# Algebraic Numbers

Further Studies in Mathematics

**Shivank Goel**
*University of Toronto Mississauga*
Supervisor: Professor Marina Tvalvazade

Fall 2024

# Contents

# 1 Primitive Polynomial

A **primitive polynomial** is a polynomial with integer coefficients in $\mathbb{Z}[x]$ such that the greatest common divisor (GCD) of its coefficients is 1. In other words, a polynomial is primitive if its coefficients have no common prime divisor.

**Example of a Primitive Polynomial:**

$$f(x) = 2x^2 + 3x + 1$$

Here, the GCD of the coefficients $\{2, 3, 1\}$ is 1, so this polynomial is primitive.

**Non-Example (Not Primitive):**

$$g(x) = 2x^2 + 4x + 6$$

In this case, the GCD of the coefficients $\{2, 4, 6\}$ is 2, so this polynomial is not primitive.

**Key Concept:** A primitive polynomial is related to the content of the polynomial, which is the GCD of its coefficients. If the content is 1, the polynomial is primitive.

# 2 Irreducible Polynomial

A **polynomial is irreducible** if it cannot be factored into the product of two non-constant polynomials with coefficients in the same ring (e.g., $\mathbb{Z}[x]$ or $\mathbb{Q}[x]$).

**Example of an Irreducible Polynomial (over $\mathbb{Q}$):**

$$f(x) = x^2 + 1$$

This polynomial cannot be factored over $\mathbb{Q}[x]$ into lower-degree polynomials, so it is irreducible over $\mathbb{Q}$.

**Non-Example (Not Irreducible):**

$$g(x) = x^2 - 1 = (x - 1)(x + 1)$$

Here, $g(x)$ can be factored into two polynomials of degree 1, so it is not irreducible.

**Key Concept:** Irreducibility refers to the inability to factor a polynomial into lower-degree polynomials with coefficients in the same field or ring.

# Summary

- **Primitive Polynomial**: Focuses on the **coefficients** of the polynomial. A polynomial is primitive if the GCD of its coefficients is 1.
- **Irreducible Polynomial**: Focuses on the **factorization** of the polynomial. A polynomial is irreducible if it cannot be factored into the product of two non-constant polynomials with coefficients in the same field or ring.

A polynomial can be both primitive and irreducible, but these properties are independent of each other:

- A polynomial can be **primitive but reducible**, e.g.,

$$f(x) = x^2 - 1 = (x - 1)(x + 1)$$

  Here, $f(x)$ is reducible but primitive, as the GCD of its coefficients is 1.

- A polynomial can be **irreducible but not primitive**, e.g.,

$$g(x) = 2x^2 + 4x + 6$$

  This polynomial is irreducible over $\mathbb{Z}$, but not primitive, as the GCD of its coefficients is 2.

**Theorem 1: 1**

Product of two primitive polynomials is primitive.

Let $f(x), g(x) \in \mathbb{Z}[x]$ be primitive polynomials, i.e., $c(f(x)) = c(g(x)) = 1$, where $c(f(x))$ denotes the content of $f(x)$, which is the greatest common divisor of the coefficients of $f(x)$.

Assume, for contradiction, that $h(x) = f(x)g(x)$ is not primitive. This would mean that $c(h(x)) \neq 1$, so there exists a prime $p$ such that $p$ divides all the coefficients of $h(x)$.

Write $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_mx^m$, where $a_i, b_j \in \mathbb{Z}$. Since $f(x)$ and $g(x)$ are primitive, $p$ does not divide all the coefficients of either $f(x)$ or $g(x)$.

Now consider the product:

$$h(x) = f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m}.$$

By assumption, $p$ divides all the coefficients of $h(x)$. In particular, $p$ divides the constant term $a_0b_0$. Thus, $p$ must divide either $a_0$ or $b_0$, but not both (since $f(x)$ and $g(x)$ are primitive).

Without loss of generality, assume $p \mid a_0$ but $p \nmid b_0$. Consider the next term in $h(x)$, which is $a_0b_1 + a_1b_0$. Since $p \mid a_0$ and $p \mid a_0b_1 + a_1b_0$, we must have $p \mid a_1b_0$. Since $p \nmid b_0$, it follows that $p \mid a_1$.

Continuing in this way, we conclude that $p$ divides all the coefficients of $f(x)$. This contradicts the assumption that $f(x)$ is primitive.

Similarly, if we had assumed $p \mid b_0$ and $p \nmid a_0$, we would have reached the conclusion that $p$ divides all the coefficients of $g(x)$, contradicting the fact that $g(x)$ is primitive.

Therefore, our assumption that $h(x)$ is not primitive must be false, and so $h(x) = f(x)g(x)$ is primitive.

**Lemma 1: Gauss Lemma**

If a monic polynomial $f(x)$ with integral coefficient factors into two monic polynomials with rational coefficient say $f(x) = g(x)h(x)$, then $g(x)$ and $h(x)$ have integral coefficients.

In other words, Reducibility over $Q$ implies reducibility over $Z$.

Let $f(x) \in \mathbb{Z}[x]$.

Given that $f(x)$ is reducible over $\mathbb{Q}$, we have $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are monic polynomials with rational coefficients, i.e. $g(x), h(x) \in \mathbb{Q}[x]$, with $\deg(g(x)) < \deg(f(x))$ and $\deg(h(x)) < \deg(f(x))$.

Assume $f(x)$ is primitive.

Since $g(x)$ and $h(x)$ have rational coefficients, let $a$ be the least common multiple of the denominators of the coefficients of $g(x)$, and $b$ the least common multiple of the denominators of the coefficients of $h(x)$.

Now multiply both sides of the equation $f(x) = g(x)h(x)$ by $ab$ to clear the denominators. This gives:

$$abf(x) = ag(x)bh(x)$$

Let $g_1(x) = ag(x)$ and $h_1(x) = bh(x)$, where $g_1(x), h_1(x) \in \mathbb{Z}[x]$.

Now let $c_1 = c(g_1(x))$ and $c_2 = c(h_1(x))$ be the contents of $g_1(x)$ and $h_1(x)$, respectively.

We can then write:

$$abf(x) = c_1 g_2(x) c_2 h_2(x)$$

where $g_2(x)$ and $h_2(x)$ are primitive polynomials.

Since the product of two primitive polynomials is primitive, $g_2(x)h_2(x)$ is primitive. Therefore, we have:

$$ab = c_1 c_2$$

which implies that $f(x)$ is primitive.

If $f(x)$ is not primitive, we can write $f(x) = cf_1(x)$, where $c = c(f(x))$ and $f_1(x)$ is primitive. Since $f_1(x)$ is reducible over $\mathbb{Z}$ (from the argument above), it follows that $f(x)$ is reducible over $\mathbb{Z}$ as well.

This completes the proof.

# 3 Algebraic Number

### Definition 2: Algebraic Number

$x$ is algbraic if $x$ is root of polynomial with integer coefficient, i.e. there are integers $a_n$, $a_{n-1}$, ..., $a_0$ such that

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

**Example.**

$x = \sqrt[3]{\frac{\sqrt{2}-3}{5}}$ is algebraic?

$x^3 = \frac{\sqrt{2}-3}{5}$

$5x^3 + 3 = \sqrt{2}$

$25x^6 + 30x^3 + 9 = 2$

$25x^6 + 30x^3 + 7 = 0$

Therefore, $x$ is algebraic.

### Definition 3: Transcendental Number

A number that is not algebraic.

**Example.**

$\pi$, $e$ are transcendental numbers.

### Definition 4: Algebraic Integers

Algebraic Integers: These are a special subset of algebraic numbers that satisfy a monic polynomial (leading coefficient 1) with integer coefficients. for example, $\sqrt{2}$ is also an algebraic integer because it satisfies $x^2 - 2 = 0$ monic polynomial with integer coefficients.

### Definition 5: Unique Minimal Polynomial

For any algebraic number $g$, there is a unique minimal polynomial over $\mathbb{Q}$. This is the irreducible monic polynomial that has $g$ as a root. It is the polynomial of the smallest degree with rational coefficients that has $g$ as a solution.

**Example.**

For example, for $\sqrt{2}$, the minimal polynomial is $x^2-2$, since this is the simplest polynomial with rational coefficients that has $\sqrt{2}$ as a root. As $x^2-2$ is irreducible over $\mathbb{Q}$, it is the unique minimal polynomial for $\sqrt{2}$. (if we factor it, we get $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$ i.e. it is reducible over $\mathbb{R}$ but not over $\mathbb{Q}$.)

## Theorem 2

For any algebraic number $g$, there is a unique irreducible monic polynomial over $\mathbb{Q}$ such that:

1. $g$ satisfies the polynomial equation $g(x)=0$,
2. Any other polynomial over $\mathbb{Q}$ that has $g$ as a root is divisible by $g(x)$.

Since $g$ is an algebraic number, it satisfies some polynomial equation with rational coefficients. Out of all such polynomials, let's choose one of the lowest degree, say $G(x)$, such that $G(g)=0$. If $G(x)$ is not monic, we divide it by its leading coefficient to create a monic polynomial $g(x)$. Now, $g(x)$ is a monic polynomial of the lowest degree that has $g$ as a root.

We now show that $g(x)$ is irreducible over $\mathbb{Q}$. Suppose, for contradiction, that $g(x)$ can be factored as:

$$g(x)=h_1(x)h_2(x)$$

where $h_1(x)$ and $h_2(x)$ are lower-degree polynomials with rational coefficients. Since $g$ is a root of $g(x)$, one of $h_1(g)=0$ or $h_2(g)=0$ must be true. This would contradict the fact that $g(x)$ was chosen to have the lowest degree, since $h_1(x)$ or $h_2(x)$ would have a smaller degree than $g(x)$. Hence, $g(x)$ must be irreducible.

Now, let $f(x)$ be any polynomial over $\mathbb{Q}$ that has $g$ as a root (i.e., $f(g)=0$). Using the division algorithm for polynomials, we can write:

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

where $r(x)$ is a remainder with degree smaller than that of $g(x)$. Since $f(g)=g(g)=0$, it follows that:

$$0=f(g)=g(g)q(g)+r(g)=0+r(g)$$

which implies that $r(g)=0$. Since the degree of $r(x)$ is less than that of $g(x)$, the only way this is possible is if $r(x)=0$. Therefore, $f(x)$ must be divisible by $g(x)$.

Finally, let's assume there is another irreducible monic polynomial, say $g_1(x)$, such that $g_1(g)=0$. Since $g_1(x)$ has $g$ as a root, and $g(x)$ is the minimal polynomial, we know $g_1(x)$ must divide $g(x)$ and vice versa. Since both polynomials are irreducible and monic, this implies that $g_1(x)=g(x)$. Thus, $g(x)$ is unique.

Therefore, for any algebraic number $g$, there exists a unique irreducible monic polynomial over $\mathbb{Q}$, and any other polynomial over $\mathbb{Q}$ with $g$ as a root is divisible by

this minimal polynomial.

### Definition 6: Degree of an Algebraic Number

The degree of an algebraic number is the degree of its minimal polynomial over $\mathbb{Q}$.

**Example.**

The degree of $\sqrt{2}$ is 2, as its minimal polynomial is $x^2 - 2$.

### Theorem 3

Among the rational numbers, the only ones that are algebraic integers are the integers $0, \pm 1, \pm 2, \pm 3, \ldots$

Any integer $m$ is an algebraic integer because it satisfies the monic polynomial $x - m = 0$, which has integer coefficients.

Now, consider a rational number $\frac{m}{q}$, where $m$ and $q$ are integers and $\gcd(m, q) = 1$. If $\frac{m}{q}$ is an algebraic integer, it must satisfy a monic polynomial with integer coefficients:

$$\left(\frac{m}{q}\right)^n + b_{n-1}\left(\frac{m}{q}\right)^{n-1} + \cdots + b_0 = 0$$

where $b_{n-1}, \ldots, b_0$ are integers. Multiplying through by $q^n$ to clear the denominators, we obtain:

$$m^n + b_{n-1}m^{n-1}q + \cdots + b_0 q^n = 0$$

This implies that $q$ must divide $m^n$. Since $\gcd(m, q) = 1$, the only possibility is $q = \pm 1$, which means $\frac{m}{q}$ must be an integer.

**Example:** - A rational integer: 2, because it satisfies $x - 2 = 0$ and is a rational number.
- An algebraic integer but not a rational integer: $\sqrt{2}$, because it satisfies $x^2 - 2 = 0$, but is not a rational number.

### Theorem 4

The minimal equation of an algebraic integer is monic with integral coefficients.

By definition, the minimal polynomial of an algebraic integer is **monic**, meaning its leading coefficient is 1. Therefore, it is assumed from the start that the polynomial is monic.

Now, let $g$ be an algebraic integer. Since $g$ is an algebraic integer, it satisfies some polynomial equation with **integer coefficients**. Let this polynomial be $f(x)$, such

that:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

where $a_n, a_{n-1}, \ldots, a_0$ are integers.

Let $g(x) = 0$ be the minimal polynomial of $g$, which is **monic** and **irreducible** over $\mathbb{Q}$. By Theorem 2, the minimal polynomial $g(x)$ divides any polynomial with $g$ as a root. Therefore, $g(x)$ divides $f(x)$, giving:

$$f(x) = g(x)h(x)$$

where $h(x)$ is another polynomial, and both $g(x)$ and $h(x)$ have rational coefficients. Since $f(x)$ has integer coefficients, by Gauss's Lemma, if a monic polynomial with rational coefficients divides a polynomial with integer coefficients, the dividing polynomial must have integer coefficients as well.

Thus, the minimal polynomial $g(x)$ of the algebraic integer $g$ must have integer coefficients.

**Theorem 5**

Let $n$ be a positive rational integer, and $g$ a complex number. Suppose we have a system of $n$ equations involving complex numbers $\theta_1, \theta_2, \ldots, \theta_n$, not all zero, given by:

$$g\theta_j = a_{j,1}\theta_1 + a_{j,2}\theta_2 + \cdots + a_{j,n}\theta_n, \quad j = 1, 2, \ldots, n$$

where $a_{j,i}$ are rational numbers. Then:

1. $g$ is an algebraic number.
2. If $a_{j,i}$ are rational integers, $g$ is an algebraic integer.

**Theorem 6**

If $\alpha$ and $\beta$ are algebraic numbers, then so are $\alpha + \beta$ and $\alpha\beta$. If $\alpha$ and $\beta$ are algebraic integers, then so are $\alpha + \beta$ and $\alpha\beta$.

# 4 Ring Theory

### Example 1: The Ring of Integers $\mathbb{Z}$

The set of integers $\mathbb{Z}$ has two operations: addition and multiplication.

- $(\mathbb{Z}, +)$ is an abelian group.
- $(\mathbb{Z}, \times)$ is not a group since there is no multiplicative inverse for every element. However, a multiplicative inverse is not required for a set to be a ring.

### Example 2: The Field of Rational Numbers $\mathbb{Q}$

The set $\mathbb{Q}$ of rational numbers has two operations: addition and multiplication.

- $(\mathbb{Q}, +)$ is an abelian group.
- $(\mathbb{Q}, \times)$ is not a group, but $(\mathbb{Q} \setminus \{0\}, \times)$ forms an abelian group.

Similarly, the sets $\mathbb{R}$ (real numbers) and $\mathbb{C}$ (complex numbers) also form rings under addition and multiplication.

### Example 3: The Gaussian Integers $\mathbb{Z}[i]$

Consider $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, where $i$ is the imaginary unit, i.e., $i^2 = -1$.

- $1 \in \mathbb{Z}[i]$, and for any integer $n \in \mathbb{Z}$, $n \in \mathbb{Z}[i]$.
- $\mathbb{Z}[i] \subseteq \mathbb{C}$, and it is closed under addition:

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

  where $a + bi \in \mathbb{Z}[i]$ and $c + di \in \mathbb{Z}[i]$.

- It is easy to verify that $\mathbb{Z}[i]$ is an abelian group under addition and is a subgroup of $(\mathbb{C}, +)$.
- $\mathbb{Z}[i]$ is closed under multiplication as well:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i,$$

  and both terms are in $\mathbb{Z}[i]$.

Thus, $\mathbb{Z}[i]$ is a ring under addition and multiplication.

### Example 4: A Non-Ring Set

Consider the set $A = \left\{a + \frac{b}{2} \mid a, b \in \mathbb{Z}\right\}$ (where $1/2$ replaces $i$). Note:

- $\frac{1}{2} \in A$, but $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4} \notin A$.

Therefore, $A$ is not closed under multiplication, and hence it is not a ring.

### Definition 7: Ring

A ring $R$ is a set with two operations, denoted by $+$ (addition) and $\times$ (multiplication), satisfying the following properties:

1. $(R, +)$ is an abelian group.
2. Multiplication is commutative, associative, and contains an identity element.
3. Addition and multiplication are distributive over each other, i.e., $\forall a, b, c \in R$:

$$(a + b)c = ac + bc \quad \text{and} \quad a(b + c) = ab + ac.$$

Examples: The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[i]$ are all rings. Additionally, the distributive property holds for $\mathbb{C}$, and thus it also holds for the sets $\mathbb{Z} \subseteq \mathbb{Z}[i] \subseteq \mathbb{C}$, and similarly for $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Distribtuive property holds for $\mathbb{C}$ so it also holds for other sets above: $\mathbb{Z} \subseteq Z[i] \subseteq \mathbb{C}$.

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

### Definition 8: Subring

Let $R$ be a ring. A subset $S$ of $R$ is called a **subring** of $R$ if it satisfies the following conditions:

- It is closed under addition and multiplication.
- It is a subgroup of $(R, +)$.
- It contains the multiplicative identity 1.

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$,$Z[i]$ are subrings of $\mathbb{C}$.

*It is possible to define rings wothout asking for multiplication to be commutative. They are called non-commutative rings. For example, the set of matrix rings: ex: $3 \times 3$ square matrices with real entries.*

*Rings can also be defined by not asking for multiplicative identity. ex: $R = 2Z = \{$ even integers $\}$ does not have 1.*

**More Examples of Rings**

1. **Zero Ring:** Let $R = \{0\}$. In this ring, the only element is 0, and here $0 = 1$. This is a trivial example of a ring.
2. $\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$: Consider the integers $\mathbb{Z}$. The set $3\mathbb{Z}$ (multiples of 3) is a subgroup of $(\mathbb{Z}, +)$. Now consider the quotient group:

   $$\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}.$$

   More generally, for any $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ is a ring. If $n > 0$, the number of elements in $\mathbb{Z}/n\mathbb{Z}$ is $n$.

   *F* or $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ is not a subring of $\mathbb{C}$.
3. **Continuous Functions:** Let $R = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is continuous}\}$. This set forms a ring under pointwise addition and multiplication of functions. There is a well-defined ring structure on this set.

# 5 Field

### Definition 9: Field

A **field** $F$ is a set equipped with two operations: addition ($+$) and multiplication ($\times$), such that the following properties are satisfied:

1. **Additive Group:**
$$(F, +) \text{ is an abelian group.}$$
This means:
   - For all $a, b \in F$, $a + b \in F$ (closure under addition).
   - There exists an element $0 \in F$ such that $a + 0 = a$ for all $a \in F$ (additive identity).
   - For every $a \in F$, there exists $-a \in F$ such that $a + (-a) = 0$ (additive inverse).
   - Addition is associative: $(a + b) + c = a + (b + c)$ for all $a, b, c \in F$.
   - Addition is commutative: $a + b = b + a$ for all $a, b \in F$.
2. **Multiplicative Group:** The set $F \setminus \{0\}$ (i.e., all non-zero elements of $F$) is an abelian group under multiplication:
   - For all $a, b \in F \setminus \{0\}$, $a \times b \in F \setminus \{0\}$ (closure under multiplication).
   - There exists an element $1 \in F$ such that $a \times 1 = a$ for all $a \in F$ (multiplicative identity).
   - For every $a \in F \setminus \{0\}$, there exists $a^{-1} \in F$ such that $a \times a^{-1} = 1$ (multiplicative inverse).
   - Multiplication is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in F$.
   - Multiplication is commutative: $a \times b = b \times a$ for all $a, b \in F \setminus \{0\}$.
3. **Distributive Property:** Addition and multiplication are distributive over each other. For all $a, b, c \in F$:
$$a \times (b + c) = a \times b + a \times c \quad \text{and} \quad (a + b) \times c = a \times c + b \times c.$$

**Key Differences Between Fields and Rings**

- In a **field**, every non-zero element has a **multiplicative inverse**. In a **ring**, this is not required. For example, in the ring of integers $\mathbb{Z}$, only 1 and $-1$ have multiplicative inverses, while in a field like $\mathbb{Q}$ (the rational numbers), every non-zero element has a multiplicative inverse.
- Multiplication in a **field** is always **commutative**, whereas rings can be either commutative or non-commutative.

**Examples of Fields**

1. **The Rational Numbers $\mathbb{Q}$:** Every non-zero rational number has a multiplicative inverse, and all field properties are satisfied.
2. **The Real Numbers $\mathbb{R}$:** The set of real numbers is a field under the usual addition and multiplication.
3. **The Complex Numbers $\mathbb{C}$:** The complex numbers form a field under addition and multiplication, where every non-zero complex number has a multiplicative inverse.
4. **Finite Fields $\mathbb{Z}/p\mathbb{Z}$:** For a prime $p$, the set $\mathbb{Z}/p\mathbb{Z}$ (integers modulo $p$) forms a field. In this case, every non-zero element has a multiplicative inverse modulo $p$. For example, $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ is a field.

**Non-Examples of Fields**

- **The Integers $\mathbb{Z}$:** While $\mathbb{Z}$ is a ring, it is not a field because most elements (other than 1 and $-1$) do not have a multiplicative inverse in $\mathbb{Z}$.

**Theorem 7: 9.13**

The set of all algebraic numbers forms a field. The set of all algebraic integers forms a ring.

We begin by recalling the definitions of a *field* and a *ring*.

## Field Properties

A field satisfies the following conditions:

1. Closure under addition and multiplication: If $a$ and $b$ are elements of the field, then $a + b$ and $a \cdot b$ are also in the field.
2. Associativity of addition and multiplication: For any $a, b, c$ in the field, $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Commutativity of addition and multiplication: For any $a, b$ in the field, $a + b = b + a$ and $a \cdot b = b \cdot a$.
4. Additive identity: There exists an element 0 such that for any $a$, $a + 0 = a$.
5. Multiplicative identity: There exists an element 1 such that for any $a$, $a \cdot 1 = a$.
6. Additive inverses: For every element $a$, there exists an element $-a$ such that $a + (-a) = 0$.
7. Multiplicative inverses: For every non-zero element $a$, there exists an element $a^{-1}$ such that $a \cdot a^{-1} = 1$.
8. Distributive property: For all $a, b, c$ in the field, $a \cdot (b + c) = a \cdot b + a \cdot c$.

### Algebraic Numbers Form a Field

Let us now show that the set of all algebraic numbers forms a field. Algebraic numbers are complex numbers that satisfy polynomial equations with rational coefficients. We verify that algebraic numbers satisfy the conditions for a field:

- **Closure under addition and multiplication**: The sum and product of two algebraic numbers is also an algebraic number. For example, $\sqrt{2} + \sqrt{3}$ is an algebraic number, and $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$ is also an algebraic number.
- **Associativity**: Algebraic numbers inherit the associative properties of addition and multiplication from complex numbers.
- **Commutativity**: Addition and multiplication of algebraic numbers are commutative because complex numbers are commutative.
- **Additive identity**: The number 0 is an algebraic number because it satisfies the polynomial equation $x = 0$, which has rational coefficients.
- **Multiplicative identity**: The number 1 is an algebraic number because it satisfies the polynomial equation $x - 1 = 0$, which has rational coefficients.
- **Additive inverse**: If $\alpha$ is an algebraic number, its additive inverse $-\alpha$ is also algebraic. For example, if $\alpha$ satisfies a polynomial, then $-\alpha$ satisfies the same equation with appropriate sign changes.
- **Multiplicative inverse**: If $\alpha \neq 0$ is an algebraic number, its multiplicative inverse $\alpha^{-1}$ is also algebraic. For example, if $\alpha$ satisfies a polynomial equation, then $\alpha^{-1}$ satisfies a polynomial equation constructed from it. For instance, 2 has an inverse $1/2$, which satisfies $2x - 1 = 0$.
- **Distributive property**: Algebraic numbers satisfy the distributive property since complex numbers satisfy the distributive property.

Since all the conditions for a field are satisfied, the set of algebraic numbers forms a **field**.

### Ring Properties

A ring satisfies the following conditions:

1. Closure under addition and multiplication.
2. Associativity of addition and multiplication.
3. Additive identity.
4. Additive inverse.

5. Distributive property.

Note that a ring does not require the existence of a multiplicative inverse.

### Algebraic Integers Form a Ring

Now, consider the set of all algebraic integers, which are algebraic numbers that satisfy monic polynomial equations with integer coefficients. We check the conditions for a ring:

- **Closure under addition and multiplication**: The sum and product of two algebraic integers are also algebraic integers. For example, $\sqrt{2} \cdot \sqrt{2} = 2$ is an algebraic integer because it satisfies $x - 2 = 0$.
- **Associativity**: Algebraic integers inherit the associative properties of addition and multiplication from complex numbers.
- **Additive identity**: The number 0 is an algebraic integer because it satisfies $x = 0$.
- **Additive inverse**: If $\alpha$ is an algebraic integer, then $-\alpha$ is also an algebraic integer. For example, if $\alpha = \sqrt{2}$, then $-\sqrt{2}$ satisfies the same equation $x^2 - 2 = 0$.
- **Distributive property**: Algebraic integers satisfy the distributive property since complex numbers do.

However, algebraic integers do not necessarily have multiplicative inverses that are also algebraic integers. For example, the inverse of 2 is $1/2$, which is an algebraic number but not an algebraic integer.

Thus, the set of algebraic integers forms a **ring**, not a field, because it lacks multiplicative inverses for all elements.

## 6 Proof of Transcendance of Pi

**Lemma 10**

Let $f$ be an integer polynomial and $n$ a positive integer.

1. If $F(x) = \frac{x^n}{(n-1)!} f(x)$, then $F(h) \equiv 0 \pmod{n}$
2. If $G(x) = \frac{x^{n-1}}{(n-1)!} f(x)$, then $G(h) \equiv f(0) \pmod{n}$

**Lemma 11**

For any polynomial $f(x) = \sum_{n=0}^{m} a_n x^n$, if we let $f^*(x) = \sum_{n=0}^{m} a_n x^n \epsilon_n(x)$, then $e^x f(h) = f(x+h) + e^{|x|} f^*(x)$

**Step 1:** Suppose $\pi$ is algebraic, so $f(\pi) = 0$ for some polynomial with integer coefficients, where $f(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_k x^k$.

Notice $i\pi$ is then algebraic because if $g(x) = f(ix)f(-ix)$, then $g(i\pi) = f(-\pi)f(\pi)$, but $f(\pi) = 0$, so $g(i\pi) = 0$.

Additionally, observe that $g(\bar{x}) = \overline{f(ix)f(-ix)} = f(i\bar{x})f(-\bar{i}x) = f(-ix)f(ix) = g(x)$, so $g(x)$ has real coefficients.

Therefore, $i\pi$ is algebraic and $g(x)$ has real coefficients.

Renaming the varaibles, we can therefore deduce an integral polynomial equa satisfied by $\pi i$:

$$c_0 + c_1x + c_2x^2 + \ldots + c_mx^m = 0 \tag{4}$$

for some integers $c_0, c_1, \cdots$.

By the Fundamental Theorem of Algebra this equation has m roots, call them $\omega_1, \omega_2, \ldots, \omega_m$ including $\pi i$. Focusing on the latter, by Euler formula,

$$e^{\pi i} = cos\pi + isin\pi = -1 + 0i$$

$$1 + e^{\pi i} = 0$$

$$e^0 + e^{\pi i} = 0$$

For the other roots as well, we have $(e^0 + e^{\omega_1}) \cdot (e^0 + e^{\omega_2}) \cdots (e^0 + e^{\omega_m}) = 0$, since at least one factor (the one corresponding to $\pi i$) is zero.

$$e^0 + (e^{\omega_1} + e^{\omega_2} + \ldots + e^{\omega_m}) + (e^{\omega_1}e^{\omega_2} + e^{\omega_1}e^{\omega_3} + \ldots + e^{\omega_{m-1}}e^{\omega_m}) + \ldots + (e^{\omega_1}e^{\omega_2} \cdots e^{\omega_m}) = 0$$

$$e^0 + (e^{\omega_1} + e^{\omega_2} + \ldots + e^{\omega_m}) + (e^{\omega_1+\omega_2} + e^{\omega_1+\omega_3} + \ldots + e^{\omega_{m-1}+\omega_m}) + \ldots + (e^{\omega_1+\omega_2+\ldots+\omega_m}) = 0$$

Note that each term in the above expression corresponds to one of the $2^m$ subsets of the set of roots $\{\omega_1, \omega_2, \ldots, \omega_m\}$, and that each exponent is a symmetric integral polynomial of those roots. Renaming the exponents, $\alpha_1, \alpha_2, \ldots, \alpha_m$, we have

$$\sum_{i=1}^{2^m} e^{\alpha_i} = 0$$

The proof will amount to showing that the left side of this equation equals a nonzero integer plus a proper fraction, and so cannot equal zero, giving us the contradiction that we sought. Recall that $\alpha_1 = 0$ and note that some of the pther $\alpha_i$ could conveincably vanish as well (not all of them, since the sum of all the roots is not zero). We now re-index the $\alpha_i$ so that the first $n$ of them are non vanishing.

$$\sum_{i=1}^{n} e^{\alpha_i} + \sum_{i=n+1}^{2^m} e^{\alpha_i} = 0$$

$$\sum_{i=1}^{n} e^{\alpha_i} + q = 0 \text{ setting the integer } q = 2^m - n \tag{5}$$

With special reference to the highest degree coefficient $c_m$ of the polynomial we now

choose any large prime $p$ satisfying

$$p > q, p > c_m, p > |(c_m\alpha_1)(c_m\alpha_2)\cdots(c_m\alpha_n)|$$

and consider the polynomial

$$\phi(x) = \frac{c_m^{p-1}}{(p-1)!}x^{p-1}[c_m^n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)]^p \tag{6}$$

whose degree is $np + p - 1$.

Multiplying En 5 by $\phi(h)$ gives

$$\phi(h)\sum_{i=1}^{n} e^{\alpha_i} + \phi(h)q = 0$$

$$\sum_{i=1}^{n} \phi(h)e^{\alpha_i} + \phi(h)q = 0 \text{ since } \phi(h) \text{ is independent of } i$$

$$\sum_{i=1}^{n}[\phi(\alpha_i + h) + e^{|\alpha_i|}\phi^*(\alpha_i)] + \phi(h)q = 0 \text{ by Lemma 11}$$

$$\sum_{i=1}^{n}\phi(\alpha_i + h) + \sum_{i=1}^{n}\phi^*(\alpha_i)e^{|\alpha_i|} + \phi(h)q = 0$$

$$s_1 + s_2 + s_3 = 0 \text{ by way of abbrevation} \tag{7}$$

(1) **We show that $s_1$ is an integer multiple of chosen prime p**

To evaluate $s_1$ we start with equation 6, and note that shifting the polynomial $\phi(x)$ by any of the displacements $\alpha_i$ creates a net additional factor $x$ i.e. $p$ of them versus $p-1$:

$$\phi(x+\alpha_i) = \frac{c_m^{p-1}}{(p-1)!}(x+\alpha_i)^{p-1}[c_m^n(x+\alpha_i-\alpha_1)(x+\alpha_i-\alpha_2)\cdots(x+\alpha_i-\alpha_{i-1})(x)(x+\alpha_i-\alpha_{i+1})\cdots(x+\alpha_i-\alpha_n)]^p$$

$$= \frac{x^p}{(p-1)!}c_m^{p-1}[c_m^n(x+\alpha_i-\alpha_1)(x+\alpha_i-\alpha_2)\cdots(x+\alpha_i-\alpha_{i-1})(x+\alpha_i-\alpha_{i+1})\cdots(x+\alpha_i-\alpha_n)]^p$$

Summing over all $i$ gives

$$\sum_{i=1}^{n}\phi(\alpha_i+h) = \frac{x^p}{(p-1)!}\sum_{i=1}^{n}c_m^{p-1}[c_m^n(x+\alpha_i-\alpha_1)(x+\alpha_i-\alpha_2)\cdots(x+\alpha_i-\alpha_{i-1})(x+\alpha_i-\alpha_{i+1})\cdots(x+\alpha_i-\alpha_n)]^p$$

The summation portion of the right side is a polynomial in x of degree $(p-1)+(n-1)p = np-1$.

Multiplying out, and combining like terms, we get:

$$\sum_{i=1}^{n} \phi(\alpha_i + h) = \frac{x^p}{(p-1)!} \sum_{j=1}^{np-1} \beta_j x^j$$

where each coefficient $\beta_j$ is a symmetric integral polynomial of the constants $c_m\alpha_1 c_m\alpha_2 \cdots c_m\alpha_m$. Recall that each $\alpha_i$ is itself a symmetric integral polynomial of $\omega_1, \omega_2, \cdots, \omega_m$, which are the roots of a polynomial having integer coefficients, with $c_m$ being the highest-degree coefficient. By Fundamental Theorem of Symmetric Polynomials we can conclude that $\beta_j$ is an integer for $j = 1, 2, \ldots, np-1$. This allows us to apply Lemma 10 to the polynomial $\sum_{i=1}^{n} \phi(\alpha_i + h)$, which gives us

$$\sum_{i=1}^{n} \phi(\alpha_i + h) \equiv 0 \pmod{p}$$

$$s_1 \equiv 0 \pmod{p} \tag{9}$$

(2) **We show that $s_2$ is an integer multiple of chosen prime p**

We will now show that $s_2$ can be made vanishingly small by choosing the prime $p$ to be sufficiently large. To do this, we apply De Moivre's formula and the triangle inequality for complex numbers:

$$|z_1 z_2| = |z_1||z_2| \quad \text{and} \quad |x - \alpha_i| \leq |x + \alpha_i| \quad \text{for } i = 1, 2, \ldots, n.$$

Using this inequality, we get the bound:

$$|(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)| \leq (|x|+|\alpha_1|)(|x|+|\alpha_2|)\ldots(|x|+|\alpha_n|)$$

From Eqn (6), we know:

$$|\phi(x)| = |\frac{c_m^{p-1}}{(p-1)!} x^{p-1} \left[c_m^n (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)\right]^p|,$$

which, using the triangle inequality, gives:

$$|\phi(x)| \leq \frac{|c_m|^{np+p-1}|x|^{p-1}[(|x|+|\alpha_1|)(|x|+|\alpha_2|)\ldots(|x|+|\alpha_n|)]^p.}{(p-1)!}$$

As $p$ increases, the factorial term $(p-1)!$ grows faster than any polynomial involving $p$. Thus, for sufficiently large $p$, $\phi(x)$ can be made arbitrarily small:

$$\phi(x) \to 0 \quad \text{as} \quad p \to \infty.$$

Similarly, $\phi^*(x)$ can be made arbitrarily small because each term of $\phi^*(x)$ differs from $\phi(x)$ only by the additional factor $\epsilon_n(x)$, which is independent of $p$. Thus:

$$\phi^*(x) \to 0 \quad \text{as} \quad p \to \infty.$$

Therefore, the sum $s_2$ defined as:

$$|s_2| = |\sum_{i=1}^{n} \phi^*(\alpha_i) e^{|\alpha_i|}| < 1 \tag{10}$$

can also be made arbitrarily small by choosing $p$ sufficiently large. Hence, we conclude that $s_2$ becomes vanishingly small for large $p$.

**Finally, we will show that $s_3$ is an integer not divisible by $p$.**

To evaluate $s_3$, recall the definition of $\phi(x)$ from Eqn (6):

$$\phi(x) = \frac{c_m^{p-1}}{(p-1)!} x^{p-1} \left[c_m^n (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)\right]^p .$$

$$\phi(x) = \frac{x^{p-1}}{(p-1)!} c_m^{p-1} [c_m^n (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)]^p$$

Multiplying out and combining like terms, we get:

$$\phi(x) = \sum_{j=1}^{np} \gamma_j x^j,$$

where each coefficient $\gamma_j$ is a symmetric integral polynomial in the constants $c_m\alpha_1, c_m\alpha_2, \dots, c_m\alpha_n$. For example, the lowest-degree coefficient is:

$$\gamma_0 = (-1)^{np} c_m^{p-1} \left[(c_m\alpha_1)^p (c_m\alpha_2)^p \dots (c_m\alpha_n)^p\right].$$

By the **Fundamental Theorem of Symmetric Polynomials**, $\gamma_j$ must be an integer for $j = 0, 1, \dots, np$.

We now apply Lemma 10(b) to Eqn (11), so that $\phi(h)$ is an integer satisfying:

$$\phi(h) \equiv \gamma_0 \pmod{p},$$

that is,

$$\phi(h) \equiv (-1)^{np} c_m^{p-1} \left[(c_m\alpha_1)^p (c_m\alpha_2)^p \dots (c_m\alpha_n)^p\right] \pmod{p}.$$

Thus,

$$s_3 = q \pmod{p}.$$

Since we defined $p$ such that $p > q$, $p > c_m$, and $p > |(c_m\alpha_1)(c_m\alpha_2)\dots(c_m\alpha_n)|$, it follows that $p$ does not divide $s_3$. Therefore, $s_3 \not\equiv 0 \pmod{p}$.

Combining this with Eqn (9) implies that neither is $s_1 + s_3$ congruent to 0 modulo $p$. In particular, it cannot be equal to zero:

$$s_1 + s_3 \neq 0,$$

and so, in absolute value:

$$|s_1 + s_3| \geq 1.$$

Combining this with Eqn (7), we get:

$$|-s_2| \geq 1 \quad \text{or} \quad |s_2| \geq 1,$$

which contradicts Eqn (10).

Thus, our original supposition that $\pi$ is algebraic was false. **QED.**

# 7 Gelfond - Schneider Theorem

**Theorem 8: Gelfond-Schneider Theorem**

If $\alpha$ and $\beta$ are algebraic numbers, with $\alpha \neq 0, 1$, and $\beta$ irrational, then $\alpha^\beta$ is transcendental.

(i) If $l, \beta$ are complex numbers with $l \neq 0$, $\beta \notin Q$ then at least one of $e^l$, $\beta$, $e^{\beta l}$ is transcendental.

(ii) If $\alpha$, $\beta$ are non zero algebraic numners with $\log \alpha$ and $\log \beta$ linearly independent over $Q$, then $\log \alpha$ and $\log \beta$ are linearly independent over algebraic numbers.

We shall show that above theorem and the statements (i) and (ii) are equivalent.

**Thm $\Rightarrow$ (i)**

Take $\alpha = e^l$ ($l \in$ complex numbers), then clearly $\alpha \neq 0$, $\alpha \neq 1$ because exponential function never takes these values except at $l = 0$ but we are excluding that case.

Now let $\beta$ be any algebraic number that is not rational ($\beta \notin Q$). Then by Gelfond-Schneider theorem, $\alpha^\beta = e^{l\beta}$ is transcendental. This means that at least one of $e^l$, $\beta$, $e^{l\beta}$ is transcendental.

**(i) $\Rightarrow$ (ii)**

In (ii) we assume $log\alpha$ and $log\beta$ are linearly independent, i.e. there are no trivial rational numbers $q_1, q_2$ such that $q_1 log\alpha + q_2 log\beta = 0$.

If $\log \alpha$ and $\log \beta$ are linearly independent then $\frac{\log \alpha}{\log \beta} \notin Q$. As if they were, then $\log \alpha = q \log \beta$ for some rational number $q$, which would imply that $\log \alpha - q \log \beta = 0$, contradicting the linear independence of $\log \alpha$ and $\log \beta$.

Let $l = \log \beta$ and $\beta_0 = \frac{\log \alpha}{\log \beta}$.

According to (i), since $l$ and $\beta_0$ are complex numbers with $l \neq 0$ and $\beta_0 \notin Q$, at least one of $e^l$, $\beta_0$, $e^{l\beta_0}$ is transcendental.

This means $\beta_0$ is transcendental because:

(1.) $e^l = e^{\log \beta} = \beta$ is algebraic, and

(2.) $e^{l\beta_0} = e^{\log \alpha} = \alpha$ is algebraic.

As $\beta_0$ is transcendental and therefore there cannot be any non trivial relation between $\log \alpha$ and $\log \beta$ over the algebraic numbers. This implies that $\log \alpha$ and $\log \beta$ are linearly independent over the algebraic numbers.

(ii) $\Rightarrow$ Thm

$\beta_0 = e^{\beta \log \alpha}$ i.e. $\alpha^\beta = e^{\beta \log \alpha}$.

By (ii) if $\log \alpha$ and $\log \beta_0$ are linealry dependent over algebraic numbers, then $\log \alpha$ and $\log \beta$ are linearly dependent over $Q$.

But by assumption of the thoerem, then $\beta \notin Q \implies \log \alpha$ and $\log \beta_0$ cannot be linearly dependennt over $Q$.

Therefore if $\beta \notin Q$ this leads to contradiction because $\log \alpha$ and $\log \beta_0$ should be L.D. over $Q$ based on (ii) but they cannot be as $\beta \notin Q$. This contradicts $\alpha^\beta = e^{\beta \log \alpha}$ must be transcendental.

Lang proved a result, similar to statement (i) above.

### Theorem 9: Lang's Theorem

Suppose $l_1$, $l_2$, and $l_3$ are linearly independent over the rationals and that $\beta_1$ and $\beta_2$ are linearly independent over the rationals. Then at least one of the numbers $e^{l_i \beta_j}$ (for $i, j = 1, 2, 3$) is transcendental.

**The Brownawell - Waldschmidt result :** The result is similar to Lang's theorem, it states that among the numbers that can be formed by taking exponentials of the number $e$, (like $e^e$, $e^{e^2}$, and so on), at least one of them is transcendental.

## 7.1 Baker's Theorem

**Theorem 10: Baker's Theorem**

Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be non-zero algebraic numbers, and suppose that the logarithms $\log \alpha_1, \log \alpha_2, \ldots, \log \alpha_m$ are linearly independent over the rationals. Then, these logarithms are also linearly independent over the algebraic numbers.

**Explanation:**

Baker's Theorem is significant because it extends the Gelfond-Schneider Theorem, which dealt with two algebraic numbers $\alpha$ and $\beta$. Baker's result tells us that if the logarithms of multiple algebraic numbers are linearly independent over the rationals, then no non-trivial linear combination of these logarithms with algebraic coefficients can be zero. This implies that many combinations of logarithms of algebraic numbers are *transcendental*, thus expanding the class of known transcendental numbers.

## 7.2 Application of Baker's Theorem: Linear Combinations of Logarithms and Diophantine Approximations

One of the key applications of results like Baker's Theorem is in studying how "far from zero" a linear combination of logarithms of algebraic numbers can be. Specifically, consider a linear combination of the form:

$$L = q_1 \log \alpha_1 + q_2 \log \alpha_2 + \cdots + q_m \log \alpha_m$$

where $\alpha_1, \alpha_2, \ldots, \alpha_m$ are algebraic numbers, and $q_1, q_2, \ldots, q_m$ are coefficients (rational or algebraic). Baker's Theorem tells us that if the logarithms are linearly independent over the rationals, then the combination $L$ cannot be exactly zero unless all the $q_i$ are zero.

The interesting question, however, is: *How close can $L$ be to zero if it is not exactly zero?*

This question is fundamental in understanding *Diophantine approximations*, which deal with how well algebraic numbers (or expressions involving them) can be approximated by rational numbers or other algebraic expressions.

## 7.3 Degree and Height of Algebraic Numbers

To answer the question of how "far from zero" a linear combination like $L$ can be, we introduce two important measures for algebraic numbers: *degree* and *height*.

**Definition 12: Degree of an Algebraic Number**

Let $\alpha$ be an algebraic number. The *degree* of $\alpha$ is the degree of the minimal polynomial $f(x)$ over $\mathbb{Z}$ that $\alpha$ satisfies, i.e., the irreducible polynomial:

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

where $a_d \neq 0$ and $f(x) \in \mathbb{Z}[x]$. The degree $d$ is the degree of this polynomial.

### Definition 13: Height of an Algebraic Number

Let $\alpha$ be an algebraic number that satisfies an irreducible polynomial $f(x)$ over the integers as defined above. The *height* of $\alpha$ is defined as the maximum absolute value of the coefficients of $f(x)$, i.e.,

$$A = \max_{0 \leq j \leq d} |a_j|$$

where $a_j$ are the coefficients of the minimal polynomial $f(x)$.

**Why Degree and Height Matter:**

The *degree* and *height* of an algebraic number help us quantify how complicated the number is. In the context of Diophantine approximations, these measures allow us to give precise bounds on how close a linear combination of logarithms of algebraic numbers can get to zero.

In particular, Baker's method can be used to give explicit lower bounds on non-zero linear combinations of logarithms, which ensures that such combinations are not too close to zero. This has important implications in areas of number theory where precise approximations are required, such as in solving Diophantine equations.

## 7.4 Lower Bound on Linear Combinations of Logarithms

### Theorem 11: Lower Bound on Linear Combinations of Logarithms

Let $\alpha_1, \ldots, \alpha_r$ be non-zero algebraic numbers with degrees at most $d$ and heights at most $A$. Let $\beta_0, \beta_1, \ldots, \beta_r$ be algebraic numbers with degrees at most $d$ and heights at most $B > 1$. Suppose that:

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_r \log \alpha_r \neq 0.$$

Then, there exist constants $C = C(r, d) > 0$ and $w = w(r) \geq 1$ such that:

$$|\Lambda| > B^{-C(\log A)^w}.$$

**Explanation:**

This theorem gives a lower bound for the absolute value of $\Lambda$, a linear combination of logarithms of algebraic numbers. The key components of the theorem are as follows:

- $\alpha_1, \ldots, \alpha_r$ are non-zero algebraic numbers with bounded degrees (at most $d$) and heights (at most $A$).
- $\beta_0, \beta_1, \ldots, \beta_r$ are algebraic coefficients with bounded degrees (at most $d$) and heights (at most $B$).

- $\Lambda$ represents a linear combination of the form:

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_r \log \alpha_r.$$

  If $\Lambda \neq 0$, the theorem guarantees that $\Lambda$ cannot be arbitrarily small; it is bounded below by the expression $B^{-C(\log A)^w}$.

Recall that the *degree* of an algebraic number $\alpha$ is the degree of its minimal polynomial over $\mathbb{Z}$, and the *height* of $\alpha$ is the maximum absolute value of the coefficients of this minimal polynomial.

The theorem applies to algebraic numbers whose degrees and heights are controlled:

- The degrees of the $\alpha_i$ and $\beta_i$ are bounded by $d$.
- The heights of the $\alpha_i$ are bounded by $A$, and the heights of the $\beta_i$ are bounded by $B > 1$.

The constants $C$ and $w$ depend only on the number of terms in the linear combination $r$ and the degrees of the algebraic numbers $d$. These constants ensure that the lower bound for $|\Lambda|$ remains significant, even as $A$ and $B$ grow.

Above theorem is a quantitative result that has important applications in Diophantine approximation. It shows that linear combinations of logarithms of algebraic numbers cannot approach zero too closely, unless they are zero. The degree and height of the algebraic numbers involved dictate how small $\Lambda$ can be.

## 7.5 Proof of Gelfond-Schneider Theorem

General outline:

The general approach to proving the Gelfond-Schneider Theorem relies on a contradiction. Suppose that $\alpha^\beta$ is algebraic. The goal is to deduce that this assumption leads to the conclusion that $\beta \in \mathbb{Q}$, which contradicts the hypothesis that $\beta \notin \mathbb{Q}$.

The proof can be broken down into several key steps:

- We begin by assuming that $\alpha^\beta$ is algebraic, and we aim to show that $\beta \in \mathbb{Q}$.
- First, we reduce the problem to the special case where both $\alpha > 0$ and $\beta$ are real numbers.
- Next, we establish several lemmas that will be used to bound the number of real roots of certain functions involving exponential terms.
- These bounds will eventually lead to a contradiction, which will complete the proof.

The core of the proof uses properties of polynomials, exponentials, and logarithms of algebraic numbers. It also makes use of Rolle's Theorem, the Maximum Modulus Principle from complex analysis, and some combinatorial arguments.

**The Special Case: $\alpha > 0$ and $\beta$ are Real**

We start by considering the special case where $\alpha > 0$ and both $\alpha$ and $\beta$ are real. To establish the result, it suffices to show that if $\alpha^\beta$ is algebraic, then $\beta \in \mathbb{Q}$.

Since $\alpha^\beta$ is algebraic, observe that $\alpha^{s_1+s_2\beta}$ is also an algebraic number for all integers $s_1$ and $s_2$. Thus, the behavior of expressions involving $\alpha$ and $\beta$ can be analyzed using properties of logarithms and exponentials.

The strategy is to show that there exist distinct pairs of integers $(s_1, s_2)$ and $(s_1', s_2')$ such that:

$$s_1 + s_2\beta = s_1' + s_2'\beta.$$

This would imply that $\beta$ is a rational number, which contradicts the assumption that $\beta \notin \mathbb{Q}$.

### Lemma 14: Lemma 1

Let $a_1(t), a_2(t), \ldots, a_n(t)$ be non-zero polynomials in $\mathbb{R}[t]$ of degrees $d_1, d_2, \ldots, d_n$, respectively. Let $w_1, w_2, \ldots, w_n$ be distinct real numbers. Then the function:

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

has at most $d_1 + d_2 + \cdots + d_n + n - 1$ real zeroes (counting multiplicities).

**Lemma Explanation:**

This lemma provides an upper bound on the number of real roots for a function that is a sum of polynomials multiplied by distinct exponential terms. Each $a_j(t)$ is a polynomial, and each $e^{w_j t}$ is an exponential with a distinct real exponent $w_j$. The lemma tells us that the total number of real roots (where $F(t) = 0$) cannot exceed the sum of the degrees of the polynomials plus $n - 1$, where $n$ is the number of terms in the sum.

The distinct exponents $w_j$ ensure that the exponential functions grow at different rates, which limits the number of real roots the function can have. This is important in applications where we need to bound the number of real solutions to transcendental equations involving both polynomial and exponential terms.

**Example to Illustrate the Lemma:**

Consider the polynomials:

$$a_1(t) = t + 1 \quad \text{and} \quad a_2(t) = 2,$$

and the distinct real exponents $w_1 = 1$ and $w_2 = 2$. According to the lemma, the function:

$$F(t) = (t + 1)e^t + 2e^{2t}$$

should have at most $d_1 + d_2 + n - 1 = 1 + 0 + 2 - 1 = 2$ real roots, where $d_1 = 1$ is the degree of $a_1(t)$, $d_2 = 0$ is the degree of $a_2(t)$, and $n = 2$ is the number of terms.

**Analyzing the roots of $F(t) = 0$:** We can factor out the exponential term $e^t$ from the

expression for $F(t)$:

$$F(t) = e^t \left((t+1) + 2e^t\right).$$

Since $e^t$ is never zero, we can reduce the equation to solving:

$$(t+1) + 2e^t = 0.$$

This equation does not have a simple algebraic solution, so we use numerical methods to estimate the real roots.

At $t = -1$, we have:

$$(-1+1) + 2e^{-1} = 0 + \frac{2}{e} > 0.$$

At $t = -2$, we have:

$$(-2+1) + 2e^{-2} = -1 + \frac{2}{e^2} \approx -1 + 0.27 < 0.$$

Thus, by the Intermediate Value Theorem, there is a root between $t = -2$ and $t = -1$.

At $t = 0$, we have:

$$(0+1) + 2e^0 = 1 + 2 = 3.$$

At $t = -3$, we have:

$$(-3+1) + 2e^{-3} = -2 + \frac{2}{e^3} \approx -2 + 0.1 < 0.$$

Thus, by the Intermediate Value Theorem again, there is another root between $t = -3$ and $t = -2$.

**Conclusion:** We found two real roots for the function $F(t) = (t+1)e^t + 2e^{2t}$, which matches the prediction of Lemma 14. According to the lemma, the function could have at most 2 real roots, and that is exactly what we found.

This example illustrates how the lemma provides an upper bound on the number of real roots when combining polynomials and exponential functions with distinct exponents.

**Proof of Lemma 1:**

We prove Lemma 14 by induction on the total degree of the polynomials involved, defined as:

$$k = d_1 + d_2 + \cdots + d_n + n.$$

**Base Case (k = 1):** If $k = 1$, then $n = 1$ and $d_1 = 0$, meaning that $a_1(t)$ is a constant polynomial. In this case, $F(t) = a_1 e^{w_1 t}$, and the lemma easily holds since $F(t)$ has at most one real root.

**Inductive Step:** Assume that the lemma holds for all cases where $k < \ell$. Now, we must show that it holds when $k = \ell$.

Let $N$ be the number of real roots of $F(t)$. By **Rolle's Theorem**, the number of real roots of the derivative $F'(t)$ is at least $N-1$. We now compute the derivative of $F(t)$:

$$F'(t) = \sum_{j=1}^{n} \left(a_j'(t) + w_j a_j(t)\right) e^{w_j t}.$$

Define new polynomials:

$$b_j(t) = a_j'(t) + w_j a_j(t),$$

so that:

$$F'(t) = \sum_{j=1}^{n} b_j(t) e^{w_j t}.$$

For $j = 1, 2, \ldots, n-1$, the degree of $b_j(t)$ is equal to $d_j$. For $j = n$, since $w_n = 0$, the degree of $b_n(t)$ is one less than the degree of $a_n(t)$.

By the inductive hypothesis, $F'(t)$ has at most $d_1 + d_2 + \cdots + d_n + n - 2$ real roots. Therefore, by Rolle's Theorem:

$$N - 1 \leq d_1 + d_2 + \cdots + d_n + n - 2,$$

which implies:

$$N \leq d_1 + d_2 + \cdots + d_n + n - 1.$$

Thus, the lemma is proven.

### Lemma 15: Lemma 2

Suppose $f(z)$ is an analytic function inside the disk $D = \{z : |z| < R\}$, and suppose it is continuous on the boundary of the disk $\{z : |z| = R\}$. Then, for all $z \in D$, we have:

$$|f(z)| \leq |f|_R,$$

where $|f|_R$ denotes the maximum value of $|f(z)|$ on the boundary of the disk $\{z : |z| = R\}$.

This lemma is a version of the Maximum Modulus Principle, a fundamental result in complex analysis. It tells us that if a function $f(z)$ is analytic in a region (here, the disk $D$) and continuous on the boundary of that region, then the maximum value of $|f(z)|$ inside the disk occurs on the boundary. In other words, the function cannot have a larger absolute value inside the disk than it does on the boundary.

### Lemma 16: Lemma 3: Upper Bound on Determinants of Analytic Functions

Let $f_1(z), f_2(z), \ldots, f_L(z)$ be analytic functions inside the disk $D = \{z : |z| < R\}$ and continuous on the boundary $\{z : |z| \leq R\}$. Let $\zeta_1, \ldots, \zeta_L$ be points such that $|\zeta_j| \leq r$ for each $j$, where $1 \leq r \leq R$.
The determinant $\Delta$ of the matrix:

$$\Delta = \det \begin{pmatrix} f_1(\zeta_1) & \cdots & f_L(\zeta_1) \\ \vdots & \ddots & \vdots \\ f_1(\zeta_L) & \cdots & f_L(\zeta_L) \end{pmatrix}$$

satisfies the bound:

$$|\Delta| \leq \left(\frac{R}{r}\right)^{-\frac{L(L-1)}{2}} L! \prod_{\lambda=1}^{L} |f_\lambda|_R,$$

where $|f_\lambda|_R$ denotes the maximum value of $|f_\lambda(z)|$ on the boundary of the disk $|z| = R$.

**Explanation of Lemma 3:**

This lemma provides an upper bound on the absolute value of the determinant $\Delta$, which is formed by evaluating a set of analytic functions $f_1(z), f_2(z), \ldots, f_L(z)$ at specific points $\zeta_1, \ldots, \zeta_L$ inside the disk.

The determinant $\Delta$ measures how "independent" the values of these functions are at the points $\zeta_1, \ldots, \zeta_L$. If the determinant is zero, it means the functions are linearly dependent at those points.

*Bound on $\Delta$:* The lemma shows that $|\Delta|$, the absolute value of the determinant, is bounded by the product of the maximum values of the functions on the boundary $|z| = R$, scaled by the ratio $\frac{R}{r}$, where $r$ is the distance of the points $\zeta_j$ from the origin.

**Why This is Important:** The determinant $\Delta$ appears in many applications of transcendental number theory, and bounding its size is crucial for proving results like the Gelfond-Schneider theorem. The lemma uses properties of analytic functions, such as their maximum modulus (Lemma 2), to control the size of $\Delta$.

In particular, the ratio $\frac{R}{r}$ reflects how the size of the disk and the location of the points $\zeta_1, \ldots, \zeta_L$ influence the determinant. As the points $\zeta_j$ approach the boundary (i.e., as $r \to R$), the determinant becomes more sensitive to the values of the functions. Lemma 3 gives an essential tool for controlling the size of determinants involving analytic functions, particularly when the functions are evaluated at points inside a disk.

**Proof of Lemma 3:**

Let $h(z)$ be the determinant of the $L \times L$ matrix whose entries are $f_j(\zeta_i z)$, for $1 \leq i, j \leq L$. That is,

$$h(z) = \det(f_j(\zeta_i z)).$$

This function $h(z)$ is analytic inside the disk $D_0 = \{z : |z| < R/r\}$ and continuous on the boundary $|z| = R/r$. Our goal is to bound $|h(z)|$.

We begin by expanding $f_j(\zeta_i z)$ as a power series:

$$f_j(\zeta_i z) = \sum_{k=0}^{M-1} b_k(j)\zeta_i^k z^k + z^M g_{i,j}(z),$$

where $b_k(j)$ are the coefficients from the series expansion, and $g_{i,j}(z)$ is analytic inside $D_0$. Here, $M = L(L-1)/2$ is chosen for simplicity.

Since the determinant is linear in its columns, we can factor out powers of $z$ in each term. This leads to the expression:

$$h(z) = z^M \cdot (\text{analytic function}) + \sum_{\text{distinct } n_1, n_2, \ldots, n_L} z^{n_1+n_2+\cdots+n_L} \cdot \det(\zeta_i^{n_j}).$$

Notice that the determinant $\det(\zeta_i^{n_j})$ is zero if the powers $n_1, n_2, \ldots, n_L$ are not distinct. The smallest sum of the powers is:

$$n_1 + n_2 + \cdots + n_L \geq 0 + 1 + 2 + \cdots + (L-1) = \frac{L(L-1)}{2}.$$

Thus, $h(z)$ is divisible by $z^M$, where $M = \frac{L(L-1)}{2}$.

Since $h(z)/z^M$ is analytic and continuous on $D_0$, we can apply Lemma 2 (Maximum Modulus Principle) to bound the size of $h(z)$ inside $D_0$. Specifically, for any $w \in D_0$, we have:

$$\left|\frac{h(w)}{w^M}\right| \leq \left|\frac{h(z)}{z^M}\right|_{R/r}.$$

This means that the maximum value of $|h(w)|$ is controlled by its values on the boundary $|z| = R/r$.

For $|z| = R/r$, we have $|\zeta_i z| \leq R$. Thus, the determinant $h(z)$ can be bounded by:

$$|h(z)|_{R/r} \leq L! \prod_{\lambda=1}^{L} |f_\lambda|_R,$$

where $|f_\lambda|_R$ is the maximum modulus of $f_\lambda(z)$ on the boundary $|z| = R$.

As $\Delta = h(1)$, we conclude that:

$$|\Delta| = |h(1)| \leq \left(\frac{r}{R}\right)^M |h(z)|_{R/r} \leq \left(\frac{r}{R}\right)^M L! \prod_{\lambda=1}^{L} |f_\lambda|_R.$$

This gives the desired bound on $|\Delta|$, where $M = \frac{L(L-1)}{2}$, and completes the proof.

### Lemma 17: Lemma 4

Let $\Delta = \det(\alpha_{i,j})_{L\times L}$, where $\alpha_{i,j}$ are algebraic numbers. Suppose there exists a positive integer $T$ such that $T\alpha_{i,j}$ is an algebraic integer for all $i, j \in \{1, 2, \ldots, L\}$. If $\Delta \neq 0$, then there is a conjugate of $\Delta$ whose absolute value is at least $T^{-L}$.

Consider the determinant $\Delta$ of the matrix $(\alpha_{i,j})$. Since $T\alpha_{i,j}$ is an algebraic integer, the determinant $T^L\Delta$ is also an algebraic integer. Therefore, all the conjugates of $T^L\Delta$ are algebraic integers.

At least one of the conjugates of $T^L\Delta$ must have an absolute value $\geq 1$ because the absolute value of an algebraic integer's conjugates cannot be arbitrarily small unless the integer is zero (which is not the case here, since $\Delta \neq 0$).

Thus, one of the conjugates of $T^L\Delta$ satisfies:

$$|\text{conjugate of } T^L\Delta| \geq 1.$$

Dividing by $T^L$, we find that at least one conjugate of $\Delta$ satisfies:

$$|\text{conjugate of } \Delta| \geq T^{-L}.$$

This completes the proof.

**Now we walk through the proof of the Gelfond-Schneider Theorem:**

Let $c$ be a sufficiently large real number (to be specified later). Consider the integers $L_0$, $L_1$, and $S$, where each of them is at least 2. Define $L = (L_0 + 1)(L_1 + 1)$.

We select $L_0$, $L_1$, and $S$ to satisfy the following inequalities:

$$cL_0 \log S \leq L, \quad cL_1 S \leq L, \quad L \leq (2S - 1)^2$$

For example, if $S$ is large, we can take:

$$L_0 = \lfloor S \log S \rfloor, \quad L_1 = \lfloor \frac{S}{\log S} \rfloor$$

(We could also take $c = \log \log S$.)

Now, consider a matrix $M$ described as follows: - Take an arrangement of the integral pairs $(s_1(i), s_2(i))$ where $|s_1| < S$ and $|s_2| < S$, for a total of $(2S - 1)^2$ pairs.

- Similarly, arrange pairs $(u(j), v(j))$ for $1 \leq j \leq L$ where $0 \leq u \leq L_0$ and $0 \leq v \leq L_1$.

Define the matrix $M$ as:

$$M(i,j) = (s_1(i) + s_2(i)\beta)^{u(j)}\, \alpha^{(s_1(i)+s_2(i)\beta)v(j)}$$

where $M$ is a $(2S-1)^2 \times L$ matrix.

We now outline the main steps for proving the result:

(i) Consider the determinant $\Delta$ of an arbitrary $L \times L$ submatrix of $M$.

(ii) Use Lemma 3 to obtain an upper bound $B_1$ for $\log|\Delta|$.

(iii) Use Lemma 4 to argue that if $\Delta \neq 0$, then $\Delta$ has an absolute value $\geq B_2$ with $B_2 > B_1$. (We assume this for contradiction.)

(iv) Conclude that $\Delta = 0$ and hence the rank of $M$ is less than $L$.

(v) Use a linear combination of the columns of $M$ to form a function $F(t)$ as in Lemma 1, with fewer than $L$ roots, such that $F(s_1(i)+s_2(i)\beta) = 0$ for $1 \leq i \leq L$.

(vi) Conclude that $\beta$ is rational.

Now, we define the functions $f_j(z)$ for each column $j$ of the matrix:

$$f_j(z) = z^{u(j)}\alpha^{v(j)z} = z^{u(j)} \exp\left(v(j)z \log\alpha\right)$$

where $z = s_1(i) + s_2(i)\beta$. Note that $u(j)$ is a non-negative integer and $\alpha^{v(j)z} = \exp(v(j)z\log\alpha)$. We fix $\log\alpha$ so that it is real. Thus, each $f_j(z)$ is an entire function.

To proceed, we need an upper bound on $|f_j(z)|$. Using the fact that:

$$|e^{z_1 z_2}| = e^{\mathrm{Re}(z_1 z_2)} \leq e^{|z_1 z_2|} = e^{|z_1||z_2|}$$

for all complex numbers $z_1$ and $z_2$, we obtain that:

$$|f_j|_R \leq R^{u(j)} e^{v(j)R|\log\alpha|}$$

for any $R > 0$.

Now, apply Lemma 3 with $r = S(1+|\beta|)$ and $R = e^2 r$. For some constant $c_1 > 0$, we obtain the bound:

$$\log|\Delta| \leq -L(L-1) + \log L! + L \max_{1\leq j\leq L}\{\log|f_j|_R\}$$

Substitute the upper bound for $|f_j|_R$:

$$\log|\Delta| \leq -L(L-1) + L\log L + LL_0 \log R + LL_1 R|\log\alpha|$$

Simplifying further:

$$\log|\Delta| \leq -L^2 + c_1(LL_0 \log S + LL_1 S)$$

The constant $c_1$ is independent of $c$. Therefore, if $c$ is sufficiently large (for example, $c \geq 4c_1$), then we conclude:

$$\log|\Delta| \leq -\frac{L^2}{2}$$

Suppose now that $T_0$ is a positive rational integer for which $T_0\alpha$, $T_0\beta$, and $T_0\alpha^\beta$ are all algebraic integers. Then $T = (T_0)^{L_0+2SL_1}$ has the property that $T$ times any element of $M$ (and hence $T$ times any element of the matrix describing $\Delta$) is an algebraic integer.

Therefore, by Lemma 4, if $\Delta \neq 0$, then there is a conjugate of $\Delta$ with absolute value at least:

$$|\text{conjugate of } \Delta| \geq T^{-L} = (T_0)^{-L(L_0+2SL_1)}.$$

It is reasonable to expect a similar inequality might hold for $|\Delta|$ itself (rather than for the absolute value of a conjugate of $\Delta$). In fact, it can be shown (and will be shown later) that if $\Delta \neq 0$, then there is a constant $c_2$ (independent of $c$) for which:

$$\log|\Delta| \geq -c_2(LL_0 \log S + SL_1L). \tag{10}$$

By using our upper bound for $\log|\Delta|$ above, we see that for $c$ sufficiently large (say, $c \geq 8c_2$ will do), we obtain that $\Delta = 0$.

Since $\Delta = \det(f_j(\zeta_i))$ as defined above, we get that the columns of $(f_j(\zeta_i))$ must be linearly dependent (over the reals). In other words, there exist real numbers $b_j$, not all zero, such that:

$$\sum_{j=1}^{L} b_j f_j(\zeta_i) = 0 \quad \text{for } 1 \leq i \leq L.$$

By considering a particular ordering of the $(u(j), v(j))$, we deduce that:

$$\sum_{v=0}^{L_1}\sum_{u=0}^{L_0} b_{(L_0+1)v+u+1}\zeta_i^u\alpha^v = 0 \quad \text{for } 1 \leq i \leq L.$$

But:

$$\sum_{v=0}^{L_1}\sum_{u=0}^{L_0} b_{(L_0+1)v+u+1}\zeta_i^u\alpha^v = \sum_{v=0}^{L_1} a_v(t)e^{w_v t}$$

where $a_v(t) = \sum_{u=0}^{L_0} b_{(L_0+1)v+u+1}t^u$, $w_v = v\log\alpha$, and $t = \zeta_i = s_1(i) + s_2(i)\beta$.

Each of the $L$ values of $\zeta_i$ is a root of $\sum_{v=0}^{L_1} a_v(t)e^{w_v t} = 0$. Since some $b_j \neq 0$, we deduce from Lemma 1 that there are at most $L_0(L_1+1) + (L_1+1) - 1 < L$ distinct real roots. Therefore, two roots $\zeta_i$ must be the same, and we can conclude that:

$$s_1(i) + s_2(i)\beta = s_1(i') + s_2(i')\beta$$

for some $i, i'$ with $1 \leq i < i' \leq L$.

On the other hand, the pairs $(s_1(i), s_2(i))$ and $(s_1(i'), s_2(i'))$ are necessarily distinct, so we can conclude that $\beta$ is rational, completing the proof of Lemma 1.

# 8 Algebraic Number Fields

Let $\xi$ be an algebraic number. Then,

$$\mathbb{Q}(\xi) = \left\{ \frac{f(\xi)}{g(\xi)} : f(x), g(x) \in \mathbb{Q}[x], g(\xi) \neq 0 \right\}.$$

**Theorem 12**

Let $\xi$ be an algebraic number of degree $n$ over $\mathbb{Q}$. Then the degree of the field $\mathbb{Q}(\xi)$ over $\mathbb{Q}$ is at most $n$. Moreover, any element of $\mathbb{Q}(\xi)$ can be uniquely written in the form

$$a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{n-1}\xi^{n-1}$$

where $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$.

**Example.**

Let $\xi = \sqrt{2}$, an algebraic number of degree 2 over $\mathbb{Q}$ as it is a root of the irreducible polynomial $x^2 - 2$. According to the theorem, any element $\alpha \in \mathbb{Q}(\xi)$ can be uniquely expressed in the form

$$\alpha = a_0 + a_1\xi$$

where $a_0, a_1 \in \mathbb{Q}$.

For instance, consider $\alpha = \frac{3+5\sqrt{2}}{4}$. We can rewrite this as

$$\alpha = \frac{3}{4} + \frac{5}{4}\sqrt{2},$$

with $a_0 = \frac{3}{4}$ and $a_1 = \frac{5}{4}$, both in $\mathbb{Q}$. This shows that every element in $\mathbb{Q}(\sqrt{2})$ can indeed be written in the form $a_0 + a_1\xi$, as required.

*Proof.* Suppose $\xi$ satisfies an irreducible polynomial $h(x) \in \mathbb{Q}[x]$ of degree $n$ given by

$$h(x) = x^n + b_1x^{n-1} + \cdots + b_n,$$

with $b_i \in \mathbb{Q}$. Since $\deg(\xi) = n$, $h(x)$ is the minimal polynomial of $\xi$ over $\mathbb{Q}$.

Let $\alpha \in \mathbb{Q}(\xi)$. Then $\alpha$ can be expressed as

$$\alpha = \frac{f(\xi)}{g(\xi)},$$

where $f(x), g(x) \in \mathbb{Q}[x]$ and $g(\xi) \neq 0$.

Since $\gcd(g(x), h(x)) = 1$, there exist polynomials $G(x), H(x) \in \mathbb{Q}[x]$ such that

$$G(x)g(x) + H(x)h(x) = 1.$$

Substituting $x = \xi$, we find that $G(\xi)g(\xi) = 1/g(\xi)$, and thus,

$$\alpha = f(\xi)G(\xi).$$

Therefore, $\alpha$ is a polynomial in $\xi$ over $\mathbb{Q}$, say $\alpha = s(\xi)$, where $s(x) \in \mathbb{Q}[x]$.

We can divide $s(x)$ by $h(x)$, obtaining

$$s(x) = q(x)h(x) + r(x),$$

where $r(x) = 0$ or $\deg(r(x)) < n$. Then,

$$\alpha = s(\xi) = r(\xi),$$

so $\alpha = a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1}$, with $a_i \in \mathbb{Q}$.

Finally, to prove uniqueness, assume

$$\alpha = a_0' + a_1'\xi + \cdots + a_{n-1}'\xi^{n-1}.$$

If $a_i \neq a_i'$ for some $i$, then $\xi$ satisfies a non-zero polynomial of degree less than $n$, a contradiction. Hence, the expression is unique. □

**Example.**

> If $K = \mathbb{Q}(2^{1/3})$, then $2^{1/3}$ is a root of the irreducible polynomial $x^3 - 2$. Thus, any element in $K$ can be written as
>
> $$a_0 + a_1 2^{1/3} + a_2 2^{2/3}$$
>
> where $a_0, a_1, a_2 \in \mathbb{Q}$.

# 9 Quadratic Fields

### Definition 18: Quadratic Field

A field $K = \mathbb{Q}(\alpha)$, where $\alpha$ is an algebraic number of degree 2, is called a quadratic field.

**Example.**

The field $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$ is a quadratic field since $\sqrt{5}$ is a root of the irreducible polynomial $x^2 - 5$.

Similarly, consider $\mathbb{Q}\left(\frac{2+\sqrt{7}}{2}\right)$. Let $\alpha = \frac{2+\sqrt{7}}{2}$. Then, $2\alpha - 2 = \sqrt{7}$, so $\alpha$ is a root of the irreducible polynomial $x^2 - 2x - 2$. Thus, $\mathbb{Q}\left(\frac{2+\sqrt{7}}{2}\right)$ is a quadratic field.

Note:

$$\mathbb{Q}\left(\frac{2+\sqrt{7}}{2}\right) = \mathbb{Q}(\sqrt{7}),$$

$$\mathbb{Q}\left(\frac{3+\sqrt{-3/7}}{5}\right) = Q(\sqrt{\frac{-3}{7}}) = Q(\sqrt{\frac{-21}{49}}) = Q(\frac{1}{7}\sqrt{-21}) = \mathbb{Q}\left(\sqrt{-21}\right),$$

$$\mathbb{Q}(\sqrt{20}) = Q(2\sqrt{5}) = \mathbb{Q}(\sqrt{5}).$$

## Proposition 19

Let $K = \mathbb{Q}(\alpha)$ be a quadratic field, where $\alpha$ is an algebraic number of degree 2. Then $K = \mathbb{Q}(\sqrt{m})$ for some square-free integer $m \neq 1$.

*Proof.* Suppose $\alpha$ satisfies a polynomial $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{Z}$. Then,

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

where $b^2 - 4ac$ is not a perfect square. Thus, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{m})$, where $m$ is a square-free integer.

□

## Claim

Given a quadratic field, there is a unique square-free integer $m \neq 1$ such that the field is $\mathbb{Q}(\sqrt{m})$.

*Proof.* Suppose $Q(\sqrt{m}) = Q(\sqrt{n})$ for two integers $m$ and $n$. This implies that $\sqrt{m}$ can be expressed in terms of $\sqrt{n}$. Therefore, there exist rational numbers $a$ and $b$ such that

$$\sqrt{m} = a + b\sqrt{n}.$$

Squaring both sides of the equation, we get:

$$m = a^2 + 2ab\sqrt{n} + b^2 n.$$

Since $\sqrt{n}$ is irrational (because $n$ is square-free and $n \neq 1$), the coefficient of $\sqrt{n}$ must be zero. Thus, we must have $2ab = 0$.

**Case Analysis:**

- **Case 1:** $b = 0$
  If $b = 0$, then $\sqrt{m} = a$, implying that $m = a^2$, a perfect square. However, this

contradicts the fact that $m$ is square-free. Therefore, $b \neq 0$.

- **Case 2:** $a = 0$
  If $a = 0$, then the equation becomes $m = b^2 n$. Since $m$ and $n$ are both square-free, the only way for this equality to hold is if $b^2 = 1$. This gives $b = \pm 1$, and thus $m = n$.

**Conclusion:** Both cases lead to a contradiction if $m \neq n$, so the only possibility is $m = n$. Therefore, there is a unique square-free integer $m \neq 1$ such that each quadratic field $Q(\sqrt{m})$ has a unique representation. □

**Recall:** If $\alpha$ is an algebraic integer, then $\alpha$ satisfies a monic polynomial with integer coefficients. If $f(x)$ is the minimal polynomial of $\alpha$, then $f(x)$ is monic, $f(x) \in \mathbb{Q}[x]$, and $f(x)$ divides any polynomial $g(x) \in \mathbb{Q}[x]$ for which $g(\alpha) = 0$; i.e., $g(x) = f(x)h(x)$ for some $h(x) \in \mathbb{Q}[x]$.

Since both $f(x)$ and $g(x)$ are monic and $g(x) \in \mathbb{Z}[x]$, by Gauss's Lemma, both $f(x)$ and $h(x)$ must be in $\mathbb{Z}[x]$. Thus, we conclude that the **minimal polynomial of an algebraic integer has all coefficients in** $\mathbb{Z}$.

Now we know that a quadratic field can be written as:

$$\mathbb{Q}(\sqrt{m}) = \left\{ a + b\sqrt{m} : a, b \in \mathbb{Q} \right\},$$

where $m$ is a square-free integer. Alternatively, we can represent elements of $\mathbb{Q}(\sqrt{m})$ as

$$\left\{ \frac{a + b\sqrt{m}}{c} : a, b, c \in \mathbb{Z},\ c > 0 \right\}.$$

Algebraic integers in $\mathbb{Q}$ are simply the usual integers, i.e., elements of $\mathbb{Z}$, also called rational integers.

### Theorem 13

Let $\mathbb{Q}(\sqrt{m})$ , m square-free $\neq 1$, be a quadratic field. Then

(i) $a + b\sqrt{m}$, $a, b \in \mathbb{Z}$, are algebraic integers in $\mathbb{Q}(\sqrt{m})$.

(ii) If $m \equiv 1 \pmod 4$, then in addition $\frac{a+b\sqrt{m}}{2}$ with $a, b$ odd, are also algebraic integers.

(iii) Every algebraic integer in $\mathbb{Q}(\sqrt{m})$ is one of these two types.

*Proof.* (i) $a, b \in \mathbb{Z}$,$a + b\sqrt{m}$ is an algebraic integer because $a$, $b$ $\sqrt{m}$ are algebraic integers and the sum and product of algebraic integers are algebraic integers.

Or : Let $\alpha = a + b\sqrt{m}$, $(\alpha - a)^2 = mb^2$. Therefore $\alpha$ satisfies a monic polynomial with integer coefficients, and therefore $\alpha$ is an algebraic integer.

(ii) Now consider the case where $m \equiv 1 \pmod 4$. Let us examine an element of the form $\frac{a+b\sqrt{m}}{2}$. To determine whether this is an algebraic integer, consider the polynomial:

$$\left(x - \frac{a+b\sqrt{m}}{2}\right)\left(x - \frac{a-b\sqrt{m}}{2}\right) = x^2 - ax + \frac{a^2 - mb^2}{4}.$$

If $a$ and $b$ are odd and $m \equiv 1 \pmod 4$, we find that

$$a^2 - mb^2 \equiv 1 - 1 \equiv 0 \pmod 4.$$

Therefore, the constant term $\frac{a^2-mb^2}{4}$ is an integer, and hence $\frac{a+b\sqrt{m}}{2}$ satisfies a monic polynomial with integer coefficients. Thus, $\frac{a+b\sqrt{m}}{2}$ is an algebraic integer.

(iii) Suppose $\alpha = \frac{a+b\sqrt{m}}{c}$, $a, b, c \in \mathbb{Z}$, $c > 0$ is an algebraic integer in $\mathbb{Q}(\sqrt{m})$. Assume that $\gcd(a, b, c) = 1$.

- If $b = 0$, then $\alpha = \frac{a}{c}$, which is a rational number. For $\alpha$ to be an algebraic integer, $\frac{a}{c}$ must be a rational integer, which is true if and only if $c$ divides $a$ (i.e., $c|a$).
- Now suppose $b \neq 0$. Then $\alpha$ is not a rational number, and the degree of $\alpha$ is 2. In fact, $\alpha$ satisfies the polynomial:

  $$\left(x - \frac{a+b\sqrt{m}}{c}\right)\left(x - \frac{a-b\sqrt{m}}{c}\right) = 0,$$

  which expands to

  $$x^2 - \frac{2a}{c}x + \frac{a^2 - mb^2}{c^2} = 0.$$

Since $\alpha$ is an algebraic integer, this polynomial must have integer coefficients if it is the minimal polynomial of $\alpha$. If $b = 0$, we know that $c|a$, so the polynomial also has integer coefficients in this case. Therefore, for both $b = 0$ and $b \neq 0$, $\alpha = \frac{a+b\sqrt{m}}{c}$ is an algebraic integer if and only if $c|2a$ and $c^2|(a^2 - mb^2)$.

**Additional Considerations:**

- Suppose $(a, c) = 1$. Let $p$ be any prime dividing both $a$ and $c$. Then $p^2|c^2$, so $p^2|(a^2 - mb^2)$. This implies $p^2|a^2$ and $p^2|mb^2$. Since $m$ is square-free, we must have $p^2|b^2$, which gives $p|b$. Therefore, $p$ divides $a$, $b$, and $c$, which contradicts our assumption that $\gcd(a, b, c) = 1$. Thus, $(a, c) = 1$.
- If $c > 2$, then $c|2a$, implying $(a, c) > 1$, which is a contradiction. Therefore, $c = 1$ or $c = 2$.
- If $c = 1$, then $\alpha = a + b\sqrt{m}$ with $a, b \in \mathbb{Z}$.

- If $c = 2$, we require $4|(a^2 - mb^2)$. Since $(a, c) = 1$, $a$ must be odd. We have:

$$a^2 \text{ (odd)} - mb^2 \text{ (odd)} \equiv 0 \pmod 4,$$

so $b^2m$ is odd, which implies that $b$ is also odd.

Thus, if $c = 2$, both $a$ and $b$ must be odd, and we find that $m \equiv 1 \pmod 4$.

Therefore:

- For $m \equiv 2$ or $3 \pmod 4$, the algebraic integers in $\mathbb{Q}(\sqrt{m})$ are of the form $a + b\sqrt{m}$, where $a, b \in \mathbb{Z}$.
- For $m \equiv 1 \pmod 4$, the algebraic integers in $\mathbb{Q}(\sqrt{m})$ are of the following two types:
  1. $a + b\sqrt{m}$, where $a, b \in \mathbb{Z}$.
  2. $\frac{a+b\sqrt{m}}{2}$, where $a$ and $b$ are odd integers.

In other words, for $m \equiv 1 \pmod 4$, the algebraic integers can also be written as $c + d\left(\frac{1+\sqrt{m}}{2}\right)$, where $c, d \in \mathbb{Z}$. □

**Properties of Algebraic Integers:** If $\alpha$ and $\beta$ are algebraic integers, then $\alpha + \beta$, $\alpha\beta$, and $-\alpha$ are also algebraic integers. Thus, the set of all algebraic integers in an algebraic number field forms a subring of that field, and hence is itself a ring.

### Proposition 20

Let $\alpha$ be an algebraic number. Then there exists a $c \in \mathbb{Z}$, $c \neq 0$, such that $c\alpha$ is an algebraic integer.

*Proof.* Suppose $\alpha$ satisfies the polynomial

$$a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0,$$

where $a_i \in \mathbb{Z}$ and not all coefficients are zero. Assume $a_0 \neq 0$. Multiply the polynomial by $a_0^{n-1}$ to obtain

$$(a_0\alpha)^n + a_1(a_0\alpha)^{n-1} + a_2a_0(a_0\alpha)^{n-2} + \cdots + a_na_0^{n-1} = 0.$$

This shows that $a_0\alpha$ satisfies a monic polynomial with integer coefficients, which means $a_0\alpha$ is an algebraic integer. Let $c = a_0$. □

## 9.1 Norm of an algebraic number in a quadratic field

Let $\alpha \in K = \mathbb{Q}(\sqrt{m})$, where $m$ is square-free. Therefore $\alpha = \frac{a+b\sqrt{m}}{c}$, $a, b, c \in \mathbb{Z}$, $c \neq 0$. Then $\overline{\alpha} = \frac{a-b\sqrt{m}}{c}$ is called the conjugate of $\alpha$ in $Q(\sqrt{m})$.

$\alpha$ and $\overline{\alpha}$ are the roots of the quadratic polynomial $x^2 - \frac{2a}{c}x + \frac{a^2-b^2m}{c^2} = 0$.

If $\alpha$ is an algebraic integer, then $\overline{\alpha}$ is also an algebraic integer.

$N(\alpha)$ = norm of $\alpha \in \mathbb{Q}(\sqrt{m})$ is defined as $N(\alpha) = \alpha\overline{\alpha} = \frac{a^2 - b^2 m}{c^2}$.

### Definition 21: Divisor of an integer in a number field

Let $K$ be an algebraic number field. Lett $\alpha$ be non zero integer (i.e. algebraic integer) in $K$. We say that $\alpha$ is a divissor of integer $\beta$ in K, if there is an integer $\gamma$ in K such that $\beta = \alpha\gamma$.

**Example.**

In the field of rational integers, we typically say $2 \mid 6$ because $6 = 2 \times 3$.

Consider $K = \mathbb{Q}(i)$, where $1 + i$ is a divisor of 2 since:

$$2 = (1 + i)(1 - i).$$

In the field $K = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$, note that $-1 \equiv 1 \pmod 4$. Therefore, the ring of all algebraic integers in $\mathbb{Q}(i)$ is:

$$\{a + b\sqrt{-1} : a, b \in \mathbb{Z}\} = \mathbb{Z} + \mathbb{Z}i = \mathbb{Z}[i],$$

where $\mathbb{Z}[i]$ denotes the set of all expressions of the form $a + bi$ with integer coefficients.

## 9.2 Unit of an algebraic integer

### Definition 22: Unit of an algebraic integer

An algebraic integer in $K$ is called a unit of $K$ if it divides 1. Thus an algebraic integer $\epsilon$ is a unit of $K$ if $\epsilon|1$ ($\epsilon$ is a divisor of 1 or $\epsilon$ divides 1), i.e. there is an integer $\epsilon'$ in $K$ such that $\epsilon\epsilon' = 1$.

**Here Unit of $K$ just means the unit of the ring of algebraic integers of $K$ in the usual sense.**

### Proposition 23

Reciprocal of a unit is also a unit

*Proof.* Let $\epsilon$ be a unit of $K$. Therefore $\epsilon$ is an algebraic integer, $\epsilon \neq 0$, such that $\epsilon|1$. So there is an algebraic integer $\epsilon'$ such that $\epsilon\epsilon' = 1$. Therefore $\epsilon'$ is a unit of $K$. But $\epsilon' = \frac{1}{\epsilon}$. Thus $\frac{1}{\epsilon}$ is a unit of $K$. □

**Theorem 14**

The units of $K$ form a subgroup of the group of non-zero elements of $K$.

*Proof.* Let $U$ be the set of units of $K$. Let $\epsilon_1$, $\epsilon_2$ be in $U$. Therefore, there are algebraic integers $\epsilon_3$ and $\epsilon_4$ in $K$ such that $\epsilon_1\epsilon_3 = 1$ and $\epsilon_2\epsilon_4 = 1$. Therefore $\epsilon_1\epsilon_2(\epsilon_3\epsilon_4) = 1$, we get that $\epsilon_1\epsilon_2$ is also a unit of $K$. Also, for $\epsilon \in U$, $\frac{1}{\epsilon}$ is a unit. Therefore $U$ is a subgroup of $K^*$. Therefore $U$ is a group. □

**Recall:** The norm of an element $\alpha$, denoted $N(\alpha)$, is defined as $N(\alpha) = \alpha\overline{\alpha}$.

$$N(\alpha) = \left(\frac{a + b\sqrt{m}}{c}\right)\left(\frac{a - b\sqrt{m}}{c}\right) = \frac{a^2 - b^2m}{c^2}.$$

Thus, $N(\alpha) \in \mathbb{Q}$.

Suppose $\alpha$ is an algebraic integer in $\mathbb{Q}(\sqrt{m})$, and let $\alpha = \frac{a+b\sqrt{m}}{c}$ as before.

- If $b = 0$, then $\alpha = \frac{a}{c}$ and $\overline{\alpha} = \frac{a}{c}$. Since $\alpha$ and $\overline{\alpha}$ are both algebraic integers, $\alpha \in \mathbb{Q}$, making $\alpha$ a rational number. Consequently, $\alpha \in \mathbb{Z}$, and we have:

$$N(\alpha) = \alpha\overline{\alpha} = \alpha^2 \in \mathbb{Z}.$$

- Now suppose $b \neq 0$. In this case, $\alpha$ is not a rational number, so the degree of $\alpha$ is 2. We observe that $\alpha$ satisfies the polynomial:

$$x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} = 0,$$

where

$$\alpha + \overline{\alpha} = \frac{2a}{c} \quad \text{and} \quad \alpha\overline{\alpha} = \frac{a^2 - b^2m}{c^2}.$$

Both $\alpha + \overline{\alpha}$ and $\alpha\overline{\alpha}$ are in $\mathbb{Q}$.

This polynomial is monic, defined over $\mathbb{Q}$, and has degree 2, so it is the minimal polynomial of $\alpha$. Since $\alpha$ is an algebraic integer, this minimal polynomial must actually have integer coefficients. Therefore:

$$\alpha\overline{\alpha} = \frac{a^2 - b^2m}{c^2} \in \mathbb{Z},$$

which implies $N(\alpha) \in \mathbb{Z}$.

**Thus, if $\alpha \in \mathbb{Q}(\sqrt{m})$ is an algebraic integer, then $N(\alpha)$ is an integer.**

**Theorem 15**

Let $\alpha$ be an integer of $K = \mathbb{Q}(\sqrt{m})$. Then $\alpha$ is a unit of $K$ if and only if $N(\alpha) = \pm 1$.

*Proof.* Suppose $\alpha$ is a unit in $K$. Then $\alpha$ is an algebraic integer in $K$, and there exists an algebraic integer $\beta$ in $K$ such that $\alpha\beta = 1$.

Taking the norm, we find that

$$N(\alpha\beta) = N(1) = 1.$$

Using the multiplicative property of the norm, we have:

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

This property holds for any elements $\alpha$ and $\beta$ in the quadratic field $K = \mathbb{Q}(\sqrt{m})$.

Since $\alpha\beta = 1$, we get $N(\alpha)N(\beta) = 1$. Since $N(\alpha)$ and $N(\beta)$ are both integers (as $\alpha$ and $\beta$ are integers in $K$), it follows that $N(\alpha) = \pm 1$.

Conversely, suppose $N(\alpha) = \pm 1$. Then $\alpha\overline{\alpha} = \pm 1$, which implies:

$$\alpha \cdot (\pm\overline{\alpha}) = 1.$$

Here, $\pm\overline{\alpha}$ is an algebraic integer in $K$, so $\alpha$ divides 1, meaning that $\alpha$ is a unit. □

**Example.**

> Find $N(3 + 4i)$ in $\mathbb{Q}(i)$.
>
> We calculate:
>
> $$N(3 + 4i) = (3 + 4i)(3 - 4i) = 3^2 + 4^2 = 9 + 16 = 25.$$
>
> Secondly, consider
> $N(\frac{3}{5} + \frac{4}{5}i) = (\frac{3}{5} + \frac{4}{5}i)(\frac{3}{5} - \frac{4}{5}i) = \frac{9}{25} + \frac{16}{25} = 1$
>
> Here the ring of algebraic in $Q(i)$ is $\{a + bi : a, b \in \mathbb{Z}\}$. Therefore $\frac{3}{5} + \frac{4}{5}i$ is not an algebraic integer in $Q(i)$.ALthough $N(\frac{3}{5} + \frac{4}{5}i) = 1$, $\frac{3}{5} + \frac{4}{5}i$ is not a unit of $Q(i)$.

**Note:** If $m \geq 2$ (i.e., $m > 0$), the quadratic field $\mathbb{Q}(\sqrt{m})$ has infinitely many units.

For example, if $m = 2$, the ring of integers of $K = \mathbb{Q}(\sqrt{2})$ is:

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

We observe that $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

$$N(1 + \sqrt{2}) = (1 + \sqrt{2})(1 - \sqrt{2}) = 1 - 2 = -1.$$

Therefore, $1 + \sqrt{2}$ is a unit in $K$.

Since $(1 + \sqrt{2})^n$ is also a unit for all $n \geq 1$, and these powers are all distinct, we obtain infinitely many units in $K$.

Now, if $m$ is a square-free integer $> 1$, consider $\alpha = a + b\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, where $a, b \in \mathbb{Z}$. Then $\alpha$ is an integer of $K = \mathbb{Q}(\sqrt{m})$.

The norm of $\alpha$ is given by:

$$N(\alpha) = a^2 - b^2 m.$$

If $N(\alpha) = 1$, i.e., $a^2 - b^2 m = 1$, then $\alpha$ is a unit in $K$. This equation:

$$x^2 - my^2 = 1,$$

is known as Pell's equation or the Brahmagupta-Bhaskara equation.

Since Pell's equation has infinitely many solutions, this proves the existence of infinitely many units in $\mathbb{Q}(\sqrt{m})$ for $m > 1$.

## 9.3 Units in Imaginary Quadratic Fields

**Theorem 16**

Let $K = \mathbb{Q}(\sqrt{m})$, where $m$ is a square-free integer with $m < 0$. The units in $K$ are as follows:

(i) For $m = -1$, the units are $\pm 1$ and $\pm i$.

(ii) For $m = -3$, the units are $\pm 1$, $\pm\omega$, and $\pm\omega^2$, where $\omega = \frac{-1+\sqrt{-3}}{2}$. These can also be written as $\pm 1$ and $\frac{\pm 1 \pm \sqrt{-3}}{2}$.

(iii) For $m \neq -1, -3$, the units are just $\pm 1$.

*Proof.* Let $\epsilon$ be a unit in $\mathbb{Q}(\sqrt{m})$. Write $\epsilon = \frac{a+b\sqrt{m}}{2}$ with $m \equiv 1 \pmod 4$, where $a$ and $b$ are odd integers.

Since $\epsilon$ is a unit, we have $N(\epsilon) = \pm 1$.

Now,

$$N(\epsilon) = \begin{cases} a^2 - b^2 m, & \text{if } m \equiv 0 \pmod 4 \\ \frac{a^2 - b^2 m}{4}, & \text{if } m \equiv 1 \pmod 4 \text{ and } a, b \text{ are odd} \end{cases}$$

Since $m$ is negative, $-m > 0$. Therefore, $N(\epsilon) > 0$, which implies $N(\epsilon) = 1$.

Consider the case $a^2 - b^2 m = 1$. If $m \leq -2$, then $a^2 - b^2 m \geq 2b^2$. If $b = 0$, then $a = \pm 1$; if $b \neq 0$, then $a^2 - b^2 m \geq 2b^2 \geq 2$. Therefore, there is no unit with $b \neq 0$ in this case.

Thus, if $m \leq -2$ and $m \not\equiv 1 \pmod 4$, then $\epsilon = \pm 1$.

For $m = -1$, we have $a^2 - mb^2 = a^2 + b^2 = 1$, giving $a = \pm 1$, $b = 0$, or $a = 0$, $b = \pm 1$. Therefore, $\epsilon = \pm 1$ or $\pm i$.

Now consider $N(\epsilon) = \frac{a^2 - b^2 m}{4}$ with $m \equiv 1 \pmod 4$ and $a, b$ odd. Then $N(\epsilon) = 1$ gives $a^2 - b^2 m = 4$.

If $m < -3$, i.e., $m \leq -7$ with $m \equiv 1 \pmod 4$, then $a^2 - b^2 m \geq 7$ if $b \neq 0$, so there are no units with $b \neq 0$ in this case. Therefore, $b = 0$, which implies $a^2 = 4$, a contradiction as $a$ is odd.

For $m = -3$, we have $a^2 + 3b^2 = 4$ with $b$ odd. For $b = \pm 1$, we find $a^2 = 1$, so $a = \pm 1$, giving $\epsilon = \frac{\pm 1 \pm \sqrt{-3}}{2}$. No units exist with $b \neq \pm 1$, as $a^2 + 3b^2 > 4$.

For $m \equiv 1 \pmod 4$, the first case $a^2 - b^2 m = 1$ gives $a = \pm 1$ and $b = 0$, so $\epsilon = \pm 1$ is the only possibility.

Therefore:

(i) For $m = -1$, the units are $\pm 1$ and $\pm i$.

(ii) For $m = -3$, the units are $\pm 1$, $\pm\omega$, and $\pm\omega^2$, where $\omega = \frac{-1+\sqrt{-3}}{2}$.

(iii) For $m \neq -1, -3$, the units are $\pm 1$.

□

## 9.4 Prime Elements in an Algebraic Number Field

### Definition 24

A prime element in $K$ is an algebriac integer $\pi$ in $K$ such that $\pi$ is a non unit and if $\pi = \alpha\beta$ ($\alpha$, $\beta$ integers of K) then either $\alpha$ is a unit or $\beta$ is a unit. (irreducible element)

### Proposition 25

Suppose $\pi$ is an algebraic integer in $Q(\sqrt{m})$ such that $N(\pi) = \pm p$, $p$ a prime number then $\pi$ is a prime in $K$.

*Proof.* Assume, for the sake of contradiction, that $\pi$ is not prime. Then we can write $\pi = \alpha\beta$ for some elements $\alpha$ and $\beta$ in $K$, where neither $\alpha$ nor $\beta$ is a unit.

Since $N(\pi) = \pm p$ and $N(\pi) = N(\alpha\beta) = N(\alpha)N(\beta)$, it follows that:

$$N(\alpha)N(\beta) = \pm p.$$

If both $\alpha$ and $\beta$ are non-units, then $N(\alpha) \neq 1$ and $N(\beta) \neq 1$. This would imply that both $N(\alpha)$ and $N(\beta)$ are divisors of $\pm p$, which is impossible since $p$ is prime and $N(\alpha), N(\beta) \neq 1$.

Thus, we reach a contradiction, and it follows that $\pi$ must be a prime in $K$. □

**Example.**

> $1 + i$ is a prime in $Q(i)$.
>
> $N(1 + i) = (1 + i)(1 - i) = 1 - i^2 = 1 + 1 = 2$, which is a prime number. Therefore $1 + i$ is a prime in $Q(i)$.

**Note:** If $\pi$ is prime on $\mathbb{Q}(\sqrt{m})$ so is $\underbrace{\epsilon\pi}_{\text{associate of}\pi}$ for any unit $\epsilon$ in $K$.

*Proof.* Suppose $\pi$ is prime. Let $\epsilon$ be a unit in $K$ and consider the element $\epsilon\pi$, which is an associate of $\pi$. Assume for contradiction that $\epsilon\pi$ is not prime, so we can write $\epsilon\pi = \alpha\beta$ for some elements $\alpha$ and $\beta$ in $K$.

Then we have:

$$\pi = (\epsilon^{-1}\alpha)\beta.$$

Since $\pi$ is prime, it must be the case that either $\epsilon^{-1}\alpha$ is a unit or $\beta$ is a unit.

If $\epsilon^{-1}\alpha$ is a unit, then $\epsilon(\epsilon^{-1}\alpha) = \alpha$ is also a unit (since a unit times a unit is a unit).

Therefore, either $\alpha$ or $\beta$ is a unit, meaning $\epsilon\pi$ satisfies the conditions of being prime. This proves that any associate of a prime element $\pi$ in $K$ is also prime. □

**Definition 26**

If $\alpha$, $\beta$ are non zero elements of ring of integers of an algebraic number field, then they are called associates if $\frac{\alpha}{\beta}$ is a unit, or equivalently if $\frac{\beta}{\alpha}$ is a unit, i.e. $\alpha = \text{unit} \times \beta$ or $\beta = \text{unit} \times \alpha$.

**Proposition 27**

Let $K = \mathbb{Q}(\sqrt{m})$, m square free $\neq 1$. Any non zero, non unit integer of $K$ can be written as a product of primes in $K$

*Proof.* Let $\alpha$ be a non-zero, non-unit element of $K$. If $\alpha$ is not prime, then there exist non-units $\alpha_1$ and $\alpha_2$ in $K$ such that $\alpha = \alpha_1\alpha_2$.

We can continue factorizing $\alpha_1$ and $\alpha_2$ if either is not prime. Proceeding in this manner, suppose the factorization process does not terminate. Then, for every $n \geq 2$, we have:

$$\alpha = \beta_1\beta_2 \dots \beta_n,$$

where each $\beta_i$ is a non-unit in $K$.

Since $\beta_i$ is a non-unit, we have $|N(\beta_i)| \geq 2$. Consequently, $|N(\alpha)| \geq 2^n$ for every $n \geq 2$.

This implies that $|N(\alpha)|$ grows without bound as $n \to \infty$, which is a contradiction because $\alpha$ has a fixed norm. Therefore, the factorization process must terminate, meaning that $\alpha$ can indeed be written as a product of primes in $K$. □

## 9.5 Euclidean Quadratic Fields

**Definition 28: Euclidean Quadratic Fields**

A quadratic field $\mathbb{Q}(\sqrt{m})$ is called Euclidean if the Euclidean algorithm holds wrt norm for integers in $K$.

**Definition 29: Euclidean Algorithm wrt norm**

Let $a$, $b$, be integers in $K$, a non zero. Then there are integers $c$, $r$ in $K$ such that $b = ac + r$ and $N(r) < N(a)$.

**Proposition 30**

Let $K = \mathbb{Q}(\sqrt{m})$ be a Euclidean Quadratic Field. Let $\alpha$, $\beta$ be twwo non zero non units of $K$ which do not have a common factor. There there are $\gamma$, $\delta$ integrs of $K$, such that

$$1 = \alpha\gamma + \beta\delta$$

*Proof.* Consider elements of the form $\alpha\gamma + \beta\delta$, where $\gamma$ and $\delta$ vary over the integers in $K$. Let $\epsilon$ be an element of this form with the minimum non-zero norm $|N(\epsilon)|$ in absolute value. Divide $\alpha$ by $\epsilon$, so we can write:

$$\alpha = \gamma'\epsilon + \delta',$$

where $|N(\delta')| < |N(\epsilon)|$.

Now, express $\delta'$ as:

$$\delta' = \alpha - \gamma'\epsilon = \alpha - \gamma'(\alpha\gamma_1 + \beta\delta_1),$$

which is a combination of $\alpha$ and $\beta$. Since $|N(\delta')| < |N(\epsilon)|$, we have $N(\delta') = 0$, implying that $\delta' = 0$. Therefore, $\epsilon$ divides $\alpha$, and similarly, $\epsilon$ divides $\beta$.

Thus, $\epsilon$ is a common factor of $\alpha$ and $\beta$. However, since $\alpha$ and $\beta$ do not have a non-trivial common factor, $\epsilon$ must be a unit.

We have $\epsilon = \alpha\gamma_1 + \beta\delta_1$, so:

$$1 = \alpha\left(\frac{\gamma_1}{\epsilon}\right) + \beta\left(\frac{\delta_1}{\epsilon}\right).$$

This shows that 1 can be written as a combination of $\alpha$ and $\beta$ with coefficients that are integers in $K$.reofore 1 is a combination of $\alpha$ and $\beta$ with integers in $K$ as coefficients.

□

**Proposition 31**

In a Euclidean Field $K$, if $\pi$ is prime then $\pi|\alpha\beta$ implies $\pi|\alpha$ or $\pi|\beta$

*Proof.* Suppose $\pi|\alpha\beta$ and $\pi \nmid \alpha$. Then $\alpha$ and $\pi$ do not have a non-trivial common factor. Therefore, there exist integers $\gamma$ and $\delta$ in $K$ such that:

$$1 = \pi\gamma + \alpha\delta.$$

Multiplying both sides by $\beta$, we get:

$$\beta = \pi\gamma\beta + \alpha\beta\delta.$$

Since $\pi|\alpha\beta$, it follows that $\pi|\beta$. □

This establishes that:

**Theorem 17**

A Euclidean Field has a unique prime factorization property, i.e. every non zero, non unit integer of $K$ is a product of primes uniquely apart from order and associates

# 10 Fermat's Last Theorem for $n = 3$ and $n = 4$

## 10.1 $x^3 + y^3 = z^3$

**Theorem 18: Fermat's Last Theorem**

Let $n \geq 3$ be an integer. Then the equation $x^n + y^n = z^n$ has no solutions over $\mathbb{Z}$.

We will prove this theorem for $n = 3$.

**Proof for $n = 3$:**

The equation $x^3 + y^3 = z^3$ was proved by Euler to have no solutions in positive integers. We will consider the following claims to prove this theorem:

**Claim: 1**

A minimization argument for $a, b, c$

**Claim: 2**

$\gcd(a + b, a^2 - ab + b^2) = 1$

**Claim: 3**

$(a + b)$ and $(a^2 - ab + b^2)$ are perfect cubes

**Claim: 4**

$$\begin{cases} a + b = p^3 \\ a^2 - ab + b^2 = q^3 \end{cases}$$ has no solutions

WTS: $\nexists a, b, c \in \mathbb{Z}^+$ such that $a^3 + b^3 = c^3$.

By contradiction, assume that $\exists a, b, c \in \mathbb{Z}^+$ such that $a^3 + b^3 = c^3$. Suppose that $a, b, c$ are such that $(a + b + c)$ is minimized.

**Definition 32: Minimized**

Minimized, here, means choosing the smallest possible value of $(a + b + c)$ among all potential solutions $(a, b, c)$ that satisfy the equation $a^3 + b^3 = c^3$.

WLOG, assume that $\gcd(a, b, c) = 1$. If not, we can divide $a, b, c$ by their gcd. The equation $a^3 + b^3 = c^3$ will still hold for the reduced values $a', b', c'$, satisfying $\gcd(a', b', c') = 1$.

The equation $a^3 + b^3 = c^3$ can be written as $(a+b)(a^2 - ab + b^2) = c^3$. We now proceed to prove Claim 2: $\gcd(a + b, a^2 - ab + b^2) = 1$.

**Proof of Claim 2:**

Assume that $d \in \mathbb{Z}$ is a common divisor of $(a + b)$ and $(a^2 - ab + b^2)$. Then $d$ divides both $(a + b)$ and $(a^2 - ab + b^2)$. Thus,

$$\begin{cases} d|(a+b) & (1) \\ d|(a^2 - ab + b^2) & (2) \end{cases}$$

From (1), $a + b \equiv 0 \pmod{d}$, which implies $a \equiv -b \pmod{d}$. Substituting $a \equiv -b \pmod{d}$ into (2), we get:

$$d|((-b)^2 - (-b)b + b^2) \implies d|(b^2 + b^2 + b^2) \implies d|3b^2.$$

This implies $d|b$ or $d|3$.

If $d|b$, then $b|d$. However, since $d|(a + b)$, we have:

$$\frac{a+b}{d} \in \mathbb{Z} \implies \frac{a}{d} + \frac{b}{d} \in \mathbb{Z} \implies \frac{a}{d} \in \mathbb{Z}.$$

Thus, $d|a$. Combining $d|a$ and $d|b$, we deduce $\gcd(a, b) \geq 1$, which contradicts the assumption $\gcd(a, b, c) = 1$.

Therefore, $d|3$, so $d = 1$ or $d = 3$.

Now considering (1), $d|(a + b) \implies 3|(a + b) \implies a \equiv -b \pmod{3}$.

Thus, $\exists k, m \in \mathbb{Z}$ such that:

$$\begin{cases} a = 3k + r, \\ b = 3m + r, \end{cases}$$

i.e., $a$ and $b$ are multiples of 3 plus the same remainder $r$.

From $a \equiv -b \pmod{3}$, we can write:

$$3k+r \equiv -(3m+r) \pmod{3} \implies 3k+r \equiv -3m-r \pmod{3} \implies 2r \equiv 0 \pmod{3} \implies r \equiv 0 \pmod{3}.$$

Thus:

$$\begin{cases} a = 3k \equiv 0 \pmod{3}, \\ b = 3m \equiv 0 \pmod{3}, \end{cases}$$

which implies:

$$\begin{cases} 3|a, \\ 3|b. \end{cases}$$

This contradicts the assumption that $\gcd(a, b, c) = 1$. Therefore, $d = 1$ is the only value

that satisfies (1) and (2).

Thus:

$$\gcd(a + b, a^2 - ab + b^2) = 1. \tag{$\pi$}$$

Now $c^3 = (a + b)(a^2 - ab + b^2)$, and from ($\pi$), we conclude:

$$\begin{cases} a + b = p^3, \quad p \in \mathbb{Z}, \\ a^2 - ab + b^2 = q^3, \quad q \in \mathbb{Z}. \end{cases}$$

**Definition 33: Perfect Cube**

$n \in \mathbb{Z}$ is a perfect cube if $\exists m \in \mathbb{Z}$ such that $n = m^3$.

We can write $a + b$ as $a + b = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, where $p_i$ are primes, $e_i \in \mathbb{Z}$, and $\exists$ at least one $e_i$ such that $3 \nmid e_i$ for $i \in \{1, \dots, k\}$.

If $a^2 - ab + b^2$ is a perfect cube, then $\exists q \in \mathbb{Z}$ such that $a^2 - ab + b^2 = q^3$. Substituting these relations, we get:

$$c^3 = (a + b)(a^2 - ab + b^2) = (p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}) q^3.$$

Assume $e_2$ is such that $3 \nmid e_2$ and $e_1 = e_3 = \dots = e_k = 3$. Then:

$$c^3 = (p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}) q^3 = p_2^{e_2} (p_1 p_3 \dots p_k q)^3.$$

Thus:

$$\left( \frac{c}{p_1 p_3 \dots p_k} \right)^3 = p_2^{e_2}.$$

Let $x = \frac{c}{p_1 p_3 \dots p_k}$. Then $x^3 = p_2^{e_2}$, where $x \in \mathbb{Q}$, $p_2$ is prime, and $e_2 \in \mathbb{Z}$ such that $3 \nmid e_2$.

Since $x \in \mathbb{Q}$, we have $x = p_2^{e_2/3}$. For $x \in \mathbb{Q}$, $\frac{e_2}{3} \in \mathbb{Z}$, which implies $3 | e_2$. This contradicts the assumption $3 \nmid e_2$.

Thus, $a + b = p_1^3 p_2^3 \dots p_k^3 = (p_1 p_2 \dots p_k)^3$, i.e., $a + b$ is a perfect cube. By the same reasoning, $a^2 - ab + b^2$ is also a perfect cube.

Hence:

$$\begin{cases} a + b = p^3, \\ a^2 - ab + b^2 = q^3. \end{cases}$$

Substituting $a = p^3 - b$ into $a^2 - ab + b^2 = q^3$, we get:

$$(p^3 - b)^2 - (p^3 - b)b + b^2 = q^3.$$

Expanding:

$$p^6 - 2p^3 b + b^2 - p^3 b + b^2 + b^2 = q^3 \implies p^6 - 3p^3 b + 3b^2 = q^3.$$

Reducing modulo $p^3$, we have:

$$p^6 - 3p^3 b + 3b^2 \equiv q^3 \pmod{p^3}.$$

This simplifies to:

$$3b^2 \equiv q^3 \pmod{p^3}.$$

To complete the proof, we show that $3b^2 \equiv q^3 \pmod{p^3}$ implies $q^3 \equiv 0 \pmod{p^3}$. Assume the contrary. If $q^3 \not\equiv 0 \pmod{p^3}$, it leads to a contradiction regarding the divisibility of $b^2$ and $p^3$. Therefore, $q^3 \equiv 0 \pmod{p^3}$, which implies $b \equiv 0 \pmod{p^3}$, contradicting the minimality of $a + b + c$.

Hence, no solutions exist for $a^3 + b^3 = c^3$ in $\mathbb{Z}^+$.

## 10.2 $x^4 + y^4 = z^4$

**Theorem 19**

The equation $x^4 + y^4 = z^4$ has no solutions in positive integers.

**Theorem 20**

The equation $x^4 + y^4 = z^2$ has no solutions in positive integers.

**Main idea:** Relate solutions to $x^2 + y^2 = z^2$ to solutions to equations $x^4 + y^4 = z^2$ and $a^2 + 4b^4 = c^4$.

Namely, for each solution $(x, y, z)$ to $x^4 + y^4 = z^2$ we construct a positive solution $(a, b, c)$ to $a^2 + 4b^4 = c^4$ with $c < z$.

Then using the solution $(a, b, c)$ we construct another solution $(x', y', z')$ with $z' < c$ and so on. This would imply that the set of values of $z$ arising in solutions to $x^4 + y^4 = z^2$ has no minimal element which contradicts to the fact that every non empty set of positive integers has a minimal element.

**Proof:**

Take any solutions $(x, y, z)$. Find a solution $(a, b, c)$ with $c < z$. Then construct a new solution $(x', y', z')$ with $z' < c \implies z' < z$.

Take any $(x, y, z)$ with $x^4 + y^4 = z^2$. Let $d = \gcd(x, y)$, where $d > 1$, and $d \mid x$ and $d \mid y$. Then, we have

$$d^4 \mid x^4 + y^4 = z^2 \implies d^2 \mid z.$$

Thus, we can define new variables as follows:

$$x_1 = \frac{x}{d}, \quad y_1 = \frac{y}{d}, \quad z_1 = \frac{z}{d^2}.$$

The greatest common divisor $\gcd(x_1, y_1, z_1)$ satisfies $x^4 + y^4 = z^2$, with $\gcd(x_1, y_1) = 1$. This implies that $(x_1^2, y_1^2, z_1)$ satisfies $x^2 + y^2 = z^2$ and $\gcd(x_1^2, y_1^2) = 1$.

Now, consider the equations:

$$x_1^2 = r^2 - s^2, \quad y_1^2 = 2rs, \quad z_1 = r^2 + s^2,$$

where $r > s > 0$, $\gcd(r, s) = 1$, and $r$ and $s$ are of different parity.

**Claim**

$r$ is odd, and $s$ is even.

Otherwise, if $r$ is even and $s$ is odd, then

$$(r^2 - s^2) \equiv 0 - 1 \equiv -1 \equiv x_1^2 \pmod 4,$$

which is impossible.

Thus, $\gcd(r, s) = 1$ and $r$ is odd, and $s$ is even. This implies $\gcd(r, 2s) = 1$. Additionally,

$$y_1^2 = r(2s) \implies r, 2s \text{ are perfect squares.}$$

Therefore, we set

$$r = c^2 \quad \text{and} \quad 2s = (2b)^2 = 4b^2 \implies s = 2b^2.$$

We now have

$$r^2 = c^2, \quad s = 2b^2, \quad \gcd(c, b) = 1.$$

Thus,

$$x_1 = r^2 - s^2 = c^4 - 4b^4.$$

We conclude that

$$x_1^2 + 4b^4 = c^4.$$

This satisfies the equation $a^2 + 4b^4 = c^4$ with $c < z$.

Next, let $h = \gcd(b, c)$, so that

$$h^4 \mid c^4 - 4b^4 = a^2 \implies h^2 \mid a.$$

Define new variables:

$$a_1 = \frac{a}{h^2}, \quad b_1 = \frac{b}{h}, \quad c_1 = \frac{c}{h}.$$

We have $\gcd(b_1, c_1) = 1$, and thus $(a_1, 2b_1^2, c_1)$ is a solution to $x^2 + y^2 = z^2$. This solution is primitive because $c^2 = r$ is odd, so $c_1^2$ is odd, and $\gcd(2b_1^2, c_1) = 1$.

Finally, let $r'$ and $s'$ have opposite parity, and $\gcd(r', s') = 1$. Then

$$a_1 = (r')^2 - (s')^2, \quad 2b_1^2 = 2r's', \quad b_1^2 = r's'.$$

Thus, we have

$$c_1^2 = (r')^2 + (s')^2.$$

By setting $z' = c_1$, we get a new solution $(x', y', z')$ satisfying the equation

$$x^4 + y^4 = z^2.$$

Furthermore, since $c_1' = z' < c < z$, we conclude that $z' \leq z$, as required.

This completes the proof that the equation $x^4 + y^4 = z^2$ has no solutions in positive integers.

# 11 Unique Factorization

**Definition 34: Unique Factorization**

An integral domain $R$ has the *unique factorization property* if:

- Every non-zero, non-unit element $a \in R$ can be expressed as a product of irreducible elements:
$$a = p_1 p_2 \cdots p_k,$$
where $p_i$ are irreducible elements.
- This factorization is unique up to the order of the factors and multiplication by units.

Such a domain is called a *unique factorization domain (UFD).*

Unique factorization ensures that prime elements behave analogously to prime numbers in $\mathbb{Z}$. For example, quadratic fields such as $\mathbb{Q}(\sqrt{m})$ may or may not exhibit unique factorization, which significantly influences their arithmetic structure.

**Theorem 21**

The fields $\mathbb{Q}(\sqrt{m})$ for $m = -1, -2, -3, -7, 2, 3$ are Euclidean and so have the unique factorization property.

**Proposition 35**

Every Euclidean domain is a unique factorization domain.

*Proof:* In a Euclidean domain:

- All ideals are principal (it is a principal ideal domain, PID).
- PIDs are UFDs because every element can be factored into irreducibles uniquely.

Thus, proving a quadratic field is Euclidean ensures it is a UFD.

**Proof of Thm 21**

Consider any integers $\alpha$ and $\beta$ in $\mathbb{Q}(\sqrt{m})$ with $\beta \neq 0$. Then

$$\frac{\alpha}{\beta} = u + v\sqrt{m},$$

where $u$ and $v$ are rational numbers. Let $x$ and $y$ be integers closest to $u$ and $v$, respectively, such that

$$0 \leq |u - x| \leq \frac{1}{2}, \quad 0 \leq |v - y| \leq \frac{1}{2}.$$

Define $\gamma = x + y\sqrt{m}$ and $\delta = \alpha - \beta\gamma$. Both $\gamma$ and $\delta$ are elements of $\mathbb{Q}(\sqrt{m})$. The norm of $\delta$ is given by

$$N(\delta) = N(\beta)N\left(\frac{\alpha}{\beta} - \gamma\right),$$

where

$$\frac{\alpha}{\beta} - \gamma = (u - x) + (v - y)\sqrt{m}$$

Thus, the norm becomes

$$N(\delta) = |N(\beta)| \cdot \left|(u - x)^2 - m(v - y)^2\right|$$

Using the bounds on $u - x$ and $v - y$ from (9.10), we have

$$(u - x)^2 \leq \frac{1}{4}, \quad m(v - y)^2 \leq \frac{|m|}{4}$$

For $m > 0$, it follows that

$$-\frac{m}{4} \leq (u - x)^2 - m(v - y)^2 \leq \frac{1}{4}$$

For $m < 0$, we obtain

$$0 \leq (u - x)^2 - m(v - y)^2 \leq \frac{1}{4} + \frac{|m|}{4}$$

Thus, for $m = 2, 3, -1, -2$, we have

$$|N(\delta)| < |N(\beta)|,$$

proving that $\mathbb{Q}(\sqrt{m})$ is Euclidean for these values of $m$.

For $m = -3$ and $m = -7$, we modify the choice of $\gamma$. Define

$$\gamma = \frac{r + s\sqrt{m}}{2},$$

where $r$ and $s$ are integers such that $r \equiv s \pmod 2$ and $|2u - r| \leq 1$, $|2v - s| \leq 1$. Then

$$\gamma \in \mathbb{Q}(\sqrt{m}),$$

and $\delta = \alpha - \beta\gamma$ satisfies

$$N(\delta) = |N(\beta)| \cdot \left|\frac{1}{4} + \frac{1}{16}(-m)\right| < |N(\beta)|.$$

Hence, $\mathbb{Q}(\sqrt{m})$ is Euclidean for $m = -3$ and $m = -7$ as well. This completes the proof.

# 12 Primes in Quadratic Fields Having the Unique Factorization Property

**Background:** In quadratic fields $\mathbb{Q}(\sqrt{m})$, the unique factorization property allows us to study the structure of primes. Rational primes $p$ in $\mathbb{Z}$ behave differently in these fields, and understanding their decomposition in $\mathbb{Q}(\sqrt{m})$ is fundamental in algebraic number theory.

**Theorem 22**

Let $\mathbb{Q}(\sqrt{m})$ have the unique factorization property. Then:
To any prime $\pi$ in $\mathbb{Q}(\sqrt{m})$, there corresponds one and only one rational prime $p \in \mathbb{Z}$ such that $\pi \mid p$.

*Proof.* The norm $N(\pi)$ of the prime $\pi$ is a positive rational integer. Since $\pi$ divides $N(\pi)$, there exist positive rational integers divisible by $\pi$. Let $n$ be the smallest such positive integer.

We claim that $n$ is a rational prime. Suppose, for contradiction, that $n$ is not a rational prime. Then $n$ can be written as $n = n_1 n_2$, where $0 < n_1 < n$ and $0 < n_2 < n$.

Since $\pi \mid n$, it must also divide $n_1$ or $n_2$ (by the unique factorization property). However, this contradicts the minimality of $n$, because $n_1$ or $n_2$ would be a smaller positive integer divisible by $\pi$. Hence, $n$ must be a rational prime, which we call $p$.

Next, we show that $\pi$ cannot divide any other rational prime $q \neq p$. Suppose $\pi \mid q$ for some other rational prime $q$. By Bezout's identity, there exist integers $x$ and $y$ such that:

$$1 = px + qy.$$

Since $\pi \mid p$ and $\pi \mid q$, it follows that $\pi \mid 1$, which is impossible because no prime can divide 1. Therefore, $\pi$ cannot divide any rational prime other than $p$.

Thus, every prime $\pi$ in $\mathbb{Q}(\sqrt{m})$ corresponds to exactly one rational prime $p$, completing the proof. □

In Theorem 22, we established that each prime $\pi$ in $\mathbb{Q}(\sqrt{m})$ corresponds to exactly one rational prime $p$ in $\mathbb{Z}$. This correspondence forms the foundation for understanding how rational primes behave in quadratic fields.

Theorem 23 builds on this result by exploring how rational primes $p$ either remain prime in $\mathbb{Q}(\sqrt{m})$, split into products of two primes, or behave in other special ways depending on $m$.

## Theorem 23

Let $\mathbb{Q}(\sqrt{m})$ have the unique factorization property. Then:

1. Any rational prime $p$ is either a prime $\pi$ of the field or a product $\pi_1\pi_2$ of two primes, not necessarily distinct, of $\mathbb{Q}(\sqrt{m})$.
2. The totality of primes $\pi, \pi_1, \pi_2$ obtained by applying part (1) to all rational primes, together with their associates, constitute the set of all primes of $\mathbb{Q}(\sqrt{m})$.
3. An odd rational prime $p$ satisfying $(p, m) = 1$ is a product $\pi_1\pi_2$ of two primes in $\mathbb{Q}(\sqrt{m})$ if and only if $\left(\frac{m}{p}\right) = 1$. Furthermore, if $p = \pi_1\pi_2$, the product of two primes, then $\pi_1$ and $\pi_2$ are not associates, but $\pi_1$ and $\overline{\pi_2}$ are, and $\pi_2$ and $\overline{\pi_1}$ are.
4. If $(2, m) = 1$, then 2 is the associate of a square of a prime if $m \equiv 3 \pmod 4$, 2 is a prime if $m \equiv 5 \pmod 8$, and 2 is the product of two distinct primes if $m \equiv 1 \pmod 8$.
5. Any rational prime $p$ that divides $m$ is the associate of the square of a prime in $\mathbb{Q}(\sqrt{m})$.

Explanation and Example

**Remark.**

> This theorem is important for understanding how rational primes behave in the extended field $\mathbb{Q}(\sqrt{m})$. Some rational primes remain prime, while others may split into a product of two primes in this new number system.

**Proof of Theorem 23 - Statement 1**

Suppose the rational prime $p$ is not a prime in $\mathbb{Q}(\sqrt{m})$. Then we can write

$$p = \pi\beta,$$

where $\pi$ is a prime in $\mathbb{Q}(\sqrt{m})$ and $\beta$ is some element of $\mathbb{Q}(\sqrt{m})$.

Taking the norm of both sides, we have

$$N(\pi)N(\beta) = N(p) = p^2.$$

Since $p$ is a rational prime, $N(p) = p^2$.

The norm $N(\pi)$ cannot be $\pm 1$ because:

1. If $N(\pi) = \pm 1$, then $\pi$ would be a *unit* in $\mathbb{Q}(\sqrt{m})$, meaning $\pi$ would not contribute meaningfully to the prime factorization.
2. A true prime element in $\mathbb{Q}(\sqrt{m})$ must be *irreducible* and not a unit. Thus, for $\pi$

to be a prime in $\mathbb{Q}(\sqrt{m})$, we require $N(\pi) \neq \pm 1$.

With this condition, we now analyze the two possible cases for $N(\beta)$.
From the norm equation $N(\pi)N(\beta) = p^2$, we have two possibilities:

1. **Case 1:** $N(\beta) = \pm 1$**.**
   If $N(\beta) = \pm 1$, then $\beta$ is a *unit* in $\mathbb{Q}(\sqrt{m})$. This implies that $\pi$ is an *associate* of $p$, meaning that $\pi$ and $p$ are essentially the same prime, differing only by a unit (such as $\pm 1$). In this case, $p$ remains a prime in $\mathbb{Q}(\sqrt{m})$.

2. **Case 2:** $N(\beta) = \pm p$**.**
   If $N(\beta) = \pm p$, then $\beta$ itself is a *prime* in $\mathbb{Q}(\sqrt{m})$ by Theorem 9.24. Thus, $p$ can be written as the product of two primes, $\pi$ and $\beta$, in $\mathbb{Q}(\sqrt{m})$.

If $p$ is not a prime in $\mathbb{Q}(\sqrt{m})$, it must factor as $p = \pi\beta$, where $\pi$ and $\beta$ are primes in $\mathbb{Q}(\sqrt{m})$. This completes the proof of statement (1).

**Proof of Theorem 23 - Statement 2**

From Statement (1), we know that every rational prime $p$ is either:

- A prime $\pi$ in $\mathbb{Q}(\sqrt{m})$, or
- A product $\pi_1\pi_2$ of two primes in $\mathbb{Q}(\sqrt{m})$.

Thus, for every rational prime $p$, we can identify primes $\pi$, $\pi_1$, and $\pi_2$ in $\mathbb{Q}(\sqrt{m})$ associated with it. These form the core set of primes in $\mathbb{Q}(\sqrt{m})$.

However, to account for *all* primes in $\mathbb{Q}(\sqrt{m})$, we must also include their **associates**. Recall that two elements in $\mathbb{Q}(\sqrt{m})$ are associates if they differ by multiplication by a unit. For example, if $\pi$ is a prime, then $-\pi$ is also a prime, as it is an associate of $\pi$.

Therefore, the total set of primes in $\mathbb{Q}(\sqrt{m})$ consists of:

- All primes $\pi$, $\pi_1$, and $\pi_2$ identified from Statement (1), and
- Their associates, which are elements of the form $u\pi$, where $u$ is a unit in $\mathbb{Q}(\sqrt{m})$.

This proves that the totality of primes obtained from Statement (1), together with their associates, constitutes the full set of primes in $\mathbb{Q}(\sqrt{m})$.

**Proof of Theorem 23 - Statement 3**

Let $p$ be an odd rational prime such that $(p, m) = 1$ (i.e., $p$ does not divide $m$) and $\left(\frac{m}{p}\right) = 1$ (i.e., $m$ is a quadratic residue modulo $p$).

From theorem 13 , we know the structure of the integers in $\mathbb{Q}(\sqrt{m})$:

1. If $m \equiv 2 \pmod 4$ or $m \equiv 3 \pmod 4$, the integers are of the form:

$$a + b\sqrt{m}, \quad \text{where } a, b \in \mathbb{Z}.$$

2. If $m \equiv 1 \pmod 4$, the integers include both:

$$a + b\sqrt{m}, \quad \text{and} \quad \frac{a + b\sqrt{m}}{2}, \quad \text{where } a, b \text{ are odd integers.}$$

These forms will be crucial for determining whether $p$ divides certain elements in $\mathbb{Q}(\sqrt{m})$. Let $p$ be an odd rational prime such that $(p, m) = 1$ and $\left(\frac{m}{p}\right) = 1$. By definition of the Legendre symbol, the condition $\left(\frac{m}{p}\right) = 1$ means there exists a rational integer $x$ such that $x^2 \equiv m \pmod p$. Then $p \mid (x^2 - m)$, which implies:

$$p \mid (x - \sqrt{m})(x + \sqrt{m}).$$

If $p$ were a prime in $\mathbb{Q}(\sqrt{m})$, it would divide one of the factors, say $x - \sqrt{m}$, so that:

$$\frac{x - \sqrt{m}}{p}, \quad \frac{x + \sqrt{m}}{p}$$

would be integers in $\mathbb{Q}(\sqrt{m})$. By Theorem 13, the integers of $\mathbb{Q}(\sqrt{m})$ are of the form $a + b\sqrt{m}$ if $m \equiv 2 \pmod 4$ or $3 \pmod 4$, and $\frac{a+b\sqrt{m}}{2}$ if $m \equiv 1 \pmod 4$. In either case, $p \mid x$ and $p \mid m$, which contradicts $(p, m) = 1$. Thus, $p$ is not a prime in $\mathbb{Q}(\sqrt{m})$.

By Statement (1) of Theorem 13, $p$ must split as $p = \pi_1\pi_2$, where $\pi_1$ and $\pi_2$ are primes in $\mathbb{Q}(\sqrt{m})$.

Now suppose that $p$ is an odd rational prime, that $(p, m) = 1$, and that $p$ is not a prime in $\mathbb{Q}(\sqrt{m})$. From the proof of Statement (1), we see that $p = \pi\beta$, $N(\beta) = \pm p$, and $N(\pi) = \pm p$. Let $\pi = a + b\sqrt{m}$, where $a$ and $b$ are rational integers or, if $m \equiv 1 \pmod 4$, halves of odd rational integers. Then:

$$a^2 - mb^2 = N(\pi) = \pm p,$$

and we have:

$$(2a)^2 - m(2b)^2 = m(2b)^2 \equiv 4p \pmod p.$$

Here $2a$ and $2b$ are rational integers, and neither is a multiple of $p$. For if $p$ divided either one, it would divide the other, and we would have $p^2 \mid (4a^2, 4b^2, 4mb^2, 4p)$, a contradiction. Therefore $(2b, p) = 1$, and there is a rational integer $w$ such that $2bw \equiv 1 \pmod p$. Multiplying both sides of the norm equation by $w^2$, we find:

$$(2aw)^2 = m(2bw)^2 \equiv m \pmod p.$$

Thus $\left(\frac{m}{p}\right) = 1$, which confirms that $p = \pi_1\pi_2$.

Next, consider the ratios of the factors $\pi$ and $\beta$:

$$\beta = \frac{p}{\pi} = \pm\frac{p}{a + b\sqrt{m}} = \pm(a - b\sqrt{m}),$$

and its conjugate:

$$\overline{\beta} = \pm(a + b\sqrt{m}).$$

From this, $\pi$ and $\overline{\beta}$ are associates, as their ratio is $\pm 1$. On the other hand, the ratio

$\pi/\beta$ is given by:

$$\frac{\pi}{\beta} = \frac{a + b\sqrt{m}}{a - b\sqrt{m}} = \frac{(2a)^2 + m(2b)^2}{4p} + \frac{8ab\sqrt{m}}{4p}.$$

This ratio is not an integer, as $p$ does not divide $8ab$, so $\pi$ and $\beta$ are not associates.

Thus, $p$ splits into distinct primes $\pi_1$ and $\pi_2$, which are not associates, completing the proof.

**Proof of Theorem 23 - Statement 4**

If $m \equiv 3 \pmod 4$, then:

$$m^2 - m = 2 \cdot \frac{m^2 - m}{2} = 2(m + \sqrt{m})(m - \sqrt{m}).$$

Thus, $2 \mid (m \pm \sqrt{m})$, so 2 cannot be a prime of $\mathbb{Q}(\sqrt{m})$. Hence, 2 is divisible by a prime $x + y\sqrt{m}$, which must have norm $\pm 2$. Therefore:

$$x^2 - my^2 = \pm 2.$$

This implies:

$$\frac{x - y\sqrt{m}}{x + y\sqrt{m}} = \frac{x^2 + my^2 - 2xy\sqrt{m}}{x^2 - my^2} = \frac{x^2 + my^2}{2} - xy\sqrt{m},$$

and similarly:

$$\frac{x + y\sqrt{m}}{x - y\sqrt{m}} = \frac{x^2 + my^2}{2} + xy\sqrt{m}.$$

Thus, $x - y\sqrt{m}$ and $x + y\sqrt{m}$ are associates, and 2 is the associate of the square of a prime when $m \equiv 3 \pmod 4$.

If $m \equiv 1 \pmod 4$, and 2 is not a prime in $\mathbb{Q}(\sqrt{m})$, then 2 is divisible by:

$$\frac{1}{2}(x + y\sqrt{m}),$$

with norm $\pm 2$. This requires $x$ and $y$ such that:

$$x^2 - my^2 = \pm 8.$$

If $x$ and $y$ are even, say $x = 2x_0$, $y = 2y_0$, then:

$$x_0^2 - my_0^2 = \pm 2.$$

Since $m \equiv 1 \pmod 4$, $x_0^2 - my_0^2$ cannot equal $\pm 2$, as $m \equiv 1 \pmod 8$ implies divisibility conditions that lead to contradictions. Therefore, $x$ and $y$ must both be odd, and:

$$x^2 - y^2 \equiv 1 \pmod 8.$$

This implies $x^2 - my^2 \equiv 0 \pmod 8$, so $m \equiv 1 \pmod 8$. Hence, 2 is divisible by primes

$\frac{1}{2}(x + y\sqrt{m})$ and $\frac{1}{2}(x - y\sqrt{m})$, which are distinct since their ratio is not a unit:

$$\frac{x + y\sqrt{m}}{x - y\sqrt{m}} = \frac{x^2 + my^2}{8} + \frac{xy\sqrt{m}}{4}.$$

The ratio is not an integer, so 2 is the product of two distinct primes when $m \equiv 1 \pmod 8$.

If $m \equiv 5 \pmod 8$, suppose 2 is not a prime. Then 2 must divide:

$$\frac{1}{2}(x + y\sqrt{m}),$$

with norm $\pm 2$. This requires $x$ and $y$ to satisfy:

$$x^2 - my^2 = \pm 8.$$

If $x, y$ are even, $x_0^2 - my_0^2 = \pm 2$, which is impossible since $m \equiv 5 \pmod 8$ leads to no solutions. Hence, 2 must remain a prime in $\mathbb{Q}(\sqrt{m})$ when $m \equiv 5 \pmod 8$.

This completes the proof.

**Proof of Theorem 23 - Statement 5**

Let $p$ be a rational prime divisor of $m$.

1. Case 1: $p = |m|$: If $p = |m|$, then:

$$m = p \cdot \sqrt{m} \cdot \sqrt{m}.$$

Thus, $p = \pm\sqrt{m} \cdot \sqrt{m}$, and $p$ is the associate of the square of a prime in $\mathbb{Q}(\sqrt{m})$ by Theorem (If the norm of an integer $a$ in $\mathbb{Q}(\sqrt{m})$ is $\pm p$, where $p$ is a rational prime, then $a$ is a prime in $\mathbb{Q}(\sqrt{m})$.).

2. Case 2: $p < |m|$: In this case, write:

$$\frac{m}{p} = \sqrt{m} \cdot \sqrt{m} \quad \text{(Equation 9.13)}.$$

By Theorem 13, $p$ is not a divisor of $\sqrt{m}$ in $\mathbb{Q}(\sqrt{m})$, and hence $p$ is not a prime in $\mathbb{Q}(\sqrt{m})$. Therefore, $p$ is divisible by a prime $\pi$ in $\mathbb{Q}(\sqrt{m})$, where:

$$N(\pi) = \pm p.$$

Since $N(\pi) = \pm p$, $\pi$ is not a divisor of $m/p$. However, by Equation (9.13), $\pi$ is a divisor of $\sqrt{m}$. Hence, $\pi^2$ divides $m$, as claimed.

The theorem we have just proved provides a method for determining the primes in quadratic fields $\mathbb{Q}(\sqrt{m})$ having the unique factorization property. For such fields $\mathbb{Q}(\sqrt{m})$, we proceed as follows:

Primes in $\mathbb{Q}(\sqrt{m})$

1. Case 1: $(p, 2m) = 1$ and $\left(\frac{m}{p}\right) = -1$: In this case, the rational prime $p$, together with all its associates in $\mathbb{Q}(\sqrt{m})$, are primes in $\mathbb{Q}(\sqrt{m})$.

2. Case 2: $(p, 2m) = 1$ and $\left(\frac{m}{p}\right) = 1$: Here, the prime $p$ factors into two primes $\pi_1$ and $\pi_2$ in $\mathbb{Q}(\sqrt{m})$, with:

$$N(\pi_1) = N(\pi_2) = p.$$

Any other factoring of $p$ will merely replace $\pi_1$ and $\pi_2$ by their associates.

3. Case 3: $(p, 2m) > 1$: For such primes $p$, they may either be primes in $\mathbb{Q}(\sqrt{m})$ or products of two primes in $\mathbb{Q}(\sqrt{m})$.

Suppose $a$ is an integer in $\mathcal{O}(\mathbb{Q}(\sqrt{m}))$ with norm:

$$N(a) = \pm p,$$

where $p$ is a rational prime. If $p \mid a$, this necessitates that $a$ itself must be a prime in $\mathbb{Q}(\sqrt{m})$.

Case: $m \not\equiv 1 \pmod 4$: We can write:

$$a = x + y\sqrt{m}, \quad N(a) = x^2 - my^2,$$

where $x, y$ are integers, both odd or both even.

Combining these facts, we arrive at the following conclusion:

Let $\mathbb{Q}(\sqrt{m})$ have the unique factorization property, and let $p$ be a rational prime such that $(p, 2m) = 1$. Suppose:

$$x^2 - my^2 = \pm p$$

has a solution $(x, y)$, where $x = a, y = b$. Then:

$$\alpha = a + b\sqrt{m}, \quad \beta = a - b\sqrt{m},$$

and the associates of $\alpha$ and $\beta$ are primes in $\mathbb{Q}(\sqrt{m})$. These are the only primes in $\mathbb{Q}(\sqrt{m})$ that divide $p$.

If $m \equiv 1 \pmod 4$, then at least one of the two equations:

$$x^2 - my^2 = \pm p$$

has a solution. Let $x = a, y = b$ be such a solution. Then the numbers:

$$\alpha = \frac{a + b\sqrt{m}}{2}, \quad \beta = \frac{a - b\sqrt{m}}{2},$$

and their associates are primes in $\mathbb{Q}(\sqrt{m})$. These are the only primes in $\mathbb{Q}(\sqrt{m})$ that divide $p$.

These results provide insight into how rational primes $p$ behave in quadratic fields $\mathbb{Q}(\sqrt{m})$ with the unique factorization property. Additionally, they offer valuable information about the solutions of certain Diophantine equations:

$$x^2 - my^2 = \pm p.$$

It must be remembered that these results apply only to those $\mathbb{Q}(\sqrt{m})$ that have the unique factorization property.

# 13 References

1. Niven, I., Zuckerman, H. S., Montgomery, H. L. (1991). *An Introduction to the Theory of Numbers*. Hardcover edition, September 3, 1991.

2. Filaseta, M. (n.d.). Notes on Algebraic Number Theory: Graduate Course. Retrieved from: https://people.math.sc.edu/filaseta/gradcourses/math785/math785notes8.pdf

3. Soundararajan, K. (n.d.). Notes on Transcendental Number Theory. Retrieved from: https://math.stanford.edu/~ksound/TransNotes.pdf

4. Wikipedia. (n.d.). Proof of Fermat's Last Theorem for Specific Exponents. Retrieved from: https://en.wikipedia.org/wiki/Proof_of_Fermat%27s_Last_Theorem_for_specific_exponents