e^k \left( -e^{-k} f(k) + e^0 f(0) + \int_0^k e^{-u} f'(u) du \right) \\
&= -e^{k-k} f(k) + e^k f(0) + e^k \int_0^k e^{-u} f'(u) du \\
&= e^k f(0) - f(k) + I(k, f').
\end{aligned}$$

Letting $m$ be the degree of $f$, then iterating this relation yields,

$$\begin{aligned}
I(k, f) &= e^k f(0) - f(k) + I(k, f') \\
&= e^k f(0) - f(k) + e^k f'(0) - f'(k) + I(k, f'') \\
&= e^k \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(k) + I(k, f^{(m+1)}) \\
&= e^k \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(k), \qquad (4)
\end{aligned}$$

since $I(k, f^{(m+1)}) = 0$. Let $F$ be the polynomial obtained from $f$ by replacing each coefficient of $f$ with its absolute value. Then,

$$\begin{aligned}
|I(k, f)| &= \left| \int_0^k e^{k-u} f(u) du \right| \\
&\leq \int_0^k |e^{k-u} f(u)| du \\
&\leq \int_0^k e^k F(u) du \\
&\leq k e^k F(k). \qquad (5)
\end{aligned}$$

We get the last inequality since all coefficients are positive. Now suppose $e$ is algebraic of degree $n$. Then, for some $a_i \in \mathbb{Z}$, with $a_0 a_n \neq 0$ we have,

$$a_n e^n + a_{n-1} e^{n-1} + \cdots + a_1 e + a_0 = 0. \qquad (6)$$

Consider

$$J := \sum_{k=0}^{n} a_k I(k, f)$$

with

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

such that $p > |a_0|$ is prime. Hence, using (4) and (6) we get,

$$\begin{aligned}
J &= \sum_{k=0}^{n} a_k I(k, f) \\
&= \sum_{k=0}^{n} a_k \left( e^k \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(k) \right) \\
&= \sum_{k=0}^{n} e^k \sum_{j=0}^{m} a_k f^{(j)}(0) - \sum_{k=0}^{n} \sum_{j=0}^{m} a_k f^{(j)}(k) \\
&= \sum_{j=0}^{m} f^{(j)}(0) \sum_{k=0}^{n} a_k e^k - \sum_{k=0}^{n} \sum_{j=0}^{m} a_k f^{(j)}(k) \\
&= - \sum_{k=0}^{n} \sum_{j=0}^{m} a_k f^{(j)}(k),
\end{aligned}$$

where $m = (n+1)p - 1$. Since $f$ has a zero of order $p$ at $1, 2, \ldots, n$ and a zero of order $p-1$ at 0, we can start the sum at $j = p-1$. For $j = p-1$, we have that

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

Now take $p > n$, then $f^{(p-1)}(0)$ is divisible by $(p-1)!$ but not by $p$. For $j \geq p$, $f^{(j)}(k)$ is divisible by $p!$ for $0 \leq k \leq n$. $J$ is divisible by $(p-1)!$ but not by $p$, and hence is nonzero. Thus, $(p-1)! \leq |J|$. On the other hand, (5) implies that,

$$\begin{aligned}
|J| &= \left| \sum_{k=0}^{n} a_k I(k, f) \right| \\
&\leq \sum_{k=0}^{n} |a_k| |I(k, f)| \\
&\leq \sum_{k=0}^{n} |a_k| k e^k F(k).
\end{aligned}$$

Let $A = \max |a_k|$, then $|a_k| \leq A$ for all $k$. So we have that

$$|J| \leq \sum_{k=0}^{n} |a_k| k e^k F(k)$$

$$\leq Ae^n \sum_{k=1}^{n} kF(k)$$

$$\leq Ae^n \sum_{k=1}^{n} k^p(k+1)^p \dots (k+n)^p$$

$$\leq Ae^n \sum_{k=1}^{n} n^p(n+1)^p \dots (2n)^p$$

$$\leq Ane^n((2n)!)^p.$$

However, one can show that $e^p \geq \frac{p^{p-1}}{(p-1)!}$, so,

$$e^{-p}p^{p-1} \leq (p-1)! \leq |J| \leq Ane^n((2n)!)^p.$$

Hence,

$$p^{p-1} \leq Ane^n e^p((2n)!)^p = BC^p$$

for $B, C$ independent of $p$, which is a contradiction for sufficiently large $p$. □

# 6 The Lindemann-Weierstrass Theorem and The Gelfond-Schneider Theroem

The generalized form of the Lindemann-Weierstrass Theorem was proven in 1885. We will state the theorem now, and take a look at the proof in Section 8.

**Theorem 6.1.** *Given distinct algebraic numbers $\alpha_1, \dots, \alpha_m$, the values $e^{\alpha_1}, \dots, e^{\alpha_m}$ are linearly independent over the field of algebraic numbers. Alternatively, given distinct algebraic numbers $\alpha_1, \dots, \alpha_m$, the equation $\sum_{j=1}^{m} a_j e^{\alpha_j} = 0$ is not possible for algebraic numbers $a_1, \dots, a_m$ where not all $a_i$ are zero.*

We will now look at some consequences of the Lindemann-Weierstrass theorem, beginning by giving an alternative proof that $e$ is transcendental.

**Theorem 6.2.** *Let $\alpha \neq 0$ be algebraic. Then, $e^\alpha$ is transcendental. In particular, $e$ is transcendental.*

*Proof.* Take $\alpha_1 = \alpha \neq 0$ and $\alpha_2 = 0$. By Theorem 6.1, $a_1e^{\alpha} + a_2e^0 = 0$ has no nonzero algebraic solution. If $e^{\alpha} = \beta$ is algebraic, then leting $a_1 = 1$ and $a_2 = -\beta$ yields a contradiction and so, $e^{\alpha}$ is transcendental. Furthermore, if we take $\alpha = 1$, it follows that $e$ is transcendental. □

**Theorem 6.3.** *$\pi$ is transcendental.*

*Proof.* Suppose $\pi$ is algebraic. By Theorems 3.6 and 3.7, we have that $\pi i$ is an algebraic number. Since $e^{\pi i} = -1$, by Theorem 6.2 it follows that $-1$ is transcendental, which is a contradiction. □

**Theorem 6.4.** *For an algebraic number $\alpha$, $\alpha \neq 0, 1$, $\ln \alpha$ is transcendental.*

*Proof.* Suppose $\ln \alpha$ is algebraic for $\alpha \neq 0, 1$. Then, by Theorem 6.2, we have that $e^{\ln \alpha}$ is transcendental. This is a contradiction since $e^{\ln \alpha} = \alpha$. □

We continue by taking a look some transcendental trigonometric functions.

**Theorem 6.5.** *$\sin \alpha$, $\cos \alpha$, and $\tan \alpha$ are transcendental for an algebraic number $\alpha$ where $\alpha \neq 0$.*

*Proof.* Note that $\{i\alpha, 2i\alpha, 0\}$ is a set of distinct algebraic numbers. Then by Theorem 6.1, we have that

$$a_1e^{i\alpha} + a_2e^{2i\alpha} + a_3e^0 \neq 0 \tag{7}$$

when at least on $a_i \neq 0$. Suppose $\sin \alpha$ is algebraic. Then by Theorems 3.6 and 3.7, $2i \sin \alpha$ is algebraic. We can rewrite $\sin \alpha$ so that $\sin \alpha = \frac{e^{i\alpha} - e^{-i\alpha}}{2i}$, which implies $2i \sin \alpha = e^{i\alpha} - e^{-i\alpha}$. Multiplying both sides by $e^{i\alpha}$ gives us $(2i \sin \alpha)e^{i\alpha} = e^{2i\alpha} - e^0$, which implies $(2i \sin \alpha)e^{i\alpha} - e^{2i\alpha} + e^0 = 0$. This contradicts (7), so $\sin \alpha$ is transcendental.

Now suppose $\cos \alpha$ is algebraic. Note, $\cos \alpha = \frac{e^{i\alpha} + e^{-i\alpha}}{2}$. This implies that $2 \cos \alpha = e^{i\alpha} + e^{-i\alpha}$. Multiplying both sides by $e^{i\alpha}$ gives us $(2 \cos \alpha)e^{i\alpha} =$

$e^{2i\alpha} + e^0$ and so $(2\cos\alpha)e^{i\alpha} - e^{2i\alpha} - e^0 = 0$. This also contradicts (7), so $\cos\alpha$ is transcendental.

Finally, suppose $\tan\alpha$ is algebraic. Then by Theorem 3.7, $\cos^2\alpha = \frac{1}{\tan^2\alpha+1}$ is algebraic. By Theorem 3.12, it follows that $\cos\alpha$ is algebraic, which is a contradiction. □

**Theorem 6.6.** *Let $\alpha$ be the solution to $x = \cos x$. Then $\alpha$ is transcendental.*

*Proof.* Suppose $\alpha$ is algebraic. Since $\alpha \neq 0$, by Theorem 6.5, $\cos\alpha$ is transcendental. But then $\alpha = \cos\alpha$ is transcendental, a contradiction. □

Hilbert's seventh problem is one of David Hilbert's 23 problems proposed in 1900. This problem was independently solved by Gelfond and Schneider in 1934. We will state this theorem without proof.

**Theorem 6.7.** *Let $\alpha$ and $\beta$ be algebraic numbers with $\alpha \neq 0, \alpha \neq 1$ and $\beta \notin \mathbb{Q}$. Then $\alpha^\beta$ is transcendental.*

The Gelfond-Schneider Theorem answers Hilbert's seventh problem and from this theorem, we can conclude several numbers that are transcendental. Note that 2 and $\sqrt{2}$ are algebraic (by Theorem 2.2) and $\sqrt{2} \notin \mathbb{Q}$. It follows directly from the Gelfond-Schneider Theorem that $2^{\sqrt{2}}$ and $\sqrt{2}^{\sqrt{2}}$ are transcendental. We can also see that $i^i$ is transcendental since $i$ is algebraic (by Theorem 3.6) and $i \notin \mathbb{Q}$.

The theorem can also be used to show that $e^\pi$ is transcendental.

**Theorem 6.8.** *$e^\pi$ is transcendental.*

*Proof.* We can see that $e^\pi = (e^{i\pi})^{-i} = (-1)^{-i}$. Then, by Theorem 6.7, since $-1$ and $-i$ are algebraic and $-i \notin \mathbb{Q}$, $e^\pi$ is transcendental. □

**Theorem 6.9.** *Let $\alpha, \beta$ be nonzero algebraic numbers with $\beta \neq 1$ and suppose $\frac{\log\alpha}{\log\beta}$ is not rational. Then $\frac{\log\alpha}{\log\beta}$ is transcendental.*

*Proof.* Suppose $\frac{\log \alpha}{\log \beta}$ is algebraic. Let $\gamma = \frac{\log \alpha}{\log \beta}$, so $\beta^\gamma = \alpha$. Then by Theorem 6.7, $\alpha$ is transcendental, a contradiction. $\square$

# 7 Open Problems

In general, it is difficult to prove that many numbers are transcendental. There are several numbers we have not yet been able to be transcendental, but we think they are. For example, $\pi e$, $\pi + e$, $\frac{\pi}{e}$, $\pi^\pi$, $e^e$, $\pi^e$, $\pi^{\sqrt{2}}$, and Euler's gamma constant have not yet been proven to be transcendental. In addition, none of these numbers have even been proven to be irrational.

We also have $\zeta(3)$, where $\zeta(s)$ is the Riemann zeta function. This number was proved to be irrational by Apéry in 1978, but is not yet proven to be transcendental. Likewise, $\zeta(n)$ where $n \geq 5$ and odd, are suspected to be transcendental, however, these numbers have not yet been proven to be irrational either.

As mentioned, we do not know if $\pi e$ and $\pi + e$ are transcendental, but we can show that at least one of them is.

**Theorem 7.1.** *At least one of $\pi e$ and $\pi + e$ is transcendental.*

*Proof.* Suppose not. Then both $\pi e$ and $\pi + e$ are algebraic. We look at the following equation,

$$
\begin{aligned}
(\pi + e)^2 - 4\pi e &= \pi^2 - 2\pi e + e^2 \\
&= (\pi - e)^2.
\end{aligned}
$$

Thus, $(\pi - e)^2$ is algebraic, and so by Theorem 3.12, $\pi - e$ is algebraic. Then, by Theorem 3.7, we have that $\frac{1}{2}[(\pi + e) + (\pi - e)] = \pi$ is algebraic. However, this contradicts Theorem 6.3, so at least one of $\pi e$ and $\pi + e$ is transcendental. $\square$

# 8 Proof of the Lindemann-Weierstrass Theorem

In this section, we will work towards the proof of the Lindemann-Weierstrass Theorem stated in Section 6 (see Theorem 6.1).

In the following subsections we will go through some background results. We state most of these results without proof. We will prove a special case of the Lindemann-Weierstrass Theorem in Subsection 8.3 and in 8.4, we show that Theorem 6.1 can be deduced from this special case.

## 8.1 Algebraic Number Fields Preliminaries

This section is a summary of some results we will assume regarding algebraic numbers and algebraic number fields, which we introduced just prior to Lemma 3.9. Proofs for these results can be found in [1] and [4]

Given algebraic numbers $\alpha_1, \ldots, \alpha_k$, let $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ be the intersection of all subfields of $\mathbb{C}$ containing $\mathbb{Q}$ and each $\alpha_i$. By the Theorem of the Primitive Element, there exits an algebraic number $\theta$ such that $\mathbb{Q}(\alpha_1, \ldots, \alpha_k) = \mathbb{Q}(\theta)$.

**Definition 8.1.** *If $f$ is the minimal polynomial of $\theta$, then the roots $\theta^{(1)}, \ldots, \theta^{(n)}$ of $f$ are called the* conjugates *of $\theta$ (we usually take $\theta^{(1)} = \theta$). $\mathbb{Q}(\theta^{(i)})$ is called a* conjugate field *to $\mathbb{Q}(\theta)$.*

**Definition 8.2.** *If we have $\mathbb{Q}(\theta) = \mathbb{Q}(\theta^{(i)})$ for each $i$, then $\mathbb{Q}(\theta)$ is called a* normal *extension of $\mathbb{Q}$.*

Given algebraic numbers $\alpha_1, \ldots, \alpha_k$, one can show that there exists an algebraic number $\theta$ such that $\mathbb{Q}(\theta)$ is normal and contains $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$.

Let $\gamma \in \mathbb{Q}(\theta)$ where $\gamma = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}$. We define the $i^{\text{th}}$ conjugate of $\gamma$ to be $\gamma^{(i)} = a_0 + a_1\theta^{(i)} + \cdots + a_{n-1}(\theta^{(i)})^{n-1}$. The following is

Lemma 9.8 in [3]. We will state this without proof.

**Lemma 8.3.** *Let $\mathbb{Q}(\theta)$ be a normal algebraic extension of degree $n$ over $\mathbb{Q}$. Then any element $\gamma$ of $\mathbb{Q}(\theta)$ and its conjugates over $\mathbb{Q}(\theta)$ are roots of degree $n$ polynomial with integer coefficients.*

Last, we will use the following lemma which is Lemma 9.9 in [3].

**Lemma 8.4.** *Let*

$$f(x) = \sum_{j=1}^{m} a_j x^{\alpha_j} \quad \text{and} \quad g(x) = \sum_{j=1}^{r} b_j x^{\beta_j},$$

*where coefficients $a_j$ and $b_j$ are nonzero complex numbers and $\alpha_j$ and $\beta_j$ are distinct algebraic numbers. Then when like terms are collected in $f(x)g(x)$, we have at least one nonzero coefficient.*

*Proof.* By earlier comments, we know that there exists some $\theta$ where $\mathbb{Q}(\theta)$ is normal and contains all $\alpha_j$ and $\beta_j$. If we take $n$ to be the degree of $\mathbb{Q}(\theta)$, then for each $\alpha_j$, there exists unique $r_{ij} \in \mathbb{Q}$ with

$$\alpha_j = \sum_{i=0}^{n-1} r_{ij} \theta^i.$$

We can order the $\alpha_j$ in the following manner: $\alpha_j$ precedes $\alpha_k$ if and only if the first nonzero term of $r_{0j} - r_{0k}, r_{1j} - r_{1k}, \ldots$ is positive. The same can be done with the $\beta_j$. Now, we can relabel the $\alpha_j$ and $\beta_j$ so that $\alpha_1$ is the first among the $\alpha_j$ and $\beta_1$ is the first among the $\beta_j$ with respect to this ordering. Thus, $\alpha_1 + \beta_1$ will be the first of all sums $\alpha_j + \beta_k$ with respect to this ordering. So when we expand $f(x)g(x)$, the term given by $a_1 b_1 x^{\alpha_1 + \beta_1}$ will have a unique exponent, and hence cannot be cancelled by any other terms in the sum. $\square$

## 8.2 Symmetric Polynomial Preliminaries

We will also require some standard results regarding symmetric polynomials, summarized in this section.

**Definition 8.5.** *We set*

$$(y - x_1)(y - x_2)\cdots(y - x_n) = y^n - \sigma_1 y^{n-1} + \sigma_2 y^{n-2} - \cdots + (-1)^n \sigma_n.$$

*Then, $\sigma_1, \ldots, \sigma_n$ are called the* elementary symmetric polynomials *in $x_1, \ldots, x_n$.*

**Definition 8.6.** *A polynomial is a* symmetric polynomial *if any permutation of its variables leaves the polynomial unchanged.*

The following lemma is a fundamental result on symmetric polynomials, given here without proof. It shows how symmetric polynomials can be expressed in terms of elementary symmetric polynomials.

**Lemma 8.7.** *If $f(x_1, \ldots, x_n)$ is a symmetric polynomial with coefficients in some field $F$, then we can write $f$ as a polynomial in the symmetric polynomials $\sigma_1, \ldots, \sigma_n$, with coefficients in $F$.*

The next two lemmas are needed in our proof of the Lindemann-Weierstrass Theorem. They are Theorem 9.2 and Lemma 9.3 in [3] and will be stated here without proof.

**Lemma 8.8.** *If we let $\beta_1, \ldots, \beta_n$ be the roots of the polynomial equation*

$$bx^n + c_1 x^{n-1} + \cdots + c_n = 0$$

*with rational coefficients, and $P(x_1, \ldots, x_n)$ be a symmetric polynomial in $x_1, \ldots, x_n$ with rational coefficients, then $P(\beta_1, \ldots, \beta_n)$ is a rational number. Moreover, if $P$ is a degree $m$ polynomial with integer coefficients, then $b^m P(\beta_1, \ldots, \beta_n)$ is an integer.*

**Lemma 8.9.** *Let $f_i(x)$ be a polynomial over a field $F$ where $1 \leq i \leq m$. For each $1 \leq j \leq q$, we can set*

$$P_j = f_1(x_j)y_1 + f_2(x_j)y_2 + \cdots + f_m(x_j)y_m,$$

*so that $P_j$ is a polynomial in $y_1, \ldots, y_m$ with coefficients $f_i(x_j)$. Then, the product of the $P_j$ has coefficients that are symmetric polynomials in $x_1, \ldots, x_q$, once like terms in $y$ have been collected.*

## 8.3 A Special Case

First, we will prove a special case of Theorem 6.1, then in the next subsection we use this case to prove the full Lindemann-Weierstrass Theorem.

**Theorem 8.10.** *Let $\alpha_1, \ldots, \alpha_m$ be distinct algebraic numbers. Then, $e^{\alpha_1}, \ldots, e^{\alpha_m}$ are linearly independent over $\mathbb{Q}$.*

*Proof.* We prove by contradiction. Suppose there are $a_i \in \mathbb{Q}$ that are not all zero with

$$\sum_{j=1}^{m} a_j e^{\alpha_j} = 0. \tag{8}$$

We may assume all $a_j$ are nonzero integers by discarding any term where $a_j = 0$, multiplying by an appropriate integer and relabelling. Using results from Section 8.1, we let $\theta$ be an algebraic number such that each $\alpha_j$ is in the normal extension $\mathbb{Q}(\theta)$. If we let the degree of $\mathbb{Q}(\theta)$ be $n$, then there are $r_{ij} \in \mathbb{Q}$ with

$$\alpha_j = \sum_{i=0}^{n-1} r_{ij}\theta^i$$

for each $j = 1, \ldots, m$. Then for $1 \leq k \leq n$, the $k^{\text{th}}$ conjugate of $\alpha_j$ is

$$\alpha_j^{(k)} = \sum_{i=0}^{n-1} r_{ij}(\theta^{(k)})^i$$

where $\theta^{(k)}$ is the $k^{\text{th}}$ conjugate of $\theta$ and $\theta^{(1)} = \theta$, and hence $\alpha_j^{(1)} = \alpha_j$. We claim that the $\alpha_j^{(k)}$ are distinct for a fixed $k$. To see this, suppose we have $\alpha_j^{(k)} = \alpha_\ell^{(k)}$ for $j \neq \ell$. It follows that

$$0 = \alpha_j^{(k)} - \alpha_\ell^{(k)} = \sum_{i=0}^{n-1}(r_{ij} - r_{i\ell})(\theta^{(k)})^i.$$

Since we have a minimal polynomial of degree $n$ for $\theta^{(k)}$ (the same polynomial for $\theta$), we must have that $r_{ij} = r_{i\ell}$ for each $i$. Thus,

$$\alpha_j = \sum_{i=0}^{n-1} r_{ij}\theta^i = \sum_{i=0}^{n-1} r_{i\ell}\theta^i = \alpha_\ell.$$

This is a contradiction since all the $\alpha_j$ are distinct.

We now consider the product

$$\prod_{k=1}^{n}\sum_{j=1}^{m} a_j e^{\alpha_j^{(k)}}.$$

Since the multiplying factor corresponding to $k = 1$ is equal to 0 by (8), the product is equal to 0. However, we can multiply out the product and collect like terms to get

$$\sum_{j=0}^{r} c_j e^{\beta_j} = 0 \tag{9}$$

where the $\beta_j$ are distinct. Since the $a_j$ are integers, the $c_j$ are integers as well. By applying Lemma 8.4 to the product $k$ times, one can see that at least one $c_j$ is nonzero. Without loss of generality, take $c_0 \neq 0$. Lastly, if we replace $\theta$ with a conjugate $\theta^{(i)}$ in the above, this would give us a permutation of the conjugates, and hence of the $\alpha_j^{(k)}$. Thus, the above product gives us a permutation of the factors and so the product remains unchanged. In (9), this permutation results in the $\beta_j$ being replaced by the conjugate $\beta_j^{(i)}$. So, by (9), we get

$$0 = \sum_{j=0}^{r} c_j e^{\beta_j^{(1)}} = \sum_{j=0}^{r} c_j e^{\beta_j^{(2)}} = \cdots = \sum_{j=0}^{r} c_j e^{\beta_j^{(n)}}. \tag{10}$$

The $\beta_j^{(i)}$ are distinct for any given $i$ since the $\beta_j^{(1)}$ are distinct.

We multiply the $i$th sum in (10) by $e^{-\beta_0^{(i)}}$ and set $\gamma_j^{(i)} = \beta_j^{(i)} - \beta_0^{(i)}$. Since the $\beta_j^{(i)}$ are distinct for any given $i$, we have that the $\gamma_j^{(i)}$ are nonzero for $j \geq 1$. This yields

$$0 = c_0 + \sum_{j=1}^{r} c_j e^{\gamma_j^{(1)}} = \cdots = c_0 + \sum_{j=1}^{r} c_j e^{\gamma_j^{(n)}} \tag{11}$$

By Lemma 8.3, we see that the conjugates $\gamma_j^{(1)}, \gamma_j^{(2)}, \ldots, \gamma_j^{(n)}$ are roots of a degree $n$ polynomial with integer coefficients. Write

$$g_j(z) = b_j \prod_{i=1}^{n}(z - \gamma_j^{(i)})$$

for each $1 \leq j \leq r$, taking $b_j$ to be a positive integer. Since the $\gamma_j^{(i)}$ are nonzero, we have that $g_j(0)$ is nonzero for all $j$.

Given a polynomial $f(z)$, define $F(z)$ to be the finite sum

$$F(z) = f(z) + f'(z) + f''(z) + \dots$$

Then we have

$$\begin{aligned}\frac{d}{dz}F(z)e^{-z} &= F'(z)e^{-z} - F(z)e^{-z} \\ &= -f(z)e^{-z}.\end{aligned}$$

This implies that

$$\begin{aligned}-e^b \int_0^b f(z)e^{-z}dz &= e^b \int_0^b \frac{d}{dz}F(z)e^{-z}dz \\ &= F(b) - F(0)e^b.\end{aligned}$$

If we replace $b$ by the $\gamma_j^{(i)}$, multiply each equation by $c_j$, and sum for all $1 \leq j \leq r$ and $1 \leq i \leq n$, we get

$$\sum_{j=1}^{r}\sum_{i=1}^{n} c_j F(\gamma_j^{(i)}) - F(0)\sum_{i=1}^{n}\sum_{j=1}^{r} c_j e^{\gamma_j^{(i)}} = -\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z)e^{-z}dz.$$

Each integral is taken along the straight line from 0 to $\gamma_j^{(i)}$. By (11) we have

$$-\sum_{i=1}^{n}\sum_{j=1}^{r} c_j e^{\gamma_j^{(i)}} = nc_0.$$

Thus, we have

$$\sum_{j=1}^{r} c_j \sum_{i=1}^{n} F(\gamma_j^{(i)}) + nc_0F(0) = -\sum_{j=1}^{r}\sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z)e^{-z}dz. \qquad (12)$$

Next, we will select a polynomial $f(z)$, that is dependent on a prime $p$ to be chosen later. Then, we will show that the left side of (12) is a nonzero integer for a large enough $p$, while the right side can be made arbitrarily small for a large enough $p$. This will give us a contradiction to complete the proof.

We set

$$f(z) = \frac{(b_1 \cdots b_r)^{prn}}{(p-1)!}(z^{p-1})\left(\prod_{j=1}^{r} g_j(z)\right)^p \qquad (13)$$

where $p$ is a prime to be chosen later. We can see that $f(0) = 0$ and for $1 \leq k \leq p-2$, $f^{(k)}(0) = 0$. We also have that $f^{(p-1)}(0) = (b_1 \cdots b_r)^{prn} \prod_{j=1}^{r}(g_j(0))^p$. We have already seen that the $g_j(0)$ are nonzero integers and the $b_j$ are positive integers, so we have that $f^{(p-1)}(0)$ is also a nonzero integer. If we choose $p > b_j$ and $p > g_j(0)$ for each $j$, this implies that $p$ does not divide $f^{(p-1)}(0)$. Now, we will show that for $k \geq p$, $f^{(k)}(0)$ is an integer divisible by $p$. If we expanded $f(z)$ as a sum of powers of $z$, then the coefficients of a power of $z$ in a term of $f^{(k)}(z)$ will contain $k$ consecutive integers as a factor. Since $k \geq p$, the product will be divisible by $p!$. Thus, the $(p-1)!$ in the denominator will cancel and yield an integer coefficient divisible by $p$. We have,

$$f^{(k)}(z) = p(b_1 \cdots b_r)^{prn} G_k(z) \tag{14}$$

where $G_k(z)$ is a polynomial with integer coefficients with a degree of at most $prn-1$ (since the degree of each of the $r$ factors $g_j(z)$ is in $n$, and we have differentiated at least $p$ times). For $k \geq p$, $f^{(k)}(0)$ is an integer divisible by $p$. Using this and the fact that for $k \leq p-2$, $f^{(k)}(0) = 0$ and that $f^{(p-1)}(0)$ is a nonzero integer not divisible by $p$, we have that $F(0) = f(0)+f'(0)+f''(0)+\ldots$ is an integer that is not divisible by $p$. If we take $p > n$ and $p > c_0$, it can be seen that $p$ does not divide the second term in the left side of (12), $nc_0F(0)$.

We will now show that the first term on the left side of (12) is divisible by $p$. Recall that $g_j(z)$ has roots $\gamma_j^{(1)}, \ldots, \gamma_j^{(n)}$. Since $(g_j(z))^p$ is a factor of $f$ for each $j$, it follows that we have $f(\gamma_j^{(i)}) = 0$ and $f^{(k)}(\gamma_j^{(i)}) = 0$ for each $i$ and $j$ and for $k = 1, \ldots, p-1$. For $k \geq p$, by (14), we have that

$$\sum_{i=1}^{n} f^{(k)}(\gamma_j^{(i)}) = p(b_1 \cdots b_r)^{prn} \sum_{i=1}^{n} G_k(\gamma_j^{(i)}).$$

Since $\sum_{i=1}^{n} G_k(x_i)$ is a symmetric polynomial of degree at most $prn-1$ and is preceded by the factor $b_j^{prn}$, Lemma 8.8 implies that the above expression is an integer that is divisible by $p$. Thus,

$$\sum_{j+1}^{r} c_j \sum_{i=1}^{n} F(\gamma_j^{(i)})$$

is an integer that is divisible by $p$.

We have seen that $nc_0F(0)$ is an integer that is not divisible by a large enough $p$, from the previous result, we have that the left side of (12) is an integer not divisible by $p$. So (12) implies that

$$1 \leq \left| \sum_{j=1}^{r} \sum_{i=1}^{n} c_j e^{\gamma_j^{(i)}} \int_0^{\gamma_j^{(i)}} f(z) e^{-z} dz \right|. \tag{15}$$

Now, set $n_1 = \max_j |c_j|$, $m_2 = \max_{i,j} \left| e^{\gamma_j^{(i)}} \right|$, $m_3 = \max_{i,j} |\gamma_j^{(i)}|$, $m_4 = \max |e^{-z}|$ where $z$ is on the straight line between 0 and $\gamma_j^{(i)}$, and $m_5 = \max \left| \prod_{j=1}^{r} g_j(z) \right|$ for $z$ on the same line. Then, $\max |z^{p-1}| = m_3^{p-1}$ for $z$ on the same line again. Note that each $m_i$ is independent of $p$. Using (13) and these bounds on (15), we get

$$\begin{aligned} 1 &\leq rnm_1m_2m_3m_4 \frac{(b_1 \cdots b_r)^{prn}}{(p-1)!} m_3^{p-1} m_5^p \\ &= rnm_1m_3m_4 \frac{((b_1 \cdots b_r)^{rn} m_3 m_5)^p}{(p-1)!} \\ &= \frac{AC^p}{(p-1)!} \end{aligned}$$

where $A$ and $C$ are nonnegative and independent of $p$. Since the limit of $\frac{C^p}{(p-1)!}$ is 0 as $p \to \infty$, for $p$ large enough, we get $\frac{AC^p}{(p-1)!} < 1$, which is a contradiction. □

## 8.4 Proof of the Lindemann-Weierstrass Theorem

We may now prove the Lindemann-Weierstrass Theorem. That is, for distinct algebraic numbers $\alpha_1, \ldots, \alpha_m$, we will show that $e^{\alpha_1}, \ldots, e^{\alpha_m}$ are linearly independent over the field of algebraic numbers.

*Proof.* Suppose we have algebraic numbers $a_i$ not all zero where

$$\sum_{j=1}^{m} a_j e^{\alpha_j} = 0. \tag{16}$$

If we remove any terms where $a_j = 0$, we can assume that all $a_j$ are nonzero. By the results from Section 8.1, we get an algebraic number $\theta$ such that each $a_j$ is in the normal extension $\mathbb{Q}(\theta)$, which implies that each of the conjugates

$a_j^{(i)}$ are also in $\mathbb{Q}(\theta)$. Now, let the degree of $\mathbb{Q}(\theta)$ over $\mathbb{Q}$ be $q$ and consider the product

$$\prod_{i=1}^{q}(a_1^{(i)}e^{\alpha_1} + a_2^{(i)}e^{\alpha_2} + \cdots + a_m^{(i)}e^{\alpha_m}),$$

equal to 0 by (16). Since each coefficient $a_j^{(i)}$ can be written as a linear combination of powers of $\theta^{(i)}$, we can view the $a_j^{(i)}$ as polynomials in $\theta^{(i)}$. Using Lemma 8.9, we can deduce that by multiplying out the product and collecting like terms, the coefficients are symmetric polynomials in $\theta^{(1)}, \ldots, \theta^{(q)}$. By Lemma 8.8, it follows that the coefficients are in $\mathbb{Q}$. By Lemma 8.4, we get that not all the coefficients are zero. Thus, we get an equation of the form given in (8), which contradicts Theorem 8.10, as we showed this is impossible. □

# References


[1] M. R. Murty and J. Esmonde, *Problems in Algebraic Number Theory, 2nd edition*, Springer-Verlag, New York, 2006.

[2] M. R. Murty and P. Rath, *Transcendental Numbers*, Springer, New York, 2014.

[3] I. Niven, *Irrational Numbers*, The Carus Mathematical Monographs, no. 11, The Mathematical Association of America, 1956.

[4] H. Pollard, *The Theory of Algebraic Numbers*, The Carus Mathematical Monographs, no. 9, The Mathematical Association of America, 1950.

[5] *Proof that e is Irrational - Mathonline.* (n.d.). Retrieved July 31, 2020, from http://mathonline.wikidot.com/proof-that-e-is-irrational

[6] *Proof that Pi is Irrational - Mathonline.* (n.d.). Retrieved July 31, 2020, from http://mathonline.wikidot.com/proof-that-pi-is-irrational

[7] *Homework 2 Solutions.* (n.d.). Retrieved July 31, 2020, from http://faculty.bard.edu/belk/math351/Homework2Solutions.pdf