Summer Number Theory Seminar 2001
Algebraic and Transcendental Numbers

Eric Patterson and Vladislav Shchogolev [*]

[*] Research was supported by Columbia University VIGRE Fellowship and advised by graduate John Zuehlke.

Contents

Abstract

This paper reviews the topics covered in the 2001 Summer Number Theory Seminar. All definitions and theorems will receive attention, but most proofs will be excluded or abbreviated. Examples will be given where the authors think necessary or interesting. This paper will focus on algebraic and transcendental number theory, but many detours into other areas of math will be made.

1 Unique Factorization

We begin by defining prime numbers.

Definition 1.1. The *prime numbers* are those numbers m which are different from 0 and ± 1 and which possess no factors other than ± 1 and $\pm m$.

With this definition, we can now state our goal for this section: establish that every integer can be factored in one and only one way, apart from order and sign, as the product of prime numbers (i.e., the Fundamental Theorem of Arithmetic). In the following discussion, we will assume that every collection, finite or infinite, of non-negative integers contains a smallest element.

Theorem 1.2. *If a, $b \in \mathbb{Z}$, $b > 0$, then $\exists$ integers q and r such that*

$$a = bq + r \qquad\qquad 0 \leq r < b.$$

The integers q and r are unique.

The proof follows from choosing q such that $q \leq \frac{a}{b}$ and $q + 1 > \frac{a}{b}$. The result is shown to be unique by assuming two different solutions, which leads to a contradiction of our choice of r. For instance, if $a = 12$ and $b = 5$, then we would choose $q = 2$, which gives $r = 2$.

$$12 = 5 \cdot 2 + 2$$

Definition 1.3. Two integers a and b are *relatively prime* if they share no factors except ± 1. We express this as $(a, b) = 1$.

For example, $(12, 5) = 1$.

Theorem 1.4. *If $(a, b) = 1$, then $\exists$ s, $t \in \mathbb{Z}$ for which $as + bt = 1$.*

Continuing with the same values of a and b, we can satisfy the above theorem with $s = -2$ and $t = 5$:

$$12 \cdot -2 + 5 \cdot 5 = 1.$$

We get the same result for $s = 7$ and $t = 17$, so the theorem clearly does not claim a unique result. The proof follows from a creative use of the divisibility theorem and the assumption about the existence of a smallest integer in a set of non-negative integers.

Definition 1.5. An integer m *divides* an integer n, written $m \mid n$, if there exists an integer q such that $n = qm$. Equivalently, m is a *factor* of n. Otherwise, m does not divide and is not a factor of n, written $m \nmid n$.

Theorem 1.6. *If p is a prime number and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. We choose to include the proof because it shows an interesting use of Theorem 1.4. If $p \mid a$, we are done, so consider instead that $p \nmid a \Rightarrow (p, a) = 1$. Thus, we can apply the previous theorem using integers l and m.

$$\begin{aligned} lp + ma &= 1 \\ lbp + mab &= b \\ p \mid ab \Rightarrow ab &= pq \\ lbp + mpq &= b \\ p(lb + mq) &= b \\ p &\mid b. \end{aligned}$$

□

For instance, if $a = 12$ and $b = 5$, $ab = 60$. The primes $2, 3, 5 \mid 60$, and each one also divides a or b. A repeated application of this theorem gives a useful corollary.

Corollary 1.7. *If a prime number p divides a product $a_1 a_2 \cdots a_n$ of integers, then it divides at least one a_i.*

We will provide a formal definition of *units* in Section 20. For now, by a unit we mean an element that divides 1; for the rational integers, the units are ± 1. Finally, we arrive at our goal:

Theorem 1.8 (Fundamental Theorem of Arithmetic). *Each integer not zero or a unit can be factored into the product of primes which are uniquely determined to within order and multiplication by units.*

We will provide a brief sketch of the proof because this theorem is rather significant. If our integer is prime, we are done. If it is not prime, we must be able to factor it into two integers, not units. If these factors are primes, we are done. Otherwise, continue the process. This process must terminate because a finite integer cannot be the product of an arbitrarily large number of integers all greater than one. If there are two such factorizations, we can conclude that each factor must appear in each factorization to within multiplication by units because the factors are prime.

2 Gaussian Integers

We now define a new class of integers and ask the same questions we have asked about integers. Consider the class G of Gaussian integers defined as:

$$G = \{\alpha = a + bi \,|\, a, b \in \mathbb{Z}\}.$$

For this class of numbers, we say that α divides β if there is a number $\gamma \in G$ such that $\beta = \alpha\gamma$. An element of G is a unit if it divides 1, and therefore every element of G. A number π in G is *prime* if it is not zero or a unit and if every factorization $\pi = \alpha\beta$ means that α or β is a unit.

With this terminology we can ask, do Gaussian integers have a unique factorization? To answer this question, we must first define the norm:

Definition 2.1. The norm $N(\alpha)$ of a Gaussian integer $\alpha = a + bi$ is defined as:

$$N\alpha = \alpha\overline{\alpha} = |\alpha|^2 = a^2 + b^2$$

We identify five important properties of the norm:

1. If α is in $\mathbb{Z}$ as well as in G, then $N\alpha = \alpha^2$
2. N$(\alpha\beta) = N\alpha\ N\beta$
3. $N\alpha = 1$ if and only if α is a unit.
4. $$N\alpha = \begin{cases} 0 & \text{if } \alpha = 0, \\ 1 & \text{if } \alpha = \pm 1 \text{ or } \pm\text{i}, \\ > 1 & \text{otherwise.} \end{cases}$$
5. If Nα is prime in $\mathbb{Z}$, then α is prime in G.

Theorem 2.2. *If α and β are Gaussian integers, $\beta \neq 0$, then $\exists$ integers π and ρ such that*

$$\alpha = \pi\beta + \rho, \qquad N\rho < N\beta$$

In proving this theorem we choose integers s and t such that

$$|A - s| \leq \frac{1}{2}, \qquad |B - t| \leq \frac{1}{2} \qquad \text{where } \alpha/\beta = A + Bi$$

Then $\pi = s + ti, \rho = \alpha - \pi\beta$ satisfies the theorem.

Theorem 2.3. *If π is a prime and $\pi|\alpha\beta$, then $\pi|\alpha$ or $\pi|\beta$.*

To prove this theorem we can proceed much as in the case of rational integers. By the same analog, the Gaussian version of the fundamental theorem of arithmetic follows from this theorem. In other words, Gaussian integers do have a unique factorization, within order and units.

3 Groups, Rings, and Fields

Before we address the topic of algebraic numbers, it will be useful to define the terms group, ring, and field.

Definition 3.1. A *group* is an ordered pair $\langle G, \circ \rangle$ where G is a non-empty set and $\circ$ is a binary operation on G satisfying the following axioms for $a,\ b,\ c \in G$:

$$
\begin{aligned}
&(a \circ b) \circ c = a \circ (b \circ c) && \text{(Associativity)} && (1)\\
&\exists\ e \in G \text{ such that } \forall\ a \in G, a \circ e = a && \text{(Existence of a Right Identity)} && (2)\\
&\forall\ a \in G\ \exists\ a' \in G \text{ such that } a \circ a' = e && \text{(Existence of a Right Inverse)} && (3)
\end{aligned}
$$

For formal purposes, we will define a binary operation.

Definition 3.2. Let A be a non-empty set. A mapping $\rho : A \times A \to A$ is called a *binary operation* on A.

Although a group is not necessarily commutative, we can show that the right identity and the right inverse are commutative. We refer to a commutative identity element as simply an identity element or a neutral element. Similarly, we refer to a commutative inverse element as simply an inverse.

Theorem 3.3. *Each right identity element of a group G is an identity element. Furthermore, this identity element is unique.*

Proof. We are given that $a \circ e = a$, and we must show $e \circ a = a\ \forall\ a \in G$. We also know that a has a right inverse, say b. This right inverse is also in G, so it too must have a right inverse.

$$
\begin{aligned}
a \circ b &= e\\
b \circ c &= e
\end{aligned}
$$

$$
\begin{aligned}
e \circ a &= (e \circ a) \circ e && \text{(Axiom 2)}\\
&= e \circ (a \circ e) && \text{(Axiom 1)}\\
&= e \circ \big(a \circ (b \circ c)\big) && \text{(Axiom 3)}\\
&= e \circ \big((a \circ b) \circ c\big) && \text{(Axiom 1)}\\
&= e \circ (e \circ c) && \text{(Axiom 3)}\\
&= (e \circ e) \circ c && \text{(Axiom 1)}\\
&= e \circ c && \text{(Axiom 2)}\\
&= (a \circ b) \circ c && \text{(Axiom 3)}\\
&= a \circ (b \circ c) && \text{(Axiom 1)}\\
&= a \circ e && \text{(Axiom 3)}\\
&= a && \text{(Axiom 2)}
\end{aligned}
$$

Now we must show that e is unique. Suppose there exists another identity element $f \in G$. Then clearly $f = f \circ e = e$. □

Theorem 3.4. *Each right inverse b of an element $a \in G$ is an inverse of a. Furthermore, each element $a \in G$ has one and only one inverse.*

Proof. We know that $a \circ b = e$; we must show that $b \circ a = e$. We know that b also has a right inverse, call it c.

$$\begin{aligned}
b \circ a &= (b \circ a) \circ e && \text{(Axiom 2)} \\
&= (b \circ a) \circ (b \circ c) && \text{(Axiom 3)} \\
&= \big(b \circ (a \circ b)\big) \circ c && \text{(Axiom 1)} \\
&= (b \circ e) \circ c && \text{(Axiom 3)} \\
&= b \circ c && \text{(Axiom 2)} \\
&= e && \text{(Axiom 3)}
\end{aligned}$$

To show uniqueness, we suppose $d \in G$ is another right inverse of a.

$$d = e \circ d = (b \circ a) \circ d = b \circ (a \circ d) = b \circ e = b.$$

□

Now we proceed with our other definitions.

Definition 3.5. Let R be any non-empty set with binary operations $+$ and $\cdot$. A *ring* is an ordered triple $\langle R, +, \cdot \rangle$ satisfying the following axioms for $a,\ b,\ c \in R$:

$$\begin{aligned}
&a + b = b + a && \text{(Commutativity under Addition)} && (4) \\
&(a + b) + c = a + (b + c) && \text{(Associativity under Addition)} && (5) \\
&\exists\ z \in R \ni z + a = a + z = a && \text{(Existence of an Additive Identity)} && (6) \\
&\forall\ a \in R\ \exists\ a^* \ni a + a^* = a^* + a = z && \text{(Existence of an Additive Inverse)} && (7) \\
&(a \cdot b) \cdot c = a \cdot (b \cdot c) && \text{(Associativity under Multiplication)} && (8) \\
&a \cdot (b + c) = a \cdot b + a \cdot c && \text{(Distributivity)} && (9)
\end{aligned}$$

The operations $+$ and $\cdot$ are not necessarily addition and multiplication as conventional notation might suggest, but we have provided names for the axioms assuming those operations. Next we look at a specific type of ring.

Definition 3.6. A *field* is a ring $\langle F, +, \cdot \rangle$ satisfying these additional axioms for $a,\ b \in F$ and z the additive identity element defined in Definition 3.5:

$$\begin{aligned}
&a \cdot b = z \Longrightarrow a = z \text{ or } b = z && \text{(Zero Divisor Law)} && (10) \\
&a \cdot b = b \cdot a && \text{(Commutativity under Multiplication)} && (11) \\
&\exists\ e \in F \ni e \cdot a = a \cdot e = a && \text{(Existence of a Multiplicative Identity)} && (12) \\
&\forall\ a \neq z,\ \exists\ a' \in F \ni a \cdot a' = a' \cdot a = e && \text{(Existence of a Multiplicative Inverse)} && (13)
\end{aligned}$$

As examples, the integers form a ring, and the rational numbers form a field. We shall soon discover other groups, rings, and fields.

4 Rational and Gaussian Primes

It is a simple proof that there are an infinite number of rational primes. Suppose there is a finite number of primes $p_1, ..., p_n$. The number $N = 1+p_1 \cdots p_n$ is not divisible by any of the p_i. Then any prime factor of N would be different from any of the p_i. This shows that, given any finite set of primes, we can generate infinitely many new primes. Therefore, as long as there is at least one prime integer, we can show that there is an infinite number of primes. Since 2 is prime in $\mathbb{Z}$, there are an infinite number of rational primes.

A similar proof will show that there are an infinite number of primes in G (the set of Gaussian primes), since G has at least one prime (3 is prime in G).

5 Congruences

Here we deal only with rational integers. Let m be a non-zero integer.

Two integers are said to be *congruent modulo m*:

$$a \equiv b(mod\, m) \qquad \text{or} \qquad a \equiv b(m),$$

if $m|(a-b)$. *Two integers are congruent modulo m if and only if they leave the same remainder on division by* $|m|$.

Here are a few important properties of congruences:

1. If $a \equiv b(m)$, then $b \equiv a(m)$
2. If $a \equiv b(m)$ and $b \equiv c(m)$, then $a \equiv c(m)$
3. If $k \in \mathbb{Z}$ and $a \equiv b(m)$, then $ka \equiv kb(m)$
4. If $a_i \equiv b_i(m)$ for $i = 1, 2, ..., n$, then
$$a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n(m),$$
$$a_1 b_1 \cdots a_n \equiv b_1 b_2 \cdots b_n(m)$$
5. If $ka \equiv kb(m)$, then $a \equiv b(m/d)$ where $d = (k, m)$

Definition 5.1. A *complete residue system* modulo m is any set of integers such that every integer is congruent to exactly one element in the set modulo m.

Consequently, any set of m integers is a complete residue system modulo m if no two of the integers are congruent to each other modulo m.

Theorem 5.2. *If $a_1, a_2, ..., a_m$ form a complete residue system modulo m, and if $(a, m) = 1$, then $aa_1, aa_2, ..., aa_m$ also form such a system.*

Theorem 5.3 (Fermat). *If p is a prime and $(a, p) = 1$, then $a^{p-1} \equiv 1(p)$.*

Corollary 5.4. *If p is a prime and $(a,p)=1$, then $a^p \equiv a(p)$.*

Theorem 5.5 (Wilson). *If p is a prime, then $(p-1)! \equiv -1(p)$.*

Theorem 5.6. *If p is a prime of the form $4m+1$, then $p \mid (n^2+1)$, where $n=(2m)!$.*

Theorem 5.7. *If p is a prime and a and b are integers, then*

$$a^p + b^p \equiv (a+b)^p \qquad (mod\, p)$$

6 Polynomials Over a Field

Definition 6.1. A *polynomial of degree n*, $n \geq 0$, over a field F is an expression of the form

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

where $a_i \in F$ and $a_n \neq 0$.

By convention, 0 is a polynomial of no degree (also called identically zero), while a constant not zero is a polynomial with $n=0$. The set of polynomials is denoted by $F[x]$. The sum or product of two polynomials is also a polynomial. A polynomial $p(x) \mid q(x)$ in $F[x]$ if $\exists\ r(x) \in F[x]$ such that $q(x) = p(x)r(x)$.

Theorem 6.2 (Fundamental Theorem of Algebra). *Every polynomial p(x) of degree $n \geq 1$ can be factored uniquely into the form*

$$p(x) = a_n(x-r_1)(x-r_2)\cdots(x-r_n) \qquad\qquad r_i \in \mathbb{C}$$

This theorem is proved in analysis. The values $r_1, ..., r_n$ are called the *roots* of $p(x)$. Two polynomials are said to be *relatively prime* if they share no common factors. A polynomial is *monic* if the leading coefficient a_n is 1. The leading coefficient plays the part of the unit and does not affect factorization.

Definition 6.3. A polynomial $p(x)$ is said to be *irreducible* if it cannot be factored into the product of two or more polynomials, each of which have degree less than $p(x)$ and are themselves polynomials over F.

The following three theorems closely parallel Theorems 1.2, 1.4 and 1.6 for rational integers.

Theorem 6.4. *Let $f(x)$ and $g(x) \neq 0$ be polynomials over F. Then there are polynomials $q(x)$ and $r(x)$ over F such that*

$$f(x) = q(x)g(x) + r(x)$$

where $r(x)=0$ or $r(x)$ has degree less than $g(x)$.

Theorem 6.5. *Let $f(x)$ and $g(x)$ be non-zero, relatively prime polynomials over F. Then,*

$$\exists\, s(x), t(x) \in F[x] \ \ni\ 1 = s(x)f(x) + t(x)g(x)$$

Note that this theorem is a special case of Hilbert's Nullstellensatz, which deals with a sum of arbitrarily many product pairs.

Theorem 6.6. *Let $p(x), f(x), g(x)$ be polynomials over F, $p(x)$ irreducible, $p(x) \mid f(x)g(x)$ over F, then $p(x)$ divides $f(x)$ or $g(x)$.*

7 The Eisenstein Irreducibility Criterion

Definition 7.1. A polynomial $p(x) \in \mathbb{Z}[x]$ is *primitive* if the coefficients have no common factors beside ± 1.

Theorem 7.2 (Gauss' Lemma). *The product of primitive polynomials is primitive.*

Note that any polynomial $f(x) \neq 0$ can be uniquely written in the form $c_f f^*(x)$ where f^* is primitive and c_f is a positive rational number.

Theorem 7.3. *If a polynomial $p(x) \in \mathbb{Z}[x]$ can be factored over $\mathbb{Q}$, it can be factored into polynomials in $\mathbb{Z}[x]$.*

Theorem 7.4 (Eisenstein's irreducibility criterion). *Let p be a prime and $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ such that*

$$p \nmid a_n,\ p^2 \nmid a_0; \qquad p \mid a_i, i = 0, 1, ..., n-1$$

Then $f(x)$ is irreducible over $\mathbb{R}$.

Let p be a prime. A polynomial of the form

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$$

is called *cyclotomic*. Substituting $x + 1$ for x, we can show that this polynomial is irreducible by the Eisenstein criterion. The same technique can be used to show that

$$\frac{x^{p^2} - 1}{x^p - 1} = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1$$

is irreducible.

8 Symmetric Polynomials

Consider the independent variables $x_1, x_2, \ldots, x_n$. A polynomial in $x_1, x_2, \ldots, x_n$ over the field F is a finite sum of the form

$$g(x_1, x_2, \ldots, x_n) = \sum_{i_1, i_2, \ldots, i_n} a_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

where $a_{i_1, i_2, \ldots, i_n} \in F$ and the i_j's are positive integers.

Definition 8.1. A polynomial is *symmetric* if it is unchanged by any permutation of the variables.

For example, the following polynomials are symmetric:

$$x_1^2 + x_2^2 + x_1x_2$$
$$x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 + 6x_1x_2x_3.$$

A very useful polynomial when dealing with symmetric polynomials is the following function of one variable z:

$$\begin{aligned} f(z) &= (z - x_1)(z - x_2)\cdots(z - x_n) \\ &= z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \cdots (-1)^n \sigma_n \end{aligned}$$

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + \cdots + x_n \\ \sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + x_2x_4 + \cdots + x_{n-1}x_n \\ &\vdots \\ \sigma_n &= x_1x_2\cdots x_n \end{aligned}$$

The σ_i are called the *elementary symmetric functions* in $x_1, x_2, \ldots, x_n$.

Theorem 8.2. *Every symmetric polynomial in $x_1, x_2, \ldots, x_n$ over a field F can be written as a polynomial over F in the elementary symmetric functions $\sigma_1, \sigma_2, \ldots, \sigma_n$. The result holds for polynomials with integer coefficients as well.*

The theorem holds for integer coefficients because the proof only uses properties of rings. The proof begins by separating the polynomial into homogeneous polynomials and then defining a method for ordering the terms of the polynomial. For the highest term of the polynomial, there is a specific term of the elementary symmetric polynomials which will cancel the highest term in the original polynomial, leaving a "lower" degree polynomial. The process repeats itself, and we get the desired result.

Theorem 8.3. *Let $f(x)$ be a polynomial of degree n over F with roots $r_1, r_2, \ldots, r_n$. Let $p(x_1, x_2, \ldots, x_n)$ be a symmetric polynomial over F. Then $p(r_1, r_2, \ldots, r_n)$ is an element of F.*

Factoring $f(x)$ into monic, first degree polynomials reveals that the elementary symmetric functions evaluated at $r_1, r_2, \ldots, r_n$ must be in F. Thus, the conclusion follows from the application of Theorem 8.2.

Corollary 8.4. *Let $f(x)$ and $g(x)$ be polynomials over a field F, and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots, \beta_k$ be their respective roots. Then the products*

$$h_1(x) = \prod_{j=1}^{k}\prod_{i=1}^{n}(x - \alpha_i - \beta_j)$$

$$h_2(x) = \prod_{j=1}^{k}\prod_{i=1}^{n}(x - \alpha_i\beta_j)$$

are polynomials in x with coefficients in F.

The corollary follows directly from the preceding theorems and the product $\prod_{j=1}^{k} f(x-\beta_j)$. This corollary will have significant effects in some later sections.

9 Numbers Algebraic over a Field

Definition 9.1. A number θ is said to be algebraic over a field F if it satisfies a polynomial in $F[x]$. θ is not necessarily in F.

Definition 9.2. The minimal polynomial for θ is the monic polynomial of least degree that is still satisfied by θ. Consequently a minimal polynomial is also irreducible.

Here are some important facts about minimal polynomials:

1. If θ is algebraic over F, it has a unique minimal polynomial.
2. Any polynomial satisfied by θ over F contains the minimal polynomial of θ as a factor.
3. If $f(x)$ and $g(x)$ are relatively prime over F they have no roots in common.
4. An irreducible polynomial of degree n over F has n distinct roots.

The concept of minimal polynomials together with Corollary 8.4 can be used to prove the following theorem:

Theorem 9.3. *The totality of numbers algebraic over a field F forms a field. In other words, the sum, product, difference and quotient of two algebraic numbers is also algebraic.*

10 Extensions of a Field

Definition 10.1. Any field K containing another field F, is called an extension of F. If θ is algebraic over F, then $K = F(\theta)$ is defined as the smallest field containing F and θ. K is called a simple algebraic extension of F.

Note that K would have to consist of all possible fractions $f(\theta)/g(\theta)$ where $f(\theta), g(\theta) \in F[\theta]$. Any other expression in θ can be simplified into such a quotient. However, the next theorem states a stronger result:

Theorem 10.2. *Every element α of $F(\theta)$ can be written uniquely in the form*

$$\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} = r(\theta)$$

where $a_i \in F$ and n is the degree of θ over F.

Definition 10.3. A multiple algebraic extension is the smallest field containing F and $\alpha_1, ..., \alpha_n$, a set of n algebraic numbers over F.

Theorem 10.4. *A multiple algebraic extension of F is a simple algebraic extension.*

Theorem 10.5. *If θ is algebraic over F, so is every element α of $F(\theta)$. Also $deg\alpha \leq deg\theta$.*

This theorem can be proved using symmetric polynomials or using a result from linear algebra to show that α satisfies a polynomial over F.

11 Algebraic and Transcendental Numbers

Finally, we can define what we mean by an algebraic number. We denote the set of algebraic numbers by $\overline{\mathbb{Q}}$.

Definition 11.1. A number is an *algebraic number* if it is algebraic over the field $\mathbb{Q}$.

Now that we have defined an algebraic number, we want to show that our definition has meaning. That is to say, we want to show that not all numbers are algebraic. This other class of numbers we call transcendental. We will use a construction by Liouville to show that transcendental numbers exist, but first we need a lemma.

Lemma 11.2. *Let θ be a real algebraic number of degree $n > 1$ over $\mathbb{Q}$. $\exists\ M > 1$, which depends on θ, $\ni \left|\theta - \dfrac{p}{q}\right| \geq \dfrac{M}{q^n}$, $\forall\ \dfrac{p}{q} \in \mathbb{Q}$ with $q > 0$.*

The proof of the lemma defines a function $f(x)$ as the primitive of lowest degree satisfied by θ. Then, it defines M' as the maximum of $|f'(x)|$ on the interval $[\theta - 1, \theta + 1]$. M is defined as $\min\left(1, \frac{1}{M'}\right)$. The proof then splits into two cases: $\left|\theta - \dfrac{p}{q}\right| \geq 1$, which is pretty straight forward, and $\left|\theta - \dfrac{p}{q}\right| < 1$, which looks at $\left|f(\theta) - f\left(\dfrac{p}{q}\right)\right|$ to get the appropriate result. Now we are equipped to show that transcendental numbers exist.

Theorem 11.3 (Liouville). $\exists\ \xi \notin \overline{\mathbb{Q}}$.

Proof. We include this proof because this seminar hinges on the existence of transcendental numbers. Let $\xi = \sum_{m=1}^{\infty} (-1)^m 2^{-m!}$ and denote by

$$\xi_k = \frac{p_k}{q_k} = \frac{p_k}{2^{k!}}$$

the sum of the first k terms of the series for ξ. Then,

$$\left|\xi - \frac{p_k}{q_k}\right| = 2^{-(k+1)!} - 2^{-(k+2)!} \cdots < 2^{-(k+1)!} < 2^{-k \cdot k!} = q_k^{-k}.$$

First we suppose ξ is algebraic of degree $n > 1$ over $\mathbb{Q}$. By the preceding inequalities, $q_k^n \left|\xi - \dfrac{p_k}{q_k}\right| \leq q_k^{n-k}$. Letting $k \to \infty$, we find that

$$\lim_{k\to\infty} q_k^n \left|\xi - \frac{p_k}{q_k}\right| = 0.$$

But by Lemma 11.2, $\exists\ M > 0 \ni$

$$\left|\xi - \frac{p_k}{q_k}\right| \geq \frac{M}{q_k^n}.$$

So

$$q_k^n \left|\xi - \frac{p_k}{q_k}\right| \geq M > 0$$

for all k, contrary to the limit 0.

Next we suppose $\xi \in \mathbb{Q}$ (i.e., ξ is an algebraic number of degree 1). Thus, $\xi = \dfrac{p}{q}$. Choose an odd $k \ni 2^{k+1} > q$. Define

$$\eta = 2^{k!}\xi q - 2^{k!}q\sum_{m=1}^{k}(-1)^m 2^{-m!} = 2^{k!}q\sum_{m=k+1}^{\infty}(-1)^m 2^{-m!}.$$

This construction clears all denominators, so $\eta \in \mathbb{N}$. But by our choice of k,

$$\eta < 2^{k!}q\frac{1}{2^{(k+1)!}} = \frac{q}{2^{k+1}} < 1,$$

a contradiction. Thus, ξ is transcendental. □

This transcendental number may seem a little contrived, but it proves what we want to prove. Later we will discover that there are many transcendental numbers that are not so contrived.

12 The Real Numbers are not Countable

Definition 12.1. The mapping $f : A \to B$ is 1-1 if $f(x_1) \neq f(x_2)$ whenever $x_1 \neq x_2$, for $x_1, x_2 \in A$.

Definition 12.2. The mapping $f : A \to B$ maps A *onto* B if $f(A) = B$.

Definition 12.3. If $\exists$ a 1-1 mapping of A onto B, then $A \sim B$, and

1. $A \sim A$
2. If $A \sim B$, then $B \sim A$.
3. If $A \sim B$ and $B \sim C$, then $A \sim C$.

Definition 12.4. For $n \in \mathbb{N}$, let J_n be the integers $1, 2, \ldots, n$; J is the set of all positive integers. For any set A,

1. A is *finite* if $A \sim J_n$ for some n including $\emptyset$.
2. A is *countable* if $A \sim J$.
3. A is *uncountable* if A is neither finite nor countable.

We assume that all real numbers have a unique binary representation. Our desired result will follow as a corollary from this theorem.

Theorem 12.5. *Let A be the set of all sequences whose elements are the digits* 0 *and* 1*. A is uncountable.*

Proof. Let E be a countable subset of A, and let E consist of the sequences $s_1, s_2, s_3, \ldots$. We construct another sequence s by the following process: if the nth digit of s_n is 1, then the nth digit of s is 0, and vice versa. Thus, the sequence s differs from every sequence in E by at least one place. Therefore, $s \notin E$, yet $s \notin A$. Therefore, E is a proper subset of A. Because E was an arbitrary countable subset of A, we conclude that all countable subsets of A are proper subsets of A. If A were countable, then it would be a countable subset of itself. We have just shown that this would imply that A is a proper subset of itself, an obvious contradiction. □

Corollary 12.6. *The real numbers are not countable.*

Using the binary sequence a_1, a_2, $a_3, \ldots$ with $a_i = 0$ or 1, we express a unique real number for each sequence:

$$a_1 \cdot (10^{-1}) + a_2 \cdot (10^{-2}) + a_3 \cdot (10^{-3}) + \cdots$$

Thus, we have defined a function taking the binary sequences to a set of real numbers. By Theorem 12.5, this set of real numbers in uncountable, and thus the real numbers are uncountable.

13 The Sufficiency of $\overline{\mathbb{Q}}$

We have defined

$$\overline{\mathbb{Q}} = \{\alpha \mid p(\alpha) = 0 \text{ for some } p(x) \in \mathbb{Z}[x]\}.$$

Why don't we introduce an extension of the algebraic numbers

$$\overline{\overline{\mathbb{Q}}} = \{\beta \mid p(\beta) = 0 \text{ for some } p(x) \in \overline{\mathbb{Q}}[x]\}?$$

We do not talk of such a set because it does not introduce any new elements.

Theorem 13.1. $\overline{\mathbb{Q}} = \overline{\overline{\mathbb{Q}}}$

The proof constructs $h(x) \in \mathbb{Z}[x]$ by taking a product of $f_i(x) \in \overline{\mathbb{Q}}[x]$ where each $f_i(x)$ has a unique permutation of the conjugates of the coefficients of $f_1(x)$. We reach our conclusion about $h(x)$ using symmetry arguments on its coefficients.

14 Decimal Expansions

Here we present a few theorems that can be used to analyze numbers by looking at their decimal expansions.

Theorem 14.1. *Let $a_1, a_2, ...$ be a sequence of positive integers, all greater than 1. Then, any real number α is uniquely expressible in the form*

$$\alpha = c_0 + \sum_{i=1}^{\infty} \frac{c_i}{a_1 a_2 \cdots a_i}$$

with integers c_i satisfying the inequalities $0 \leq c_i \leq a_i - 1$ for all $i \geq 1$, and $c_i < a_i - 1$ for infinitely many i.

Now we can present the next theorem for irrationality based on decimal expansions.

Theorem 14.2. *Let a_i be as in the previous theorem, and let c_i satisfy the result. Assume that infinitely many of the $c_i \neq 0$, and that each prime number divides infinitely many of the a_i. Then α (as described in the previous theorem) is irrational.*

15 Simple Irrationalities

We now turn our attention to some theorems that prove certain types of expressions yield irrational numbers.

Theorem 15.1. *If the real number x satisfies an equation*

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

with each $c_i \in \mathbb{Z}$, then x is either an integer or an irrational number.

Proof. Suppose $x \in \mathbb{Q}$, then $x = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b > 0$, and $(a, b) = 1$. Then

$$\begin{aligned} x^n &= -c_1 x^{n-1} - c_2 x^{n-2} - \cdots - c_n \\ \frac{a^n}{b^n} &= \frac{-1}{b^{n-1}}(c_1 a^{n-1} + c_2 a^{n-2} b + \cdots + c_n b^{n-1}) \\ a^n &= -b(c_1 a^{n-1} + c_2 a^{n-2} b + \cdots + c_n b^{n-1}). \end{aligned}$$

If $b > 1$, then any prime divisor p of b would divide $a^n \implies p \mid a$ and $p \mid b$, a contradiction of $(a, b) = 1 \implies b = 1$. So if $x \in \mathbb{Q}$, then $x \in \mathbb{Z}$. Otherwise, x must be irrational. □

We can construct some familiar irrational numbers from this theorem. For example, $\sqrt{2}$ and $\sqrt{3}$ satisfy $x^2 - 2 = 0$ and $x^2 - 3 = 0$, respectively. By the theorem, these numbers are irrational. As a simple corollary, we provide the following:

Corollary 15.2. *If m is a positive integer which is not the nth power of an integer, then $\sqrt[n]{m}$ is irrational.*

Now we want to show that trigonometric functions taken at rational values give irrational values. The methodology of this proof is repeated throughout this section, so we will provide the proof for the first theorem. Before we get to that, we must provide two lemmas.

Lemma 15.3. *If*

$$h(x) = \frac{x^n g(x)}{n!}$$

where $g(x) \in \mathbb{Z}[x]$, then $h^{(j)}(0) \in \mathbb{Z}$ for $j = 0, 1, 2, \ldots$. Moreover, with the possible exception of $j = n$, $(n+1) \mid h^{(j)}(0)$. The possible exception for $j = n$ is unnecessary if $g(0) = 0$.

The proof follows by looking at the explicit expression of $h^{(j)}(0)$.

Lemma 15.4. *If $f(x)$ is a polynomial in $(r-x)^2$, then $f^{(j)}(r) = 0$ for any odd integer j.*

Again, the proof follows from explicitly writing $f^{(j)}(r) = 0$.

Theorem 15.5. *For any non-zero $r \in \mathbb{Q}$, $\cos r \notin \mathbb{Q}$.*

Proof. Since $\cos -r = \cos r$, we will prove for $r = \dfrac{a}{b}$ with $a, b \in \mathbb{N}$ and $b > 0$. Let

$$f(x) = \frac{x^{p-1}(a-bx)^{2p}(2a-bx)^{p-1}}{(p-1)!} = \frac{(r-x)^{2p}\{r^2-(r-x)^2\}^{p-1}b^{3p-1}}{(p-1)!}$$

where p is an odd prime to be specified.

For $0 < x < r$,

$$0 < f(x) < \frac{r^{2p}\{r^2\}^{p-1}b^{3p-1}}{(p-1)!} = \frac{r^{4p-2}b^{3p-1}}{(p-1)!}.$$

Let

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - f^{(6)}(x) + \cdots - f^{(4p-2)}(x).$$

Thus,

$$\begin{aligned}\frac{d}{dx}\{F'(x)\sin x - F(x)\cos x\} &= F^{(2)}(x)\sin x + F'(x)\cos x - [F'(x)\cos x - F(x)\sin x] \\ &= F^{(2)}(x)\sin x + F(x)\sin x \\ &= f(x)\sin x.\end{aligned}$$

Using the Fundamental Theorem of Calculus, we find that

$$\int_0^r f(x)\sin x\,dx = F'(r)\sin r - F(r)\cos r + F(0).$$

By Lemma 15.4, $f(x)$ is a polynomial in $(r-x)^2 \implies F'(r) = 0$. By Lemma 15.3, $f(x)$ has the form of $h(x)$ with $n = p-1 \implies p \mid f^{(j)}(0)$ unless $j = p-1$. Examining the $p-1$st derivative, we find that

$$f^{(p-1)}(0) = \frac{(p-1)!a^{2p}(2a)^{p-1}}{(p-1)!} = a^{2p}(2a)^{p-1}.$$

Thus, choosing $p > a \implies p \nmid f^{(p-1)}(0)$ and $p \mid f^{(j)}(0)$ for all other j. Therefore, $F(0) \in \mathbb{Z} \ni p \nmid F(0)$. Let $F(0) = q$; $(p,q) = 1$.

Now look at $F(r)$.

$$\begin{aligned} f(r-x) &= \frac{x^{2p}\{r^2 - x^2\}^{p-1}b^{3p-1}}{(p-1)!} \\ &= \frac{x^{2p}\{a^2 - b^2x^2\}^{p-1}b^{p+1}}{(p-1)!} \end{aligned}$$

So $f(r-x)$ has the form of $h(x)$ from the lemma with $n = p-1$ and $g(x) = x^{p+1}\{a^2 - b^2x^2\}^{p-1}b^{p+1}$. Thus, every $f^{(j)}(r) \in \mathbb{Z}$ is divisible by p because $g(0) = 0$. For some $m \in \mathbb{Z}$, $F(r) = pm$. Returning to the integral, we have

$$\int_0^r f(x)\sin x\,dx = -pm\cos r + q.$$

Assume $\cos r \in \mathbb{Q}$; then $\cos r = \dfrac{d}{k}$.

$$\int_0^r f(x)\sin x\,dx = -pm\frac{d}{k} + q \implies k\int_0^r f(x)\sin x\,dx = -pmd + kq$$

If we add another requirement to p: $p > k \implies p \nmid kq$.

$$\begin{aligned} &\implies p \nmid (-pmd + kq) \\ &\implies -pmd + kq \neq 0 \end{aligned}$$

But $-pmd + kq \in \mathbb{Z}$.

$$\begin{aligned} \left| k\int_0^r f(x)\sin x\,dx \right| &< kr\frac{r^{4p-2}b^{3p-1}}{(p-1)!} \\ &= kr^3b^2\frac{\{r^4b^3\}^{p-1}}{(p-1)!} \\ &= \frac{c_1c_2^{p-1}}{(p-1)!} \end{aligned}$$

where the constants $c_1 = kr^3b^2$ and $c_2 = r^4b^3$ are independent of p. Thus, as $p \to \infty$,

$$\frac{c_1c_2^{p-1}}{(p-1)!} \to 0.$$

Therefore, we can choose p sufficiently large so that

$$-1 < k \int_0^r f(x) \sin x \, dx < 1.$$

But

$$k \int_0^r f(x) \sin x \, dx = -qmd + kq$$

is a non-zero integer. Thus, we have a contradiction. □

Corollary 15.6. *π is irrational.*

Proof. If $\pi \in \mathbb{Q}$, then $\cos \pi \notin \mathbb{Q}$, but $\cos \pi = -1$. □

Corollary 15.7. *The trigonometric functions are irrational at non-zero rational values of the arguments.*

Proof. If $\sin r \in \mathbb{Q}$ for $r \in \mathbb{Q}$, $r \neq 0$, then $1 - 2\sin^2 r = \cos 2r \in \mathbb{Q}$. But this conclusion contradicts the theorem since $2r \in \mathbb{Q}$.

If $\tan r \in \mathbb{Q}$ for $r \in \mathbb{Q}$, $r \neq 0$, then

$$\cos 2r = \frac{1 - \tan^2 r}{1 + \tan^2 r} \in \mathbb{Q}.$$

Again, we find a contradiction of the theorem.

For the same r, $\csc r$, $\sec r$, $\cot r \notin \mathbb{Q}$ because they are reciprocals of irrationals. □

Corollary 15.8. *Any non-zero value of an inverse trigonometric function is irrational for rational arguments.*

Proof. We will prove for $\arccos r$ because the other proofs are similar. For $r \in \mathbb{Q}$, assume $\arccos r = \rho \in \mathbb{Q}$. Then $r = \cos \rho$ is rational, contrary to the theorem. □

Theorem 15.9. *The hyperbolic functions are irrational for non-zero rational values of the arguments.*

The proof of this theorem is almost identical to the proof of Theorem 15.5. The function $F(x)$ does not alternate sign in this proof, and the function to which we apply the Fundamental Theorem of Calculus is slightly different. Once the theorem is proven for $\cosh r$, $\sinh r$ and $\tanh r$ follow by the same logic as the above corollaries. We also get the same result for the inverse hyperbolic functions.

Theorem 15.10. *If $r \in \mathbb{Q}$, $r \neq 0$, then $e^r \notin \mathbb{Q}$. If $r \in \mathbb{Q}$, $r > 0$ and $r \neq 1$, then $\log r \notin \mathbb{Q}$.*

Proof. We could proceed in a similar fashion as the previous two theorems, but instead we will use what we know about the hyperbolic functions. Since $r = \log e^r$, it suffices to prove for e^r. If $e^r \in \mathbb{Q}$, then $e^{-r} \in \mathbb{Q}$, and so

$$\cosh r = \frac{e^r + e^{-r}}{2} \in \mathbb{Q},$$

a contradiction. □

Theorem 15.11. *$\forall\ r \in \mathbb{Q}$, $r > 0$, $\log_q r \notin \mathbb{Q}$ unless $r = q^n$ for some $n \in \mathbb{Z}$.*

The proof follows from letting $r = \frac{a}{b}$, a fraction in lowest terms. Then, assuming $log_q r = \frac{c}{d}$, also a fraction in lowest terms, we get a contradiction by showing that $(c, d) \neq 1$.

Theorem 15.12. *e satisfies no relation of the form*

$$a_m e^m + a_{m-1} e^{m-1} + \cdots + a_1 e + a_0 = 0$$

for $a_i \in \mathbb{Z}$ not all zero (i.e., e is transcendental).

We include this theorem in a section on irrationality because the method of proof is similar to others in this section. We will not go through all the steps of the proof, but in analogy to the other similar proofs, we have

$$f(x) = \frac{x^{p-1}(x-1)^p(x-2)^p \cdots (x-m)^p}{(p-1)!}$$
$$F(x) = f(x) + f'(x) + f^{(2)} + \cdots + f^{(mp+p-1)}(x).$$

We differentiate $e^{-x}F(x)$ and apply the Fundamental Theorem of Calculus. The rest of the proof proceeds as expected with a few small variations.

16 Bases, Finite Extensions, Conjugates and Discriminants

Definition 16.1. K is an extension of F. A set of numbers in K, $\alpha_1, \alpha_2, ..., \alpha_r$ is linearly dependent (over F) if it is possible to find numbers $c_1, c_2, ..., c_r \in F$, not all zero, such that

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_r\alpha_r = 0.$$

Otherwise the numbers α_i are linearly independent.

Definition 16.2. A set of numbers $\beta_1, \beta_2, ..., \beta_s$ in K forms a basis for K over F if for each $\beta \in K$, $\exists\ d_1, d_2, ..., d_s \in F$, unique numbers, such that

$$\beta = d_1\beta_1 + d_2\beta_2 + \cdots + d_s\beta_s$$

A basis is consequently linearly independent, for otherwise the numbers would not be unique. Note that by Theorem 10.2, $1, \theta, ..., \theta^{n-1}$ is a basis for $F(\theta)$.

Theorem 16.3. *All bases for K over F have the same number of elements.*

The previous theorem suggests the following definition. K is a *finite extension* of degree n over F. We write $n = (K/F)$. Any n linearly independent elements in K form a basis for K.

Theorem 16.4. *If $\alpha_1, \alpha_2, ..., \alpha_n$ is a basis for K over F and*

$$\beta_j = \sum_{i=1}^{n} a_{ij}\alpha_i\,, \qquad j = 1, 2, ..., n$$

where a_{ij} are in F, then $\beta_1, \beta_2, ..., \beta_n$ is also a basis if and only if $\det a_{ij} \neq 0$.

Theorem 16.5. *An extension K of F is finite if and only if it is a simple algebraic extension.*

The previous theorem equates the concepts of a finite extension and a simple algebraic extension.

Theorem 16.6. *If K is finite over F, and E over K, then E is finite over F. Moreover*

$$(E/F) = (E/K) \cdot (K/F)$$

Corollary 16.7. *If K is a finite extension of degree n over F, then any element α of K is algebraic over F. Additionally, the degree of α divides n.*

Theorem 16.8. *If α satisfies the equation*

$$\alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 = 0$$

where the α_i are algebraic over F, then α is algebraic over F.

Let $K = F(\theta)$, $n = (K/F)$ and $\alpha \in K$. The degree of α over F is m. We can write α uniquely as

$$\alpha = \sum_{i=0}^{n-1} c_i\theta^i = r(\theta)$$

where $c_i \in F$.

Definition 16.9. Denote the conjugates for θ as $\theta_1, ..., \theta_n$. We can now define the conjugates of α for $F(\theta)$:

$$\alpha_i = r(\theta_i), \qquad i = 1, ..., n$$

Theorem 16.10. *The conjugates of α for $F(\theta)$ are the conjugates over $F(\theta)$ each repeated n/m times. Secondly, α is in F if and only if all conjugates for $F(\theta)$ are the same. Lastly, $F(\alpha) = F(\theta)$ if and only if all its conjugates for $F(\theta)$ are distinct.*

Definition 16.11. Let $\alpha_1, \alpha_2, ..., \alpha_n$ be a basis. Let $\alpha_j^{(i)}$, $i = 1, ..., n$, be the conjugates of α_j for K. The discriminant for the basis is then:

$$\triangle[\alpha_1, ..., \alpha_n] = \left|\alpha_j^{(i)}\right|^2$$

Theorem 16.12. *The discriminant of any basis for $F(\theta)$ is in F and is never zero. If F, θ and its conjugates are all real, then the discriminant of any basis is positive.*

17 Algebraic Integers and Integral Bases

This section seeks to define integers in algebraic number fields. These results will prove useful in the proof of the Gelfond-Schneider Theorem.

We would like our definition of algebraic integers to fulfill the following axioms based on the behavior of the rational integers and Gaussian integers:

1. They form a ring.
2. If α is an integer in $\mathbb{Q}(\theta)$, and $\alpha \in \mathbb{Q}$, then $\alpha \in \mathbb{Z}$.
3. If α is an integer, the conjugates of α are also integers.
4. If $\gamma \in \mathbb{Q}(\theta)$, then $n\gamma$ is an algebraic integer for some non-zero $n \in \mathbb{Z}$.

We find that the following definition fulfills the desired axioms:

Definition 17.1. An algebraic number is an *algebraic integer* if its minimal polynomial is in $\mathbb{Z}[x]$.

By our definition of conjugates, Axiom 3 must be satisfied. Axiom 2 clearly follows because the minimal polynomial of a rational number is of degree one, and if the it fits the definition of algebraic integer, then the minimal polynomial gives:

$$x + a_0 = 0 \Longrightarrow x = -a_0 \in \mathbb{Z}.$$

Now we want to show that the algebraic integers form a ring.

Lemma 17.2. *If α satisfies any monic $f(x) \in \mathbb{Z}[x]$, then $\alpha \in \mathbb{I}$.*

The proof follows by dividing $f(x)$ by the minimal polynomial of α and noticing that the minimal polynomial must be monic with integral coefficients.

Theorem 17.3 (Verification of Axiom 1). *If $\mathbb{Q}(\theta)$ is an algebraic number field, then the integers in it form a ring.*

Proof. We will prove that the algebraic integers are closed under addition; the other properties are similarly verified. We provide this proof because it reveals an important use of Corollary 8.4. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots, \beta_k$ be the conjugates over $\mathbb{Q}$ of the algebraic integers $\alpha = \alpha_1$ and $\beta = \beta_1$, respectively.

By the conclusions in the Section 8, we know that the elementary symmetric functions evaluated at $\beta_1, \beta_2, \ldots, \beta_k$ are integers, and thus, any symmetric polynomial in $\beta_1, \beta_2, \ldots, \beta_k$ is an integer.

Let $f(x)$ be the minimal polynomial for α. Define

$$h(x) = \prod_{j=1}^{k} f(x - \beta_j).$$

The function $f(x)$ has integral coefficients, so the coefficients of $h(x)$ are symmetric polynomials in $\beta_1, \beta_2, \ldots, \beta_k$ with integral coefficients. Therefore, $h(x) \in \mathbb{Z}[x]$. Since $f(x)$ is monic, so is $h(x)$. Because $f(\alpha_1) = 0$, we get

$$\begin{aligned} h(\alpha + \beta) &= h(\alpha_1 + \beta_1) \\ &= f(\alpha_1 + \beta_1 - \beta_1) \prod_{j=2}^{k} f(\alpha_1 + \beta_1 - \beta_j) \\ &= 0. \end{aligned}$$

By Lemma 17.2, $\alpha+\beta \in \mathbb{I}$. Also, $\alpha+\beta$ is closed in $\mathbb{Q}(\theta)$ because $\alpha, \beta \in \mathbb{Q}(\theta)$. □

Corollary 17.4. *The totality of algebraic integers forms a ring.*

The proof is exactly as above except that we do not restrict α and β to the same algebraic number field. Another conclusion that we can reach by similar means is found in the next theorem.

Theorem 17.5. *If α satisfies*

$$f(x) = x^n + \gamma_{n-1}x^{n-1} + \cdots + \gamma_0 = 0$$

for $\gamma_i \in \mathbb{I}$, then $\alpha \in \mathbb{I}$.

The proof defines

$$h(x) = \prod \left(x^n + \gamma_{n-1}^{(i_{n-1})} x^{n-1} + \cdots + \gamma_0^{(i_0)} \right)$$

over all conjugates $\gamma_j^{(i_j)}$. The rest mirrors the above proof.

Next, we prove that the fourth and final axiom follows from our definition of algebraic integers.

Theorem 17.6 (Verification of Axiom 4). *If θ is an algebraic number, $\exists\ r \in \mathbb{Z}$, $r \neq 0$, $\ni r\theta \in \mathbb{I}$.*

Proof. We know that θ satisfies some

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

for $a_i \in \mathbb{Z}$. Thus, $a_n\theta$ satisfies

$$x^n + a_{n-1}x^{n-1} + a_{n-2}a_n x^{n-2} + a_{n-3}a_n^2 x^{n-3} + \cdots + a_0 a_n^{n-1} = 0,$$

a monic polynomial with integer coefficients. □

Now we move on to define integral bases.

Definition 17.7. A set of algebraic integers $\alpha_1, \alpha_2, \ldots, \alpha_s$ is an *integral basis* of $\mathbb{Q}(\theta)$ if every algebraic integer α in $\mathbb{Q}(\theta)$ can be uniquely expressed as

$$\alpha = b_1\alpha_1 + b_2\alpha_2 + \cdots + b_s\alpha_s$$

with $b_i \in \mathbb{Z}$.

Lemma 17.8. *An integral basis is a basis.*

The proof follows from the definition of integral basis and the fact that $\forall\, \beta \in \mathbb{Q}\ \exists\ r \in \mathbb{N} \ni r\beta \in \mathbb{I}$. Note that if $\deg \mathbb{Q}(\theta) = n$, then $s = n$.

Lemma 17.9. *If $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a basis of $\mathbb{Q}(\theta)$ over $\mathbb{Q}$ consisting only of algebraic integers, then $\triangle[\alpha_1, \alpha_2, \ldots, \alpha_n] \in \mathbb{Z}$.*

The proof follows directly from the axioms established at the beginning of this section and Theorem 10.2.

Theorem 17.10. *Every algebraic number field has at least one integral basis.*

This proof considers all bases whose elements are algebraic integers. By the lemma, the discriminants are integers, so we can choose the basis with discriminant of minimum absolute value. If we suppose that such a basis is not an integral basis, we can construct another basis with integer elements whose discriminant has a smaller absolute value, contrary to our choice of basis.

Theorem 17.11. *All integral bases for a field $\mathbb{Q}(\theta)$ have the same discriminant.*

The proof takes two arbitrary integral bases, and expresses each in terms of the other. Taking the discriminants reveals that the discriminants must be the same.

18 Liouville Inequality and Transcendental Sums

Definition 18.1. Let α be an algebraic number, and $\mathbb{I}$ is the set of algebraic numbers. Then $den(\alpha)$ denotes the least positive integer d, such that $d\alpha \in \mathbb{I}$.

Definition 18.2. Let $\overline{|\alpha|}$ denote the maximum of the absolute values of α and its conjugates.

Theorem 18.3 (Liouville inequality). *If α is a nonzero algebraic number with $deg(\alpha) = n$, then*

$$log\,|\alpha| \geq -2n\, max\{log\overline{|\alpha|}, log\, den(\alpha)\}$$

This inequality can be used to prove the following two theorems:

Theorem 18.4. *If α is an algebraic number with $0 < |\alpha| < 1$, then $\sum_{k=1}^{\infty} \alpha^{k!}$ is transcendental.*

Theorem 18.5. *Let d be an integer greater than 1. If α is an algebraic number with $0 < |\alpha| < 1$, then $\sum_{k=0}^{\infty} \alpha^{d^k}$ is transcendental.*

19 The Generalized Lindemann Theorem

In this section, we will outline the logic behind the Generalized Lindemann Theorem, a very interesting result of transcendental number theory. Because the theorem requires many preliminary lemmas, we will state the theorem now so that the goal is clear from the beginning.

Theorem 19.1 (The Generalized Lindemann Theorem). *Given any distinct algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_m$, the values $e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_m}$ are linearly independent over the field of algebraic numbers. Equivalently, the equation*

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

is impossible for $a_1, a_2, \ldots, a_m \in \overline{\mathbb{Q}}$, not all zero.

Now we must provide the preliminary information. The proof requires many results from symmetric polynomials and algebraic fields; we will not repeat theorems which we have already proven.

Theorem 19.2. *Let $\beta_1, \beta_2, \ldots, \beta_n$ be roots of*

$$f(x) = bx^n + c_1x^{n-1} + \cdots + c_n = 0$$

in which $b, c_i \in \mathbb{Z}$. Let $P(x_1, x_2, \ldots, x_n)$ be symmetric in $x_1, x_2, \ldots, x_n$ with rational coefficients. Then, $P(\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Q}$. If P has integer coefficients and is of degree t, then $b^tP(\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}$.

Most of this theorem has been proven in the symmetric polynomial section. The last statement follows from the fact that $b\beta_1, b\beta_2, \ldots, b\beta_n$ are roots of

$$b^{n-1}f(\frac{x}{b}) = x^n + c_1x^{n-1} + bc_2x^{n-2} + \cdots + b^{n-1}c_n = 0.$$

Lemma 19.3. *Consider the q polynomials $P_1, P_2, \ldots, P_q$ in $y_1, y_2, \ldots, y_m$*

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

for $j = 1, 2, \ldots, q$ with coefficients $f_i(x_j)$, where all the $f_i(x) \in F[x]$ for some field F. The product

$$\prod_{j=1}^{q} P_j$$

with the terms in y being collected has coefficients which are symmetric in $x_1, x_2, \ldots, x_q$.

Any permutation of the product clearly leaves the sum of terms in y_i's unchanged.

Now we must provide a new definition:

Definition 19.4. $\mathbb{Q}(\theta)$ is *normal* over $\mathbb{Q}$ if any polynomial irreducible over $\mathbb{Q}$ that has one root in $\mathbb{Q}(\theta)$ has all roots in $\mathbb{Q}(\theta)$.

Theorem 19.5. *Given any algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_s$, $\exists\, \theta \in \overline{\mathbb{Q}} \ni \mathbb{Q}(\theta) \supset \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_s)$ and $\mathbb{Q}(\theta)$ is normal. That is to say, a multiple algebraic extension can always be contained in a normal, simple algebraic extension.*

The proof has two parts. First, we know that $\exists\, \gamma \ni \mathbb{Q}(\gamma) = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_s)$. The conjugates of γ create a multiple algebraic extension that can be set equal to a simple algebraic extension of θ. Second, we show that $\mathbb{Q}(\theta)$ is normal. In simple terms, this is done by writing any element ρ of $\mathbb{Q}(\theta)$ as a polynomial in the conjugates of gamma. Then, we create a new polynomial in x which has rational coefficients because of its symmetry properties. Also, ρ satisfies its minimal polynomial and the new construction, the minimal polynomial divides the construction, and all roots of the construction are in $\mathbb{Q}(\theta)$.

Lemma 19.6. *Let $\mathbb{Q}(\theta)$ be a normal algebraic extension of degree n over $\mathbb{Q}$ with conjugates $\theta = \theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$. These conjugates regarded as polynomials in θ, are merely permuted by the substitution of $\theta^{(i)}$ for θ. More generally, if $F(x) \in \mathbb{Q}[x]$, then the set*

$$F(\theta^{(1)}), F(\theta^{(2)}), \ldots, F(\theta^{(n)})$$

is permuted by the substitution of $\theta^{(i)}$ for θ.

The proof of the lemma is more subtle than its statement may suggest. If the minimal polynomial for θ is

$$x^n + b_1 x^{n-1} + b_n = 0,$$

then we need to use the reduction rule

$$\theta^n = -b_1\theta^{n-1} - \cdots - b_n$$

on the conjugates of θ written as polynomials in θ. After some manipulation, we reach a point where substitution of the conjugates creates a permutation or θ satisfies a polynomial of degree $n-1$. Since θ is of degree n, we can agree on the former conclusion.

Lemma 19.7. *Any element γ of $\mathbb{Q}(\theta)$ and its conjugates over $\mathbb{Q}(\theta)$ satisfy a polynomial equation of degree n with integral coefficients.*

The elementary symmetric polynomials in the conjugates of γ are symmetric polynomials in the conjugates of θ. The elementary symmetric polynomials can construct the minimal polynomial for γ with rational coefficients. Multiplying by the least common denominator finishes the proof.

Lemma 19.8. *Consider*

$$f(x) = \sum_{j=1}^{m} a_j x^{\alpha_j} \qquad g(x) = \sum_{j=1}^{t} b_j x^{\beta_j}$$

with non-zero complex coefficients a_j and b_j and $\alpha_j, \beta_j \in \overline{\mathbb{Q}}$. Assume all α_j are distinct and all β_j are distinct. Taking the product $f(x)g(x)$ and combining terms with equal exponents guarantees at least one non-zero coefficient.

We find a simple, normal algebraic extension $\mathbb{Q}(\theta)$ which contains all α_j's and all β_j's. Then we write the α_j's and β_j's as polynomials in θ. After defining a method for ordering our terms, we find that we are guaranteed that the first term of the product has a unique exponent that will not cancel.

Now we can outline the proof of the Generalized Lindemann Theorem. First we outline the proof of a modified version of the theorem, in which we only prove linear independence over the rational numbers.

Theorem 19.9. *Given any m distinct algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_m$, the values $e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_m}$ are linearly independent over $\mathbb{Q}$.*

Assume

$$\sum_{j=1}^{m} a_j \exp(\alpha_j) = 0$$

for $a_j \in \mathbb{Q}$, not all zero. Throw out all terms with $a_j = 0$ and multiply through by a suitable integer to get $a_j \in \mathbb{Z}$. Use Theorem 19.5 to write all

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

Then we have conjugates

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

for the n conjugates of θ, which will be distinct. The product

$$\prod_{k=1}^{n}\sum_{j=1}^{m} a_j \exp(\alpha_j^{(k)}) = \sum_{j=0}^{r} c_j \exp(\beta_j) = 0 \tag{14}$$

with distinct β_j by collecting terms. Note that $a_j \in \mathbb{Z} \implies c_j \in \mathbb{Z}$, and by Lemma 19.8 the c_j do not vanish. In Equation (14), substituting $\theta^{(i)}$ permutes the factors and makes $\beta_j \to \beta_j^{(i)}$.

$$\Rightarrow 0 = \sum_{j=0}^{r} c_j \exp(\beta_j^{(1)}) = \sum_{j=0}^{r} c_j \exp(\beta_j^{(2)}) = \cdots = \sum_{j=0}^{r} c_j \exp(\beta_j^{(n)}) \tag{15}$$

Multiply the respective sums by $\exp\{-\beta_0^{(1)}\}, \exp\{-\beta_0^{(2)}\}, \ldots, \exp\{-\beta_0^{(n)}\}$. Let

$$\gamma_j^{(i)} = \beta_j^{(i)} - \beta_0^{(i)}$$

for $j = 1, 2, \ldots, r$ and all i. Note that all $\gamma_j^{(i)} \neq 0$ because the $\beta_j^{(i)}$ are necessarily distinct for fixed i. Equation (15) implies

$$0 = c_0 + \sum_{j=1}^{r} c_j \exp(\gamma_j^{(1)}) = c_0 + \sum_{j=1}^{r} c_j \exp(\gamma_j^{(2)}) = \cdots = c_0 + \sum_{j=1}^{r} c_j \exp(\gamma_j^{(n)}).$$

By Lemma 19.7, $\gamma_j^{(1)}, \gamma_j^{(2)}, \ldots, \gamma_j^{(n)}$ are roots of a polynomial with integer coefficients

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

for all j.

Next, the proof makes use of the method found in the simple irrationality section. We will provide the appropriate $f(z)$ and $F(z)$, but the details of this section are excluded because we only intend to outline the proof.

$$f(z) = \frac{(b_1 b_2 \cdots b_r)^{prn} z^{p-1} \{\prod_{j=1}^{r} g_j(z)\}^p}{(p-1)!}$$

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

We apply the Fundamental Theorem of Calculus to

$$\{F(z) \exp(-z)\}' = -f(z) \exp(-z).$$

The only deviations from the established method is multiplication of the integral by c_j and $\exp(\gamma_j^{(i)})$ and summing over all i and j. The limits of the integral are 0 and $\gamma_j^{(i)}$.

After carrying out the prescribed method, the modified theorem is proven. Now we need to expand the proof to algebraic coefficients. We begin by assuming

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

for $a_j, \alpha_j \in \overline{\mathbb{Q}}$. Then we take conjugates of a_j over some field $\mathbb{Q}(\theta)$ containing all a_j. Then,

$$\prod_{i=1}^{q} \sum_{j=1}^{m} a_j^{(i)} \exp(\alpha_j) = 0.$$

Lemma 19.3 $\implies$ the product has coefficients symmetric in $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(q)}$. Then, Theorem 19.2 $\implies$ the product has rational coefficients. And Lemma 19.8 $\implies$ the product is not identically zero. Thus Equation (16) implies a contradiction of Theorem 19.9.

The Generalized Lindemann Theorem provides us with a simple way of proving the transcendence of some common expressions.

Theorem 19.10. *The following numbers are transcendental:*

1. e and π

2. $e^\alpha, \sin\alpha, \cos\alpha, \tan\alpha, \sinh\alpha, \cosh\alpha,$ and $\tanh\alpha$ for every non-zero $\alpha \in \overline{\mathbb{Q}}$.

3. $\log\alpha, \arcsin\alpha,$ and the other inverses of functions in the second list.

Proof. The proof of this theorem has many redundancies, so we only provide a few select proofs.
e: Let $\alpha_j = j \in \mathbb{N} \subset \overline{\mathbb{Q}}$. Then e does not satisfy

$$\sum_{j=0}^{m} a_j e^j = 0 \qquad\qquad a_j \in \overline{\mathbb{Q}}.$$

e^α: $\forall\ \alpha \in \overline{\mathbb{Q}}$, $j \in \mathbb{N}$, $\alpha j \in \overline{\mathbb{Q}}$

$$\implies \sum_{j=0}^{m} a_j (e^\alpha)^j = \sum_{j=0}^{m} a_j e^{\alpha j} \neq 0 \qquad\qquad a_j \in \overline{\mathbb{Q}}.$$

π: Assume $\pi \in \overline{\mathbb{Q}}$. The algebraic numbers form a field $\implies i\pi \in \overline{\mathbb{Q}} \implies e^{i\pi}$ is transcendental. This is a contradiction because $e^{i\pi} = -1$.
$\sin\alpha$: Assume $\sin\alpha \in \overline{\mathbb{Q}}$. Let $\sin\alpha = a$. Then

$$e^{i\alpha} - e^{-i\alpha} - 2iae^0 = \cos\alpha + i\sin\alpha - \cos\alpha + i\sin\alpha - 2i\sin\alpha = 0$$

contrary to the linear independence of $e^{i\alpha}, e^{-i\alpha}$, and e^0 over $\mathbb{Q}$.
$\sinh\alpha$: If $\sinh\alpha \in \overline{\mathbb{Q}}$, then

$$\frac{e^\alpha - e^{-\alpha}}{2} \in \overline{\mathbb{Q}},$$

a contradiction.
$\log\alpha$: Assume $a = \log\alpha \in \overline{\mathbb{Q}}$ for $\alpha \in \overline{\mathbb{Q}}$. Then $e^a = \alpha \in \overline{\mathbb{Q}}$. But $a \in \overline{\mathbb{Q}} \implies e^a = \alpha$ is transcendental, a contradiction. □

Theorem 19.11. *If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are linearly independent over $\overline{\mathbb{Q}}$, then $e^{\alpha_1}, e^{\alpha_2}, \ldots, e^{\alpha_n}$ are algebraically independent over $\overline{\mathbb{Q}}$.*

We must show that

$$\sum_{j_1, j_2, \ldots, j_n} c_{j_1, j_2, \ldots, j_n} (e^{\alpha_1})^{j_1} (e^{\alpha_2})^{j_2} \cdots (e^{\alpha_n})^{j_n} \neq 0$$

for non-zero $c_{j_1, j_2, \ldots, j_n} \in \overline{\mathbb{Q}}$. We can rewrite this expression as

$$\sum_{j_1, j_2, \ldots, j_n} c_{j_1, j_2, \ldots, j_n} \exp\left(\alpha_1 j_1 + \alpha_2 j_2 + \cdots + \alpha_n j_n\right) \neq 0.$$

As long as the j_i's are not all zero, we know that not all terms vanish. The sum cannot be identically zero by the Generalized Lindemann Theorem.

20 Units and Primes in Algebraic Number Fields

We now wish to extend our concepts of units, primes, and divisibility to algebraic integers. Consider integers in a fixed algebraic number field $K = \mathbb{Q}(\theta)$.

Definition 20.1. For $\alpha, \beta \in K$, α *divides* β, written $\alpha \mid \beta$, if $\dfrac{\alpha}{\beta}$ is an integer of $\mathbb{Q}(\theta)$.

Definition 20.2. ϵ is a *unit* if $\epsilon \mid 1$.

Theorem 20.3. *The units form a group under multiplication.*

Proof. If we have two units a and b, then $\exists$ d and $e \ni$

$$a \cdot d = 1 \qquad b \cdot e = 1.$$

Associativity holds because units are algebraic integers. We can show that, therefore, the units are closed under multiplication:

$$(a \cdot b) \cdot (d \cdot e) = (a \cdot d) \cdot (b \cdot e) = 1 \Longrightarrow a \cdot b \mid 1.$$

The multiplicative identity axiom is fulfilled by the unit 1. The multiplicative inverse axiom follows from that fact that for any unit $a \ \exists \ d \ni a \cdot d = 1 \Longrightarrow d$ is a unit. □

Definition 20.4. α is a *prime* if $\alpha \neq 0$, α is not a unit, and any factorization $\alpha = \gamma\beta \Longrightarrow \gamma$ or β is a unit.

Definition 20.5. If $\alpha \in \mathbb{I}$ of K and $n = (K/\mathbb{Q})$, then α has n conjugates $\alpha_1, \alpha_2, \ldots, \alpha_n$ for$K$. The *norm* of α, $N(\alpha)$ or $N\alpha$. is $\alpha_1\alpha_2\cdots\alpha_n$.

Lemma 20.6. $N\alpha \in \mathbb{Z}$

The norm of α is simply the constant term of α's minimal polynomial raised to some power, which is obviously an integer.

Lemma 20.7. $N(\alpha\beta) = N\alpha \cdot N\beta$

The lemma follows from the explicit expression of both sides of the equation.

Lemma 20.8. *α is a unit $\Longleftrightarrow N\alpha = \pm 1$.*

The lemma follows directly from the definition of unit, the definition of the norm, and the previous lemma.

Theorem 20.9. *If $N(\alpha)$ is a rational prime, α is prime in K.*

The theorem follows from factoring α and taking the norm of the factorization. The converse does not hold. For example, 3 is a prime in $\mathbb{Q}(i)$, but $N(3) = 9$ in $\mathbb{Q}(i)$.

Theorem 20.10. *Every integer in K, not zero or a unit, can be factored into a product of primes.*

The proof is identical to the proof of the Fundamental Theorem of Arithmetic except that one must take the norm of the factorization to guarantee that it stops.

Corollary 20.11. *There are infinite primes in an algebraic field.*

The same argument that we used for rational integers works here.

21 Cauchy's Theorem

We digress into complex variables because we require results from them to prove the Gelfond-Schneider Theorem.

Definition 21.1. A subset A of $\mathbb{C}$ is *disconnected* if $\exists$ open sets U and V in $\mathbb{C}$ that obey the following three conditions:

1. U and V are disjoint

2. $A \bigcap U \neq \emptyset$ and $A \bigcap V \neq \emptyset$

3. $A \subset U \bigcup V$

A set A is *connected* if it is not disconnected.

Definition 21.2. A non-empty set D in the complex plane that is both open and connected is a *domain* in $\mathbb{C}$.

Definition 21.3. A sequence $\langle z_n \rangle$ in $\mathbb{C}$ has the complex number z_0 as an accumulation point if $\forall\ \epsilon > 0$, $\Delta(z_0, \epsilon)$ contains z_n for infinitely many values of n.

Definition 21.4. A subset A of the complex plane is *compact* if each sequence in A has an accumulation point that belongs to A.

Theorem 21.5. *Any pair of distinct points z_0 and z_1 in a plane domain D can be made the endpoints of a polygonal arc lying in D.*

Lemma 21.6. *Suppose that U is an open set in the complex plane and that K is a compact subset of U. $\exists$ a radius $r > 0 \ni\ \forall\ z \in K$, $\Delta(z, r)$ is contained in U.*

Theorem 21.7 (Cantor's Theorem). *Suppose that $\langle K_n \rangle$ is a sequence of non-empty compact sets in $\mathbb{C}$ satisfying $K_1 \supset K_2 \supset K_3 \cdots$. Then $\bigcap_{n=1}^{\infty} K_n$ is not empty.*

Definition 21.8. A function f is *analytic in* U if U is a non-empty open subset of the complex plane, f is a complex-valued function whose domain-set contains U, and f is differentiable at every point in U.

Definition 21.9. A *path* γ in the complex plane is a continuous function of the type $\gamma : [a, b] \to \mathbb{C}$, where $[a, b]$ is a closed interval of real numbers. The range of γ is called its *trajectory*, denoted by $|\gamma|$. The *initial* and *terminal points* are $\gamma(a)$ and $\gamma(b)$, respectively. When these values coincide, γ is a *closed* path.

Definition 21.10. A path $\gamma(t) = x(t) + iy(t)$ for $a \leq t \leq b$ is *smooth* if its derivative $\dot{\gamma}(t)$ with respect to the real parameter t, $\dot{\gamma}(t) = \dot{x}(t) + i\dot{y}(t)$, exists for each t in $[a, b]$ and if the function $\dot{\gamma}$ is continuous on the interval $[a, b]$.

A path is *piecewise smooth* provided there is a partition $P : a = t_0 < t_1 < \cdots < t_n = b$ of the interval $[a, b]$ with the property that the restriction of γ to each of the intervals $[t_{k-1}, t_k]$, $1 \leq k \leq n$, is a smooth path.

Lemma 21.11. *Let D be a domain in the complex plane, and let z_0 and z_1 be points of D, not excluding the case $z_0 = z_1$. $\exists$ a piecewise smooth path in D with initial point z_0 and terminal point z_1.*

Lemma 21.12. *Suppose that $f : A \to \mathbb{C}$ and $g : A \to \mathbb{C}$ are continuous functions and that γ and β are piecewise smooth paths in A.*

$$\int_\gamma [f(z) + g(z)]\,dz = \int_\gamma f(z)\,dz + \int_\gamma g(z)\,dz; \tag{i}$$

$$\int_\gamma cf(z)\,dz = c\int_\gamma f(z)\,dz \textit{ for any complex constant } c; \tag{ii}$$

$$\int_{-\gamma} f(z)\,dz = -\int_\gamma f(z)\,dz; \tag{iii}$$

$$\textit{if } \gamma + \beta \textit{ is defined, then } \int_{\gamma+\beta} f(z)\,dz = \int_\gamma f(z)\,dz + \int_\beta f(z)\,dz; \tag{iv}$$

$$\left|\int_\gamma f(z)\,dz\right| \leq \int_\gamma |f(z)|\,|dz|\,. \tag{v}$$

Theorem 21.13. *Suppose that a function f is continuous in an open set U and that F is a primitive for f in U. If $\gamma : [a, b] \to U$ is a piecewise smooth path, then*

$$\int_\gamma f(z)\,dz = \Big[F(z)\Big]_{\gamma(a)}^{\gamma(b)}.$$

In particular, under the above hypotheses it is true that

$$\int_\gamma f(z)\,dz = 0$$

for every closed, piecewise smooth path γ in U.

Lemma 21.14. *If a function f is analytic in an open set U, then $\int_{\partial R} f(z)\,dz = 0$ for every closed rectangle R in U.*

Lemma 21.15. *If a function f is continuous in an open set U and analytic in $U \sim \{z_0\}$ for some points $z_0 \in U$, then*

$$\int_{\partial R} f(z)\,dz = 0$$

$\forall$ closed rectangle $R \in U$.

Lemma 21.16. *Let Δ be an open disk on the complex plane, and let f be a continuous function in Δ with the property that $\int_{\partial R} f(z)\,dz$ for every closed rectangle R in Δ whose sides are parallel to coordinate axes. Then f has a primitive in Δ. In particular, $\int_\gamma f(z)\,dz = 0$ for every closed, piecewise smooth path γ in this disk.*

Theorem 21.17 (Cauchy's Theorem – Local Form). *Suppose that Δ is an open disk in the complex plane and that f is a function which is analytic in Δ (or, more generally, is continuous in Δ and analytic in $\Delta \sim \{z_0\}$ for some point $z_0 \in \Delta$). Then $\int_\gamma F(z)\,dz = 0$ for every closed, piecewise smooth path $\gamma \in \Delta$.*

This theorem follows from Lemma 21.15 and Lemma 21.16.

Lemma 21.18. *Let γ be a piecewise smooth path in the complex plane, let h be a function that is continuous on $|\gamma|$, and let k be a positive integer. The function H defined in the open set $U = \mathbb{C} \sim |\gamma|$ by*

$$H(z) = \int_\gamma \frac{h(\zeta)\,d\zeta}{(\zeta - z)^k}$$

is an analytic function whose derivative is given by

$$H'(z) = k \int_\gamma \frac{h(\zeta)\,d\zeta}{(\zeta - z)^{k+1}}.$$

Definition 21.19. The *winding number $n(\gamma, z)$ of γ about z* is defined by the formula

$$n(\gamma, z) = \frac{1}{2\pi i} \int_\gamma \frac{d\zeta}{\zeta - z}.$$

Theorem 21.20 (Cauchy's Integral Formula – Local Form). *For a function f analytic in an open disk Δ and a closed piecewise smooth path γ in Δ, we have*

$$n(\gamma, z) f(z) = \frac{1}{2\pi i} \int_\gamma \frac{f(\zeta)\,d\zeta}{\zeta - z}$$

$\forall$ $z \in \Delta \sim |\gamma|$.

Proof. Fixing a point $z \in \Delta \sim |\gamma|$ and considering the function $g : \Delta \to \mathbb{C}$ defined as

$$g(\zeta) = \begin{cases} \dfrac{[f(\zeta) - f(z)}{\zeta - z} & \text{if } \zeta \neq z, \\ f'(z) & \text{if } \zeta = z \end{cases}$$

we see that g is analytic in $\Delta \sim \{z\}$. It is also at least continuous at z. Thus, we can apply Theorem 21.17.

$$\begin{aligned} 0 &= \int_\gamma g(\zeta)\, d\zeta \\ &= \int_\gamma \frac{[f(\zeta) - f(z)}{\zeta - z}\, d\zeta \\ &= \int_\gamma \frac{f(\zeta)\, d\zeta}{\zeta - z} - f(z) \int_\gamma \frac{d\zeta}{\zeta - z} \\ &= \int_\gamma \frac{f(\zeta)\, d\zeta}{\zeta - z} - 2\pi i n(\gamma, z) f(z), \end{aligned}$$

which gives our result

$$n(\gamma, z) f(z) = \frac{1}{2\pi i} \int_\gamma \frac{f(\zeta)\, d\zeta}{\zeta - z}.$$

□

Definition 21.21. A *cycle* or a *piecewise smooth cycle* is a finite sequence of closed piecewise smooth paths in the complex plane.

Definition 21.22. A cycle σ in an open set U is *homologous to zero in U* if $n(\sigma, 0) = 0$ for every z in $\mathbb{C} \sim U$. Two cycles $\sigma_0 = (\gamma_1, \gamma_2, \ldots, \gamma_p)$ and $\sigma_1 = (\beta_1, \beta_2, \ldots, \beta_q)$ in U are *homologous in U* if the cycle $\sigma = (\gamma_1, \gamma_2, \ldots, \gamma_p,\ -\beta_1, -\beta_2, \ldots, -\beta_q)$ is homologous to zero in U. Two non-closed piecewise smooth paths λ_0 and λ_1 in U are *homologous in U* if λ_0 and λ_1 share both the same initial point and the same terminal point and if the closed path $\gamma = \lambda_0 - \lambda_1$ is homologous to zero in U.

Theorem 21.23 (Cauchy's Theorem). *For a cycle σ in an open set U, $\int_\sigma f(z)\, dz = 0$ for every analytic function f in $U \iff \sigma$ is homologous to zero in U.*

Proof. Assume $\int_\sigma f(z)\, dz = 0$ for every analytic function f in U. If $z \in \mathbb{C} \sim U$, then $f : U \to \mathbb{C}$ defined by $f(\zeta) = (\zeta - z)^{-1}$ is clearly analytic. Therefore,

$$0 = \int_\sigma f(\zeta)\, d\zeta = \int_\sigma \frac{d\zeta}{\zeta - z} = 2\pi i n(\sigma, z).$$

That is to say, $n(\sigma, z) = 0$ for every $z \in \mathbb{C} \sim U$, and thus σ is homologous to zero in U.

Assuming that σ is homologous to zero in U has a more complicated proof, which we will only outline. Consider the set $V = \{z \in \mathbb{C} \sim |\sigma| : n(\sigma, z) = 0\}$. The set $K = \mathbb{C} \sim V$ is compact, lies in U, and contains $|\sigma|$. Use Lemma 21.6 to determine a $\delta > 0 \ni \ \forall\ z \in K$, $\Delta(z, \delta)$ lies inside U. Then, we can create a partition of the complex plane of non-overlapping closed squares of side length $\delta/2$. K must be closed, so it can intersect only a finite number of these squares. The disks Δ_j of radius $\delta/2$ concentric with the squares $Q_1, Q_2, \ldots, Q_r$ intersecting K must be contained by U and must contain the squares with which they are concentric.

Consider an analytic function f in U. Fix a point z in the interior of a square Q_m. The local Cauchy integral formula on the disk Δ_m gives

$$f(z) = n(\partial Q_m, z)f(z) = \frac{1}{2\pi i}\int_{\partial Q_m} \frac{f(\zeta)\,d\zeta}{\zeta - z}.$$

For $j \neq m$, $n(\partial Q_j, z) = 0$, so

$$0 = n(\partial Q_j, z)f(z) = \frac{1}{2\pi i}\int_{\partial Q_j} \frac{f(\zeta)\,d\zeta}{\zeta - z}.$$

For any z in the interior of any Q_j,

$$f(z) = \frac{1}{2\pi i}\sum_{j=1}^{r}\int_{\partial Q_j} \frac{f(\zeta)\,d\zeta}{\zeta - z}.$$

If we look at the sides of the squares, we notice that integration along the side of one square cancels the integration from another side. The only integrations that do not cancel come from sides that are not shared and, thus, do not intersect K. Call these sides $\lambda_1, \lambda_2, \ldots, \lambda_q$:

$$f(z) = \frac{1}{2\pi i}\sum_{k=1}^{q}\int_{\partial \lambda_k} \frac{f(\zeta)\,d\zeta}{\zeta - z}. \tag{17}$$

Use Lemma 21.18 to show that Equation 17 holds for all z of $|\sigma|$. Assume

$\sigma = (\gamma_1, \gamma_2, \ldots, \gamma_p)$. Then use Equation 17 to get

$$\begin{aligned}
\int_\sigma f(z)\,dz &= \int_\sigma \left\{ \frac{1}{2\pi i} \sum_{k=1}^{q} \int_{\lambda_k} \frac{f(\zeta)\,d\zeta}{\zeta - z} \right\} dz \\
&= \frac{1}{2\pi i} \sum_{l=1}^{p} \sum_{k=1}^{q} \int_{\gamma_l} \left\{ \int_{\lambda_k} \frac{f(\zeta)\,d\zeta}{\zeta - z} \right\} dz \\
&= \frac{1}{2\pi i} \sum_{k=1}^{q} \sum_{l=1}^{p} \int_{\lambda_k} \left\{ \int_{\gamma_l} \frac{f(\zeta)\,dz}{\zeta - z} \right\} d\zeta \\
&= \sum_{k=1}^{q} \int_{\lambda_k} f(\zeta) \left\{ \sum_{l=1}^{p} \frac{1}{2\pi i} \int_{\gamma_l} \frac{dz}{\zeta - a} \right\} d\zeta \\
&= -\sum_{k-1}^{q} \int_{\lambda_k} f(\zeta) \left\{ \frac{1}{2\pi i} \int_\sigma \frac{dz}{z - \zeta} \right\} d\zeta \\
&= -\sum_{k=1}^{q} \int_{\lambda_k} f(\zeta) n(\sigma, \zeta)\,d\zeta \\
&= -\sum_{k=1}^{1} \int_{\lambda_k} f(\zeta) \cdot 0\,d\zeta = 0.
\end{aligned}$$

□

Theorem 21.24 (Cauchy's Integral Formula). *Suppose that a function f is analytic in an open set U and that σ is a cycle in U which is homologous to zero in this set. Then*

$$n(\sigma, z) f(z) = \frac{1}{2\pi i} \int_\sigma \frac{f(\zeta)\,d\zeta}{\zeta - z}$$

$\forall\ z \in U \sim |\sigma|$.

The proof mirrors the local proof almost exactly.

Corollary 21.25. *For a function f analytic in an open set U and cycles σ_1 and σ_2 in U that are homologous in this set,*

$$\int_{\sigma_1} f(z)\,dz = \int_{\sigma_2} f(z)\,dz.$$

Corollary 21.26. *For a function f analytic in an open set U with non-closed piecewise smooth paths λ_0 and $\lambda_1 \in U$ that are homologous in this set,*

$$\int_{\lambda_0} f(z)\,dz = \int_{\lambda_1} f(z)\,dz.$$

Definition 21.27. A subset E of U is a *discrete subset of* U if E has no limit point that belongs to U.

Definition 21.28. A function f has an *isolated singularity* at a point z_0 of the complex plane provided there exists an $r > 0$ with the property that f is analytic in the punctured disk $\Delta^*(z_0, r)$, yet not analytic in the full open disk $\Delta(z_0, r)$.

Definition 21.29. A function f is *analytic modulo isolated singularities in an open set U* under the following conditions: there is a discrete subset E of U, the *singular set of f in U*, with the feature that f is analytic in the open set $U \sim E$, but has a singularity at each point of E.

Using the notation from Definition 21.28, take for granted that f can be represented in Δ^* as $f(z) = \sum_{n=-\infty}^{\infty} a_n(z - z_0)^n$. Then, we have the following definitions:

Definition 21.30. f has a *removable singularity* at z_0 if $a_n = 0$ for every negative index n.

Definition 21.31. $S(z) = \sum_{n=1}^{\infty} a_{-n}(z - z_0)^{-n}$ is the *singular part of f at z_0*.

Definition 21.32. The coefficient a_{-1} in the singular function S is called the *residue of f at z_0*, notated $\operatorname{Res}(z_0, f)$.

Theorem 21.33 (Residue Theorem). *For a function f analytic modulo isolated singularities in an open set U, E the singular set of f in U, and a cycle $\sigma \in U \sim E$ homologous to zero in U,*

$$\int_\sigma f(z)\,dz = 2\pi i \sum_{z\in E} n(\sigma, z) \operatorname{Res}(z, f).$$

Proof. We will only outline this proof. Using the properties of E and $n(\sigma, z)$, show that $n(\sigma, z) \neq 0$ for only finitely many points $z \in E$. Let these finitely many points be $\zeta_1, \zeta_2, \ldots, \zeta_p$. Let $V = (U \sim E) \bigcup \{\zeta_1, \zeta_2, \ldots, \zeta_p\}$. Conclude that $n(\sigma, z) = 0 \; \forall \; z \in \mathbb{C} \sim V$ (i.e., σ is homologous to 0 in V).

Let S_k be the singular part of f at the point ζ_k. S_k is analytic in $\mathbb{C} \sim \{\zeta_k\}$; $f - S_k$ has a removable singularity at ζ_k. The function $g = f - S_1 - S_2 - \cdots - S_p$ is analytic in V except for removable singularities at $\zeta_1, \zeta_2, \ldots, \zeta_p$. Remove these singularities to make g analytic in V. Use Cauchy's Theorem to assert

$$\begin{aligned} 0 = \int_\sigma g(z)\,dz &= \int_\sigma f(z)\,dz - \sum_{k=1}^{p} \int_\sigma S_k(z)\,dz \\ \implies \int_\sigma f(z)\,dz &= \sum_{k=1}^{p} \int_\sigma S_k(z)\,dz. \end{aligned}$$

Let $S(z) = \sum_{n=1}^{\infty} a_{-n}(z - \zeta_0)^{-n}$ for an arbitrary $\zeta_0 \in E$. S converges normally in $\mathbb{C} \sim \{\zeta_0\}$, and converges uniformly on $|\sigma|$, which allows the computation

$$\begin{aligned} \int_\sigma S(z)\,dz &= \int_\sigma \left(\sum_{n=1}^{\infty} \frac{a_{-n}}{(z - \zeta_0)^n} \right) dz = \sum_{n=1}^{\infty} a_{-n} \int_\sigma \frac{dz}{(z - \zeta_0)^n} \\ &= a_{-1} \int_\sigma \frac{dz}{z - \zeta_0} = 2\pi i n(\sigma, \zeta_0) \operatorname{Res}(\zeta_0, f). \end{aligned}$$

Thus, we can conclude

$$\int_{\sigma} f(z)\,dz = 2\pi i \sum_{k=1}^{p} n(\sigma,\zeta_k)\,\mathrm{Res}(\zeta_k, f) = 2\pi i \sum_{z\in E} n(\sigma,z)\,\mathrm{Res}(z,f).$$

□

22 The Gelfond-Schneider Theorem

The Gelfond-Schneider Theorem gives the solution to Hilbert's seventh problem, which was published in the year 1900. The theorem was proved in 1934 by Gelfond and independently in 1935 by Schneider.

The theorem can be stated in the following two equivalent ways:

Theorem 22.1. *If α and β are algebraic numbers with $\alpha \neq 0, \alpha \neq 1$, and if $\beta \notin \mathbb{Q}$, then any value of α^{β} is transcendental.*

Theorem 22.2. *If α and γ are non-zero algebraic numbers, and if $\alpha \neq 1$, then $(\log\gamma)/(\log\alpha)$ is either rational or transcendental.*

The second version of the theorem implies that, for example,

$$\log_{10} r = \frac{\log r}{\log 10}$$

is transcendental if r is not a power of 10.

The following lemmas are useful in proving the theorem.

Lemma 22.3 (Vandermonde determinant). *Consider a determinant with non-zero element ρ_j^a in the j-th row and the $1+a$-th column, with $j = 1, 2, ..., t$ and $a = 0, 1, ..., t-1$. Then the determinant vanishes if and only if $\rho_j = \rho_k$ for some distinct pair of subscripts j, k.*

Lemma 22.4. *Consider m equations in n unknowns:*

$$a_{k1}x_1 + \cdots + a_{kn}x_n = 0, \qquad k = 1, 2, \cdots, m,$$

with $a_{ij} \in \mathbb{Z}$, and with $0 < m < n$. Let the positive integer A be defined such that $A \geq |a_{ij}|, \forall i, j$. Then there is a non-trivial solution $x_1, x_2, \cdots, x_n$ in rational integers of our m equations such that

$$|x_j| < 1 + (nA)^{m/(n-m)}, \qquad j = 1, 2, \cdots, n$$

Lemma 22.5. *Consider consider a field K of finite degree, a subset $\mathbb{I}$ of algebraic integers in K and p equations in q unknowns:*

$$\alpha_{k1}\xi_1 + \cdots + \alpha_{kn}\xi_n = 0, \qquad k = 1, 2, \cdots, p,$$

with $\alpha_{ij} \in \mathbb{I}$, and with $0 < p < q$. Let $A \geq 1$ be an upper bound on the absolute values of the coefficients and their conjugates , $A \geq ||\alpha_{ij}||, \forall i, j$. Then there is *a positive constant c depending on the field K and not on p, q or the coefficients, such that the equations have a non-trivial solution $\xi_1, \xi_2, \cdots, \xi_q$ in integers of K such that*

$$||\xi_k|| < c + c(cqA)^{p/(q-p)}, \qquad k = 1, 2, \cdots, p$$

One application of the Gelfond-Schneider theorem is the following theorem, the Gaussian version of Fermat's last theorem.

Theorem 22.6. *If a, b, c are strictly positive integers and n is a Gaussian integer, then the $a^n + b^n = c^n$ has a solution only when $n = \pm 1$ and ± 2.*

Proof. Let $n = p + iq$ where $p, q \in \mathbb{Z}$. Then we can write our equation and its conjugate:

$$a^{p+iq} + b^{p+iq} = c^{p+iq}$$
$$a^{p-iq} + b^{p-iq} = c^{p-iq}$$

We multiply the two together:

$$a^{2p} + b^{2p} + (ab)^p \left(\frac{a}{b}\right)^{iq} + (ab)^p \left(\frac{b}{a}\right)^{iq} = c^{2p}$$

Let $z = \frac{a}{b}$. Substituting z and multiplying by z^{iq} we get:

$$(ab)^p z^{2iq} + (a^{2p} + b^{2p} - c^{2p}) z^{iq} + (ab)^p = 0$$

Now z^{iq} satisfies a polynomial with integer coefficients. However, we know z^{iq} must be transcendental by the Gelfond-Schneider theorem, unless of course $z = 1$ or $q = 0$.

If $q = 0$, then we have Fermat's Last Theorem, and we are done.

Otherwise, $z = 1$ and so $a = b$. Then we can take the norms of both sides of our original equation, and solve for c:

$$2a^{p+iq} = c^{p+iq}$$
$$2a^p = c^p$$
$$c = a\sqrt[p]{2}$$

Since c must be an integer, $p = \pm 1$. Then, dividing both sides of the first equation by a^{p+iq}, we get:

$$2 = \left(\frac{c}{a}\right)^{p+iq}$$

so q must be zero, and we are done.

□

23 The Riemann Zeta-Function

The zeta-function can be used to show that certain infinite sums yield transcendental numbers.

Definition 23.1. The Riemann ζ-function is defined as a function of real numbers greater than 1 by

$$\zeta(s) \equiv \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Definition 23.2. The kth Bernoulli number B_k is defined as $k!$ times the kth coefficient in the Taylor series for $\frac{t}{e^t-1}$

Theorem 23.3.

$$\zeta(2k) = (-1)^k \pi^{2k} \frac{2^{2k-1}}{(2k-1)!} \left(-\frac{B_{2k}}{2k} \right).$$

This gives rise to the following examples:

$$\zeta(2) = \frac{\pi^2}{6}, \qquad \zeta(4) = \frac{\pi^4}{90}, \qquad \zeta(6) = \frac{\pi^6}{945}$$

Note that the formula implies $\zeta(2k)$ is transcendental for all k.

24 Examples

This section demonstrates various conclusions from concepts developed in the previous sections.

Example 1. 1 and i form an integral basis for $\mathbb{Q}(i)$. Furthermore, $\mathbb{Q}(i)$ and G, the set of Gaussian integers, are the same set.

We already know that 1 and i are a basis for $\mathbb{Q}(i)$, so every integer $\alpha \in \mathbb{Q}(i)$ can be written $\alpha = a + bi$ for $a, b \in \mathbb{Q}$. We must show that $a, b \in \mathbb{Z}$. The minimal polynomial for α is

$$(x - a - bi)(x - a + bi) = x^2 - 2ax + a^2 + b^2 = 0.$$

Because α is an algebraic integer, $2a, (a^2 + b^2) \in \mathbb{Z}$. Suppose that a and b are not integers. Then

$$2a \in \mathbb{Z} \Longrightarrow \exists\, p \ni a = \frac{p}{2}$$

in which p is odd.

$$b \in \mathbb{Q} \Longrightarrow b = \frac{x}{y}$$

with $(x, y) = 1$. Then, $\exists\, k \in \mathbb{Z} \ni$

$$\frac{p^2}{4} + \frac{x^2}{y^2} = k$$
$$p^2y^2 + 4x^2 = 4y^2k.$$

Therefore,

$$4 \mid p^2y^2 \Longrightarrow 4 \mid y^2 \Longrightarrow 2 \mid y$$

because p is odd. So we can express $y = 2r$ for some integer r.

$$p^2r^2 + x^2 = 4r^2k \Longrightarrow r^2 \mid x^2 \Longrightarrow r \mid x$$

But $(x, y) = (x, 2r) = 1 \Longrightarrow r = 1 \Longrightarrow y = 2 \Longrightarrow x$ is odd. The equation

$$p^2 + x^2 = 4k$$

implies that $4k$ must be an even positive integer because both p^2 and x^2 are positive odd integers.

$$4 \mid 4k \Longrightarrow 4 \mid (p^2 + x^2) \Longrightarrow p^2 \equiv -x^2 \bmod 4$$

For the square of any odd integer, we have

$$(2x + 1)^2 \bmod 4 = (4x^2 + 4x + 1) \bmod 4 = 1 \Longrightarrow 4 \nmid (p^2 + x^2).$$

We see that a rational a implies a contradiction, but is it possible for $a \in \mathbb{Z}$ while $b \in \mathbb{Q}$? Then, we would have

$$a^2 + \frac{x^2}{y^2} = k.$$

But $k - a^2 \in \mathbb{Z}$, so this case implies that $b \in \mathbb{Z}$.

To show that $G \sim \mathbb{Q}(i)$, recall the definition of G:

$$G = \{\alpha = a + bi \mid a, b \in \mathbb{Z}\}.$$

We have just shown that all elements of $\mathbb{Q}(i)$ can be written in the same form as the elements of G.

Example 2. If 1 and i form an integral basis for $\mathbb{Q}(i)$, then can we conclude that the algebraic extension of an algebraic integer θ of degree 2 has the integral basis 1 and θ? A counter example is simple to find. Consider the polynomial $x^2 - 162 = 0$, which has solutions $x = \pm 9\sqrt{2}$. If we adjoin one solution with the rational numbers, $\mathbb{Q}(9\sqrt{2})$, we can check our proposition. Any element of $\mathbb{Q}(9\sqrt{2})$ can be written as $a + b \cdot 9\sqrt{2}$ with $a, b \in \mathbb{Q}$ by Theorem 10.2. Let $a = 1$ and $b = 1/3$. The algebraic number $1 + (1/3) \cdot 9\sqrt{2} = 1 + 3\sqrt{2} \in \mathbb{Q}(9\sqrt{2})$ is actually an algebraic integer, contrary to $1/3 \notin \mathbb{Z}$, as seen by its minimal polynomial:

$$(x - 1 - 3\sqrt{2})(x - 1 + 3\sqrt{2}) = x^2 - 2x - 17.$$

Example 3. Is there a relationship among the field extensions $\mathbb{Q}\left(\theta^{(1)}\right), \mathbb{Q}\left(\theta^{(2)}\right), \ldots,$ $\mathbb{Q}\left(\theta^{(n)}\right)$ of the conjugates of algebraic numbers $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$?

We begin by looking at at a simple quadratic field extension $\mathbb{Q}(\sqrt{6})$, which has a basis 1 and $\sqrt{6}$. We know by Theorem 16.11 that 1 and $-\sqrt{6}$ is also a basis for $\mathbb{Q}\left(\sqrt{6}\right)$ because

$$\begin{pmatrix} 1 \\ -\sqrt{6} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{6} \end{pmatrix}$$

and

$$\begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix} = -1 \neq 0.$$

The field extension $\mathbb{Q}(-\sqrt{6})$ of the conjugate of $\sqrt{6}$ also has the basis 1 and $-\sqrt{6}$, so the field extensions share all elements, that is to say $\mathbb{Q}(\sqrt{6}) = \mathbb{Q}(-\sqrt{6})$.

We find that the same conclusion can be reached about the field extensions of conjugates of any minimal polynomial of degree 2. For a minimal polynomial over the rational numbers, we multiply through by the greatest common denominator to get a polynomial of the form

$$ax^2 + bx + c = 0, \qquad a, b, c \in \mathbb{Z}$$

which is known to have solutions

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

We can find find a matrix relationship between the bases of the field extensions $\mathbb{Q}\left(\dfrac{-b + \sqrt{b^2 - 4ac}}{2a}\right)$ and $\mathbb{Q}\left(\dfrac{-b - \sqrt{b^2 - 4ac}}{2a}\right)$ which has a nonzero determinant:

$$\begin{pmatrix} 1 \\ \frac{-b-\sqrt{b^2-4ac}}{2a} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{-b}{a} & -1 \end{pmatrix} \begin{pmatrix} 1 \\ \frac{-b+\sqrt{b^2-4ac}}{2a} \end{pmatrix}$$

and

$$\begin{vmatrix} 1 & 0 \\ \frac{-b}{a} & -1 \end{vmatrix} = -1 \neq 0.$$

This connection among field extensions of conjugates does not continue with algebraic numbers of degree 3. Consider for example

$$x^3 - 2 = 0$$

(note that we do not consider $x^3 - 1 = 0$ because it is not a minimal polynomial). First we want to find all the conjugates, so we factor out the real solution and then use the quadratic formula:

$$\left(x - \sqrt[3]{2}\right)\left(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}\right) = 0$$
$$x = \sqrt[3]{2},\ \sqrt[3]{2}\left(\frac{-1 \pm i\sqrt{3}}{2}\right).$$

The extension $\mathbb{Q}\left(\sqrt[3]{2}\right)$ contains no complex numbers, so it does not contain the other conjugates of $\sqrt[3]{2}$.

Consider one of the other extensions, $\mathbb{Q}\left(\sqrt[3]{2}\left[\left(-1 + i\sqrt{3}\right)/2\right]\right)$, which has a basis

$$1,\ \sqrt[3]{2}\left(\frac{-1 + i\sqrt{3}}{2}\right),\ \text{and}\ \sqrt[3]{4}\left(\frac{-1 - i\sqrt{3}}{2}\right).$$

So every $\alpha \in \mathbb{Q}\left(\sqrt[3]{2}\left[\left(-1+i\sqrt{3}\right)/2\right]\right)$ can be written as

$$\alpha = a_1 + a_2\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right) + a_3\sqrt[3]{4}\left(\frac{-1-i\sqrt{3}}{2}\right)$$

with $a_i \in \mathbb{Q}$. If $a_2 = a_3 = 0$, then $\alpha \in \mathbb{Q}$. If either a_2 or $a_3 \neq 0$, then $\alpha \in \mathbb{C}$. Therefore, the real irrational conjugate $\sqrt[3]{2} \notin \mathbb{Q}\left(\sqrt[3]{2}\left[\left(-1+i\sqrt{3}\right)/2\right]\right)$. We also find that

$$\alpha \neq \sqrt[3]{2}\left(\frac{-1-i\sqrt{3}}{2}\right)$$

because such an α has no rational term ($a_1 = 0$) and no terms with $\sqrt[3]{4}$ ($a_3 = 0$). We cannot choose a rational a_2 such that

$$a_2\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right) = \sqrt[3]{2}\left(\frac{-1-i\sqrt{3}}{2}\right).$$

This conclusion holds generally for minimal polynomials of the form

$$x^3 - n = 0$$

for $n \in \mathbb{Q}$. Notice that such a polynomial is minimal as long as $n \neq q^3$ for any $q \in Q$. We might suppose an exception exists if $n^2 = p^3$ for some $p \in \mathbb{Q}$ because it will change the third basis element. This exception actually does not exist because if $n^2 = p^3$, then $\exists\ q \in \mathbb{Q}$ such that $n = q^3$. This conclusion follows from applying the Fundamental Theorem of Arithmetic to the numerator and denominator of $n^2 = p^3 = \dfrac{x}{y}$. Factoring x into a product of primes reveals that every prime must be raised to at least the sixth power for our equality to hold. Similarly, y is a product of primes to at least the sixth power. Thus, the numerator and denominator of n are products of primes to at least the third power.

Example 4. Let $\omega = \dfrac{-1+i\sqrt{3}}{2}$ and $\sigma = \dfrac{-1-i\sqrt{3}}{2}$. We have found that $\mathbb{Q}\left(\sqrt[3]{2}\right)$, $\mathbb{Q}\left(\sqrt[3]{2}\omega\right)$, and $\mathbb{Q}\left(\sqrt[3]{2}\sigma\right)$ are different fields. If we adjoin all three, we know we can find an equivalent simple algebraic extension $\mathbb{Q}\left(\theta\right)$.

We use the method used in the proof of Theorem 10.3 to find $\mathbb{Q}(\theta) = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\omega\right)$. Let $\alpha_1 = \beta_3 = \sqrt[3]{2}$, $\alpha_2 = \beta_1 = \sqrt[3]{2}\omega$, and $\alpha_3 = \beta_2 = \sqrt[3]{2}\sigma$. Then we must find the x's that satisfy:

$$\begin{aligned}
\alpha_1 + x\beta_1 &= \alpha_1 + x\beta_2\\
\alpha_1 + x\beta_1 &= \alpha_1 + x\beta_3\\
\alpha_1 + x\beta_1 &= \alpha_2 + x\beta_2\\
\alpha_1 + x\beta_1 &= \alpha_2 + x\beta_3\\
\alpha_1 + x\beta_1 &= \alpha_3 + x\beta_2\\
\alpha_1 + x\beta_1 &= \alpha_3 + x\beta_3.
\end{aligned}$$

These solutions are: $x = 0, -\sigma, 1, \omega$. We can pick any other x, say $x = 2$, and let

$$\theta = \alpha_1 + x\beta_1 = \sqrt[3]{2} + 2 \cdot \sqrt[3]{2}\omega = i\sqrt[3]{2}\sqrt{3}.$$

The fact that $\mathbb{Q}\left(i\sqrt[3]{2}\sqrt{3}\right) = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\omega\right)$ follows from the rest of the proof. We could then try to find a γ such that $\mathbb{Q}(\gamma) = \mathbb{Q}\left(i\sqrt[3]{2}\sqrt{3}, \sqrt[3]{2}\sigma\right)$, which would require finding the minimal polynomial for $i\sqrt[3]{2}\sqrt{3}$ and then finding all its conjugates. Instead, we notice that

$$\sqrt[3]{2}\sigma = \frac{-1}{2}(i\sqrt[3]{2}\sqrt{3}) + \frac{-1}{36}(i\sqrt[3]{2}\sqrt{3})^4,$$

so $\sqrt[3]{2}\sigma \in \mathbb{Q}(i\sqrt[3]{2}\sqrt{3})$. For any $\alpha \in \mathbb{Q}(\theta)$, $\mathbb{Q}(\theta, \alpha) = \mathbb{Q}(\theta)$ because $\mathbb{Q}(\theta, \alpha)$ is defined to be the *smallest* field containing $\mathbb{Q}$ and both θ and α. $\mathbb{Q}(\theta)$ fits this definition. Therefore $\mathbb{Q}(\sqrt[3]{2}\sigma, i\sqrt[3]{2}\sqrt{3}) = \mathbb{Q}(i\sqrt[3]{2}\sqrt{3})$, and thus $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\sigma) = \mathbb{Q}(i\sqrt[3]{2}\sqrt{3})$.

Example 5. The proof of Theorem 19.5 suggests a method for generating normal simple algebraic extensions; namely, a simple algebraic extension equal to a multiple algebraic extension of conjugates will always be normal.

For some $\gamma \in \overline{\mathbb{Q}}$ of degree n, we have conjugates $\gamma_1, \gamma_2, \ldots, \gamma_n$. By Theorem 10.3, there exists θ such that $\mathbb{Q}(\gamma_1, \gamma_2, \ldots, \gamma_n) = \mathbb{Q}(\theta)$. For any $\rho \in \mathbb{Q}(\theta)$, we must show that all conjugates of ρ are also in $\mathbb{Q}(\theta)$. By a generalization of Theorem 10.2, any element of $\mathbb{Q}(\theta) = \mathbb{Q}(\gamma_1, \gamma_2, \ldots, \gamma_n)$ can be written as a polynomial in of $\gamma_1, \gamma_2, \ldots, \gamma_n$ with rational coefficients (instead of a polynomial in θ with rational coefficient). Let $\rho = f(\gamma_1, \gamma_2, \ldots, \gamma_n)$. Let

$$G(x) = \prod \{x - f(\gamma_{i_1}, \gamma_{i_2}, \ldots, \gamma_{i_n})\}$$

over all permutations of $i_1, i_2, \ldots, i_n$. The coefficients of $G(x)$ are symmetric polynomials in its roots $f(\gamma_{i_1}, \gamma_{i_2}, \ldots, \gamma_{i_n})$. Any permutation of $\gamma_1, \gamma_2, \ldots, \gamma_n$ merely permutes the $f(\gamma_{i_1}, \gamma_{i_2}, \ldots, \gamma_{i_n})$ among themselves. Thus, the coefficients of $G(x)$ are symmetric polynomials in $\gamma_1, \gamma_2, \ldots, \gamma_n$ and so are rational numbers by Theorem 8.3. The polynomials $g(x)$ and $G(x)$ share the root ρ, and because $g(x)$ is minimal, $g(x)$ must be a factor of $G(x)$. But all roots of $G(x) = 0$ are elements of $\mathbb{Q}(\theta)$ because they can all be written as polynomials in $\gamma_1, \gamma_2, \ldots, \gamma_n$. All roots of $g(x) = 0$ are also roots of $G(x) = 0$ because $g(x)$ is a factor of $G(x)$; therefore, all roots of $g(x) = 0$ are elements of $\mathbb{Q}(\theta)$ as desired.

In Example 4, we found that $\mathbb{Q}(i\sqrt[3]{2}\sqrt{3}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\sigma)$ where $\sqrt[3]{2}, \sqrt[3]{2}\omega$, and $\sqrt[3]{2}\sigma$ are conjugates of $x^3 - 2 = 0$. Therefore, $\mathbb{Q}(i\sqrt[3]{2}\sqrt{3})$ is normal.

Example 6. The set of all polynomials with integer coefficients is countable.

We have already agreed that every set of positive integers has a smallest element. Thus, a set of infinitely many unique positive integers will have a unique smallest element. We can map such a set to the positive integers by letting the smallest element correspond to 1. If we remove the smallest element from the set, we will have a new unique smallest element, which will correspond to 2. We can continue this pattern to map a set of infinitely many unique positive integers to the positive integers.

If we can map the set of polynomials $\in \mathbb{Z}[x]$ to a set of positive integers, then that set can be mapped to the positive integers, from which we can conclude our desired result.

We assign two primes to each term of a polynomial in ascending order. The constant term will be assigned 2 and 3; the first degree term will be assigned 5 and 7; the second degree term will be assigned 11 and 13; and so on. We have proven that there exist infinitely many primes, so this method of assignment can account for a polynomial of any degree. The smaller prime assigned to each term will stand for a positive coefficient, and the larger prime will stand for a negative coefficient. The primes will be raised to the absolute value of their coefficients; for a polynomial of degree n, notice that only n primes will be raised to powers even though we will have $2n$ possible primes for that polynomial. We assign a number to the polynomial by multiplying together all the primes to their appropriate powers. For instance, the polynomial

$$12x^3 - 7x^2 + 8x - 2$$

would be assigned the number

$$3^2 \cdot 5^8 \cdot 13^7 \cdot 17^{12} = 1285266141470731324726300781 25.$$

As we can see, the assigned numbers get incredibly large very easily. Nevertheless, we know that each such number is unique from the Fundamental Theorem of Arithmetic. Thus, we have mapped the set of polynomials $\in \mathbb{Z}[x]$ to a set of infinitely many unique rational integers, which can be mapped to the set of positive integers. Thus, the set of polynomials $\in \mathbb{Z}[x]$ is countable.

Note that not all positive integers will be assigned a polynomial. For example, $12 = 2^2 \cdot 3$, which would imply that the constant term has both a positive and a negative coefficient. Also, the ordering of the polynomials does not relate any information about their complexity (not in the imaginary sense). For instance, x^2+x+1, which is assigned $2\cdot 5\cdot 11 = 110$, would probably be considered more complex than $x - 20$, which is assigned $3^{20} \cdot 5 = 17433922005$. We can use a similar method for proving the countability of polynomials $\in \mathbb{Q}[x]$, but we would need three primes per term (one for a positive numerator, one for a negative numerator, and one for the denominator) causing the assigned numbers to become even larger. If we agreed that polynomials with the same solutions were equivalent and did not need separate numbers, we could map $\mathbb{Q}[x] \to \mathbb{Z}[x]$. Unfortunately, polynomials $\in \mathbb{Z}[x]$ could be equivalent with different numbers, such as x^2+x+1 and $2x^2+2x+2$. Therefore, the attempt to assign one number to polynomials with the same solutions is laborious because we would have to determine which polynomials are equivalent in this way.

Similarly, the countability of the algebraic numbers is possible but laborious. First, we would only order minimal polynomials; thus, we would have to check each polynomial for this feature. Second, we would start the assignment of primes to coefficients with 3 instead of 2. We would reserve 2 to indicate which solution to our polynomial we desired. We would order the solutions first according to their arguments in the complex plane, and then by their magnitudes. The number assigned to the first solution would have a factor of 2, that assigned to the second would have a factor of 2^2, etc.

Example 7. We can use Lemma 22.5, which we used in the Gelfond-Schneider Theorem, to find a bound for the solutions to a set of equations:

$$\begin{aligned}\alpha_{11}\xi_1 + \alpha_{12}\xi_2 + \cdots + \alpha_{1q}\xi_q &= 0\\ \alpha_{21}\xi_1 + \alpha_{22}\xi_2 + \cdots + \alpha_{2q}\xi_q &= 0\\ &\vdots\\ \alpha_{p1}\xi_1 + \alpha_{p2}\xi_2 + \cdots + \alpha_{pq}\xi_q &= 0\end{aligned}$$

in which $0 < p < q$ and $\alpha_{ij} \in \overline{\mathbb{Q}}$. We will work out a specific example in which $\alpha_{ij} \in \mathbb{Q}(i)$. Let $\alpha_{ij} = i + j\sqrt{-1}$, $p = 3$, and $q = 4$:

$$\begin{aligned}(1+i)\xi_1 + (1+2i)\xi_2 + (1+3i)\xi_3 + (1+4i)\xi_4 &= 0\\ (2+i)\xi_1 + (2+2i)\xi_2 + (2+3i)\xi_3 + (2+4i)\xi_4 &= 0\\ (3+i)\xi_1 + (3+2i)\xi_2 + (3+3i)\xi_3 + (3+4i)\xi_4 &= 0.\end{aligned}$$

Notice that $\max_{i,j} \|\alpha_{ij}\| = \|3+4i\| = 25$. Recall that $\|\xi_j\| < c + c(cqA)^{\frac{p}{q-p}}$. We have determined $A \leq 25$, so we have only to determine c in our bound. According to the proof, we choose $c > hc_2$ and $c > h \max_j \|\beta_j\|$ in which $h = \deg \mathbb{Q}(i) = 2$, $1 + c_1 \max_j \|\beta_j\| > c_2 \geq c_1 \max_j \|\beta_j\|$, $c_1 > \frac{\max(i,j)}{\max_{i,j} \|\alpha_{ij}\|}$, and β_j are the basis elements of $\mathbb{Q}(i)$. So we choose β_j to be 1 and i; $\max_j \|\beta_j\| = 1$; $\dfrac{4}{25} < c_1 = 1$; $c_2 = 1 \cdot 1 = 1$; and thus $2 < c = 3$. Therefore,

$$\|\xi_j\| < 3 + 3(3 \cdot 4 \cdot 25)^3 = 27000003.$$

We see that even for the simple algebraic numbers we constructed, this bound gets very large.

Example 8. We can rewrite some simple symmetric polynomials in the elementary symmetric polynomials to demonstrate Theorem 8.2. We begin with

$$x_1^2 + x_2^2 + \cdots + x_n^2.$$

Using the method in the proof, we know we will need the elementary symmetric polynomials

$$\begin{aligned}\sigma_1^2 =& (x_1^2 + x_2^2 + \cdots + x_n^2)\\ &+ 2(x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \ldots x_{n-1}x_n)\\ \sigma_2 =& x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \ldots x_{n-1}x_n.\end{aligned}$$

Then, we can write

$$x_1^2 + x_2^2 + \cdots + x_n^2 = \sigma_1^2 - 2\sigma_2.$$

We can similarly treat

$$x_1^3 + x_2^3 + \cdots + x_n^3,$$

for which we will need

$$\begin{aligned}
\sigma_1^3 =& (x_1^3 + x_2^3 + \cdots + x_n^3) \\
&+ 3(x_1^2x_2 + x_1^2x_3 + \cdots + x_1^2x_n + x_2^2x_3 + \cdots + x_{n-1}x_n^2) \\
&+ 3(x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n) \\
\sigma_1\sigma_2 =& (x_1^2x_2 + x_1^2x_3 + \cdots + x_1^2x_n + x_2^2x_3 + \cdots + x_{n-1}x_n^2) \\
&+ 3(x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n) \\
\sigma_3 =& (x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n).
\end{aligned}$$

Then we see that

$$x_1^3 + x_2^3 + \cdots + x_n^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 6\sigma_3.$$

Example 9. Define *roots of unity* to be solutions to polynomials of the form

$$x^k - 1 = 0$$

for positive integers k. For example, ± 1 and $\dfrac{-1 \pm i\sqrt{3}}{2}$ are roots of unity. We can show that the roots of unity form a group under multiplication.

First, we show that for roots of unity α and β, $\alpha\beta$ is also a root of unity. By definition, there exist positive integers l and m such that

$$\begin{aligned}
\alpha^l - 1 &= 0 & \beta^m - 1 &= 0 \\
\alpha^l &= 1 & \beta^m &= 0.
\end{aligned}$$

Therefore,

$$(\alpha^l)^m = 1^m = 1 \quad \text{and} \quad (\beta^m)^l = 1^l = 1.$$

Let $k = l \cdot m$ so that $\alpha\beta$ satisfies

$$x^k - 1 = 0$$

because

$$(\alpha\beta)^{lm} = (\alpha^l)^m \cdot (\beta^m)^l = 1.$$

We have established that multiplication is a binary operator on this set. Associativity must hold because these are all algebraic numbers. The root of unity 1 satisfies the criterion for the multiplicative identity. Now we show that a multiplicative inverse exists. Let α satisfy $x^l - 1 = 0$. The equation $x^l - 1 = 0$ gives l roots of unity $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_l$. We can factor our polynomial

$$(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_l) = 0$$

where each α_i also satisfies $x^l - 1 = 0$ (i.e., $\alpha_i^l = 1$). When we take the product $\alpha_1\alpha_2\cdots\alpha_l$ we must get the constant term of the polynomial, 1. Let the inverse of α be

$$\frac{1}{\alpha_1} = \alpha_2\alpha_3\cdots\alpha_l.$$

This number satisfies $x^l - 1 = 0$ because

$$\begin{aligned}\left(\frac{1}{\alpha_1}\right)^l - 1 &= (\alpha_2\alpha_3\cdots\alpha_l)^l - 1\\ &= \alpha_2^l\alpha_3^l\cdots\alpha_l^l - 1\\ &= 1^l1^l\cdots1^l - 1\\ &= 1 - 1\\ &= 0.\end{aligned}$$

Example 10. In this example, we look at a few properties of polynomials of the form $x^n - 1 = 0$.

Roots of such polynomials must all have a norm of 1 on the complex plane. Therefore they can be written in the form $e^{i\theta}$. These roots are always located on a unit circle, separated by equal angles of rotation.

To see this, label the roots x_k, ordered by their arguments. Then $x_k = e^{i\theta_k}$. Substituting into the polynomial

$$(e^{i\theta_k})^n - 1 = 0$$

$$e^{i\theta_k n} = e^{i2\pi k} \text{ where } k \in \mathbb{Z}$$

Therefore:

$$\begin{aligned}\theta_k n &= 2\pi k\\ \frac{\theta}{2\pi} &= \frac{k}{n}\end{aligned}$$

Since k is an integer, the θ_k must be distributed evenly. This also means that the k's are a complete residue system modulo n.

Raising any root to an integer power is equivalent multiply its angle θ by that power, thereby rotating to a different root on the circle. Therefore, raising the k-th root to successive integer powers will yield all the other roots if and only if $(k, n) = 1$.

Example 11. Now we can prove a more general version of Theorem 15.1:

Theorem 24.1. *Given a polynomial*

$$f(x) = c_nx^n + \cdots + c_0 = 0$$

where $c_nc_0 \neq 0$, *then then for any rational roots* $\frac{a}{b}$, *where* $(a, b) = 1$, *of* $f(x)$, $a \mid c_0$ *and* $b \mid c_n$.

Proof. Let $x = \frac{a}{b}$ be a root for $f(x)$. Then:

$$0 = c_n \frac{a^n}{b^n} + c_{n-1} \frac{a^{n-1}}{b^{n-1}} + \cdots + c_1 \frac{a}{b} + c_0$$

$$0 = c_n a^n + c_{n-1} a^{n-1} b + \cdots + c_1 a b^{n-1} + c_0 b^n$$

Both a and b divide 0, and so they must both divide the right side of the equation. a is a factor of all the terms of the right side except the last. Therefore $a \mid c_0 b^n$. Since $(a, b) = 1$, then $a \mid c_0$. Likewise, b is a factor of all the terms except the first one, so $b \mid c_n a^n$. Once again, $b \nmid a$, so $b \mid c_n$. □

Example 12. Corollary 16.7 states that any element of $K = F(\theta)$ must have degree m that divides the degree of K. From this we can draw a family of conclusions. In general, any algebraic number of degree m cannot lie in an extension of degree n if $m \nmid n$. For example:

1. if θ has a fifth degree minimal polynomial, then $\sqrt{2}$ cannot expressed in terms of a polynomial in θ.
2. $\sqrt[3]{2}$ is not in $\mathbb{Q}(\sqrt[7]{6})$
3. $\sqrt[7]{6}$ is not in $\mathbb{Q}(\sqrt[15]{8})$

Example 13. In this example we show that the transcendence of e^π follows from the Gelfond-Schneider theorem.

We note the special formula for taking the logarithm of a complex number:

$$\forall z \in \mathbb{C},\ \log z = \ln |z| + i \arg(z)$$

Since i and $-2i$ are both algebraic, by the Gelfond-Schneider theorem, i^{-2i} is transcendental. Furthermore:

$$\begin{aligned} i^{-2i} &= e^{-2i \log i} \\ &= e^{-2i\left(\ln 1 + i\frac{\pi}{2}\right)} \\ &= e^{-2i\left(i\frac{\pi}{2}\right)} \\ &= e^{\pi} \\ &= 1 + \pi + \frac{\pi^2}{2} + \frac{\pi^3}{6} + \cdots \end{aligned}$$

Therefore e^π is also transcendental.

References

[1] Robert E. Greene and Steven G. Krantz, *Function Theory of One Complex Variable*, Wiley, New York, 1997.

[2] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta Functions*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1977.

[3] Joseph Landin, *Introduction to Algebraic Structures*, Dover, New York, 1989.

[4] Kumiko Nishioka, *Mahler Functions and Transcendence*, Lecture Notes in Mathematics 1631, Springer-Verlag, Berlin, 1996.

[5] Ivan Niven, *Irrational Numbers*, Fourth ed., Carus Mathematical Monographs, Mathematical Association of America, 1997.

[6] Bruce P. Palka, *An Introduction to Complex Function Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1991.

[7] Harry Pollard and Harold G. Diamond, *The Theory of Algebraic Numbers*, Third ed., Dover, New York, 1998.

[8] Walter Rudin, *Principles of Mathematical Analysis*, Second ed., McGraw-Hill, New York, 1964.

[9] John Zuelke *Fermat's Last Theorem for Gaussian Integer Exponents*, American Mathematical Monthly, Vol. 106.1, Jan. 1999, p. 49.