Algebraic Numbers
MAT397 , Fall 2024

SHIVANK GOEL

September, 2024

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.

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 of Differences

- **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.

Combining the Concepts

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:

$$abf(x) = c_1g_2(x)c_2h_2(x)$$

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.

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.

π, 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: 9.8

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 $g(x)$.

Step 1: Finding the Polynomial of Lowest Degree 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.

Step 2: Proving that $g(x)$ is Irreducible 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.

Step 3: Any Polynomial with g as a Root is Divisible by $g(x)$ 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 $g(x)$.

Step 4: Proving Uniqueness of $g(x)$ 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.

Conclusion 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: 9.9

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

Step 1: Integers Are Algebraic Integers Any regular integer m is an algebraic integer because it satisfies the monic polynomial $x - m = 0$. This is a monic polynomial (the leading coefficient is 1) with integer coefficients, so by definition, every integer is an algebraic integer.

Step 2: Rational Numbers that Are Algebraic Integers Must Be Integers Now, let's suppose we have a rational number $\frac{m}{q}$ (where m and q are integers and $\gcd(m, q) = 1$, meaning they have no common factors other than 1). We want to see if this rational number can be an algebraic integer.

- Since $\frac{m}{q}$ 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:

$$m^n + b_{n-1}m^{n-1}q + \cdots + b_0q^n = 0$$

Now, observe that this equation implies q must divide m^n (the first term on the left-hand side). Since m and q have no common factors (we assumed $\gcd(m, q) = 1$), the only way q can divide m^n is if $q = \pm 1$.

- Therefore, $\frac{m}{q}$ must be an integer because $q = \pm 1$.

Conclusion: This shows that the only rational numbers that are algebraic integers are the integers themselves, $0, \pm 1, \pm 2, \ldots$.

Additional Explanation: - The term rational integer is used in algebraic number theory to distinguish regular integers from other types of algebraic integers that are not rational numbers. For example, $\sqrt{2}$ is an algebraic integer because it satisfies the equation $x^2 - 2 = 0$, but it's not a **rational integer** because it's not a rational number.

Example: - Rational integer: 2, because it satisfies $x - 2 = 0$, and it's also a rational number. - Algebraic integer but not a rational integer: $\sqrt{2}$, because it satisfies $x^2 - 2 = 0$, but it's not a rational number.

Thus, the integers are the only rational numbers that can be algebraic integers.

Theorem 4: 9.10

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

Step 1: The Equation is Monic by Definition By definition, the minimal polynomial of an algebraic integer is **monic**, meaning its leading coefficient is 1. Therefore, there is no need to prove that the polynomial is monic, as it is assumed from the start.

Step 2: Showing that the Coefficients are Integers 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:

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

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 9.8**, the minimal polynomial $g(x)$ divides any polynomial with g as a root. Therefore, $g(x)$ divides $f(x)$, which gives:

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

where $h(x)$ is another polynomial, and both $g(x)$ and $h(x)$ have rational coefficients.

Since $f(x)$ is monic and has integer coefficients, $g(x)$ and $h(x)$ must be monic as well.

By **Gauss Lemma**, if a monic polynomial with rational coefficients divides a polynomial with integer coefficients, then the dividing polynomial must have integer coefficients. Hence, the minimal polynomial $g(x)$ of the algebraic integer g must have integer coefficients.

Theorem 5: 9.11

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: 9.12

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

1 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: 3×3 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.

2 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 α is an algebraic number, its additive inverse $-\alpha$ is also algebraic. For example, if α 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 α^{-1} is also algebraic. For example, if α satisfies a polynomial equation, then α^{-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 α 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.

3 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 π 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 πi:

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

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 πi. 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 πi) 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 α_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 α_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 $\mathbf{s_1}$ 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 α_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 β_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 α_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 β_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 $\mathbf{s_2}$ 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 γ_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**, γ_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 π is algebraic was false. **QED.**