

Galois Theory

Archived study guides

These archived materials are no longer updated. This archive was exported from a saved copy of these guides.

Export date: 2026-10-05T19:26:30.244Z

Contents

- Unit 1 – Field Theory and Polynomial Equations - 4 guides
- Unit 2 – Field Extensions and Algebraic Elements - 4 guides
- Unit 3 – Splitting Fields and Algebraic Closures - 3 guides
- Unit 4 – Separable and Inseparable Extensions - 3 guides
- Unit 5 – Automorphisms and Fixed Fields - 3 guides
- Unit 6 – Introduction to Group Theory - 3 guides
- Unit 7 – Galois Groups and Galois Extensions - 3 guides
- Unit 8 – The Fundamental Theorem of Galois Theory - 3 guides
- Unit 9 – Galois' Criterion for Radical Solvability - 3 guides
- Unit 10 – Finite Fields and Their Applications - 3 guides
- Unit 11 – Constructibility and Impossibility Results - 3 guides
- Unit 12 – Galois Theory: Modern Math Applications - 4 guides

Unit 1 – Field Theory and Polynomial Equations

1.1 Fields and their properties

Fields are the building blocks of modern algebra, providing a framework for understanding numbers and their operations. They extend the concept of number systems, allowing us to work with rational, real, and complex numbers, as well as more abstract structures.

In this section, we'll dive into the definition and properties of fields, explore examples and non-examples, and examine key theorems. Understanding fields is crucial for grasping more advanced concepts in algebra and number theory.

Fields and their Properties

Definition and Essential Axioms

- A field is a set F together with two binary operations, addition (+) and multiplication ($\cdot$), that satisfy the following axioms:
- Closure under addition and multiplication: For all a, b in F , both $a + b$ and $a \cdot b$ are in F
- Associativity of addition and multiplication: For all a, b, c in F , $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Commutativity of addition and multiplication: For all a, b in F , $a + b = b + a$ and $a \cdot b = b \cdot a$
- Existence of additive and multiplicative identity elements: There exist elements 0 and 1 in F such that for all a in F , $a + 0 = a$ and $a \cdot 1 = a$
- Existence of additive inverses: For each a in F , there exists an element $-a$ in F such that $a + (-a) = 0$
- Existence of multiplicative inverses: For each non-zero a in F , there exists an element a^{-1} in F such that $a \cdot a^{-1} = 1$
- Distributivity of multiplication over addition: For all a, b, c in F , $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Properties of Identity and Inverse Elements

- The uniqueness of the additive identity: If 0 and $0'$ are both additive identities, then $0 = 0'$
- The uniqueness of the multiplicative identity: If 1 and $1'$ are both multiplicative identities, then $1 = 1'$
- The uniqueness of additive inverses: For each a in F , if $-a$ and $-a'$ are both additive inverses of a , then $-a = -a'$
- The uniqueness of multiplicative inverses: For each non-zero a in F , if a^{-1} and $(a')^{-1}$ are both multiplicative inverses of a , then $a^{-1} = (a')^{-1}$
- The multiplicative identity is not equal to the additive identity: $1 \neq 0$
- The additive inverse of the additive identity is itself: $-0 = 0$
- The multiplicative inverse of the multiplicative identity is itself: $1^{-1} = 1$

- For all a in F , $a \cdot 0 = 0$

Identifying Fields vs Non-fields

Examples of Fields

- Common examples of fields include:
- The rational numbers ($\mathbb{Q}$) under the usual addition and multiplication operations
- The real numbers ($\mathbb{R}$) under the usual addition and multiplication operations
- The complex numbers ($\mathbb{C}$) under the usual addition and multiplication operations
- Finite fields ($\mathbb{F}_p$) exist for any prime number p , where the elements are the integers modulo p under addition and multiplication modulo p

Examples of Non-fields

- The integers ($\mathbb{Z}$) under the usual addition and multiplication operations do not form a field because not every non-zero integer has a multiplicative inverse within $\mathbb{Z}$
- For example, 2 does not have a multiplicative inverse in $\mathbb{Z}$ because there is no integer a such that $2a = 1$
- The set of 2×2 matrices with real entries under matrix addition and multiplication does not form a field because not every non-zero matrix has a multiplicative inverse
- For example, the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ does not have a multiplicative inverse
- The set of continuous functions on the interval $[0, 1]$ under point-wise addition and multiplication does not form a field because not every non-zero function has a multiplicative inverse
- For example, the function $f(x) = x$ does not have a multiplicative inverse

Arithmetic Operations in Fields

Performing Addition, Subtraction, Multiplication, and Division

- Addition and multiplication in a field must be performed according to the field axioms, ensuring closure, associativity, commutativity, and distributivity
- The additive identity (0) and multiplicative identity (1) elements must be used appropriately in computations
- Additive inverses are used to perform subtraction: $a - b = a + (-b)$
- Multiplicative inverses (reciprocals) are used to perform division: $a \div b = a \cdot b^{-1}$, for non-zero b

Arithmetic in Finite Fields

- In finite fields ($\mathbb{F}_p$), arithmetic operations are performed modulo p
- The multiplicative inverse of an element a is the unique element b such that $ab \equiv 1 \pmod{p}$
- For example, in $\mathbb{F}_5$, the multiplicative inverse of 2 is 3 because $2 \cdot 3 \equiv 1 \pmod{5}$
- Addition and multiplication tables can be constructed for finite fields to facilitate computations

• + 0 1 2 0 0 1 2 1 1 2 0 2 2 0 1

For example, the addition table for F_3 is:

Theorems of Field Properties

Uniqueness of Identity and Inverse Elements

- The uniqueness of the additive identity: If 0 and 0' are both additive identities, then $0 = 0'$
- Proof: Let 0 and 0' be additive identities. Then, $0 = 0 + 0' = 0'$
- The uniqueness of the multiplicative identity: If 1 and 1' are both multiplicative identities, then $1 = 1'$
- Proof: Let 1 and 1' be multiplicative identities. Then, $1 = 1 \cdot 1' = 1'$
- The uniqueness of additive inverses: For each a in F , if $-a$ and $-a'$ are both additive inverses of a , then $-a = -a'$
- Proof: Let $-a$ and $-a'$ be additive inverses of a . Then, $-a = -a + 0 = -a + (a + (-a')) = (-a + a) + (-a') = 0 + (-a') = -a'$
- The uniqueness of multiplicative inverses: For each non-zero a in F , if $a^{(-1)}$ and $(a')^{(-1)}$ are both multiplicative inverses of a , then $a^{(-1)} = (a')^{(-1)}$
- Proof: Let $a^{(-1)}$ and $(a')^{(-1)}$ be multiplicative inverses of a . Then, $a^{(-1)} = a^{(-1)} \cdot 1 = a^{(-1)} \cdot (a \cdot (a')^{(-1)}) = (a^{(-1)} \cdot a) \cdot (a')^{(-1)} = 1 \cdot (a')^{(-1)} = (a')^{(-1)}$

Properties of Zero and One

- The multiplicative identity is not equal to the additive identity: $1 \neq 0$
- Proof: Assume $1 = 0$. Then, for any a in F , $a = a \cdot 1 = a \cdot 0 = 0$, which contradicts the existence of non-zero elements in F
- The additive inverse of the additive identity is itself: $-0 = 0$
- Proof: -0 is the unique element such that $0 + (-0) = 0$. Since $0 + 0 = 0$, we conclude that $-0 = 0$
- The multiplicative inverse of the multiplicative identity is itself: $1^{(-1)} = 1$
- Proof: $1^{(-1)}$ is the unique element such that $1 \cdot 1^{(-1)} = 1$. Since $1 \cdot 1 = 1$, we conclude that $1^{(-1)} = 1$
- For all a in F , $a \cdot 0 = 0$
- Proof: $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Adding the additive inverse of $a \cdot 0$ to both sides yields $0 = a \cdot 0$

1.2 Polynomial rings and irreducible polynomials

Polynomial rings are the backbone of field theory, forming a crucial link between abstract algebra and concrete equations. They provide a structured way to work with polynomials, offering tools to analyze their properties and relationships.

Irreducible polynomials play a starring role in this mathematical drama. Like prime numbers in integer arithmetic, they're the building blocks of polynomial factorization. Understanding them is key to solving complex equations and constructing new fields.

Polynomial rings and properties

Definition and notation

- Polynomial ring denoted as $R[x]$ set of all polynomials with coefficients from a ring R
- Coefficients come from a ring R (integers, real numbers, complex numbers)
- Examples of polynomial rings: $\mathbb{Z}[x]$ (integers), $\mathbb{R}[x]$ (real numbers), $\mathbb{C}[x]$ (complex numbers)

Algebraic properties

- Polynomial rings are commutative rings satisfy commutative property of addition and multiplication
- $f(x) + g(x) = g(x) + f(x)$
- $f(x) \cdot g(x) = g(x) \cdot f(x)$
- Polynomial rings have a unity element constant polynomial 1
- Polynomial rings are integral domains if the coefficient ring R is an integral domain
- No zero divisors: if $f(x) \cdot g(x) = 0$, then either $f(x) = 0$ or $g(x) = 0$
- Example: $\mathbb{Z}[x]$ is an integral domain, but $\mathbb{Z}_6[x]$ (integers modulo 6) is not

Degree and leading coefficient

- Degree of a polynomial highest power of the variable in the polynomial
- Example: $f(x) = 3x^4 + 2x^2 - 5$ has degree 4
- Leading coefficient coefficient of the highest degree term
- Example: In $f(x) = 3x^4 + 2x^2 - 5$, the leading coefficient is 3
- Zero polynomial has degree $-\infty$ by convention
- Constant polynomials have degree 0

Irreducible polynomials

Definition and properties

- Irreducible polynomial cannot be factored into the product of two non-constant polynomials over a given field
- Analogous to prime numbers in the integers
- Example: $x^2 + 1$ is irreducible over $\mathbb{R}$, but reducible over $\mathbb{C}$ as $(x + i)(x - i)$
- Irreducibility depends on the field being considered

Irreducibility over specific fields

- Over the field of real numbers $\mathbb{R}$, a polynomial is irreducible if and only if it is:
- Linear (degree 1)

- Quadratic (degree 2) with a negative discriminant ($b^2 - 4ac < 0$)
- Over the field of complex numbers $\mathbb{C}$, every polynomial of degree greater than 0 is reducible
- Fundamental Theorem of Algebra: every non-constant polynomial has a root in $\mathbb{C}$
- Eisenstein's criterion sufficient condition for a polynomial to be irreducible over the field of rational numbers $\mathbb{Q}$
- If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ with integer coefficients, and there exists a prime p such that:
 - p divides $a_0, a_1, \dots, a_{n-1}$
 - p does not divide a_n
 - p^2 does not divide a_0
- Then $f(x)$ is irreducible over $\mathbb{Q}$
- Example: $f(x) = x^3 + 3x + 6$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with $p = 3$
- The polynomial $x^p - x$ is irreducible over the field of integers modulo p , where p is a prime number
- Used in the construction of finite fields

Polynomial arithmetic

Addition and subtraction

- Polynomial addition performed by adding the coefficients of like terms
- Example: $(3x^2 + 2x - 1) + (2x^2 - 3x + 4) = 5x^2 - x + 3$
- Polynomial subtraction performed by subtracting the coefficients of like terms
- Example: $(3x^2 + 2x - 1) - (2x^2 - 3x + 4) = x^2 + 5x - 5$
- Degree of the sum or difference of two polynomials is at most the maximum of the degrees of the individual polynomials

Multiplication

- Polynomial multiplication performed by multiplying each term of one polynomial by each term of the other polynomial and then adding the like terms
- Example: $(3x + 2)(2x - 1) = 6x^2 + x - 2$
- Degree of the product of two polynomials is the sum of the degrees of the individual polynomials
- $\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x))$
- Leading coefficient of the product of two polynomials is the product of the leading coefficients of the individual polynomials
- $LC(f(x) \cdot g(x)) = LC(f(x)) \cdot LC(g(x))$
- Multiplication of polynomials is commutative, associative, and distributive over addition

Polynomial division and GCD

Division algorithm

- Division algorithm for polynomials: given two polynomials $f(x)$ and $g(x)$ with $g(x) \neq 0$, there exist unique polynomials $q(x)$ (quotient) and $r(x)$ (remainder) such that:
- $f(x) = g(x)q(x) + r(x)$
- $\deg(r(x)) < \deg(g(x))$
- Example: Dividing $f(x) = x^3 + 2x^2 - 3x + 1$ by $g(x) = x^2 + 1$ gives:
- $q(x) = x + 1$ and $r(x) = x + 2$
- $f(x) = (x^2 + 1)(x + 1) + (x + 2)$
- Division algorithm is the basis for the Euclidean algorithm for finding the GCD of two polynomials

Greatest common divisor (GCD)

- GCD of two polynomials polynomial of the highest degree that divides both polynomials without a remainder
- GCD of two polynomials can be found using the Euclidean algorithm involves repeated application of the division algorithm
- Example: GCD of $f(x) = x^3 - 3x + 2$ and $g(x) = x^2 - 1$ is $x - 1$
- If the GCD of two polynomials is 1, the polynomials are called relatively prime or coprime
- Bézout's identity: if the GCD of two polynomials $f(x)$ and $g(x)$ is $d(x)$, then there exist polynomials $a(x)$ and $b(x)$ such that:
- $a(x)f(x) + b(x)g(x) = d(x)$
- Example: For $f(x) = x^3 - 3x + 2$ and $g(x) = x^2 - 1$ with $d(x) = x - 1$, we have:
- $a(x) = -x$ and $b(x) = x^2 - x - 1$
- $(-x)(x^3 - 3x + 2) + (x^2 - x - 1)(x^2 - 1) = x - 1$

1.3 Roots and factorization of polynomials

Roots and factorization are key to understanding polynomials over fields. They help us break down complex equations into simpler parts, revealing their structure and solutions. This knowledge is crucial for solving polynomial equations and exploring field extensions.

Unique factorization of polynomials mirrors prime factorization of integers. It allows us to express polynomials as products of irreducible factors, providing insights into their properties and roots. This concept forms the foundation for more advanced topics in field theory.

Polynomial Roots over Fields

Finding Roots and Their Multiplicities

- A root or zero of a polynomial $p(x)$ is a value r such that $p(r) = 0$

- The fundamental theorem of algebra states that every non-constant polynomial with complex coefficients has at least one complex root
- For example, the polynomial $x^2 + 1$ has no real roots, but it has the complex roots i and $-i$
- Over the real numbers, a polynomial of odd degree always has at least one real root, while a polynomial of even degree may have no real roots
- The polynomial $x^3 - 1$ has the real root 1 and the complex roots $-\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$
- The multiplicity of a root is the number of times it appears as a factor in the polynomial
- A root with multiplicity 1 is called a simple root
- For instance, in the polynomial $(x - 1)^2(x + 1)$, the root 1 has multiplicity 2, and the root -1 has multiplicity 1

Properties and Techniques for Finding Roots

- The sum of the multiplicities of all roots of a polynomial is equal to the degree of the polynomial
- A polynomial of degree n has exactly n roots, counting multiplicities
- Descartes' rule of signs can be used to determine the possible number of positive and negative real roots of a polynomial
- The number of positive real roots is either equal to the number of sign changes between consecutive nonzero coefficients or is less than it by an even number
- The number of negative real roots is the number of sign changes of $f(-x)$ or is less than it by an even number

Factoring Polynomials over Fields

Factoring over Different Fields

- Factoring a polynomial involves expressing it as a product of irreducible polynomials, which cannot be factored further
- Over the real numbers, a polynomial can be factored into a product of linear factors (corresponding to real roots) and irreducible quadratic factors (corresponding to complex conjugate pairs of roots)
- The polynomial $x^3 - 1$ can be factored as $(x - 1)(x^2 + x + 1)$ over the real numbers
- Over the complex numbers, the fundamental theorem of algebra guarantees that every polynomial can be factored into a product of linear factors
- The polynomial $x^3 - 1$ can be factored as $(x - 1)(x - \omega)(x - \omega^2)$ over the complex numbers, where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ is a cube root of unity
- Over finite fields, polynomials can be factored using techniques such as the Berlekamp algorithm or Cantor-Zassenhaus algorithm

Irreducibility Criteria

- Eisenstein's criterion can be used to determine the irreducibility of a polynomial with integer coefficients over the rational numbers

- If a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ with integer coefficients satisfies:
- p divides each a_i for $i = 0, 1, \dots, n-1$,
- p does not divide a_n , and
- p^2 does not divide a_0 ,
- then $f(x)$ is irreducible over the rational numbers
- For example, the polynomial $x^3 + 3x + 3$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with $p = 3$

Euclidean Algorithm for Polynomials

The Euclidean Algorithm and Its Applications

- The Euclidean algorithm is an efficient method for finding the greatest common divisor (GCD) of two polynomials
- The algorithm involves repeatedly dividing the polynomials and replacing the divisor with the remainder until the remainder is zero
- The last non-zero remainder is the GCD
- The extended Euclidean algorithm can be used to find the coefficients of a linear combination of the polynomials that equals their GCD (Bézout's identity)
- For polynomials $f(x)$ and $g(x)$, the extended Euclidean algorithm finds polynomials $s(x)$ and $t(x)$ such that $s(x)f(x) + t(x)g(x) = \gcd(f(x), g(x))$

Properties of the GCD

- The GCD of two polynomials is unique up to multiplication by a non-zero constant
- If the GCD of two polynomials is 1, the polynomials are said to be relatively prime or coprime
- For example, the polynomials $x^2 + 1$ and $x^3 - 1$ are coprime, as their GCD is 1

Unique Factorization of Polynomials

The Unique Factorization Theorem

- The unique factorization theorem states that every non-zero polynomial over a field can be written as a product of irreducible polynomials in a unique way, up to the order of the factors and multiplication by non-zero constants
- Irreducible polynomials over a field are the analogues of prime numbers in the ring of integers
- An irreducible polynomial cannot be factored into a product of two polynomials of lower degree over the same field
- For example, over the real numbers, the polynomial $x^2 + 1$ is irreducible, while over the complex numbers, it factors as $(x + i)(x - i)$

Applications and Implications

- The unique factorization theorem allows for the development of a theory of divisibility for polynomials over fields, similar to the theory of divisibility for integers

- For polynomials $f(x)$ and $g(x)$, we say $f(x)$ divides $g(x)$ if there exists a polynomial $q(x)$ such that $g(x) = q(x)f(x)$
- The theorem is essential for understanding the structure of polynomial rings and their ideals, which play a crucial role in algebraic geometry and number theory
- Polynomial rings over fields have many properties similar to the ring of integers, such as the existence of a division algorithm and the ability to perform polynomial long division

1.4 The Fundamental Theorem of Algebra

The Fundamental Theorem of Algebra is a cornerstone of complex analysis and polynomial theory. It states that every non-constant polynomial with complex coefficients has at least one complex root, linking algebra and complex numbers in a profound way.

This theorem is crucial for understanding polynomial behavior and solving equations. It guarantees that a degree- n polynomial has exactly n complex roots, counting multiplicities, which is essential for factoring and finding solutions in various mathematical and practical applications.

The Fundamental Theorem of Algebra

Statement and Equivalence

- The Fundamental Theorem of Algebra states that every non-constant single-variable polynomial with complex coefficients has at least one complex root
- Equivalently, the theorem asserts that the field of complex numbers is algebraically closed, meaning that every polynomial equation has a solution in the complex number system
- For example, the polynomial $x^2 + 1 = 0$ has no real roots, but it has two complex roots: i and $-i$
- Similarly, the polynomial $x^4 + 2x^2 + 1 = 0$ can be factored as $(x^2 + 1)^2 = 0$, revealing the complex roots i and $-i$, each with multiplicity 2

Roots and Multiplicities

- The theorem guarantees that a polynomial of degree n will have exactly n complex roots, counted with their multiplicities
- For instance, a cubic polynomial ($n = 3$) will have three complex roots, which may include real roots and repeated roots
- The polynomial $x^3 - 6x^2 + 11x - 6 = (x - 1)(x - 2)(x - 3)$ has three real roots: 1, 2, and 3
- Multiplicity refers to the number of times a root appears in the factorization of the polynomial
- A root with multiplicity m will appear m times in the linear factorization
- For example, the polynomial $x^4 - 5x^3 + 8x^2 - 4x = x(x - 1)(x - 2)^2$ has roots 0, 1, and 2, with 2 having multiplicity 2

Significance in Mathematics

- The Fundamental Theorem of Algebra establishes a deep connection between algebra and complex analysis, showing that the study of polynomial equations is intrinsically linked to the properties of complex numbers

- This connection allows for the application of powerful tools from complex analysis to solve problems in algebra and vice versa
- For example, the theorem implies that every polynomial can be factored into linear terms over the complex numbers, a property that is not true for real numbers alone

Applying the Fundamental Theorem of Algebra

Finding Roots of Polynomials

- To find the roots of a polynomial, factor the polynomial into linear factors of the form $(x - r)$, where r represents a root of the polynomial
- For example, to find the roots of $x^3 - 6x^2 + 11x - 6$, factor it as $(x - 1)(x - 2)(x - 3)$, revealing the roots 1, 2, and 3
- Use techniques such as polynomial long division, synthetic division, or factoring by grouping to identify the linear factors and their corresponding roots
- Polynomial long division can be used to divide a polynomial by a linear factor, resulting in a lower-degree polynomial and a remainder
- Synthetic division is a shortcut method for dividing a polynomial by a linear factor of the form $(x - r)$

Complex Roots and Conjugate Pairs

- When a polynomial has real coefficients, complex roots always occur in conjugate pairs ($a + bi$ and $a - bi$)
- For example, the polynomial $x^4 + 1$ has complex roots $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, $-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$, and $\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$
- The sum of the multiplicities of all roots of a polynomial equals the degree of the polynomial
- In the previous example, each root has a multiplicity of 1, and the sum of the multiplicities (4) equals the degree of the polynomial (4)

Proof of the Fundamental Theorem of Algebra

Liouville's Theorem and Entire Functions

- One common proof of the Fundamental Theorem of Algebra relies on Liouville's theorem from complex analysis, which states that every bounded entire function is constant
- An entire function is a function that is holomorphic (complex differentiable) on the whole complex plane
- A bounded function is a function whose absolute value is always less than some fixed real number
- Assume that a polynomial $P(z)$ of degree n has no complex roots. Then, $1/P(z)$ is a bounded entire function, which contradicts Liouville's theorem. Therefore, $P(z)$ must have at least one complex root

Other Proof Techniques

- Another proof uses the Maximum Modulus Principle, which states that if a function is holomorphic in a region and continuous on its boundary, then the maximum absolute value of the function occurs on the boundary
- This principle can be used to show that a polynomial must have a root within any closed disk in the complex plane
- Other proofs of the Fundamental Theorem of Algebra employ techniques such as:
 - The Argument Principle, which relates the number of zeros and poles of a meromorphic function to a contour integral of its logarithmic derivative
 - Rouché's theorem, which compares the number of zeros of two functions based on their behavior on a closed contour
 - The Gauss–Lucas theorem, which states that the roots of the derivative of a polynomial lie within the convex hull of the roots of the original polynomial

Significance of the Fundamental Theorem of Algebra

Historical Development

- The Fundamental Theorem of Algebra was first conjectured by Peter Rothe in 1608, but the first complete proof was given by Carl Friedrich Gauss in 1799
- Gauss's proof was not entirely rigorous by modern standards, and several mathematicians, including Argand, Cauchy, and d'Alembert, worked to develop more rigorous proofs in the 19th century

Implications in Mathematics

- The Fundamental Theorem of Algebra has significant implications in various fields of mathematics:
- In algebra, it guarantees the existence of splitting fields for polynomials and establishes the algebraic closure of the complex numbers
- In complex analysis, it underlies the study of holomorphic functions and their behavior
- In number theory, it is connected to the study of algebraic integers and the properties of number fields

Applications

- The theorem also has practical applications in areas such as:
 - Control theory, where the roots of characteristic polynomials determine the stability of systems
 - Signal processing, where the roots of polynomials are used in filter design and frequency analysis
 - Quantum mechanics, where the roots of polynomials appear in the study of energy levels and wave functions

Unit 2 – Field Extensions and Algebraic Elements

2.1 Field extensions and their properties

Field extensions are like building blocks in algebra, letting us create bigger fields from smaller ones. They're crucial for understanding how numbers and polynomials behave in different mathematical worlds.

This topic dives into the types of extensions, how to build them, and their properties. We'll explore algebraic and transcendental extensions, learn to construct new fields, and see how the degree of an extension shapes its structure.

Field extensions and properties

Definition and key characteristics

- A field extension is a field that contains a given base field as a subfield
- If E is an extension field of F , then $F \subseteq E$
- The base field F and the extension field E have the same characteristic
- The characteristic is the smallest positive integer p such that $p \cdot 1 = 0$, or 0 if no such integer exists
- If $\alpha \in E$ is the root of some polynomial $f(x) \in F[x]$, then $F(\alpha)$ is the smallest subfield of E containing both F and α

Types of field extensions

- Algebraic extensions
 - If every element of E is the root of some polynomial with coefficients in F , then E is an algebraic extension of F
 - Example: The field of complex numbers ($\mathbb{C}$) is an algebraic extension of the field of real numbers ($\mathbb{R}$) because every complex number is a root of a polynomial with real coefficients
- Transcendental extensions
 - If E is not an algebraic extension of F , then E is a transcendental extension of F
 - Example: The field of rational functions $\mathbb{Q}(x)$ is a transcendental extension of $\mathbb{Q}$ because x is not the root of any polynomial with rational coefficients

Constructing field extensions

Using polynomials

- Given a field F and a polynomial $f(x) \in F[x]$, the quotient ring $F[x]/(f(x))$ is a field extension of F if and only if $f(x)$ is irreducible over F
- Example: $\mathbb{R}[x]/(x^2 + 1)$ is isomorphic to the field of complex numbers $\mathbb{C}$, which is an extension of $\mathbb{R}$

- The field extension $F(\alpha)$ can be constructed by adjoining a root α of an irreducible polynomial $f(x) \in F[x]$ to the base field F
- Example: $\mathbb{Q}(\sqrt{2})$ is constructed by adjoining $\sqrt{2}$, a root of the irreducible polynomial $x^2 - 2$, to $\mathbb{Q}$

Using rational expressions

- If E is an extension field of F and $\alpha \in E$, then $F(\alpha)$ consists of all rational expressions in α with coefficients in F
- Example: The field $\mathbb{Q}(\pi)$ consists of all rational expressions in π with rational coefficients, such as $\frac{3\pi^2 + 1}{2\pi - 7}$

Degree of field extensions

Definition and properties

- The degree of a field extension E over F , denoted $[E:F]$, is the dimension of E as a vector space over F
- If E is a finite extension of F , then $[E:F]$ is finite
- If $[E:F] = n$, then every element of E can be uniquely expressed as a linear combination of n basis elements with coefficients in F
- The degree formula: If $F \subseteq K \subseteq E$ are fields, then $[E:F] = [E:K] \cdot [K:F]$

Quadratic extensions

- If $[E:F] = 2$, then $E = F(\sqrt{d})$ for some $d \in F$ that is not a perfect square in F
- Example: $\mathbb{Q}(\sqrt{2})$ is a quadratic extension of $\mathbb{Q}$ with degree 2

Base field vs extension field

Automorphisms and Galois groups

- If E is an extension field of F , then every F -linear map from E to E is either the zero map or an automorphism of E that fixes every element of F
- The set of all F -automorphisms of E forms a group under composition, called the Galois group of E over F , denoted $\text{Gal}(E/F)$
- Example: The Galois group of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is $\{1, \sigma\}$, where σ is the automorphism that maps $\sqrt{2}$ to $-\sqrt{2}$

Galois extensions and the Fundamental Theorem

- If E is a finite extension of F , then $|\text{Gal}(E/F)| \leq [E:F]$
- If equality holds, then E is called a Galois extension of F
- The Fundamental Theorem of Galois Theory establishes a correspondence between the subgroups of $\text{Gal}(E/F)$ and the intermediate fields between F and E , for a Galois extension E of F
- Example: For the Galois extension $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$, the Fundamental Theorem provides a one-to-one correspondence between the subgroups of the Galois group and the intermediate fields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$

, and $\mathbb{Q}(\sqrt{2}, i)$

2.2 Algebraic and transcendental elements

Algebraic and transcendental elements are key concepts in field extensions. Algebraic elements are roots of polynomials over the base field, while transcendental elements aren't. Understanding these helps classify field extensions and their properties.

Proving element types involves finding polynomials for algebraic elements or showing none exist for transcendental ones. This knowledge is crucial for constructing and analyzing different types of field extensions, which form the foundation of Galois theory.

Algebraic vs Transcendental Elements

Definition and Characteristics

- An element α in a field extension L/K is algebraic over K when it is a root of some nonzero polynomial $f(x)$ with coefficients in K
- An element α in a field extension L/K is transcendental over K when it is not algebraic over K , meaning there is no nonzero polynomial $f(x)$ with coefficients in K such that $f(\alpha) = 0$
- Every element in a field extension L/K is either algebraic or transcendental over K , but not both

Subfields and Extension Types

- The set of all elements in L that are algebraic over K forms a subfield of L called the algebraic closure of K in L
- If every element in a field extension L/K is algebraic over K , the extension is called an algebraic extension ($\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, where $\sqrt{2}$ is a root of $x^2 - 2$)
- If not every element in a field extension L/K is algebraic over K , the extension is called a transcendental extension ($\mathbb{Q}(\pi)$ over $\mathbb{Q}$, where π is not a root of any nonzero polynomial with rational coefficients)

Proving Element Type

Proving Algebraic Elements

- To prove that an element α in a field extension L/K is algebraic over K , find a nonzero polynomial $f(x)$ with coefficients in K such that $f(\alpha) = 0$
- The polynomial $f(x)$ is called the minimal polynomial of α over K when it is monic, has the smallest degree among all polynomials with α as a root, and has coefficients in K
- The degree of the minimal polynomial of an algebraic element α over K is called the degree of α over K , denoted $[K(\alpha):K]$

Proving Transcendental Elements

- To prove that an element α in a field extension L/K is transcendental over K , show that there is no nonzero polynomial $f(x)$ with coefficients in K such that $f(\alpha) = 0$
- This can be done by assuming the existence of such a polynomial and deriving a contradiction, or by using the properties of transcendental elements

- If α is transcendental over K , then $[K(\alpha):K]$ is infinite

Constructing Extensions

Constructing Algebraic Extensions

- To construct an algebraic extension, adjoin a root of a polynomial with coefficients in the base field to the base field
- Examples of algebraic extensions include:
 - $\mathbb{Q}(i)$ over $\mathbb{Q}$, where i is a root of the polynomial $x^2 + 1$
 - Finite fields $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, where p is a prime and n is a positive integer

Constructing Transcendental Extensions

- To construct a transcendental extension, adjoin an element that is not a root of any nonzero polynomial with coefficients in the base field to the base field
- Examples of transcendental extensions include:
 - $\mathbb{Q}(e)$ over $\mathbb{Q}$, where e is the base of the natural logarithm and is not a root of any nonzero polynomial with rational coefficients
 - The field of rational functions $K(x)$ over a field K , where x is an indeterminate

Properties of Element Types

Properties of Algebraic Elements

- The set of algebraic elements in a field extension L/K forms a subfield of L
- If α is algebraic over K and β is algebraic over $K(\alpha)$, then β is algebraic over K (transitivity of algebraic extensions)
- If α and β are algebraic over K , then $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and α/β (if $\beta \neq 0$) are also algebraic over K

Properties of Transcendental Elements and Extensions

- The set of transcendental elements in a field extension L/K does not form a subfield of L
- If α is transcendental over K , then $K(\alpha)$ is isomorphic to the field of rational functions $K(x)$
- The algebraic closure of a field K is the smallest algebraically closed field containing K , denoted $\bar{K}$ (unique up to isomorphism and contains all the roots of polynomials with coefficients in K)
- Transcendental extensions are essential in the study of transcendental numbers, such as π and e , which have important applications in mathematics and other fields

2.3 Minimal polynomials and algebraic degree

Minimal polynomials are key to understanding algebraic elements in field extensions. They help determine if an element is algebraic and provide a way to construct field extensions. The degree of a minimal polynomial equals the dimension of the field extension it creates.

Algebraic degree, determined by the minimal polynomial, tells us how "complex" an element is over a field. It's crucial for understanding the structure of field extensions and plays a vital role in solving polynomial equations and studying field automorphisms.

Minimal Polynomials for Algebraic Elements

Definition and Properties

- An element α in an extension field E of a field F is algebraic over F if there exists a non-zero polynomial $f(x)$ in $F[x]$ such that $f(\alpha) = 0$
- The minimal polynomial of an algebraic element α over a field F is the unique monic polynomial $m(x)$ in $F[x]$ of least degree such that $m(\alpha) = 0$
- The minimal polynomial of an algebraic element is irreducible over the base field
- If α is algebraic over F , then $F(\alpha)$ is the smallest subfield of E containing both F and α (example: $\mathbb{Q}(\sqrt{2})$ is the smallest subfield of $\mathbb{R}$ containing both $\mathbb{Q}$ and $\sqrt{2}$)
- If α is transcendental over F , then there is no non-zero polynomial $f(x)$ in $F[x]$ such that $f(\alpha) = 0$ (example: π is transcendental over $\mathbb{Q}$)

Algebraic Elements and Field Extensions

- If α is algebraic over F with minimal polynomial $m(x)$, then $F(\alpha)$ is isomorphic to the quotient ring $F[x]/(m(x))$
- The degree of the field extension $F(\alpha)$ over F is equal to the algebraic degree of α over F
- If α and β are algebraic over F with minimal polynomials $m(x)$ and $n(x)$ respectively, then $\alpha + \beta$ and $\alpha\beta$ are also algebraic over F
- The minimal polynomial of $\alpha + \beta$ divides the polynomial $m(x + y)$ in $F[x, y]$
- The minimal polynomial of $\alpha\beta$ divides the polynomial $m(xy)$ in $F[x, y]$
- If α is algebraic over F and β is algebraic over $F(\alpha)$, then β is algebraic over F
- The minimal polynomial of β over F divides the polynomial obtained by substituting the minimal polynomial of α into the minimal polynomial of β over $F(\alpha)$

Computing Minimal Polynomials

Finding the Minimal Polynomial

- To find the minimal polynomial of an algebraic element α over a field F , first find a non-zero polynomial $f(x)$ in $F[x]$ such that $f(\alpha) = 0$
- Factor $f(x)$ into irreducible factors over F . The minimal polynomial $m(x)$ will be one of these irreducible factors
- Substitute α into each irreducible factor. The factor that evaluates to 0 is the minimal polynomial $m(x)$
- If necessary, divide $m(x)$ by its leading coefficient to obtain a monic polynomial
- Verify that $m(\alpha) = 0$ and that no polynomial of lower degree in $F[x]$ has α as a root

Examples

- Find the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$:
- The polynomial $x^2 - 2$ has $\sqrt{2}$ as a root, so $f(x) = x^2 - 2$
- $f(x)$ is already irreducible over $\mathbb{Q}$, so $m(x) = x^2 - 2$
- $m(x)$ is monic, and no polynomial of lower degree in $\mathbb{Q}[x]$ has $\sqrt{2}$ as a root
- Find the minimal polynomial of $i + \sqrt{2}$ over $\mathbb{Q}$:
- The polynomial $x^4 - 2x^2 + 9$ has $i + \sqrt{2}$ as a root, so $f(x) = x^4 - 2x^2 + 9$
- $f(x)$ factors into $(x^2 - 2x - 3)(x^2 + 2x - 3)$ over $\mathbb{Q}$
- Substituting $i + \sqrt{2}$ into each factor, we find that $m(x) = x^2 - 2x - 3$
- $m(x)$ is monic, and no polynomial of lower degree in $\mathbb{Q}[x]$ has $i + \sqrt{2}$ as a root

Algebraic Degree and Minimal Polynomials

Definition and Properties

- The algebraic degree of an element α over a field F is the degree of its minimal polynomial $m(x)$ over F
- If the minimal polynomial of α over F is linear, then α is in F , and the algebraic degree is 1
- If the minimal polynomial of α over F has degree $n > 1$, then the algebraic degree of α over F is n
- The algebraic degree of α over F is equal to the dimension of $F(\alpha)$ as a vector space over F

Examples

- The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$, so the algebraic degree of $\sqrt{2}$ over $\mathbb{Q}$ is 2
- The dimension of $\mathbb{Q}(\sqrt{2})$ as a vector space over $\mathbb{Q}$ is also 2, with basis $\{1, \sqrt{2}\}$
- The minimal polynomial of $i + \sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2x - 3$, so the algebraic degree of $i + \sqrt{2}$ over $\mathbb{Q}$ is 2
- The dimension of $\mathbb{Q}(i + \sqrt{2})$ as a vector space over $\mathbb{Q}$ is also 2, with basis $\{1, i + \sqrt{2}\}$

Minimal Polynomials vs Field Extensions

Isomorphism and Degree

- If α is algebraic over F with minimal polynomial $m(x)$, then $F(\alpha)$ is isomorphic to the quotient ring $F[x]/(m(x))$
- The degree of the field extension $F(\alpha)$ over F is equal to the algebraic degree of α over F
- This follows from the isomorphism between $F(\alpha)$ and $F[x]/(m(x))$, as the dimension of $F[x]/(m(x))$ as a vector space over F is equal to the degree of $m(x)$

Algebraic Elements and Field Extensions

- If α and β are algebraic over F with minimal polynomials $m(x)$ and $n(x)$ respectively, then $\alpha + \beta$ and $\alpha\beta$ are also algebraic over F
- The minimal polynomial of $\alpha + \beta$ divides the polynomial $m(x + y)$ in $F[x, y]$
- The minimal polynomial of $\alpha\beta$ divides the polynomial $m(xy)$ in $F[x, y]$
- If α is algebraic over F and β is algebraic over $F(\alpha)$, then β is algebraic over F
- The minimal polynomial of β over F divides the polynomial obtained by substituting the minimal polynomial of α into the minimal polynomial of β over $F(\alpha)$
- This result allows us to build larger field extensions by adjoining algebraic elements step by step (example: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be constructed by first adjoining $\sqrt{2}$ to $\mathbb{Q}$, then adjoining $\sqrt{3}$ to $\mathbb{Q}(\sqrt{2})$)

2.4 Simple and multiple extensions

Field extensions are like building blocks for bigger number systems. Simple extensions add just one new element, while multiple extensions toss in several. It's like adding a single spice to your cooking versus creating a whole new flavor profile.

Understanding these extensions helps us grasp how more complex number systems are built. Simple extensions are easier to work with, but multiple extensions give us more flexibility. It's all about finding the right balance between simplicity and power in our mathematical toolkit.

Simple vs Multiple Extensions

Differentiating Between Simple and Multiple Extensions

- A field extension L/K is simple if there exists an element $\alpha \in L$ such that $L = K(\alpha)$, meaning L is generated by adjoining a single element α to K ($\mathbb{Q}(\sqrt{2})/\mathbb{Q}$)
- A field extension L/K is multiple if L cannot be generated by adjoining a single element to K , but instead requires adjoining multiple elements ($\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$)
- The degree of a simple extension $K(\alpha)/K$ equals the degree of the minimal polynomial of α over K , denoted $[K(\alpha) : K] = \deg(\min_K(\alpha))$
- The degree of a multiple extension L/K is the product of the degrees of the simple extensions that compose it
- If $L = K(\alpha_1, \dots, \alpha_n)$, then $[L : K] = [K(\alpha_1) : K] \cdot \dots \cdot [K(\alpha_n) : K(\alpha_1, \dots, \alpha_{n-1})]$

Constructing Examples of Simple and Multiple Extensions

- The field extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a simple extension, as it is generated by adjoining the single element $\sqrt{2}$ to $\mathbb{Q}$
- The field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is a multiple extension, as it requires adjoining both $\sqrt{2}$ and $\sqrt{3}$ to $\mathbb{Q}$ and cannot be generated by a single element
- The field extension $\mathbb{Q}(i)/\mathbb{Q}$, where i is the imaginary unit, is a simple extension with degree 2, as the minimal polynomial of i over $\mathbb{Q}$ is $x^2 + 1$

- The field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$ is a multiple extension with degree 8, as it is composed of three simple extensions, each with degree 2

Constructing Field Extensions

Primitive Element Theorem and Simple Extensions

- The Primitive Element Theorem states that if L/K is a finite separable extension, then L/K is simple, i.e., $L = K(\alpha)$ for some $\alpha \in L$
- This theorem implies that every finite separable extension can be generated by adjoining a single element to the base field
- The element α is called a primitive element of the extension L/K
- The Primitive Element Theorem simplifies the construction and study of finite separable extensions by reducing them to simple extensions

Decomposing Multiple Extensions into Simple Extensions

- If L/K is a finite extension and K is a perfect field (e.g., characteristic 0 or finite field), then L/K can be decomposed into a tower of simple extensions
- This decomposition allows for the study of multiple extensions by breaking them down into a sequence of simpler extensions
- The tower of simple extensions can be represented as $K = K_0 \subset K_1 \subset \dots \subset K_n = L$, where each K_{i+1}/K_i is a simple extension
- The degree of the multiple extension L/K is the product of the degrees of the simple extensions in the tower

Properties of Field Extensions

Structure of Simple and Multiple Extensions

- Simple extensions have a more straightforward structure, as they are generated by a single element and their degree is determined by the minimal polynomial of that element
- The minimal polynomial of the generating element α over K determines the algebraic properties of the simple extension $K(\alpha)/K$
- Multiple extensions have a more complex structure, as they are generated by multiple elements and their degree is the product of the degrees of the constituent simple extensions
- The structure of a multiple extension depends on the relationships between the generating elements and their minimal polynomials over the base field

Algebraic Properties of Extensions

- An element $\alpha \in L$ is algebraic over K if it is a root of some non-zero polynomial with coefficients in K
- A field extension L/K is algebraic if every element of L is algebraic over K
- The minimal polynomial of an algebraic element α over K is the unique monic polynomial of lowest degree with coefficients in K that has α as a root

- If α is algebraic over K , then the simple extension $K(\alpha)/K$ is a finite extension with degree equal to the degree of the minimal polynomial of α over K

Galois Theory and Extensions

Galois Groups and Field Extensions

- Galois theory studies the relationship between field extensions and their corresponding Galois groups, which are groups of automorphisms that fix the base field
- A field extension L/K is Galois if it is both normal (every irreducible polynomial over K that has a root in L splits completely in L) and separable (every element of L is separable over K)
- The Galois group of an extension L/K , denoted $\text{Gal}(L/K)$, is the group of all automorphisms of L that fix K
- The Fundamental Theorem of Galois Theory establishes a one-to-one correspondence between the subgroups of the Galois group and the intermediate fields of a Galois extension

Simple Extensions in Galois Theory

- Simple extensions play a crucial role in Galois theory, as they are the building blocks for constructing and understanding more complex extensions
- The Galois group of a simple extension $K(\alpha)/K$ is isomorphic to a subgroup of the permutation group of the roots of the minimal polynomial of α over K
- The degree of a simple Galois extension $K(\alpha)/K$ equals the order of its Galois group $\text{Gal}(K(\alpha)/K)$
- Simple extensions with Galois groups that are cyclic of prime order are particularly important in Galois theory, as they are the fundamental building blocks for constructing abelian extensions

Multiple Extensions and the Galois Correspondence

- Multiple extensions can be studied using Galois theory by decomposing them into a tower of simple extensions and analyzing the Galois groups of each step in the tower
- The Galois correspondence allows for a deeper understanding of the structure and properties of multiple extensions by relating them to the subgroup structure of their Galois groups
- The Fundamental Theorem of Galois Theory establishes a lattice isomorphism between the lattice of intermediate fields of a Galois extension L/K and the lattice of subgroups of the Galois group $\text{Gal}(L/K)$
- This correspondence enables the study of multiple extensions by examining the relationships between the Galois groups of the simple extensions in the tower and their corresponding intermediate fields

Unit 3 – Splitting Fields and Algebraic Closures

3.1 Splitting fields and their construction

Splitting fields are crucial in understanding polynomial roots and field extensions. They're the smallest fields containing all roots of a given polynomial, unique up to isomorphism. This concept bridges basic field theory with more advanced Galois theory.

Constructing splitting fields involves adjoining roots to the base field step-by-step. The process reveals important properties like field degree and Galois group structure, connecting polynomial behavior to abstract algebra and number theory.

Splitting Fields for Polynomials

Definition and Properties

- A splitting field of a polynomial $f(x)$ over a field F is the smallest field extension of F that contains all the roots of $f(x)$
- The splitting field is obtained by adjoining all the roots of $f(x)$ to the base field F (adjoining means adding elements to the field to create a larger field)
- The splitting field is unique up to isomorphism, meaning that any two splitting fields of a polynomial over the same base field are isomorphic (have the same structure and properties)
- The degree of the splitting field over the base field is equal to the order of the Galois group of the polynomial (the Galois group is the group of field automorphisms that fix the base field)

Examples

- The splitting field of $x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$, obtained by adjoining $\sqrt{2}$ to $\mathbb{Q}$
- The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a primitive cubic root of unity

Constructing Splitting Fields

Step-by-Step Process

- To construct a splitting field, first factor the polynomial completely over the base field
- If all the roots are already in the base field, then the base field itself is the splitting field
- If some roots are not in the base field, adjoin one root at a time to the base field until all roots are included. The resulting field is the splitting field
- The process of adjoining a root α to a field F is denoted by $F(\alpha)$ and is the smallest field containing both F and α
- When adjoining multiple roots, the order in which they are adjoined does not matter; the resulting splitting field will be the same up to isomorphism

Examples

- To construct the splitting field of $x^4 - 1$ over $\mathbb{Q}$:
- Factor: $x^4 - 1 = (x - 1)(x + 1)(x - i)(x + i)$
- Adjoin i to $\mathbb{Q}$: $\mathbb{Q}(i)$
- All roots are in $\mathbb{Q}(i)$, so this is the splitting field
- To construct the splitting field of $x^3 - 2$ over $\mathbb{Q}$:
- Adjoin $\sqrt[3]{2}$ to $\mathbb{Q}$: $\mathbb{Q}(\sqrt[3]{2})$
- Adjoin ω (a primitive cubic root of unity) to $\mathbb{Q}(\sqrt[3]{2})$: $\mathbb{Q}(\sqrt[3]{2}, \omega)$
- All roots are in $\mathbb{Q}(\sqrt[3]{2}, \omega)$, so this is the splitting field

Uniqueness of Splitting Fields

Proving Uniqueness up to Isomorphism

- Let E and E' be two splitting fields of a polynomial $f(x)$ over a field F . To prove uniqueness, we need to show that E and E' are isomorphic
- Define a homomorphism $\phi : F[x]/(f(x)) \rightarrow E$ by sending x to a root α of $f(x)$ in E . This homomorphism is surjective because E is generated by α over F
- Similarly, define another homomorphism $\phi' : F[x]/(f(x)) \rightarrow E'$ by sending x to a root α' of $f(x)$ in E' . This homomorphism is also surjective
- By the first isomorphism theorem, $F[x]/(f(x)) \cong E$ and $F[x]/(f(x)) \cong E'$. Therefore, $E \cong E'$, proving the uniqueness of splitting fields up to isomorphism

Examples

- The splitting field of $x^2 - 2$ over $\mathbb{Q}$ is unique up to isomorphism, whether constructed as $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(-\sqrt{2})$
- The splitting field of $x^4 - 2$ over $\mathbb{Q}$ is unique up to isomorphism, whether constructed as $\mathbb{Q}(\sqrt[4]{2}, i)$ or $\mathbb{Q}(\sqrt[4]{2}, -i)$

Degree of Splitting Fields

Determining the Degree

- The degree of a splitting field E over its base field F is equal to the order of the Galois group G of the polynomial $f(x)$ over F , denoted as $[E : F] = |G|$
- The Galois group G is the group of all automorphisms of E that fix F elementwise
- To find the degree of the splitting field, determine the order of the Galois group by examining the permutations of the roots of $f(x)$ that preserve the field operations
- If the polynomial $f(x)$ factors into linear factors over F , then the degree of the splitting field is equal to the degree of the polynomial

- If $f(x)$ is irreducible over F and has degree n , then the degree of the splitting field is a divisor of $n!$

Examples

- The splitting field of $x^2 - 2$ over $\mathbb{Q}$ has degree 2 over $\mathbb{Q}$ because the Galois group has order 2 (the identity and the automorphism that swaps $\sqrt{2}$ and $-\sqrt{2}$)
- The splitting field of $x^4 - 2$ over $\mathbb{Q}$ has degree 8 over $\mathbb{Q}$ because the Galois group has order 8 (the dihedral group D_4)

3.2 Algebraic closures and their properties

Algebraic closures are the ultimate playground for polynomials. They're fields where every polynomial finds a home for its roots. This concept is crucial for understanding how polynomials behave and how different fields relate to each other.

In this part of our journey, we'll explore what makes algebraic closures special. We'll see how they're built, why they're unique, and how they connect to other key ideas in field theory.

Algebraic Closures of Fields

Definition and Key Properties

- An algebraic closure of a field F is a field K containing F such that every non-constant polynomial in $F[x]$ has a root in K
- The algebraic closure of F is an algebraic extension of F , meaning that every element of K is algebraic over F (a root of some non-zero polynomial with coefficients in F)
- The algebraic closure of a field is the smallest algebraically closed field containing it
- The algebraic closure of a field F is an algebraic extension of F , and every algebraic extension of F can be embedded into the algebraic closure

Examples of Algebraically Closed Fields

- The complex numbers $\mathbb{C}$ are the algebraic closure of the real numbers $\mathbb{R}$
- Every polynomial with real coefficients has a root in $\mathbb{C}$
- The algebraic closure of a finite field $\mathbb{F}_q$ is an infinite field containing all the roots of polynomials over $\mathbb{F}_q$
- For example, the algebraic closure of $\mathbb{F}_2$ contains elements like $\sqrt{2}$ and $\sqrt[3]{2}$, which are not in $\mathbb{F}_2$

Existence and Uniqueness of Algebraic Closures

Existence of Algebraic Closures

- Every field F has an algebraic closure, which can be constructed as the union of all algebraic extensions of F
- The proof of existence involves Zorn's Lemma, a powerful tool in set theory and abstract algebra
- Zorn's Lemma states that if every chain in a partially ordered set has an upper bound, then the set contains at least one maximal element

- This is used to show that the union of all algebraic extensions of a field F is an algebraic closure of F

Uniqueness of Algebraic Closures

- The algebraic closure of a field is unique up to isomorphism, meaning that any two algebraic closures of a field F are isomorphic as fields over F
- The uniqueness of algebraic closures can be proved using the properties of splitting fields and the fact that any two splitting fields of a polynomial over a field are isomorphic
- If K_1 and K_2 are two algebraic closures of F , then for any polynomial $f(x) \in F[x]$, its splitting fields in K_1 and K_2 are isomorphic over F
- This isomorphism can be extended to an isomorphism between K_1 and K_2 over F

Properties of Algebraic Closures

Algebraic and Normal Extension Properties

- The algebraic closure of a field is algebraically closed, meaning that every non-constant polynomial with coefficients in the algebraic closure has a root in the algebraic closure
- The algebraic closure of a field is a normal extension, meaning that every irreducible polynomial over the field either has no roots or splits completely in the algebraic closure
- A polynomial $f(x)$ splits completely in a field K if it factors into linear terms:
 $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ with $\alpha_i \in K$

Separability and Infinite Extension Properties

- The algebraic closure of a field is a separable extension, meaning that every element in the algebraic closure is separable over the base field (its minimal polynomial has distinct roots)
- An element α is separable over a field F if its minimal polynomial $m(x)$ over F has distinct roots in an algebraic closure of F
- The algebraic closure of a field is an infinite extension unless the field is already algebraically closed
- For example, the algebraic closure of $\mathbb{Q}$ is an infinite extension of $\mathbb{Q}$, while $\mathbb{C}$ is its own algebraic closure

Algebraic Closures vs Splitting Fields

Relationship between Algebraic Closures and Splitting Fields

- A splitting field of a polynomial $f(x)$ over a field F is the smallest field extension of F in which $f(x)$ factors into linear factors
- The splitting field of a polynomial over a field is a subfield of the algebraic closure of the field
- The algebraic closure of a field F can be constructed as the union of all splitting fields of polynomials over F
- Every polynomial in $F[x]$ splits in its splitting field, which is contained in the algebraic closure of F

Finite Extensions and Galois Theory

- Every finite extension of a field F is contained in a splitting field of some polynomial over F , which is itself contained in the algebraic closure of F
- For example, the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a primitive cube root of unity
- The Galois group of a polynomial over a field F is the group of automorphisms of its splitting field that fix F , and it plays a crucial role in studying the relationship between a field and its algebraic closure
- The Galois group of $x^3 - 2$ over $\mathbb{Q}$ is the symmetric group S_3 , which permutes the roots $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$

3.3 Normal extensions

Normal extensions are a key concept in Galois Theory, bridging the gap between field extensions and polynomial splitting. They're special because every irreducible polynomial with a root in the extension splits completely there.

Understanding normal extensions is crucial for grasping the Fundamental Theorem of Galois Theory. They're closely tied to splitting fields and help us analyze the structure of field extensions and their automorphisms.

Normal Extensions

Definition and Properties

- An extension L/K is normal if every irreducible polynomial in $K[x]$ that has a root in L splits completely in $L[x]$
- Example: The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is normal because the minimal polynomial $x^3 - 2$ splits completely in $\mathbb{Q}(\sqrt[3]{2})[x]$
- A normal extension is algebraic, meaning every element of L is a root of some polynomial in $K[x]$
- The composition of normal extensions is normal
- If L/K and M/L are normal, then M/K is normal
- Example: If $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(\sqrt{2})$ are normal, then $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ is normal
- Every finite extension of a finite field is normal
- Example: The extension $\mathbb{F}_8/\mathbb{F}_2$ is normal

Equivalence of Definitions

- Prove that an extension L/K is normal if and only if L is the splitting field of a family of polynomials in $K[x]$
- Show that an extension L/K is normal if and only if every K -embedding of L into an algebraic closure of K maps L onto itself
- Example: For the normal extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, any $\mathbb{Q}$ -embedding of $\mathbb{Q}(\sqrt{2})$ into $\mathbb{C}$ maps $\mathbb{Q}(\sqrt{2})$ onto itself

- Demonstrate that an algebraic extension L/K is normal if and only if the fixed field of the group of K -automorphisms of L is precisely K
- Example: For the normal extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, the fixed field of the group of $\mathbb{Q}$ -automorphisms of $\mathbb{Q}(\sqrt{2})$ is precisely $\mathbb{Q}$

Normal Extensions and Splitting Fields

Characterization

- A finite extension L/K is normal if and only if L is the splitting field of some polynomial $f(x)$ in $K[x]$
- Example: The extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ is normal because it is the splitting field of the polynomial $x^4 - 2$
- If L/K is normal, then L is the splitting field of the minimal polynomial of any element α in L over K
- Every splitting field is a normal extension
- Example: The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \omega)$, which is a normal extension

Fundamental Theorem of Galois Theory

- Use the Fundamental Theorem of Galois Theory to check if the corresponding Galois group acts transitively on the roots of the minimal polynomial of a primitive element of L over K
- Example: For the normal extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$, the Galois group acts transitively on the roots of the minimal polynomial $x^4 - 2$ of the primitive element $\sqrt{2} + i$

Definitions of Normal Extensions

Refer to the content under "Definition and Properties" and "Equivalence of Definitions" in the "Normal Extensions" section above.

Identifying Normal Extensions

Checking Irreducible Polynomials

- Check if every irreducible polynomial in $K[x]$ that has a root in L splits completely in $L[x]$
- Example: To show that $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ is normal, check that every irreducible polynomial in $\mathbb{Q}[x]$ with a root in $\mathbb{Q}(\sqrt{2}, i)$ splits completely in $\mathbb{Q}(\sqrt{2}, i)[x]$

Verifying Splitting Fields

- Determine if L is the splitting field of some polynomial $f(x)$ in $K[x]$
- Example: To show that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is normal, verify that it is the splitting field of the polynomial $x^3 - 2$

Examining Embeddings and Automorphisms

- Verify if every K -embedding of L into an algebraic closure of K maps L onto itself
- Examine if the fixed field of the group of K -automorphisms of L is precisely K , assuming L/K is algebraic

- Example: To show that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal, verify that every $\mathbb{Q}$ -embedding of $\mathbb{Q}(\sqrt{2})$ into $\mathbb{C}$ maps $\mathbb{Q}(\sqrt{2})$ onto itself and that the fixed field of the group of $\mathbb{Q}$ -automorphisms of $\mathbb{Q}(\sqrt{2})$ is precisely $\mathbb{Q}$

Unit 4 – Separable and Inseparable Extensions

4.1 Separable polynomials and extensions

Separable polynomials and extensions are key concepts in Galois Theory. They help us understand the structure of field extensions and their automorphisms. Separable polynomials have distinct roots, while separable extensions are built from these polynomials.

These ideas are crucial for the Fundamental Theorem of Galois Theory. They allow us to connect field extensions with their Galois groups, providing a powerful tool for solving polynomial equations and understanding field theory.

Separable Polynomials

Properties of Separable Polynomials

- A polynomial $f(x)$ over a field F is separable if it has distinct roots in some extension field of F
- The multiplicity of a root α of $f(x)$ is the largest positive integer m such that $(x - \alpha)^m$ divides $f(x)$
- A root is simple if it has multiplicity 1
- A polynomial is separable if and only if all its roots are simple
- The derivative $f'(x)$ of a polynomial $f(x)$ is the polynomial obtained by differentiating each term of $f(x)$ with respect to x
- A polynomial $f(x)$ is separable if and only if $f(x)$ and $f'(x)$ are relatively prime ($\gcd(f(x), f'(x)) = 1$)
- The product of separable polynomials is separable ($f(x)$ and $g(x)$ separable implies $f(x)g(x)$ separable)
- If $f(x)$ is a separable polynomial over F and E is an extension of F , then $f(x)$ is also separable over E

Examples of Separable Polynomials

- The polynomial $f(x) = x^2 - 2$ over $\mathbb{Q}$ is separable because it has distinct roots $\pm\sqrt{2}$ in the extension field $\mathbb{Q}(\sqrt{2})$
- The polynomial $g(x) = x^3 - 3x + 1$ over $\mathbb{Q}$ is separable because $\gcd(g(x), g'(x)) = \gcd(x^3 - 3x + 1, 3x^2 - 3) = 1$
- The polynomial $h(x) = (x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$ is separable because it is the product of separable polynomials $(x^2 - 2)$ and $(x^2 - 3)$

Separable Extensions

Characterization of Separable Extensions

- An algebraic extension E/F is separable if every element of E is the root of a separable polynomial over F

- For a finite extension E/F , the following are equivalent:
 1. E/F is separable
 2. There exists a primitive element $\alpha \in E$ such that $E = F(\alpha)$ and the minimal polynomial of α over F is separable
 3. Every irreducible polynomial in $F[x]$ that has a root in E is separable
- Every splitting field is a separable extension
- If E/F is a finite separable extension, then E is the splitting field of some separable polynomial over F

Examples of Separable Extensions

- Finite fields over their prime subfields ($\mathbb{F}_{p^n}/\mathbb{F}_p$ is separable for any prime p and positive integer n)
- $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$ is separable for any positive integer n because the minimal polynomial of $\sqrt[n]{2}$ over $\mathbb{Q}$ is $x^n - 2$, which is separable
- The splitting field of $x^4 - 2$ over $\mathbb{Q}$ is a separable extension of $\mathbb{Q}$ because $x^4 - 2$ is a separable polynomial

Definitions of Separable Extensions

Equivalent Definitions of Separable Extensions

- Theorem: Let E/F be a finite extension. The following are equivalent:
 1. E/F is separable
 2. There exists a primitive element $\alpha \in E$ such that $E = F(\alpha)$ and the minimal polynomial of α over F is separable
 3. Every element of E is the root of a separable polynomial over F
 4. Every irreducible polynomial in $F[x]$ that has a root in E is separable

Proof of Equivalence

- The proof involves showing the implications $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (1)$ using properties of minimal polynomials, primitive elements, and the separability of irreducible factors
- $(1) \Rightarrow (2)$: If E/F is separable, then there exists a primitive element $\alpha \in E$ such that $E = F(\alpha)$ and the minimal polynomial of α over F is separable (Primitive Element Theorem)
- $(2) \Rightarrow (3)$: If α is a primitive element of E/F with a separable minimal polynomial, then every element of E can be expressed as a polynomial in α and is thus the root of a separable polynomial over F
- $(3) \Rightarrow (4)$: If every element of E is the root of a separable polynomial over F , then every irreducible polynomial in $F[x]$ that has a root in E must be separable (as it divides a separable polynomial)
- $(4) \Rightarrow (1)$: If every irreducible polynomial in $F[x]$ that has a root in E is separable, then E/F is separable by definition

Separability of Polynomials and Extensions

Determining Separability of Polynomials

- To determine if a polynomial $f(x)$ over F is separable, check if $f(x)$ and $f'(x)$ are relatively prime using the Euclidean algorithm
- Example: $f(x) = x^3 - 2$ over $\mathbb{Q}$ is separable because $\gcd(f(x), f'(x)) = \gcd(x^3 - 2, 3x^2) = 1$
- Alternatively, factor $f(x)$ into irreducible factors over F and check if all factors have multiplicity 1
- Example: $g(x) = (x^2 - 2)(x - 1)^2$ over $\mathbb{Q}$ is not separable because $(x - 1)$ has multiplicity 2

Determining Separability of Extensions

- For a finite extension E/F , find a primitive element α such that $E = F(\alpha)$ and check if the minimal polynomial of α over F is separable
- Example: $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is separable because the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$, which is separable
- Alternatively, factor the minimal polynomials of elements in E over F and check if all irreducible factors are separable
- Example: $\mathbb{F}_4/\mathbb{F}_2$ is separable because the minimal polynomial of any element in $\mathbb{F}_4$ over $\mathbb{F}_2$ is either x or $x^2 + x + 1$, both of which are separable
- Use the properties of separable extensions, such as the fact that every splitting field is separable, to determine the separability of a given extension
- Example: The splitting field of $x^4 - 2$ over $\mathbb{Q}$ is a separable extension of $\mathbb{Q}$ because $x^4 - 2$ is a separable polynomial

Examples of Inseparable Extensions

- $\mathbb{F}_p(x^{1/p})/\mathbb{F}_p(x)$ is inseparable for any prime p because the minimal polynomial of $x^{1/p}$ over $\mathbb{F}_p(x)$ is $y^p - x$, which is not separable
- $\mathbb{F}_p(t^{1/p})/\mathbb{F}_p(t)$ is inseparable for any prime p because the minimal polynomial of $t^{1/p}$ over $\mathbb{F}_p(t)$ is $y^p - t$, which is not separable

4.2 Inseparable extensions and their characteristics

Inseparable extensions are a fascinating twist in field theory, occurring only in fields with prime characteristic. They're the rebels of algebraic extensions, breaking the usual rules we're used to with separable polynomials and normal extensions.

These extensions are characterized by repeated roots and zero derivatives. They mess with our usual understanding of field extensions, leading to unique properties like trivial Galois groups and non-normal extensions. Understanding inseparable extensions is crucial for grasping the full picture of field theory.

Inseparable Polynomials and Extensions

Definition and Properties

- An irreducible polynomial $f(x)$ over a field F is called inseparable if it has repeated roots in some extension field of F
- The derivative $f'(x)$ of an inseparable polynomial $f(x)$ is identically zero
- An algebraic extension K/F is inseparable if there exists an element α in K such that the minimal polynomial of α over F is inseparable
- In an inseparable extension, there exist elements that are not separable over the base field

Characteristic of the Base Field

- The characteristic of the base field F must be a prime number p for an inseparable extension to exist
- If the characteristic is zero or a composite number, all irreducible polynomials are separable
- Example: Inseparable extensions can occur in fields of characteristic 2, 3, 5, etc.

Characteristics of Inseparable Extensions

Properties of Elements in Inseparable Extensions

- Every element α in an inseparable extension K/F satisfies an equation of the form $\alpha^{p^n} = a$ for some a in F and some positive integer n
- This property is a consequence of the inseparability of the minimal polynomial of α
- Example: If K/F is an inseparable extension of characteristic 3, an element α in K might satisfy an equation like $\alpha^{3^2} = a$ for some a in F
- The Frobenius endomorphism $\phi : K \rightarrow K$ defined by $\phi(\alpha) = \alpha^p$ is not an automorphism in an inseparable extension
- In a separable extension, the Frobenius endomorphism is always an automorphism

Degree and Normality of Inseparable Extensions

- The degree of an inseparable extension is always a power of the characteristic p
- This is because the minimal polynomial of an inseparable element has a degree that is a power of p
- Example: An inseparable extension of a field of characteristic 5 might have degree 5, 25, 125, etc.
- Inseparable extensions are not normal extensions
- A normal extension is an algebraic extension that is the splitting field of a family of polynomials
- Inseparable extensions do not satisfy this property because inseparable polynomials do not split into linear factors
- The Galois group of an inseparable extension is trivial (consists only of the identity automorphism)
- This is a consequence of the lack of normality and the fact that the Frobenius endomorphism is not an automorphism

Properties of Inseparable Extensions

Perfect Fields and Inseparable Extensions

- A field F of characteristic p is perfect if and only if every algebraic extension of F is separable
- In other words, a field is perfect if it has no inseparable extensions
- Example: The field of rational functions $\mathbb{F}_p(t)$ over a finite field $\mathbb{F}_p$ is perfect
- In a perfect field, the Frobenius endomorphism is an automorphism
- This is because all minimal polynomials are separable, so the Frobenius endomorphism does not introduce any inseparability
- If K/F is an algebraic extension and F is perfect, then K is perfect
- Proof: Let α be an element of K . Since K/F is algebraic, α is algebraic over F . As F is perfect, the minimal polynomial of α over F is separable. Thus, α is separable over F , and since this holds for all α in K , K is perfect
- If K/F is an inseparable extension, then F is not perfect
- Proof: If K/F is inseparable, there exists an element α in K with an inseparable minimal polynomial over F . This implies that F cannot be perfect, as perfect fields only admit separable extensions

Relationship Between Separable and Inseparable Extensions

- Every algebraic extension K/F can be decomposed into a tower of extensions $K/K_s/F$, where K_s/F is separable and K/K_s is purely inseparable
- K_s is the separable closure of F in K , which is the largest separable subextension of K/F
- Example: If K/F is an inseparable extension, it can be decomposed into $K/K_s/F$, where K_s/F is the maximal separable subextension and K/K_s is purely inseparable
- The degree of an algebraic extension K/F is the product of its separable degree and inseparable degree
- $[K : F] = [K : F]_s \cdot [K : F]_i$, where $[K : F]_s$ is the separable degree and $[K : F]_i$ is the inseparable degree
- The separable degree $[K : F]_s$ is the degree of the separable closure K_s/F , and the inseparable degree $[K : F]_i$ is the degree of the purely inseparable extension K/K_s

Inseparable Degree of an Extension

Definition and Properties

- The inseparable degree of an algebraic extension K/F , denoted $[K : F]_i$, is the degree of the largest inseparable subextension of K/F
- It measures the extent to which the extension is inseparable
- Example: If K/F is a purely inseparable extension of degree 9, then $[K : F]_i = 9$
- For a finite extension K/F , the inseparable degree is equal to the degree of the extension of K over the separable closure of F in K

- $[K : F]_i = [K : K_s]$, where K_s is the separable closure of F in K
- The inseparable degree is always a power of the characteristic p of the base field F
- This is because inseparable extensions have degrees that are powers of p

Computing the Inseparable Degree

- To compute the inseparable degree, find the largest subextension L/F of K/F such that every element of L is inseparable over F
- The degree $[L : F]$ is the inseparable degree of K/F
- Example: To find the inseparable degree of K/F , look for the largest intermediate field L such that L/F is purely inseparable. The degree of this extension is $[K : F]_i$
- If K/F is a finite extension, then $[K : F] = [K : F]_s \cdot [K : F]_i$, where $[K : F]_s$ is the separable degree and $[K : F]_i$ is the inseparable degree
- This formula relates the total degree of the extension to its separable and inseparable components
- Example: If $[K : F] = 12$ and $[K : F]_s = 3$, then $[K : F]_i = 4$ because $12 = 3 \cdot 4$

4.3 Perfect fields and separable closure

Perfect fields and separable closures are crucial concepts in Galois Theory. They help us understand when all algebraic extensions are separable and how to construct the largest separable extension of a field. These ideas are key to studying field extensions and their properties.

Understanding perfect fields and separable closures allows us to analyze the structure of field extensions more deeply. We can determine when all polynomials have distinct roots and explore the relationship between a field and its largest separable extension, shedding light on important algebraic properties.

Perfect fields

Properties of perfect fields

- A field F is perfect if every irreducible polynomial over F is separable, meaning it has distinct roots in an algebraic closure of F
- In a perfect field, every algebraic extension is separable
- This implies that for a perfect field F , any polynomial $f(x) \in F[x]$ that factors into linear terms in an algebraic closure of F already factors into linear terms in F itself
- A field of characteristic 0 is always perfect (examples: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$)
- A field of characteristic $p > 0$ is perfect if and only if every element of the field is a p -th power
- In other words, the Frobenius endomorphism $x \mapsto x^p$ is surjective for a perfect field of characteristic p

Examples of perfect fields

- The prime field $\mathbb{F}_p$ and all its finite extensions are perfect fields
- For instance, $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5$, etc. are all perfect
- If F is perfect, then any algebraic extension of F is also perfect

- For example, if $F = \mathbb{Q}$ is perfect, then $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, and any other algebraic extension of $\mathbb{Q}$ is also perfect
- The algebraic closure of a perfect field is also perfect
- So, the algebraic closures $\overline{\mathbb{Q}}$, $\overline{\mathbb{F}_p}$, etc. are all perfect fields

Separable closure of a field

Existence and uniqueness of separable closure

- The separable closure F_s of a field F is the largest separable extension of F inside an algebraic closure of F
- To prove existence, consider the composite of all separable extensions of F inside an algebraic closure
- This composite is a separable extension of F and contains all other separable extensions
- Thus, the composite is the separable closure F_s
- To prove uniqueness, suppose F_s and F'_s are two separable closures of F
- Then there exists an F -isomorphism between F_s and F'_s by the universal property of the separable closure
- This means the separable closure is unique up to isomorphism over F

Properties of separable closure

- The separable closure is the smallest separably closed extension of a field
- A field K is separably closed if every separable polynomial over K has a root in K
- Any finite separable extension of F is contained in the separable closure of F
- For example, if $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $K \subseteq \mathbb{Q}_s$
- If $F \subseteq K \subseteq F_s$, where F_s is the separable closure of F , then K is separable over F
- This follows from the fact that F_s is separable over F , and any intermediate field is also separable over F

Constructing separable closures

Construction process

- To construct the separable closure of a field F , first construct an algebraic closure F_a of F
- Inside F_a , consider the set S of all elements that are separable over F
- An element $\alpha \in F_a$ is separable over F if its minimal polynomial over F is separable
- Show that S is a subfield of F_a containing F
- This involves proving that S is closed under addition, multiplication, and taking inverses
- Prove that S is the separable closure of F by showing that it is separable over F and contains all separable extensions of F

- To show S is separable over F , use the fact that every element in S is separable over F
- To show S contains all separable extensions, use the definition of S and the properties of the algebraic closure

Special cases

- In characteristic 0, the separable closure coincides with the algebraic closure
- This is because every irreducible polynomial over a field of characteristic 0 is separable
- So, $\mathbb{Q}_S = \overline{\mathbb{Q}}$, $\mathbb{R}_S = \overline{\mathbb{R}}$, etc.
- In characteristic $p > 0$, the separable closure is obtained by adjoining all p -power roots of elements in F
- This means that $F_S = F(x_1^{1/p^\infty}, x_2^{1/p^\infty}, \dots)$ for all $x_i \in F$
- For example, if $F = \mathbb{F}_p(t)$, then $F_S = \mathbb{F}_p(t^{1/p^\infty})$

Separable closure in field extensions

Applications of separable closure

- Use the fact that the separable closure is the smallest separably closed extension of a field
- This can help determine if a given field extension is separably closed or not
- Any finite separable extension of F is contained in the separable closure of F
- This can be used to study the structure of finite separable extensions and their relation to the separable closure
- If $F \subseteq K \subseteq F_S$, where F_S is the separable closure of F , then K is separable over F
- This property can be used to prove that certain field extensions are separable

Absolute Galois group

- The Galois group of the separable closure over F is called the absolute Galois group of F , denoted $\text{Gal}(F_S/F)$
- The absolute Galois group acts on the set of algebraic extensions of F and the set of separable extensions of F
- This action is defined by the restriction of automorphisms in $\text{Gal}(F_S/F)$ to the subfields of F_S
- Use the separable closure to study the structure of the absolute Galois group and its relation to the arithmetic properties of the base field
- For example, the absolute Galois group of $\mathbb{Q}$ is closely related to the arithmetic of the rational numbers
- The absolute Galois group of a finite field $\mathbb{F}_q$ is isomorphic to the profinite completion of $\mathbb{Z}$, denoted $\hat{\mathbb{Z}}$

Unit 5 – Automorphisms and Fixed Fields

5.1 Field automorphisms and their properties

Field automorphisms are the backbone of Galois Theory. They're special functions that shuffle elements of a field while keeping its structure intact. Think of them as secret codes that rearrange numbers but still let you do math with them.

These automorphisms form groups, which are like clubs of functions that play well together. By studying these groups, we can unlock hidden relationships between fields and their subfields. It's like having a master key to understand how different number systems fit together.

Field automorphisms

Definition and properties

- A field automorphism is a bijective homomorphism from a field to itself that preserves the field operations of addition and multiplication
- Bijective means the function is both one-to-one (injective) and onto (surjective)
- Homomorphism means the function preserves the algebraic structure of the field
- The identity map on a field, which maps every element to itself, is always an automorphism
- The composition of two field automorphisms, obtained by applying one automorphism followed by the other, is again a field automorphism
- The inverse of a field automorphism, which "undoes" the automorphism, is also a field automorphism
- Field automorphisms fix the prime subfield elementwise
- The prime subfield is the smallest subfield of a field (e.g., $\mathbb{Q}$ for $\mathbb{R}$ or $\mathbb{C}$)
- Elementwise means each element of the prime subfield is mapped to itself by the automorphism

Examples of field automorphisms

- The complex conjugation map $z \mapsto \bar{z}$ is an automorphism of the complex numbers $\mathbb{C}$
- It fixes the real numbers $\mathbb{R}$ elementwise
- The Frobenius automorphism $x \mapsto x^p$ is an automorphism of a finite field $\mathbb{F}_{p^n}$ of characteristic p
- It fixes the prime subfield $\mathbb{F}_p$ elementwise
- For a Galois extension L/K , any K -automorphism of L (i.e., an automorphism of L that fixes K elementwise) is a field automorphism of L

Automorphism groups of field extensions

Automorphism group of a field

- The set of all automorphisms of a field forms a group under function composition, called the automorphism group of the field

- Function composition is associative, and the identity map serves as the identity element
- The inverse of an automorphism is also an automorphism, ensuring closure
- The automorphism group of a field extension L/K is the subgroup of the automorphism group of L consisting of automorphisms that fix K elementwise
- These automorphisms are also called K -automorphisms of L
- The automorphism group of a finite field $\mathbb{F}_{p^n}$ is a cyclic group generated by the Frobenius automorphism
- The order of this group is n , the degree of the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$

Automorphism group and splitting fields

- The automorphism group of a splitting field of a separable polynomial $f(x)$ over K is isomorphic to a subgroup of the permutation group of the roots of $f(x)$
- A splitting field is the smallest field extension of K in which $f(x)$ factors into linear factors
- The permutation group of the roots consists of all permutations of the roots that preserve the algebraic relationships among them
- For a Galois extension L/K , the automorphism group of L/K is called the Galois group of the extension
- The Galois group acts faithfully on the roots of the minimal polynomial of any primitive element of the extension

Applications of field automorphisms

Conjugacy and orbits

- Field automorphisms can be used to prove the transitivity of conjugacy for field extensions
- If α and β are conjugate over K , and β and γ are conjugate over K , then α and γ are also conjugate over K
- Automorphisms can be applied to equations and polynomials to obtain new solutions or polynomials with the same splitting field
- If σ is an automorphism and α is a solution to a polynomial equation, then $\sigma(\alpha)$ is also a solution
- The orbit of an element under the action of the automorphism group can provide insights into the structure of the field extension
- The orbit of α is the set $\{\sigma(\alpha) : \sigma \in \text{Aut}(L/K)\}$, where $\text{Aut}(L/K)$ is the automorphism group of L/K
- The orbits partition the field extension into disjoint sets

Fixed fields and subfields

- The fixed field of a subgroup H of the automorphism group of a field extension L/K is the subfield of L consisting of elements fixed by every automorphism in H
- $\text{Fix}(H) = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in H\}$
- For a Galois extension L/K , the Fundamental Theorem of Galois Theory establishes a one-to-one correspondence between the intermediate fields of L/K and the subgroups of the Galois group of L/K

- The correspondence associates each intermediate field M with the subgroup $\text{Aut}(L/M)$ and each subgroup H with the fixed field $\text{Fix}(H)$

Theorems for field automorphisms

Artin's Lemma and the Theorem of the Primitive Element

- Artin's Lemma states that if a field automorphism σ fixes a subfield K and an element α is algebraic over K , then σ permutes the conjugates of α over K
- The conjugates of α are the roots of the minimal polynomial of α over K
- The Theorem of the Primitive Element asserts that a finite separable extension L/K is simple if and only if there exists a primitive element
- A simple extension is an extension generated by a single element, i.e., $L = K(\alpha)$ for some $\alpha \in L$
- A primitive element is an element that generates the entire extension

Dedekind's Lemma and the Fundamental Theorem of Galois Theory

- Dedekind's Lemma proves that if M/L and L/K are Galois extensions, then M/K is Galois if and only if the automorphism groups of M/L and L/K intersect trivially
- The intersection of the automorphism groups is $\text{Aut}(M/L) \cap \text{Aut}(L/K) = \{\text{id}_M\}$, where id_M is the identity automorphism on M
- The Fundamental Theorem of Galois Theory establishes a correspondence between intermediate fields of a Galois extension and subgroups of its Galois group
- The correspondence preserves inclusions and degrees: if $H_1 \subseteq H_2$ are subgroups of the Galois group, then $\text{Fix}(H_2) \subseteq \text{Fix}(H_1)$ and $[L : \text{Fix}(H_1)] = |H_1|$

5.2 Fixed fields and the Fundamental Theorem of Galois Theory

Fixed fields and the Fundamental Theorem of Galois Theory are key concepts in understanding field extensions. They link automorphisms, subfields, and subgroups, providing a powerful framework for analyzing field structures.

This correspondence allows us to translate problems between group theory and field theory. By studying subgroups of the Galois group, we can uncover properties of subfields and vice versa, simplifying complex algebraic questions.

Fixed fields of automorphisms

Definition and properties

- The fixed field of a group of automorphisms G of a field extension K/F consists of all elements of K fixed by every automorphism in G
- If G is a group of automorphisms of a field K , the fixed field of G , denoted by $\text{Fix}(G)$ or K^G , forms a subfield of K
- The fixed field equals the intersection of all fields fixed by each individual automorphism in G

- The degree of the extension $K/\text{Fix}(G)$ matches the order of the group G , expressed as $[K : \text{Fix}(G)] = |G|$
- The Galois group of the extension $K/\text{Fix}(G)$ is isomorphic to the group G

Characterization and examples

- For a cyclic group $G = \langle \sigma \rangle$ generated by an automorphism σ , the fixed field $\text{Fix}(G)$ consists of elements $a \in K$ satisfying $\sigma(a) = a$
- In the extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$, the fixed field of the automorphism $\sigma : \sqrt{2} \mapsto -\sqrt{2}, i \mapsto i$ is $\mathbb{Q}(i)$
- For the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, the fixed field of the Galois group $G = \{\text{id}, \sigma, \sigma^2, \sigma^3\}$, where $\sigma : \sqrt[4]{2} \mapsto i\sqrt[4]{2}$, is $\mathbb{Q}$
- In the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, the fixed field of the subgroup $H = \{\text{id}, \sigma\}$, where $\sigma : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$, is $\mathbb{Q}(\sqrt{3})$

Fundamental Theorem of Galois Theory

Statement and interpretation

- The Fundamental Theorem of Galois Theory establishes a one-to-one correspondence between subfields of a Galois extension and subgroups of its Galois group
- For a Galois extension K/F with Galois group G , there exists a bijection between subfields of K containing F and subgroups of G , given by $H \mapsto \text{Fix}(H)$ and $E \mapsto \text{Gal}(K/E)$
- The correspondence reverses inclusions: for subgroups H_1 and H_2 of G with $H_1 \subseteq H_2$, we have $\text{Fix}(H_2) \subseteq \text{Fix}(H_1)$
- The degree of the extension K/E equals the index of the corresponding subgroup $\text{Gal}(K/E)$ in G , expressed as $[K : E] = [G : \text{Gal}(K/E)]$
- A subfield E is a Galois extension of F if and only if the corresponding subgroup $\text{Gal}(K/E)$ is a normal subgroup of G , in which case the Galois group of E/F is isomorphic to the quotient group $G/\text{Gal}(K/E)$

Examples and consequences

- In the extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$, the subgroup $H = \{\text{id}, \sigma\}$, where $\sigma : \sqrt{2} \mapsto -\sqrt{2}, i \mapsto i$, corresponds to the subfield $\mathbb{Q}(i)$
- For the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ with Galois group $G = \{\text{id}, \sigma, \sigma^2, \sigma^3\}$, the subgroup $H = \{\text{id}, \sigma^2\}$ corresponds to the subfield $\mathbb{Q}(\sqrt{2})$
- The Fundamental Theorem implies that for a Galois extension K/F , the subfield F corresponds to the entire Galois group G , while the field K corresponds to the trivial subgroup $\{\text{id}\}$
- As a consequence of the Fundamental Theorem, a finite extension K/F is Galois if and only if $|\text{Aut}(K/F)| = [K : F]$

Galois correspondence

Finding corresponding subfields and subgroups

- To find the subfield corresponding to a given subgroup H of the Galois group G , calculate the fixed field $\text{Fix}(H)$ by identifying elements of K fixed by every automorphism in H
- To find the subgroup corresponding to a given subfield E of K containing F , calculate the Galois group $\text{Gal}(K/E)$ by finding automorphisms of K that fix every element of E
- The Galois correspondence preserves the lattice structure of subgroups and subfields: the intersection of subgroups corresponds to the compositum of subfields, and the join of subgroups corresponds to the intersection of subfields
- The Galois correspondence helps determine the lattice of subfields of a Galois extension by studying the lattice of subgroups of its Galois group

Examples and applications

- In the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, the subgroup $H = \{\text{id}, \sigma\}$, where $\sigma: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$, corresponds to the subfield $\mathbb{Q}(\sqrt{3})$
- For the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ with Galois group $G = \{\text{id}, \sigma, \sigma^2\}$, where $\sigma: \sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$ and ω is a primitive cube root of unity, the subfield $\mathbb{Q}(\omega)$ corresponds to the subgroup $\{\text{id}, \sigma\}$
- The Galois correspondence can be used to prove that for a Galois extension K/F with Galois group G , the number of subfields of K containing F equals the number of subgroups of G
- In cryptography, the Galois correspondence is applied to construct finite fields with desired properties for use in encryption and error correction codes

Applying the Fundamental Theorem

Solving problems in field theory

- Use the Fundamental Theorem to determine the existence and uniqueness of subfields with specific properties, such as degree or Galois group
- Apply the Galois correspondence to construct field extensions with desired properties by finding appropriate subgroups of the Galois group
- Utilize the Fundamental Theorem to prove theorems about the structure of field extensions, such as the existence of intermediate fields or the solvability of polynomial equations
- Employ the Galois correspondence to simplify the computation of Galois groups by working with subfields instead of automorphisms
- Use the Fundamental Theorem to study relationships between different field extensions and their Galois groups, such as compositums, intersections, and quotients

Examples and applications

- Prove that for a Galois extension K/F with Galois group G , there exists a unique subfield E of K containing F with $[E : F] = n$ if and only if G has a unique subgroup of index n

- Construct a field extension $K/\mathbb{Q}$ with Galois group isomorphic to the dihedral group D_4 by finding a polynomial whose splitting field has D_4 as its Galois group and applying the Galois correspondence
- Use the Fundamental Theorem to prove that a polynomial $f(x) \in F[x]$ is solvable by radicals if and only if its Galois group over F is a solvable group
- Determine the Galois group of the splitting field of $x^4 - 2$ over $\mathbb{Q}$ by studying the lattice of subfields and applying the Galois correspondence
- Investigate the relationship between the splitting fields of polynomials $f(x)$ and $g(x)$ over a field F by examining the subgroups of the Galois group of the compositum of their splitting fields

5.3 Isomorphism extension theorem

The isomorphism extension theorem is a key tool in Galois theory, allowing us to extend field isomorphisms to larger extensions. It states that any isomorphism between subfields can be extended to an isomorphism between their larger field extensions.

This theorem is crucial for understanding the structure of field extensions and their automorphisms. It helps us construct new field extensions, prove uniqueness of algebraic closures, and establish the fundamental theorem of Galois theory.

Isomorphism Extension Theorem

Statement and Proof

- The isomorphism extension theorem states that if K is an extension field of F and $\sigma : F \rightarrow L$ is an isomorphism from F to a subfield of L , then σ can be extended to an isomorphism from K to an extension field of L
- To prove the theorem, let $K = F(\alpha)$ for some $\alpha \in K$
- The minimal polynomial of α over F , denoted $f(x)$, is also the minimal polynomial of $\sigma(\alpha)$ over $\sigma(F)$
- Adjoin a root β of $f(x)$ to L to create the extension field $L(\beta)$
- Define a function $\tau : K \rightarrow L(\beta)$ by $\tau(g(\alpha)) = g(\beta)$ for any polynomial $g(x) \in F[x]$
- τ is well-defined because if $g(\alpha) = h(\alpha)$ in K , then $g(x) - h(x)$ is divisible by $f(x)$ in $F[x]$, so $g(\beta) - h(\beta) = 0$ in $L(\beta)$
- τ is a homomorphism because $\tau(g(\alpha) + h(\alpha)) = \tau(g(\alpha)) + \tau(h(\alpha))$ and $\tau(g(\alpha)h(\alpha)) = \tau(g(\alpha))\tau(h(\alpha))$
- τ is injective because if $\tau(g(\alpha)) = 0$, then $g(\beta) = 0$, so $f(x)$ divides $g(x)$ in $L[x]$, and thus in $F[x]$, implying $g(\alpha) = 0$
- τ is surjective because any element of $L(\beta)$ can be written as $g(\beta)$ for some $g(x) \in L[x]$, and $g(\beta) = \tau(g(\alpha))$
- Therefore, τ is an isomorphism extending σ to a map from K to $L(\beta)$

Properties and Consequences

- The extension field M is not unique, but it is isomorphic to any other extension of L that admits an isomorphism extending σ

- For example, if $K = \mathbb{Q}(\sqrt{2})$ and $L = \mathbb{Q}(\sqrt{3})$, then both $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$ are suitable choices for M
- If K is a finite extension of F , then the extension M of L can be chosen to be a finite extension of the same degree
- For instance, if $[K : F] = n$, then $[M : L] = n$ as well
- When extending an automorphism of a field to its algebraic closure, the isomorphism extension theorem ensures that the extended automorphism is unique
- This property is crucial in the study of Galois groups and their actions on algebraic closures

Applying the Isomorphism Extension Theorem

Extending Field Isomorphisms

- Given an isomorphism $\sigma : F \rightarrow L$ between fields F and L , and an extension K of F , the isomorphism extension theorem guarantees the existence of an extension field M of L and an isomorphism $\tau : K \rightarrow M$ extending σ
- For example, if $F = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, and $K = \mathbb{Q}(\sqrt[3]{2})$, then M can be chosen as $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$
- The extended isomorphism τ preserves the properties of σ , such as its action on specific elements or its compatibility with field operations
- If $\sigma(\sqrt{2}) = \sqrt{2}$, then $\tau(\sqrt[3]{2})$ must be a cube root of 2 in M

Constructing Field Extensions

- The isomorphism extension theorem can be used to construct field extensions with desired properties by extending isomorphisms from a base field
- For instance, to construct a field extension of $\mathbb{Q}$ containing both $\sqrt{2}$ and $\sqrt{3}$, one can start with the isomorphism $\sigma : \mathbb{Q} \rightarrow \mathbb{Q}$ and extend it to $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
- This technique is particularly useful when working with algebraic extensions, as it allows for the creation of splitting fields and the study of their Galois groups
- The splitting field of a polynomial $f(x)$ over a field F can be constructed by successively extending isomorphisms to adjoin roots of $f(x)$

Solving Problems with the Isomorphism Extension Theorem

Fundamental Theorem of Galois Theory

- The isomorphism extension theorem is a crucial tool in proving the fundamental theorem of Galois theory, which establishes a correspondence between intermediate fields of a Galois extension and subgroups of its Galois group
- In the proof of the fundamental theorem, the isomorphism extension theorem is used to show that if H is a subgroup of the Galois group $G(E/F)$, then the fixed field E^H is a Galois extension of F with Galois group isomorphic to H
- This is done by extending the inclusion map $F \rightarrow E^H$ to an isomorphism between E and an extension of E^H , and then using the properties of fixed fields to show that this extension is Galois with the desired

Galois group

- The theorem also plays a role in proving the surjectivity of the Galois correspondence, by showing that every intermediate field of a Galois extension arises as the fixed field of some subgroup of the Galois group

Algebraic Closures and Extension Isomorphisms

- The isomorphism extension theorem is used to prove the uniqueness of the algebraic closure of a field up to isomorphism, by showing that any two algebraic closures are isomorphic via an isomorphism fixing the base field
- This result is important in the study of algebraic geometry and the classification of algebraic varieties
- In the study of algebraic extensions, the isomorphism extension theorem helps to determine whether two given extensions are isomorphic by examining their isomorphisms over the base field
- For example, to show that $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{4})$ are isomorphic, one can construct an isomorphism between $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{4})$ extending the identity map on $\mathbb{Q}$

Importance of the Isomorphism Extension Theorem

Foundational Result in Field Theory

- The isomorphism extension theorem is a foundational result in field theory, as it guarantees the existence of isomorphisms between extension fields under certain conditions
- This property is essential in the study of field extensions and their relationships to one another
- The theorem plays a central role in the classification of fields, particularly in understanding the structure of algebraic extensions and their automorphism groups
- For instance, the theorem is used to prove that the Galois group of a separable extension is always finite, which is a key fact in the classification of finite fields

Applications in Galois Theory and Beyond

- In Galois theory, the isomorphism extension theorem is indispensable for establishing the correspondence between intermediate fields and subgroups of the Galois group, which is the main focus of the theory
- Without the theorem, it would be much harder to prove the fundamental results of Galois theory and to understand the intricate relationships between field extensions and their symmetries
- The theorem also has applications beyond Galois theory, such as in the study of transcendental extensions and the construction of field extensions with prescribed properties
- For example, the theorem can be used to prove the existence of transcendental extensions of a given field, by extending isomorphisms from the base field to larger extension fields
- Recognizing the significance of the isomorphism extension theorem allows mathematicians to appreciate the interconnectedness of various concepts in field theory and to apply the theorem effectively in problem-solving
- A deep understanding of the theorem and its implications is essential for anyone working in algebraic number theory, algebraic geometry, or related fields

Unit 6 – Introduction to Group Theory

6.1 Groups, subgroups, and group actions

Groups, subgroups, and group actions form the foundation of abstract algebra. These concepts help us understand the structure and symmetry in mathematical systems, from simple number operations to complex geometric transformations.

By studying these ideas, we gain powerful tools for analyzing and solving problems in various fields. Group theory's applications range from cryptography to quantum mechanics, making it a crucial area of study in modern mathematics and science.

Groups and their properties

Definition and axioms

- A group is a set G together with a binary operation $*$ satisfying the group axioms:
- Closure: For all $a, b \in G$, $a * b \in G$
- Associativity: For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$
- Identity: There exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$
- Inverses: For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

Group properties

- The order of a group is the number of elements in the group
- A group is finite if its order is finite, and infinite otherwise
- A group is abelian (or commutative) if $a * b = b * a$ for all $a, b \in G$
- Examples of abelian groups include $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{R}^*, \cdot)$
- A group is cyclic if it can be generated by a single element
- For each positive integer n , there exists a unique cyclic group of order n (up to isomorphism), denoted $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$
- The center of a group G is the set of elements that commute with every element of G
- The center is always a subgroup of G
- The direct product of two groups $(G, *)$ and $(H, \circ)$ is the group $(G \times H, \cdot)$ where the operation $\cdot$ is defined by $(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)$

Subgroups and their relationships

Subgroup definition and test

- A subset H of a group G is a subgroup if H is itself a group under the same operation as G
- The subgroup test states that H is a subgroup of G if and only if H is nonempty and closed under the group operation and inverses

- The trivial subgroup $\{e\}$ and the group G itself are always subgroups of G
- A proper subgroup is a subgroup that is not the whole group

Cosets and Lagrange's Theorem

- If H is a subgroup of G , then the left cosets of H in G are the sets of the form $aH = \{ah : h \in H\}$ for each $a \in G$
- Similarly, the right cosets are the sets $Ha = \{ha : h \in H\}$
- In general, left and right cosets may differ, but they coincide when H is a normal subgroup
- Lagrange's Theorem states that if G is a finite group and H is a subgroup of G , then the order of H divides the order of G
- As a consequence, the order of any element of a finite group divides the order of the group
- The index of a subgroup H in G , denoted $[G : H]$, is the number of left (or right) cosets of H in G
- Lagrange's Theorem implies that $[G : H] = |G|/|H|$

Normal subgroups

- A normal subgroup is a subgroup N of G such that $gNg^{-1} = N$ for all $g \in G$
- Every subgroup of an abelian group is normal
- The kernel of a group homomorphism is always a normal subgroup of the domain

Group actions

Definition and properties

- A group action of a group G on a set X is a function $\cdot : G \times X \rightarrow X$ satisfying the following properties:
 1. $e \cdot x = x$ for all $x \in X$, where e is the identity element of G
 2. $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$ and $x \in X$
- The orbit of an element $x \in X$ under the action of G is the set $\text{Orb}(x) = \{g \cdot x : g \in G\}$
- The orbits form a partition of X
- The stabilizer of an element $x \in X$ is the set $\text{Stab}(x) = \{g \in G : g \cdot x = x\}$
- The stabilizer is always a subgroup of G

Orbit-Stabilizer Theorem and types of actions

- The Orbit-Stabilizer Theorem states that for any $x \in X$, there is a bijection between the orbit of x and the set of left cosets of $\text{Stab}(x)$ in G
- As a consequence, $|\text{Orb}(x)| = [G : \text{Stab}(x)]$
- A group action is faithful if the only group element that fixes every $x \in X$ is the identity
- Equivalently, the action is faithful if the homomorphism from G to $\text{Sym}(X)$ defined by the action is injective

- A group action is transitive if for any $x, y \in X$, there exists $g \in G$ such that $g \cdot x = y$
- Equivalently, the action is transitive if it has only one orbit

Group theorems

Subgroup and normal subgroup theorems

- Prove that the intersection of two subgroups is also a subgroup
- Prove that the center of a group is a normal subgroup
- Prove that the kernel of a group homomorphism is a normal subgroup of the domain
- Prove that if G is a group and N is a normal subgroup of G , then the quotient group G/N , consisting of cosets of N in G , is a well-defined group under the operation $(aN)(bN) = (ab)N$

Isomorphism theorems and Cayley's Theorem

- Prove the First Isomorphism Theorem: If $\phi : G \rightarrow H$ is a group homomorphism, then $G/\ker(\phi) \cong \text{im}(\phi)$
- Prove Cayley's Theorem: Every group G is isomorphic to a subgroup of the symmetric group acting on G
- Prove that if a group G acts transitively on a set X and H is the stabilizer of a point $x \in X$, then there is a bijection between X and the set of left cosets of H in G

6.2 Normal subgroups and quotient groups

Normal subgroups and quotient groups are key concepts in group theory. They help us understand group structure and relationships between groups. Normal subgroups are special because they allow us to create quotient groups, which simplify our study of the original group.

The first isomorphism theorem is a powerful tool for problem-solving in group theory. It connects homomorphisms, normal subgroups, and quotient groups, helping us classify groups and prove important relationships between different group structures.

Normal subgroups and their significance

Definition and properties of normal subgroups

- A subgroup H of a group G is normal if and only if $gH = Hg$ for all g in G , where $gH = \{gh \mid h \in H\}$ and $Hg = \{hg \mid h \in H\}$
- Equivalently, a subgroup H is normal if and only if $gHg^{-1} \subseteq H$ for all g in G , or $gHg^{-1} = H$ for all g in G
- Normal subgroups are invariant under conjugation by elements of the group G
- The trivial subgroup $\{e\}$ and the entire group G are always normal subgroups of G

Importance of normal subgroups

- Normal subgroups allow the construction of quotient groups, which can simplify the study of the original group

- The kernel of a group homomorphism is always a normal subgroup, and the image of a group homomorphism is isomorphic to the quotient group of the domain by the kernel
- Normal subgroups play a crucial role in the classification of groups up to isomorphism
- Many important subgroups, such as the center of a group, the commutator subgroup, and the subgroup generated by the n th powers of elements in a group, are normal subgroups

Quotient groups and their structure

Construction of quotient groups

- Given a normal subgroup N of a group G , the quotient group (or factor group) G/N is the set of all left cosets of N in G , with the operation $(aN)(bN) = (ab)N$ for a, b in G
- The elements of the quotient group are the cosets of the normal subgroup, and the group operation is well-defined because the subgroup is normal
- The canonical projection map $\pi: G \rightarrow G/N$ defined by $\pi(g) = gN$ is a surjective group homomorphism with kernel N

Properties of quotient groups

- The order of the quotient group G/N is equal to the index of N in G , denoted $[G:N]$, which is the number of distinct left (or right) cosets of N in G
- The quotient group G/N is abelian if and only if N contains the commutator subgroup $[G, G]$
- The quotient group $G/Z(G)$, where $Z(G)$ is the center of G , is isomorphic to the inner automorphism group $\text{Inn}(G)$ of G
- The quotient group $G/[G, G]$, where $[G, G]$ is the commutator subgroup of G , is isomorphic to the abelianization of G , which is the largest abelian quotient of G

Isomorphism theorem for problem-solving

First isomorphism theorem

- The first isomorphism theorem states that if $\varphi: G \rightarrow H$ is a group homomorphism, then the kernel of φ , denoted $\ker(\varphi)$, is a normal subgroup of G , and the image of φ , denoted $\text{im}(\varphi)$, is isomorphic to the quotient group $G/\ker(\varphi)$
- The first isomorphism theorem can be used to prove that any surjective homomorphism $\varphi: G \rightarrow H$ induces an isomorphism between $G/\ker(\varphi)$ and H
- The first isomorphism theorem can be applied to prove the fundamental theorem of homomorphisms, which states that for any group homomorphism $\varphi: G \rightarrow H$, there exists a unique group homomorphism $\psi: G/\ker(\varphi) \rightarrow H$ such that $\varphi = \psi \circ \pi$, where π is the canonical projection map

Applications of the first isomorphism theorem

- The first isomorphism theorem can be used to classify groups up to isomorphism by studying their quotient groups
- The first isomorphism theorem can be applied to solve problems involving the structure of groups and their homomorphisms

- The first isomorphism theorem can be used to prove the existence of certain subgroups or quotient groups (e.g., the existence of the abelianization of a group)
- The first isomorphism theorem can be used to establish relationships between different groups and their properties (e.g., the relationship between the center and the inner automorphism group of a group)

Theorems involving normal subgroups and quotient groups

Theorems for proving normality

- To prove that a subgroup H of a group G is normal, it suffices to show that $gHg^{-1} \subseteq H$ for all g in G , or equivalently, that $gHg^{-1} = H$ for all g in G
- The normalizer of a subgroup H in G , denoted $N_G(H)$, is the largest subgroup of G in which H is normal
- A subgroup H of a group G is normal if and only if its left cosets and right cosets coincide, i.e., $gH = Hg$ for all g in G

Correspondence and isomorphism theorems

- The correspondence theorem establishes a bijection between the subgroups of G containing a normal subgroup N and the subgroups of the quotient group G/N
- The third isomorphism theorem states that if H and N are normal subgroups of G with $N \subseteq H$, then $(G/N)/(H/N) \cong G/H$, where H/N is a normal subgroup of G/N
- The second isomorphism theorem (or diamond isomorphism theorem) states that if H and K are subgroups of G with K normal, then HK is a subgroup of G , $H \cap K$ is a normal subgroup of H , and $H/(H \cap K) \cong HK/K$

6.3 The Sylow theorems and their applications

The Sylow theorems are game-changers in group theory. They tell us about special subgroups called Sylow p -subgroups in finite groups. These theorems help us understand group structure and are key to classifying finite groups.

Knowing the Sylow theorems is crucial for tackling problems in group theory. They're like a Swiss Army knife for group analysis, helping us figure out subgroup existence, count subgroups, and even prove some groups aren't simple. Super handy stuff!

Sylow theorems for finite groups

Introduction to Sylow theorems

- The Sylow theorems are a set of three powerful theorems in group theory that provide information about the existence and properties of certain subgroups of a finite group, known as Sylow p -subgroups
- These theorems are named after the Norwegian mathematician Ludwig Sylow, who proved them in 1872
- The Sylow theorems are essential tools in the study of finite groups, as they allow for the classification of groups of small order and the determination of various structural properties of finite groups
- The theorems are particularly useful in the study of finite simple groups, which are the building blocks of all finite groups

Statements of the Sylow theorems

- The first Sylow theorem states that if G is a finite group and p is a prime number dividing the order of G , then G contains a Sylow p -subgroup, which is a subgroup of order p^k , where p^k is the highest power of p dividing the order of G
- The second Sylow theorem states that all Sylow p -subgroups of a finite group G are conjugate to each other, meaning that if P and Q are Sylow p -subgroups of G , then there exists an element g in G such that $gPg^{-1} = Q$
- The third Sylow theorem states that the number of Sylow p -subgroups of a finite group G , denoted by n_p , satisfies the following conditions:
 - n_p divides the order of G
 - n_p is congruent to 1 modulo p
 - $n_p = [G : N_G(P)]$, where $N_G(P)$ is the normalizer of a Sylow p -subgroup P in G

Existence and number of Sylow p -subgroups

Determining the existence of Sylow p -subgroups

- To determine the existence of a Sylow p -subgroup in a finite group G , one needs to check if the order of G is divisible by a prime number p
- If the order of G is divisible by p , then by the first Sylow theorem, G contains at least one Sylow p -subgroup
- For example, if G is a group of order 60, then G has Sylow 2-subgroups (order 4), Sylow 3-subgroups (order 3), and Sylow 5-subgroups (order 5)

Calculating the number of Sylow p -subgroups

- The number of Sylow p -subgroups, denoted by n_p , can be determined using the third Sylow theorem
- n_p must divide the order of G and be congruent to 1 modulo p
- The number of Sylow p -subgroups can also be calculated using the formula $n_p = [G : N_G(P)]$, where $N_G(P)$ is the normalizer of a Sylow p -subgroup P in G
- In some cases, the number of Sylow p -subgroups can be uniquely determined based on the order of the group and the prime number p
- For example, if p does not divide $[G : N_G(P)]$, then there is only one Sylow p -subgroup
- If a group G has a unique Sylow p -subgroup for some prime p , then this subgroup must be normal in G

Classifying groups of small order

Groups of prime power order

- For groups of order p^n , where p is a prime number, there is only one Sylow p -subgroup, which is the group itself
- This implies that groups of prime power order are always solvable

- Examples of groups of prime power order include the cyclic group of order p ($\mathbb{Z}_p$) and the dihedral group of order 2^n ($D_{\{2^n\}}$)

Groups of order pq

- For groups of order pq , where p and q are distinct primes, the Sylow theorems can be used to show that such groups are either cyclic or isomorphic to a semidirect product of cyclic groups
- If p does not divide $q-1$, then the group must be cyclic ($\mathbb{Z}_{pq}$)
- If p divides $q-1$, then the group is isomorphic to a semidirect product of $\mathbb{Z}_q$ and $\mathbb{Z}_p$ ($\mathbb{Z}_q \rtimes \mathbb{Z}_p$)
- Examples of groups of order pq include $\mathbb{Z}_{15}$ (cyclic) and $\mathbb{Z}_3 \rtimes \mathbb{Z}_5$ (non-cyclic)

Proving the non-simplicity of certain groups

- The Sylow theorems can be used to prove that certain groups of small order, such as groups of order 15 or 21, are not simple and must have normal subgroups
- For a group of order 15, the Sylow theorems imply that there is only one Sylow 3-subgroup and one Sylow 5-subgroup, both of which must be normal
- For a group of order 21, the Sylow theorems imply that there is only one Sylow 7-subgroup, which must be normal

Structure and properties of finite groups

Existence of normal subgroups

- The Sylow theorems can be used to prove the existence of normal subgroups in certain finite groups
- If a group G has a unique Sylow p -subgroup for some prime p , then this subgroup must be normal in G
- The existence of normal subgroups is essential in the study of group extensions and the classification of finite groups

Solvability of certain groups

- The Sylow theorems can be used to prove the solvability of certain groups, such as groups of prime power order or groups with a unique Sylow p -subgroup for some prime p
- A group G is solvable if it has a series of subgroups $1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$, where each quotient G_{i+1}/G_i is abelian
- The solvability of a group has important implications for its structure and representation theory

Orders of elements in finite groups

- The Sylow theorems can be used to determine the possible orders of elements in a finite group
- If G is a finite group and p is a prime dividing the order of G , then G must contain elements of order p
- The existence of elements of certain orders can provide information about the structure and properties of the group, such as its center or its conjugacy classes

Applications to finite simple groups

- The Sylow theorems are particularly useful in the study of finite simple groups, as they provide information about the possible orders and structures of such groups, which can be used to classify them or prove their uniqueness
- For example, the Sylow theorems can be used to prove that the alternating group A_5 is the only non-abelian simple group of order 60
- The classification of finite simple groups, which was completed in the early 1980s, relies heavily on the Sylow theorems and their applications to the structure and properties of finite groups

Unit 7 – Galois Groups and Galois Extensions

7.1 Galois groups of polynomials and field extensions

Galois groups are key to understanding polynomial roots and field extensions. They reveal symmetries in algebraic structures, showing how roots are related and which field elements stay fixed under certain transformations. This concept bridges abstract algebra and number theory.

The Fundamental Theorem of Galois Theory connects subgroups of Galois groups to intermediate fields. This link helps classify field extensions, determine solvability of equations, and uncover hidden relationships between different mathematical objects. It's a cornerstone of modern algebra.

Galois groups of polynomials and field extensions

Definition and properties of Galois groups

- The Galois group of a polynomial $f(x)$ over a field F , denoted $Gal(f/F)$, is the group of automorphisms of the splitting field of $f(x)$ that fix the base field F
- The Galois group of a field extension L/K , denoted $Gal(L/K)$, is the group of automorphisms of L that fix the base field K
- The elements of the Galois group permute the roots of the polynomial while preserving the field operations and fixing the elements of the base field
- For example, if $f(x) = x^3 - 2$ over $\mathbb{Q}$, the Galois group permutes the roots $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, where ω is a primitive cube root of unity
- The Galois group is a subgroup of the symmetric group on the roots of the polynomial
- In the previous example, the Galois group is isomorphic to S_3 , the symmetric group on three elements
- The order of the Galois group divides the degree of the splitting field extension over the base field

Examples and applications of Galois groups

- The Galois group of a quadratic polynomial $ax^2 + bx + c$ over $\mathbb{Q}$ is:
 - Trivial if the discriminant $b^2 - 4ac$ is a perfect square in $\mathbb{Q}$
 - Isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if the discriminant is not a perfect square
- The Galois group of a cyclotomic extension $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of integers modulo n
- For example, the Galois group of $\mathbb{Q}(\zeta_5)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$
- The Galois group of a finite field extension is always a finite group, and its order is equal to the degree of the extension
- For instance, the Galois group of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is a cyclic group of order n

Determining Galois groups

Techniques for finding Galois groups

- To find the Galois group of a polynomial, first determine its splitting field by finding all the roots of the polynomial
- Identify the automorphisms of the splitting field that fix the base field, which form the Galois group
- These automorphisms can be found by examining the action on the roots of the polynomial or on the generators of the field extension
- For simple extensions, the Galois group can be determined by examining the minimal polynomial of the extension
- If the minimal polynomial has distinct roots, the Galois group is a subgroup of the symmetric group on the roots
- Determine the Galois group by examining the action of automorphisms on the roots of the polynomial or on the generators of the field extension

Examples of determining Galois groups

- The Galois group of $x^4 - 2$ over $\mathbb{Q}$ is the dihedral group of order 8, D_4
- The splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$, and the automorphisms are determined by their action on $\sqrt[4]{2}$ and i
- The Galois group of $x^3 - 3x + 1$ over $\mathbb{Q}$ is the symmetric group S_3
- The polynomial has three distinct real roots, and any permutation of these roots defines an automorphism of the splitting field
- The Galois group of $x^p - x - 1$ over $\mathbb{F}_p$ is a cyclic group of order p
- The polynomial is irreducible over $\mathbb{F}_p$, and its splitting field is a degree p extension of $\mathbb{F}_p$

Galois groups and splitting fields

Relationship between Galois groups and splitting fields

- The splitting field of a polynomial $f(x)$ over a field F is the smallest field extension of F containing all the roots of $f(x)$
- The Galois group of a polynomial acts transitively on the roots of the polynomial in the splitting field
- This means that for any two roots α and β , there exists an automorphism in the Galois group that maps α to β
- The fixed field of the Galois group (elements unchanged by all automorphisms in the group) is precisely the base field

Galois correspondence

- The Galois correspondence establishes a one-to-one correspondence between the subgroups of the Galois group and the intermediate fields between the base field and the splitting field

- The correspondence reverses inclusions: if $H \leq G$ are subgroups of the Galois group, then their fixed fields satisfy $\text{Fix}(G) \subseteq \text{Fix}(H)$
- For example, if L/K is a Galois extension with Galois group G , and H is a subgroup of G , then the fixed field L^H is an intermediate field between K and L
- The Galois correspondence allows the study of field extensions by examining the subgroup structure of their Galois groups

Fundamental Theorem of Galois Theory

Statement and implications of the theorem

- The Fundamental Theorem of Galois Theory states that for a Galois extension L/K with Galois group G , there is a one-to-one correspondence between the subgroups of G and the intermediate fields between K and L
- The correspondence associates each subgroup H of G with its fixed field $L^H = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in H\}$
- The correspondence associates each intermediate field M with its automorphism group $\text{Aut}(L/M) = \{\sigma \in G : \sigma(x) = x \text{ for all } x \in M\}$
- The Fundamental Theorem allows the classification of all intermediate fields of a Galois extension using the subgroup structure of the Galois group
- The degree of an intermediate field over the base field equals the index of its corresponding subgroup in the Galois group

Galois extensions and the Fundamental Theorem

- An extension L/K is Galois if and only if it is normal (every irreducible polynomial in $K[x]$ that has a root in L splits completely in L) and separable (every element in L is separable over K)
- For example, the splitting field of a separable polynomial is always a Galois extension
- The Galois group of a finite Galois extension is always isomorphic to a subgroup of the symmetric group on the roots of a defining polynomial for the extension
- This follows from the fact that the Galois group permutes the roots of the defining polynomial
- The Fundamental Theorem provides a powerful tool for studying the structure of Galois extensions and their intermediate fields

7.2 Galois extensions and their properties

Galois extensions are a key concept in field theory, combining normality and separability. They're crucial for understanding the relationship between field extensions and their automorphism groups, forming the foundation of Galois theory.

The Fundamental Theorem of Galois Theory establishes a one-to-one correspondence between intermediate fields of a Galois extension and subgroups of its Galois group. This powerful result connects algebra and number theory, revealing deep insights into field structures.

Galois Extensions: Definition and Properties

Definition and Examples

- A Galois extension is a field extension L/K such that L is the splitting field of a separable polynomial $f(x) \in K[x]$
- Examples of Galois extensions:
 - $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$
 - $\mathbb{Q}(i)/\mathbb{Q}$
 - The splitting field of $x^n - 1$ over $\mathbb{Q}$ for any positive integer n
- Examples of non-Galois extensions:
 - $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal
 - $\mathbb{F}_p(t^p)/\mathbb{F}_p(t)$ is not separable, where $\mathbb{F}_p$ is the field with p elements and t is transcendental over $\mathbb{F}_p$

Equivalent Characterizations

- For a field extension L/K , the following conditions are equivalent to L/K being Galois:
 - L/K is a normal extension (every irreducible polynomial in $K[x]$ that has a root in L splits completely in $L[x]$) and a separable extension (every element of L is separable over K)
 - L is the splitting field of a separable polynomial $f(x) \in K[x]$
 - L is the fixed field of $\text{Aut}(L/K)$, the group of automorphisms of L that fix K

Equivalence of Galois Extension Characterizations

Fundamental Theorem of Galois Theory

- The Fundamental Theorem of Galois Theory establishes the equivalence of the three characterizations of Galois extensions:
 1. L/K is a normal and separable extension
 2. L is the splitting field of a separable polynomial $f(x) \in K[x]$
 3. L is the fixed field of $\text{Aut}(L/K)$

Proving the Equivalence

- To prove $(1) \Rightarrow (2)$:
 - Construct a separable polynomial $f(x) \in K[x]$ by taking the product of the minimal polynomials of a basis for L over K
 - Show that L is the splitting field of $f(x)$
- To prove $(2) \Rightarrow (3)$:
 - Use the fact that automorphisms permute roots of polynomials to show that L is fixed by $\text{Aut}(L/K)$
- To prove $(3) \Rightarrow (1)$:

- Use the properties of the fixed field and the fact that the elements of L are the roots of polynomials in $K[x]$ to show that L/K is normal and separable

Properties of Galois Extensions: Normality vs Separability

Normality

- A normal extension L/K is a field extension such that every irreducible polynomial in $K[x]$ that has a root in L splits completely in $L[x]$
- Examples of normal extensions:
 - $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$
 - The splitting field of any polynomial over a field

Separability

- A separable extension L/K is a field extension such that every element of L is separable over K (i.e., its minimal polynomial over K has distinct roots)
- In characteristic 0, every extension is separable
- In characteristic $p > 0$, an extension L/K is separable if and only if L is linearly disjoint from $K^{(1/p)}$ over K
- Examples of separable extensions:
 - $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$
 - $\mathbb{F}_p(t)/\mathbb{F}_p$, where t is transcendental over $\mathbb{F}_p$

Properties of Galois Extensions

- The composition of Galois extensions is Galois. If L/K and M/L are Galois, then M/K is Galois
- The Galois group $\text{Aut}(L/K)$ of a Galois extension L/K is a finite group whose order is equal to the degree $[L : K]$ of the extension

Galois Correspondence: Subgroups vs Intermediate Fields

Fundamental Theorem of Galois Theory

- The Fundamental Theorem of Galois Theory establishes a one-to-one correspondence between the intermediate fields of a Galois extension L/K and the subgroups of the Galois group $\text{Aut}(L/K)$

Correspondence between Subgroups and Intermediate Fields

- For each intermediate field M ($K \subseteq M \subseteq L$), the corresponding subgroup is $\text{Aut}(L/M)$, the group of automorphisms of L that fix M
- For each subgroup $H \subseteq \text{Aut}(L/K)$, the corresponding intermediate field is the fixed field $L^H = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in H\}$

Properties of the Correspondence

- The correspondence reverses inclusions:

- If $M_1 \subseteq M_2$ are intermediate fields, then $\text{Aut}(L/M_2) \subseteq \text{Aut}(L/M_1)$ as subgroups of $\text{Aut}(L/K)$
- The degree $[L : M]$ of an intermediate field M is equal to the index $[\text{Aut}(L/K) : \text{Aut}(L/M)]$ of its corresponding subgroup in the Galois group
- Normal subgroups of $\text{Aut}(L/K)$ correspond to Galois extensions M/K within the extension L/K

7.3 Computing Galois groups

Computing Galois groups is a crucial skill in Galois theory. It involves finding the automorphisms of a splitting field that fix the base field. This process helps us understand the structure of field extensions and their symmetries.

Galois groups connect polynomials to field theory and group theory. By computing them, we can determine if equations are solvable by radicals and uncover deep relationships between different mathematical structures. It's a powerful tool for solving algebraic problems.

Galois Groups of Polynomials

Splitting Fields and Galois Groups

- The splitting field of a polynomial $f(x)$ over a field F is the smallest field extension of F that contains all the roots of $f(x)$
- The Galois group of $f(x)$ over F , denoted $\text{Gal}(f/F)$ or $\text{Gal}(E/F)$ where E is the splitting field, is the group of automorphisms of the splitting field that fix the base field F
- Example: For the polynomial $f(x) = x^3 - 2$ over $\mathbb{Q}$, the splitting field is $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$, where ω is a primitive third root of unity
- The Galois group is a subgroup of the symmetric group S_n , where n is the degree of $f(x)$

Computing Galois Groups using Splitting Fields

- To compute the Galois group, first find the splitting field by adjoining the roots of $f(x)$ to the base field F
- Example: For $f(x) = x^4 - 2$ over $\mathbb{Q}$, adjoin $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$, and $-i\sqrt[4]{2}$ to $\mathbb{Q}$ to obtain the splitting field
- Determine the automorphisms of the splitting field that fix F
- These automorphisms can be found by examining the permutations of the roots that preserve the coefficients of $f(x)$
- Example: For $f(x) = x^4 - 2$, the automorphisms are generated by $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$ and $\sqrt[4]{2} \mapsto -\sqrt[4]{2}$, forming the dihedral group D_4

Galois Groups of Field Extensions

Minimal Polynomials and Galois Groups

- The minimal polynomial of an element α over a field F is the monic polynomial of lowest degree with coefficients in F that has α as a root

- If $E = F(\alpha)$ is a field extension, the minimal polynomial of α over F can be used to determine the Galois group $Gal(E/F)$
- The degree of the minimal polynomial equals the degree of the field extension $[E : F]$
- The roots of the minimal polynomial are the conjugates of α under the action of the Galois group
- By examining the permutations of the roots that preserve the coefficients of the minimal polynomial, the Galois group can be determined
- Example: For $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$, the minimal polynomial is $x^4 - 10x^2 + 1$, and the Galois group is the Klein four-group V_4

Galois Extensions and Fixed Fields

- An extension E/F is Galois if and only if F is the fixed field of $Gal(E/F)$
- The fixed field of a subgroup H of $Gal(E/F)$ is the set of elements in E that are fixed by every automorphism in H
- Properties of field extensions (such as normality and separability) and their corresponding subgroups can be used to compute Galois groups
- Example: If E/F is a Galois extension and $[E : F] = p$ is prime, then $Gal(E/F)$ is cyclic of order p

Galois Group Computation Techniques

Fundamental Theorem of Galois Theory

- The Fundamental Theorem of Galois Theory establishes a one-to-one correspondence between the intermediate fields of a Galois extension and the subgroups of its Galois group
- For a Galois extension E/F , there is a bijection between the intermediate fields K (with $F \subseteq K \subseteq E$) and the subgroups H of $Gal(E/F)$
- This correspondence allows for the computation of Galois groups by examining the lattice of intermediate fields
- Example: For the splitting field of $x^4 - 2$ over $\mathbb{Q}$, the lattice of intermediate fields corresponds to the subgroup lattice of D_4

Galois Correspondence

- The Galois correspondence relates the lattice of intermediate fields to the lattice of subgroups of the Galois group
- If K is an intermediate field, then $Gal(E/K)$ is a subgroup of $Gal(E/F)$
- If H is a subgroup of $Gal(E/F)$, then the fixed field of H is an intermediate field
- This correspondence can be used to determine the Galois group by analyzing the intermediate fields and their corresponding subgroups
- Example: For the splitting field of $x^3 - 2$ over $\mathbb{Q}$, the intermediate fields $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\omega)$ correspond to subgroups of order 2 and 3, respectively, in the Galois group S_3

Degree vs Order in Galois Theory

Degree of Splitting Field and Order of Galois Group

- The degree of the splitting field E over the base field F , denoted $[E : F]$, is equal to the order (number of elements) of the Galois group $\text{Gal}(E/F)$
- This relationship is a consequence of the Fundamental Theorem of Galois Theory
- If $f(x)$ is a separable polynomial of degree n over F , then the splitting field E has degree dividing $n!$ over F
- Example: For $f(x) = x^3 - 2$ over $\mathbb{Q}$, the splitting field has degree 6, which divides $3! = 6$

Galois Groups as Subgroups of Symmetric Groups

- The Galois group of a separable polynomial $f(x)$ is a subgroup of the symmetric group S_n , and its order divides $n!$
- Understanding this relationship can help in determining the possible Galois groups for a given polynomial or field extension
- Example: For a separable quartic polynomial, the Galois group must be a subgroup of S_4 , which has order dividing $4! = 24$, narrowing down the possible Galois groups to S_4 , A_4 , D_4 , V_4 , or C_4

Unit 8 – The Fundamental Theorem of Galois Theory

8.1 Statement and proof of the Fundamental Theorem

The Fundamental Theorem of Galois Theory is a game-changer in field theory. It links intermediate fields of a Galois extension to subgroups of its Galois group, creating a powerful tool for studying field extensions and their automorphisms.

This theorem simplifies finding intermediate fields and enables constructing extensions with specific properties. It bridges algebra and group theory, allowing us to solve problems in one realm by tackling them in the other.

Fundamental Theorem of Galois Theory

Statement and Implications

- The Fundamental Theorem of Galois Theory establishes a one-to-one correspondence between the intermediate fields of a Galois extension and the subgroups of its Galois group
- If L/K is a Galois extension with Galois group G , then there is a bijection between the set of intermediate fields F (with $K \subseteq F \subseteq L$) and the set of subgroups H of G
- The bijection maps each intermediate field F to the subgroup $\text{Gal}(L/F)$ of G , and each subgroup H of G to the fixed field L^H
- The Fundamental Theorem implies that the lattice of intermediate fields is isomorphic to the lattice of subgroups of the Galois group, with the order reversed
- The degree of an intermediate field extension F/K is equal to the index $[G : \text{Gal}(L/F)]$ of the corresponding subgroup in the Galois group

Applications and Significance

- The Fundamental Theorem provides a powerful tool for studying the structure of field extensions and their automorphism groups
- It allows us to determine the degree of an extension by examining the corresponding subgroup of the Galois group (cyclotomic extensions, splitting fields of polynomials)
- The theorem simplifies the problem of finding all intermediate fields of a Galois extension to the problem of finding all subgroups of its Galois group
- It enables the construction of field extensions with desired properties by specifying the structure of the Galois group (constructing regular polygons, solving polynomial equations)
- The Fundamental Theorem has applications in various branches of mathematics, including algebraic number theory, algebraic geometry, and the theory of equations

Proving the Fundamental Theorem

Fixed Fields and Subgroups

- Step 1: Prove that if H is a subgroup of the Galois group G , then the fixed field L^H is an intermediate field of the extension L/K
- Step 2: Show that if F is an intermediate field of L/K , then the Galois group $\text{Gal}(L/F)$ is a subgroup of G
- Step 3: Establish that the fixed field of $\text{Gal}(L/F)$ is F itself, i.e., $(L^{\text{Gal}(L/F)}) = F$
- Step 4: Prove that the Galois group of the fixed field L^H is H itself, i.e., $\text{Gal}(L/L^H) = H$

Bijection and Degree Relation

- Step 5: Demonstrate that the correspondence between intermediate fields and subgroups of the Galois group is a bijection
- Show that the maps $F \mapsto \text{Gal}(L/F)$ and $H \mapsto L^H$ are inverses of each other
- Prove that the composition of these maps in either order yields the identity map (on intermediate fields or subgroups)
- Step 6: Prove that the degree of an intermediate field extension F/K is equal to the index $[G : \text{Gal}(L/F)]$ of the corresponding subgroup in the Galois group
- Use the fact that $[L : K] = [L : F][F : K]$ and $[L : K] = |G|$
- Apply Lagrange's theorem to relate the index of the subgroup to the degree of the extension

Significance of the Fundamental Theorem

Connecting Algebra and Group Theory

- The Fundamental Theorem provides a deep connection between the algebraic structure of field extensions and the group-theoretic structure of their automorphism groups
- It allows us to study the properties of field extensions by examining the corresponding subgroups of the Galois group, and vice versa
- The theorem establishes a dictionary between field-theoretic and group-theoretic concepts (intermediate fields $\leftrightarrow$ subgroups, degree $\leftrightarrow$ index, normal extensions $\leftrightarrow$ normal subgroups)
- It enables the transfer of problems and techniques between the realms of field theory and group theory (solubility by radicals $\leftrightarrow$ solvable groups)

Simplifying Problems and Computations

- The Fundamental Theorem simplifies the problem of finding all intermediate fields of a Galois extension to the problem of finding all subgroups of its Galois group
- It allows us to determine the degree of an intermediate field extension by computing the index of the corresponding subgroup in the Galois group
- The theorem provides a method for constructing field extensions with specific properties by controlling the structure of the Galois group (constructing regular polygons, solving polynomial equations)

- It enables the computation of Galois groups and the study of their structure using techniques from group theory (Sylow theorems, group actions)

Field Extension Degree vs Galois Group Order

Equality for Galois Extensions

- For a Galois extension L/K with Galois group G , the degree of the extension $[L : K]$ is equal to the order of the Galois group $|G|$
- This relationship is a consequence of the Fundamental Theorem of Galois Theory
- It follows from the fact that the fixed field of the entire Galois group G is the base field K , i.e., $L^G = K$
- The equality $[L : K] = |G|$ holds for any Galois extension, regardless of its specific structure or properties

Subgroup Index and Intermediate Field Degree

- If F is an intermediate field of L/K , then the degree of the extension F/K is equal to the index $[G : \text{Gal}(L/F)]$ of the corresponding subgroup in the Galois group
- The degree of the extension L/F is equal to the order of the subgroup $\text{Gal}(L/F)$
- These relationships follow from the Fundamental Theorem and the multiplicativity of field extension degrees, i.e., $[L : K] = [L : F][F : K]$
- The relationship between subgroup index and intermediate field degree allows us to compute the degree of an extension by studying its Galois group (using Lagrange's theorem, group actions)

8.2 Correspondence between subfields and subgroups

The Galois correspondence is a powerful tool that connects subfields and subgroups in field extensions. It establishes a one-to-one relationship between intermediate fields of a Galois extension and subgroups of its Galois group, preserving inclusion and degree.

This correspondence forms the heart of the Fundamental Theorem of Galois Theory. It allows us to study field extensions by examining group structures, and vice versa, providing deep insights into the algebraic relationships between fields and their automorphisms.

Galois Correspondence

Establishing the One-to-One Correspondence

- The Fundamental Theorem of Galois Theory establishes a one-to-one correspondence between the intermediate fields of a Galois extension and the subgroups of its Galois group
- For a Galois extension L/K with Galois group G , there exists a bijective map $\varphi : \{\text{intermediate fields of } L/K\} \rightarrow \{\text{subgroups of } G\}$ given by $\varphi(E) = \text{Gal}(L/E)$ for each intermediate field E
- The map φ associates each intermediate field E with its corresponding subgroup $\text{Gal}(L/E)$ of the Galois group G
- The inverse map $\varphi^{(-1)} : \{\text{subgroups of } G\} \rightarrow \{\text{intermediate fields of } L/K\}$ is given by $\varphi^{(-1)}(H) = L^H$ (the fixed field of H) for each subgroup H of G

- The inverse map $\varphi^{(-1)}$ associates each subgroup H of the Galois group G with its corresponding fixed field L^H

Preservation of Inclusion and Degree

- The correspondence preserves inclusion: if $E_1 \subseteq E_2$ are intermediate fields, then $\varphi(E_2) \subseteq \varphi(E_1)$ as subgroups of G
- If one intermediate field is contained in another, their corresponding subgroups have the reverse inclusion relation
- Similarly, if $H_1 \subseteq H_2$ are subgroups of G , then $\varphi^{(-1)}(H_1) \supseteq \varphi^{(-1)}(H_2)$ as intermediate fields
- If one subgroup is contained in another, their corresponding intermediate fields have the reverse inclusion relation
- The degree of an intermediate field E over K is equal to the index of its corresponding subgroup $\varphi(E)$ in G : $[E : K] = [G : \varphi(E)]$
- This relation connects the degree of an intermediate field with the index of its corresponding subgroup in the Galois group

Intermediate Fields and Subgroups

Determining the Galois Correspondence

- To find the Galois correspondence, first determine if the given field extension L/K is Galois by checking if it is both normal and separable
- A field extension is normal if every irreducible polynomial in $K[x]$ that has a root in L splits completely in $L[x]$
- A field extension is separable if every element of L is separable over K , meaning its minimal polynomial over K has distinct roots
- Compute the Galois group $G = \text{Gal}(L/K)$ by finding all the K -automorphisms of L
- A K -automorphism of L is a field automorphism of L that fixes every element of K
- Identify all the intermediate fields E of L/K and all the subgroups H of G
- Intermediate fields are fields that lie between K and L in the field extension L/K
- Subgroups are non-empty subsets of G that are closed under the group operation and taking inverses

Finding Corresponding Subgroups and Intermediate Fields

- For each intermediate field E , find its corresponding subgroup $\varphi(E) = \text{Gal}(L/E)$ by determining the K -automorphisms of L that fix E
- The subgroup $\text{Gal}(L/E)$ consists of all K -automorphisms of L that map elements of E to themselves
- For each subgroup H of G , find its corresponding intermediate field $\varphi^{(-1)}(H) = L^H$ by computing the fixed field of H
- The fixed field L^H is the set of all elements in L that are fixed by every automorphism in H

- Verify that the correspondence preserves inclusion and that $[E : K] = [G : \varphi(E)]$ for each pair of corresponding intermediate fields and subgroups
- This step ensures that the Galois correspondence is indeed a one-to-one correspondence with the desired properties

Lattice Structure of Galois Correspondence

Isomorphic Lattices of Intermediate Fields and Subgroups

- The Galois correspondence preserves the lattice structure of intermediate fields and subgroups, forming two isomorphic lattices
- A lattice is a partially ordered set in which every pair of elements has a unique least upper bound (join) and a unique greatest lower bound (meet)
- The lattice of intermediate fields is ordered by inclusion ($\subseteq$), with the join operation being the compositum of fields ($\vee$) and the meet operation being the intersection of fields ($\wedge$)
- The compositum $E_1 \vee E_2$ is the smallest field containing both E_1 and E_2
- The intersection $E_1 \wedge E_2$ is the largest field contained in both E_1 and E_2
- The lattice of subgroups is ordered by inclusion ($\subseteq$), with the join operation being the generated subgroup ($\langle \rangle$) and the meet operation being the intersection of subgroups ($\cap$)
- The generated subgroup $\langle H_1, H_2 \rangle$ is the smallest subgroup containing both H_1 and H_2
- The intersection $H_1 \cap H_2$ is the largest subgroup contained in both H_1 and H_2

Reversal of Order and Extremal Elements

- The Galois correspondence reverses the order of the lattices: if $E_1 \subseteq E_2$ are intermediate fields, then $\varphi(E_2) \subseteq \varphi(E_1)$ as subgroups, and if $H_1 \subseteq H_2$ are subgroups, then $\varphi^{(-1)}(H_1) \supseteq \varphi^{(-1)}(H_2)$ as intermediate fields
- The inclusion relation between intermediate fields and subgroups is reversed under the Galois correspondence
- The minimal element of the intermediate fields lattice is K , corresponding to the maximal element G of the subgroups lattice
- The base field K is the smallest intermediate field, and its corresponding subgroup is the entire Galois group G
- The maximal element of the intermediate fields lattice is L , corresponding to the minimal element $\{1\}$ of the subgroups lattice
- The Galois extension L is the largest intermediate field, and its corresponding subgroup is the trivial subgroup $\{1\}$ consisting only of the identity element

Applications of Galois Correspondence

Determining Number and Degree of Intermediate Fields

- Use the Galois correspondence to determine the number and degree of intermediate fields for a given Galois extension based on the subgroups of its Galois group

- The number of intermediate fields is equal to the number of subgroups of the Galois group
- The degree of each intermediate field over the base field is equal to the index of its corresponding subgroup in the Galois group

Proving the Fundamental Theorem of Algebra

- Utilize the Galois correspondence to prove the Fundamental Theorem of Algebra by showing that the splitting field of a separable polynomial is a Galois extension
- The Fundamental Theorem of Algebra states that every non-constant polynomial with complex coefficients has a complex root
- The splitting field of a polynomial is the smallest field extension in which the polynomial splits into linear factors
- A separable polynomial is a polynomial whose roots are distinct

Constructing Field Extensions with Prescribed Galois Groups

- Apply the Galois correspondence to construct examples of field extensions with prescribed Galois groups, such as cyclic or symmetric groups
- A cyclic group is a group generated by a single element
- The symmetric group S_n is the group of all permutations of n elements

Determining Solvability by Radicals

- Employ the Galois correspondence to determine the solvability of polynomial equations by radicals based on the solvability of their Galois groups
- A polynomial equation is solvable by radicals if its roots can be expressed using arithmetic operations and taking roots (square roots, cube roots, etc.)
- A group is solvable if it has a composition series with abelian factors

Studying the Absolute Galois Group

- Use the Galois correspondence to study the structure of the absolute Galois group $Gal(\bar{K}/K)$ for a given field K , where $\bar{K}$ is its algebraic closure
- The algebraic closure of a field K is the smallest algebraically closed field containing K
- The absolute Galois group of K is the Galois group of its algebraic closure over K , which encodes important information about the field K

8.3 Applications of the Fundamental Theorem

The Fundamental Theorem of Galois Theory links field extensions to group theory, revealing deep connections in algebra. This powerful tool helps us understand polynomial solvability, finite fields, and geometric constructions.

Applications of the theorem are far-reaching. We can determine which equations are solvable by radicals, analyze the structure of finite fields, and even prove the impossibility of certain geometric constructions using only a compass and straightedge.

Solvability of Polynomial Equations

Fundamental Theorem and Solvability

- The Fundamental Theorem of Galois Theory establishes a correspondence between subfields of a splitting field and subgroups of the Galois group
- A polynomial equation is solvable by radicals if and only if its Galois group is solvable
- Solvable means the group has a composition series with abelian factor groups
- The Galois group of a polynomial is solvable if and only if the polynomial can be solved by radicals (using addition, subtraction, multiplication, division, and taking roots)

Insolvability of Higher Degree Equations

- The general polynomial equation of degree 5 or higher is not solvable by radicals
- This is demonstrated by the insolvability of the quintic equation (fifth-degree polynomial)
- Galois theory proves that the Galois group of a general quintic is not solvable, thus the equation cannot be solved by radicals
- Examples of insolvable quintics include $x^5 - 4x + 2 = 0$ and $x^5 + 3x + 1 = 0$

Constructing Splitting Fields and Galois Groups

Splitting Fields

- A splitting field of a polynomial $f(x)$ over a field F is the smallest field extension of F that contains all the roots of $f(x)$
- To construct a splitting field, adjoin the roots of the polynomial to the base field successively until all roots are contained in the extension
- Example: For $f(x) = x^3 - 2$ over $\mathbb{Q}$, adjoin $\sqrt[3]{2}$ to obtain the splitting field $\mathbb{Q}(\sqrt[3]{2})$

Galois Groups

- The Galois group of a polynomial $f(x)$ over a field F is the group of automorphisms of the splitting field of $f(x)$ that fix F
- The Galois group can be determined by examining the permutations of the roots that preserve the relationships between the roots and the coefficients of the polynomial
- Example: For $f(x) = x^4 - 2$ over $\mathbb{Q}$, the Galois group is the dihedral group D_4 , generated by the permutations (1234) and (13)
- The Fundamental Theorem of Galois Theory allows for the identification of intermediate fields and their corresponding subgroups of the Galois group

Structure of Finite Fields

Properties of Finite Fields

- Finite fields, also known as Galois fields, are fields with a finite number of elements

- The order of a finite field is always a prime power, denoted as $GF(p^n)$, where p is a prime number and n is a positive integer
- Every finite field is the splitting field of the polynomial $x^{p^n} - x$ over its prime subfield $GF(p)$

Galois Groups and Subfields of Finite Fields

- The Galois group of a finite field $GF(p^n)$ over its prime subfield $GF(p)$ is cyclic and generated by the Frobenius automorphism
- The subfields of a finite field correspond to the subgroups of its Galois group, which are also cyclic and of order dividing n
- Example: $GF(2^6)$ has subfields $GF(2^3)$ and $GF(2^2)$ corresponding to subgroups of orders 2 and 3 in its Galois group
- The multiplicative group of a finite field is cyclic, and its generators are called primitive elements

Geometric Constructions and Field Extensions

Constructibility and Solvability

- Classical geometric construction problems involve constructing geometric figures using only a compass and straightedge
- The constructibility of a geometric figure is equivalent to the solvability of a corresponding polynomial equation by radicals
- A real number is constructible if and only if it lies in a field extension of the rationals obtained by a finite number of quadratic extensions
- Example: $\sqrt{2}$ is constructible because it lies in the quadratic extension $\mathbb{Q}(\sqrt{2})$

Famous Construction Problems

- The Fundamental Theorem of Galois Theory can be used to determine the minimum field extension required for a given construction
- Famous construction problems, such as doubling the cube, trisecting an angle, and squaring the circle, can be proven impossible using Galois theory
- Doubling the cube corresponds to solving the equation $x^3 = 2$, which is not solvable by radicals
- Trisecting an angle corresponds to solving the equation $4x^3 - 3x - \cos(\theta) = 0$, which is not solvable by radicals for general angles θ
- Squaring the circle corresponds to constructing a square with the same area as a given circle, which is equivalent to constructing π , a transcendental number not contained in any finite extension of the rationals

Unit 9 – Galois' Criterion for Radical Solvability

9.1 Solvable groups and radical extensions

Solvable groups are the key to understanding which polynomials can be solved by radicals. They have a special structure that allows us to break them down into simpler pieces, just like we can break down radical solutions into simpler steps.

Radical extensions are fields we build by adding roots to our starting field. They're closely tied to solvable groups. If a polynomial's Galois group is solvable, we can solve it using radicals. This connection is at the heart of Galois theory.

Solvable Groups and Their Properties

Definition and Subnormal Series

- A group G is solvable if it has a finite subnormal series $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_n = \{e\}$ such that each factor group G_i/G_{i+1} is abelian
- The subnormal series is a chain of subgroups, each normal in the previous one, ending with the trivial subgroup $\{e\}$
- The factor groups G_i/G_{i+1} are the quotient groups formed by adjacent subgroups in the series

Properties and Examples

- Every abelian group is solvable, as the subnormal series can be chosen to have length 1 (the group itself and the trivial subgroup)
- The class of solvable groups is closed under taking subgroups, quotient groups, and extensions
- If G is solvable and $H \leq G$, then H is solvable
- If G is solvable and $N \triangleleft G$, then G/N is solvable
- If $N \triangleleft G$, N and G/N are solvable, then G is solvable
- A finite group is solvable if and only if its composition series has factors that are all cyclic groups of prime order
- The symmetric group S_n is solvable for $n \leq 4$, but not for $n \geq 5$ (S_5 is the smallest non-solvable symmetric group)
- Solvable groups play a crucial role in the study of solutions to polynomial equations by radicals

Solvable Groups vs Radical Extensions

Solvability by Radicals

- A polynomial $f(x) \in F[x]$ is solvable by radicals if its splitting field over F can be obtained by successively adjoining roots of elements

- The roots of a polynomial solvable by radicals can be expressed using radicals, which are solutions to equations of the form $x^n = a$
- The Abel-Ruffini theorem states that for $n \geq 5$, there exist polynomials of degree n that are not solvable by radicals, as their Galois groups are not solvable

Galois Groups and Solvability

- The Galois group of a polynomial $f(x)$ over a field F is solvable if and only if $f(x)$ is solvable by radicals over F
- If a polynomial has a solvable Galois group, then its roots can be expressed using radicals
- The solvability of a polynomial's Galois group determines whether the polynomial can be solved by radicals

Constructing Radical Extensions

Definition and Process

- A radical extension of a field F is an extension field obtained by adjoining roots of elements of F
- To construct a radical extension for a polynomial $f(x) \in F[x]$: 1. Factor $f(x)$ into irreducible factors over F 2. For each irreducible factor $g(x)$, adjoin a root α of $g(x)$ to F to obtain a larger field $F(\alpha)$ 3. Repeat the process of factoring and adjoining roots until $f(x)$ splits completely in the resulting extension field
- The splitting field of $f(x)$ over F is the smallest field containing F and all the roots of $f(x)$, and it is a radical extension if $f(x)$ is solvable by radicals

Examples

- Consider the polynomial $f(x) = x^3 - 2$ over $\mathbb{Q}$
- $f(x)$ is irreducible over $\mathbb{Q}$, so adjoin a root $\sqrt[3]{2}$ to obtain $\mathbb{Q}(\sqrt[3]{2})$
- $f(x)$ splits completely in $\mathbb{Q}(\sqrt[3]{2})$, so this is the splitting field and a radical extension
- For the polynomial $g(x) = x^4 - 4x^2 + 2$ over $\mathbb{Q}$
- Factor $g(x) = (x^2 - 2)^2 - 2 = ((x^2 - 2) - \sqrt{2})((x^2 - 2) + \sqrt{2})$
- Adjoin $\sqrt{2}$ to $\mathbb{Q}$ to obtain $\mathbb{Q}(\sqrt{2})$
- Factor the quadratic terms in $\mathbb{Q}(\sqrt{2})$ and adjoin their roots to obtain the splitting field

Determining Solvability of Groups

Techniques and Criteria

- Check if the group is abelian. If so, it is solvable
- For a non-abelian group, try to find a subnormal series with abelian factor groups
- If the group is finite, examine its composition series and check if all factor groups are cyclic of prime order

- For the symmetric group S_n , it is solvable for $n \leq 4$ and not solvable for $n \geq 5$
- Use the closure properties of solvable groups:
- If a group is built from solvable groups using extensions, subgroups, or quotients, then it is solvable
- If a group has a non-solvable subgroup or quotient group, then the original group is not solvable

Examples

- The alternating group A_4 is solvable, as it has a subnormal series $A_4 \supseteq V_4 \supseteq \{e\}$ with abelian factor groups (V_4 is the Klein four-group)
- The dihedral group D_8 is solvable, as it has a subnormal series $D_8 \supseteq \langle r^2, s \rangle \supseteq \langle r^2 \rangle \supseteq \{e\}$ with abelian factor groups (r is rotation, s is reflection)
- The quaternion group Q_8 is not solvable, as it has a non-abelian subgroup isomorphic to Q_8 itself
- The general linear group $GL_2(\mathbb{Z}_3)$ is solvable, as it has a composition series with cyclic factor groups of prime order

9.2 Galois' criterion for solvability by radicals

Galois' criterion links polynomial solvability to group theory. It states a polynomial is solvable by radicals if and only if its Galois group is solvable. This powerful tool helps determine which equations have algebraic solutions.

Understanding Galois' criterion is key to grasping the limits of algebraic solutions. It explains why we can't solve all polynomials with radicals and connects abstract algebra to concrete mathematical problems we've struggled with for centuries.

Galois' Criterion for Solvability

Statement of Galois' Criterion

- Galois' criterion states that a polynomial $f(x) \in F[x]$ is solvable by radicals over a field F if and only if its Galois group $Gal(f/F)$ is solvable
- A group G is solvable if it has a subnormal series $G = G_0 \supset G_1 \supset \dots \supset G_n = \{e\}$ such that each quotient group G_i/G_{i+1} is abelian for $i = 0, 1, \dots, n-1$

Key Concepts in Galois' Criterion

- The splitting field of a polynomial $f(x)$ over F is the smallest field extension of F that contains all the roots of $f(x)$
- The Galois group $Gal(f/F)$ is the group of automorphisms of the splitting field of $f(x)$ that fix the base field F
- Solvability by radicals means that the roots of the polynomial can be expressed using the four basic arithmetic operations ($+$, $-$, $\times$, $\div$) and taking n th roots (radicals) of elements in the base field F

Applying Galois' Criterion

Determining Solvability by Radicals

- To apply Galois' criterion, first determine the Galois group $Gal(f/F)$ of the polynomial $f(x)$ over the field F
- Examine the structure of the Galois group to determine if it is solvable, i.e., if it has a subnormal series with abelian quotient groups
- Common solvable groups include abelian groups, cyclic groups, dihedral groups of order $2n$ for odd n , and the alternating group A_4
- Common non-solvable groups include the symmetric groups S_n for $n \geq 5$ and the alternating groups A_n for $n \geq 5$
- If the Galois group is solvable, the polynomial is solvable by radicals. If the Galois group is not solvable, the polynomial is not solvable by radicals

Examples of Applying Galois' Criterion

- For example, the general polynomial of degree n is solvable by radicals for $n \leq 4$ because its Galois group is a subgroup of S_4 , which is solvable
- However, for $n \geq 5$, the general polynomial is not solvable by radicals because its Galois group contains A_5 , which is not solvable
- The cyclotomic polynomial $\Phi_n(x)$ is always solvable by radicals because its Galois group is abelian (isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$)
- The polynomial $x^5 - 4x + 2$ is not solvable by radicals over $\mathbb{Q}$ because its Galois group is isomorphic to S_5

Galois Group and Solvability

Relationship between Galois Group and Solvability

- The Galois group encodes the symmetries of the roots of a polynomial, and its structure determines whether the polynomial is solvable by radicals
- If the Galois group is solvable, the roots can be expressed in terms of radicals because the extension fields in the splitting field can be constructed by adjoining radicals successively
- If the Galois group is not solvable, there is no way to express the roots using radicals because the extension fields cannot be constructed by adjoining radicals

Consequences of Galois' Criterion

- The solvability of the Galois group is related to the existence of a radical extension of the base field that contains all the roots of the polynomial
- The unsolvability of the general quintic polynomial by radicals is a consequence of the fact that its Galois group, S_5 , is not solvable
- The Abel-Ruffini theorem, which states that there is no general algebraic solution for polynomials of degree 5 or higher, follows from the unsolvability of S_5

- Galois' criterion provides a powerful tool for determining the solvability of polynomials and understanding the limitations of algebraic solutions

Necessity and Sufficiency of Galois' Criterion

Proving Necessity

- To prove necessity, assume the polynomial $f(x)$ is solvable by radicals over F
- Show that its splitting field can be obtained by successively adjoining radicals, and use this to construct a subnormal series of the Galois group with abelian quotient groups
- The key steps involve expressing the roots in terms of radicals and using the properties of radical extensions to build the subnormal series

Proving Sufficiency

- To prove sufficiency, assume the Galois group $Gal(f/F)$ is solvable, and use the subnormal series to construct a radical extension of F that contains all the roots of $f(x)$
- Use the Fundamental Theorem of Galois Theory to establish a correspondence between the intermediate fields of the splitting field and the subgroups of the Galois group
- Show that the abelian quotient groups in the subnormal series correspond to radical extensions of the intermediate fields
- The proof relies on the properties of solvable groups, the Fundamental Theorem of Galois Theory, and the correspondence between field extensions and subgroups of the Galois group

Significance of Necessity and Sufficiency

- The necessity and sufficiency of Galois' criterion demonstrate the deep connection between the algebraic structure of the Galois group and the solvability of polynomials by radicals
- The equivalence between solvability by radicals and having a solvable Galois group highlights the fundamental role of Galois theory in understanding the nature of algebraic equations
- The proof of Galois' criterion showcases the power and elegance of the Fundamental Theorem of Galois Theory and its applications in solving classical problems in algebra

9.3 Unsolvability of the general quintic

The unsolvability of the general quintic equation marks a turning point in algebra. It shows that not all polynomial equations can be solved using simple formulas, unlike quadratic, cubic, and quartic equations.

This revelation led to the development of Galois theory, which connects algebra and group theory. By examining the symmetries of polynomial roots, mathematicians can determine whether an equation is solvable by radicals or not.

Unsolvability of the Quintic

Historical Context

- The problem of solving polynomial equations has a long history, with solutions for quadratic ($ax^2 + bx + c = 0$), cubic ($ax^3 + bx^2 + cx + d = 0$), and quartic ($ax^4 + bx^3 + cx^2 + dx + e = 0$) equations discovered in the 16th century by mathematicians such as Scipione del Ferro, Niccolò Tartaglia, and Gerolamo Cardano
- Attempts to find a general solution for quintic equations ($ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$) were unsuccessful, despite the efforts of many mathematicians like Leonhard Euler and Joseph-Louis Lagrange
- The unsolvability of the general quintic remained a major open problem in mathematics until the early 19th century when mathematicians began to develop new algebraic tools
- Évariste Galois developed the theory of Galois groups, which provided the tools necessary to prove the unsolvability of the general quintic by radicals

Galois Theory and the Quintic

- Galois theory studies the symmetries of polynomial equations and their roots, which are captured by the Galois group of the equation
- The Galois group of a polynomial equation is a group of permutations of the equation's roots that preserve the algebraic relationships among them
- The solvability of a polynomial equation by radicals is closely related to the structure of its Galois group
- A polynomial equation is solvable by radicals if and only if its Galois group is a solvable group, meaning it has a composition series with abelian factor groups

Proving the Quintic's Unsolvability

The Galois Group of the Quintic

- The general quintic equation is of the form $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$, where a, b, c, d, e , and f are complex coefficients and $a \neq 0$
- The Galois group of the general quintic is the symmetric group S_5 , which consists of all permutations of 5 elements
- S_5 has order 120, meaning it contains 120 distinct permutations
- The alternating group A_5 , which consists of all even permutations in S_5 , is a normal subgroup of S_5 with index 2, i.e., $S_5/A_5 \cong \mathbb{Z}_2$

Simplicity of the Alternating Group

- A_5 is a simple group, meaning it has no nontrivial normal subgroups
- The simplicity of A_5 can be proven using the fact that it has no subgroups of index 2, 3, or 4
- The composition series of S_5 is $S_5 \supset A_5 \supset \{e\}$, where $\{e\}$ is the trivial group containing only the identity element

- Since A_5 is simple, the factor group $A_5/\{e\} \cong A_5$ is not abelian, and therefore, the composition series of S_5 is not a series of abelian groups

Conclusion of Unsolvability

- As the composition series of S_5 is not a series of abelian groups, S_5 is not a solvable group
- Consequently, the general quintic equation is not solvable by radicals, as its Galois group is S_5
- This proof demonstrates the power of Galois theory in determining the solvability of polynomial equations and the limitations of the methods used to solve lower-degree equations

Key Steps in the Proof

1. Determine the Galois group of the general quintic equation, which is the symmetric group S_5
2. Show that the alternating group A_5 is a normal subgroup of S_5 and that $S_5/A_5 \cong Z_2$
3. Prove that A_5 is a simple group by demonstrating that it has no subgroups of index 2, 3, or 4
4. Construct the composition series of S_5 ($S_5 \supset A_5 \supset \{e\}$) and demonstrate that it is not a series of abelian groups, as $A_5/\{e\} \cong A_5$ is not abelian
5. Conclude that S_5 is not a solvable group, and therefore, the general quintic equation is not solvable by radicals

Implications of the Unsolvable Quintic

Limitations of Classical Methods

- The unsolvability of the general quintic demonstrates that not all polynomial equations can be solved by radicals, which are expressions involving only arithmetic operations and n th roots
- This result highlights the limitations of the methods used to solve lower-degree polynomial equations, such as the quadratic formula and Cardano's formula for cubic equations
- The proof of the unsolvability of the general quintic shows that these classical methods cannot be extended to higher-degree equations in general

Advancements in Abstract Algebra

- The unsolvability of the general quintic showcases the power and utility of Galois theory in studying polynomial equations and their solutions
- Galois theory not only provided the tools to prove the unsolvability of the quintic but also laid the foundation for the development of modern abstract algebra
- The study of Galois groups and their properties led to further advancements in the theory of groups, rings, and fields, which have become essential tools in various branches of mathematics

Practical Implications

- The unsolvability of the general quintic has practical implications beyond pure mathematics
- In many fields, such as physics, engineering, and computer science, problems often lead to polynomial equations that need to be solved

- The result shows that certain problems may not have closed-form solutions expressible in terms of radicals, and numerical or approximation methods may be necessary to find solutions
- Understanding the limitations of classical solution methods can guide researchers and practitioners in choosing appropriate approaches to solve problems involving higher-degree polynomial equations

Unit 10 – Finite Fields and Their Applications

10.1 Structure and properties of finite fields

Finite fields are like secret codes for math nerds. They're special number systems with a limited set of elements, always a power of a prime number. Understanding their structure and properties is key to unlocking their power in cryptography and coding theory.

In this section, we'll dive into the nitty-gritty of finite fields. We'll explore how they're built, their unique characteristics, and the cool tricks you can do with their arithmetic. Get ready to level up your finite field game!

Finite Fields and Characteristics

Definition and Properties

- A finite field is a field that contains a finite number of elements, also known as a Galois field
- The order (number of elements) of a finite field is always a prime power, denoted as $q = p^n$, where p is a prime number and n is a positive integer
- There exists a unique finite field (up to isomorphism) for each prime power order $q = p^n$, denoted as $GF(q)$ or F_q

Characteristic of a Finite Field

- The characteristic of a finite field is the smallest positive integer m such that $m * 1 = 0$, where 1 is the multiplicative identity of the field
- In a finite field of order $q = p^n$, the characteristic is always the prime p
- For example, in the finite field $GF(2^3)$, the characteristic is 2
- This means that for any element a in $GF(2^3)$, $2 * a = 0$

Constructing Finite Fields

Quotient Rings and Irreducible Polynomials

- Finite fields can be constructed as quotient rings of polynomial rings over the integers modulo a prime
- An irreducible polynomial is a polynomial that cannot be factored into the product of two non-constant polynomials over a given field
- To construct a finite field of order $q = p^n$, find an irreducible polynomial $f(x)$ of degree n over the field $\mathbb{Z}_p$ (integers modulo p)

Elements and Arithmetic Operations

- The elements of the finite field are the polynomials of degree less than n with coefficients in $\mathbb{Z}_p$, with arithmetic operations performed modulo $f(x)$

- For example, in $GF(2^2)$ constructed using the irreducible polynomial $f(x) = x^2 + x + 1$, the elements are $\{0, 1, x, x + 1\}$
- The multiplicative group of a finite field is cyclic, generated by a primitive element
- A primitive element is a generator of the multiplicative group, meaning that every non-zero element can be expressed as a power of the primitive element

Arithmetic in Finite Fields

Addition and Subtraction

- Addition in a finite field is performed by adding the coefficients of the corresponding terms of the polynomials modulo the characteristic p
- For example, in $GF(2^2)$, $(x + 1) + (x) = 1$ because $1 + 1 \equiv 0 \pmod{2}$
- Subtraction in a finite field is performed by subtracting the coefficients of the corresponding terms of the polynomials modulo the characteristic p
- For example, in $GF(2^2)$, $(x + 1) - (x) = 1$ because $1 - 1 \equiv 0 \pmod{2}$

Multiplication and Division

- Multiplication in a finite field is performed by multiplying the polynomials and then reducing the result modulo the irreducible polynomial $f(x)$ and the characteristic p
- For example, in $GF(2^2)$ with $f(x) = x^2 + x + 1$, $(x + 1) * (x) = x^2 + x \equiv 1 \pmod{f(x)}$
- Division in a finite field is performed by multiplying the dividend by the inverse of the divisor, where the inverse is computed using the extended Euclidean algorithm
- For example, in $GF(2^2)$ with $f(x) = x^2 + x + 1$, $(x + 1)/(x) = (x + 1) * (x + 1) \equiv 1 \pmod{f(x)}$ because $(x + 1)$ is the inverse of (x)

Properties of Finite Fields

Primitive Elements

- Every finite field has a primitive element, which is a generator of the multiplicative group of the field
- The number of primitive elements in a finite field of order q is $\phi(q - 1)$, where ϕ is Euler's totient function
- For example, in $GF(2^3)$, there are $\phi(7) = 6$ primitive elements
- Primitive elements are used in various applications, such as constructing pseudo-random number generators and designing error-correcting codes

Trace and Norm Functions

- The trace and norm functions are important maps between finite fields and their subfields, which can be used to analyze the structure and properties of the fields
- The trace function $Tr_{F_q/F_p}(a)$ of an element a in F_q is the sum of its conjugates over the subfield F_p
- The norm function $N_{F_q/F_p}(a)$ of an element a in F_q is the product of its conjugates over the subfield F_p

- These functions have various properties, such as linearity and multiplicativity, which can be used to solve equations and study the structure of finite fields

10.2 Multiplicative group of finite fields

Finite fields are like secret code playgrounds, with their own special rules. The multiplicative group of a finite field is the cool kids' club where only non-zero elements hang out. It's a tight-knit group where everyone's connected through multiplication.

This group is cyclic, meaning one special element can generate all the others. It's like having a master key that unlocks everything. Understanding this group's structure is crucial for solving tricky math problems and creating unbreakable codes in the digital world.

Multiplicative group of a finite field

Definition and properties

- A finite field $\mathbb{F}_q$ is a field with a finite number of elements, where q is a prime power ($q = p^n$ for some prime p and positive integer n)
- The multiplicative group of a finite field $\mathbb{F}_q$, denoted as $\mathbb{F}_q^*$, is the set of all nonzero elements of $\mathbb{F}_q$ under the operation of multiplication
- The multiplicative group $\mathbb{F}_q^*$ is a cyclic group of order $q - 1$, meaning that every element can be expressed as a power of a single element called a primitive element or generator
- The multiplicative group $\mathbb{F}_q^*$ satisfies the group axioms:
- Closure: For any $a, b \in \mathbb{F}_q^*$, $ab \in \mathbb{F}_q^*$
- Associativity: For any $a, b, c \in \mathbb{F}_q^*$, $(ab)c = a(bc)$
- Identity element: The element 1 is the identity element, such that $1a = a1 = a$ for all $a \in \mathbb{F}_q^*$
- Inverses: For every $a \in \mathbb{F}_q^*$, there exists an element $a^{-1} \in \mathbb{F}_q^*$ such that $aa^{-1} = a^{-1}a = 1$

Lagrange's theorem and subgroups

- Lagrange's theorem states that the order of any subgroup of $\mathbb{F}_q^*$ divides the order of $\mathbb{F}_q^*$, which is $q - 1$
- The subgroups of $\mathbb{F}_q^*$ are also cyclic and their orders divide $q - 1$
- The number of subgroups of order d is equal to $\phi(d)$, where $d \mid (q - 1)$ and ϕ is Euler's totient function, which counts the number of positive integers less than or equal to d that are coprime to d
- Example: In the finite field $\mathbb{F}_7$, the multiplicative group $\mathbb{F}_7^*$ has order 6 and subgroups of orders 1, 2, and 3

Order of elements in the group

Definition and properties

- The order of an element a in the multiplicative group $\mathbb{F}_q^*$ is the smallest positive integer k such that $a^k = 1$

- The order of an element a divides the order of the multiplicative group, $q - 1$, according to Lagrange's theorem
- If a is a primitive element (generator) of $\mathbb{F}_q^*$, then the order of a is equal to $q - 1$
- The order of the identity element 1 is always 1

Euler's theorem and determining orders

- Euler's theorem states that for any element a in $\mathbb{F}_q^*$, $a^{(q-1)} \equiv 1 \pmod{q}$, which can be used to determine the order of elements
- To find the order of an element a , one can factor $q - 1$ and check if $a^d \equiv 1 \pmod{q}$ for each divisor d of $q - 1$, starting from the smallest divisor
- Example: In $\mathbb{F}_{11}^*$, the element 2 has order 10 because $2^{10} \equiv 1 \pmod{11}$, and no smaller positive integer satisfies this condition

Cyclic structure of the group

Primitive elements and generators

- The multiplicative group $\mathbb{F}_q^*$ is a cyclic group, which means that it can be generated by a single element called a primitive element or generator
- A primitive element α generates all the nonzero elements of $\mathbb{F}_q^*$ through its powers:
 $\mathbb{F}_q^* = \{1, \alpha, \alpha^2, \dots, \alpha^{(q-2)}\}$
- The number of primitive elements in $\mathbb{F}_q^*$ is equal to $\phi(q - 1)$, where ϕ is Euler's totient function
- Example: In $\mathbb{F}_7^*$, the primitive elements are 3 and 5 because they generate all the nonzero elements: $\{1, 3, 2, 6, 4, 5\}$ and $\{1, 5, 4, 6, 2, 3\}$, respectively

Subgroups and their generators

- The subgroups of $\mathbb{F}_q^*$ are also cyclic and their orders divide $q - 1$
- The generators of a subgroup of order d are the elements whose orders are equal to d
- Example: In $\mathbb{F}_{13}^*$, the subgroup of order 4 is $\{1, 3, 9, 1\}$, and its generators are 3 and 9

Applications of the multiplicative group

Solving problems in finite field arithmetic

- The structure of the multiplicative group $\mathbb{F}_q^*$ can be used to solve various problems in finite field arithmetic, such as:
- Finding inverses: To find the inverse of an element a in $\mathbb{F}_q^*$, one can use the extended Euclidean algorithm or Fermat's little theorem: $a^{-1} \equiv a^{(q-2)} \pmod{q}$
- Solving equations: To solve the equation $ax \equiv b \pmod{q}$ for x , multiply both sides by a^{-1} to obtain $x \equiv a^{-1}b \pmod{q}$

- Computing powers: To compute a^n in $\mathbb{F}_q^*$, use the fact that $a^n \equiv a^{(n \bmod (q-1))} \pmod{q}$ to reduce the exponent modulo $q-1$

Cryptographic applications

- Discrete logarithm problem: Given elements a and b in $\mathbb{F}_q^*$, find an integer x such that $a^x \equiv b \pmod{q}$. This problem is believed to be computationally difficult and forms the basis for several cryptographic systems
- Diffie-Hellman key exchange: A secure key exchange protocol that relies on the difficulty of the discrete logarithm problem in the multiplicative group of a finite field
- Alice and Bob agree on a finite field $\mathbb{F}_q$ and a primitive element α
- Alice chooses a secret integer a and sends α^a to Bob
- Bob chooses a secret integer b and sends α^b to Alice
- Both Alice and Bob can compute the shared secret α^{ab} , but an eavesdropper cannot determine this value from the exchanged messages
- ElGamal encryption: A public-key cryptosystem based on the discrete logarithm problem in the multiplicative group of a finite field, used for secure communication
- Bob chooses a finite field $\mathbb{F}_q$, a primitive element α , and a secret integer b , and publishes $(\mathbb{F}_q, \alpha, \alpha^b)$ as his public key
- To encrypt a message m for Bob, Alice chooses a random integer r and sends the ciphertext $(c_1, c_2) = (\alpha^r, m \cdot (\alpha^b)^r)$
- To decrypt the ciphertext, Bob computes $m = c_2 \cdot (c_1^b)^{-1}$

10.3 Applications in coding theory and cryptography

Finite fields are the backbone of modern coding theory and cryptography. They provide the mathematical foundation for error-correcting codes, ensuring reliable data transmission, and secure communication protocols that protect our digital lives.

From simple binary fields to complex extension fields, finite fields enable powerful algorithms. They're used in everything from error detection in CDs to secure online transactions, making them essential for our interconnected world.

Coding theory and cryptography principles

Error detection and correction in coding theory

- Coding theory studies methods for efficiently and accurately transmitting data over noisy channels
- The main goals of coding theory are error detection and error correction
- Error detection and correction are achieved through the use of redundancy in the transmitted data
- Examples of error-correcting codes include:
 - Hamming codes
 - Reed-Solomon codes

- Turbo codes
- Low-density parity-check (LDPC) codes

Secure communication in cryptography

- Cryptography studies techniques for secure communication in the presence of adversaries
- Cryptography aims to ensure confidentiality, integrity, and authenticity of information
- Confidentiality, integrity, and authenticity are achieved through the use of mathematical algorithms and protocols
- Symmetric-key cryptography uses a single shared key for both encryption and decryption (AES, DES)
- Public-key cryptography uses a pair of keys: a public key for encryption and a private key for decryption (RSA, ECC)
- Hash functions create fixed-size digests of input data, which are useful for ensuring data integrity and creating digital signatures (SHA-256, MD5)

Finite fields for linear codes

Finite field fundamentals

- Finite fields, also known as Galois fields, are algebraic structures with a finite number of elements
- Finite fields satisfy certain properties, such as closure under addition and multiplication
- Examples of finite fields include:
 - The binary field $GF(2)$ with elements $\{0, 1\}$
 - The prime field $GF(p)$ with elements $\{0, 1, \dots, p-1\}$ for a prime p
 - Extension fields $GF(p^n)$ constructed using polynomials over $GF(p)$

Constructing linear codes using finite fields

- Linear codes are a class of error-correcting codes that can be constructed using finite fields
- Each codeword in a linear code is a linear combination of basis vectors
- The generator matrix of a linear code is used to encode messages
- The parity-check matrix of a linear code is used for error detection and correction
- The Hamming distance between two codewords is the number of positions in which they differ
- The minimum distance of a code determines its error-correcting capabilities
- Cyclic codes, such as BCH and Reed-Solomon codes, are a subclass of linear codes with additional algebraic structure that allows for efficient encoding and decoding algorithms

Finite fields in cryptography design

Finite fields in symmetric-key and public-key cryptography

- Finite fields are used in the design of various cryptographic algorithms

- The Advanced Encryption Standard (AES) is a symmetric-key encryption algorithm that uses finite field arithmetic in its substitution-permutation network
- AES provides strong security and efficient implementation using finite field operations
- Elliptic curve cryptography (ECC) uses the algebraic structure of elliptic curves over finite fields to construct public-key cryptosystems
- ECC offers smaller key sizes compared to traditional schemes like RSA while maintaining the same level of security

Finite fields in key exchange and digital signatures

- Diffie-Hellman key exchange is a protocol for establishing a shared secret key over an insecure channel
- Diffie-Hellman key exchange can be implemented using the multiplicative group of a finite field
- Digital signature algorithms, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), rely on the properties of finite fields
- ECDSA is used to create and verify digital signatures in various applications (Bitcoin, SSL/TLS)

Cryptographic security analysis using finite fields

Computational complexity of finite field problems

- The security of cryptographic systems based on finite fields depends on the computational complexity of certain mathematical problems
- The discrete logarithm problem in a finite field is the problem of finding an integer x such that $g^x = h$, given elements g and h in the field
- The discrete logarithm problem is believed to be computationally infeasible for large field sizes
- The elliptic curve discrete logarithm problem is a variant of the discrete logarithm problem that uses the group of points on an elliptic curve over a finite field
- The elliptic curve discrete logarithm problem is considered even harder to solve than the standard discrete logarithm problem

Cryptanalysis and security considerations

- The security of cryptographic systems can be analyzed using various attack models
- Attack models include the chosen-plaintext attack, chosen-ciphertext attack, and side-channel attacks
- Cryptanalysis techniques, such as linear and differential cryptanalysis, can be used to assess the strength of cryptographic algorithms and identify potential weaknesses
- The security of a cryptographic system also depends on the proper implementation and management of cryptographic keys
- Secure protocols for key exchange and distribution are essential for maintaining the overall security of the system
- Examples of secure key exchange protocols include:

- Diffie-Hellman key exchange
- Elliptic Curve Diffie-Hellman (ECDH)
- Key encapsulation mechanisms (KEM) in post-quantum cryptography

Unit 11 – Constructibility and Impossibility Results

11.1 Constructible numbers and geometric constructions

Constructible numbers and geometric constructions are fundamental concepts in Galois Theory. They bridge abstract algebra with classical geometry, revealing surprising connections between field theory and compass-and-straightedge constructions.

Understanding these concepts helps explain why some geometric problems are impossible to solve with basic tools. This knowledge sheds light on the limitations of classical geometry and the power of algebraic methods in solving geometric puzzles.

Constructible Numbers and Properties

Definition and Basic Properties

- Constructible numbers are real numbers that can be constructed using a compass and straightedge starting from the unit length
- The set of constructible numbers forms a subfield of the real numbers, closed under:
 1. Addition
 2. Subtraction
 3. Multiplication
 4. Division
 5. Taking square roots
- All rational numbers and some irrational numbers are constructible (e.g., $\sqrt{2}$)

Non-Constructible Numbers and Cardinality

- Not all real numbers are constructible, such as:
 - π , the ratio of a circle's circumference to its diameter
 - e , the base of the natural logarithm
- The set of constructible numbers is countable, meaning it can be put into a one-to-one correspondence with the natural numbers
- In contrast, the set of real numbers is uncountable, having a larger cardinality than the set of constructible numbers

Constructible Numbers vs Field Extensions

Relationship to Field Extensions

- Constructible numbers are closely related to the concept of field extensions in abstract algebra

- The set of constructible numbers is the smallest subfield of the real numbers containing the rational numbers and closed under taking square roots
- A real number α is constructible if and only if there exists a finite tower of quadratic extensions $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n$ such that $\alpha \in F_n$

Degree of Extension and Constructibility

- The degree of the extension $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ must be a power of 2 for α to be constructible
- If the degree of the extension is not a power of 2, then the number is not constructible using compass and straightedge alone
- Examples:
 - $\sqrt{2}$ is constructible because $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, which is a power of 2
 - $\sqrt[3]{2}$ is not constructible because $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, which is not a power of 2

Geometric Constructions with Compass and Straightedge

Basic Constructions

- Basic constructions include:
 1. Bisecting a line segment
 2. Bisecting an angle
 3. Constructing a perpendicular line to a given line through a point
 4. Constructing a parallel line to a given line through a point
- These constructions form the foundation for more complex geometric constructions

Constructible Regular Polygons

- Constructing regular polygons with a number of sides that is a Fermat prime or a product of distinct Fermat primes is possible using compass and straightedge
- Fermat primes are prime numbers of the form $2^{2^n} + 1$, where n is a non-negative integer
- The only known Fermat primes are:
 - 3
 - 5
 - 17
 - 257
 - 65537
- Examples of constructible regular polygons:
 - Equilateral triangle (3 sides)
 - Square (4 sides)

- Regular pentagon (5 sides)
- Examples of non-constructible regular polygons:
- Regular heptagon (7 sides)
- Regular nonagon (9 sides)

Proving Constructibility of Numbers and Figures

Proving Constructibility

- Proving the constructibility of a number or geometric figure involves showing that it can be obtained using a finite number of steps involving only compass and straightedge constructions
- The constructibility of a regular polygon with n sides is equivalent to the constructibility of:
 1. The angle $\frac{2\pi}{n}$
 2. The complex number $\cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$
- The Gauss-Wantzel theorem states that a regular polygon with n sides is constructible if and only if $n = 2^k p_1 p_2 \cdots p_m$, where:
 - $k \geq 0$
 - $p_1, p_2, \dots, p_m$ are distinct Fermat primes

Proving Non-Constructibility

- Proving the non-constructibility of certain numbers or figures involves showing that they cannot be obtained using only compass and straightedge constructions
- Examples of non-constructible numbers:
 - π
 - e
- Examples of non-constructible geometric problems:
 - Trisecting an arbitrary angle
 - Doubling the cube (constructing a cube with twice the volume of a given cube)
 - Squaring the circle (constructing a square with the same area as a given circle)
- The non-constructibility of certain geometric problems can be proved using the relationship between constructible numbers and field extensions

11.2 Impossibility of angle trisection and cube duplication

Angle trisection and cube duplication stumped mathematicians for centuries. These ancient Greek problems seemed simple but proved impossible using just a compass and straightedge. Their study led to major breakthroughs in algebra and geometry.

The proofs of impossibility rely on field theory and Galois theory. They show that certain numbers, like the cosine of a trisected angle or the cube root of 2, can't be constructed geometrically. This reveals deep connections between algebra and geometry.

Significance of Angle Trisection and Cube Duplication

Historical Importance

- The problems of angle trisection and cube duplication, along with the problem of squaring the circle, are known as the three classical problems of antiquity in mathematics
- These problems originated in ancient Greece, where mathematicians sought to find constructions using only a compass and straightedge
- The angle trisection problem involves constructing an angle that is one-third the measure of a given arbitrary angle
- The cube duplication problem, also known as the Delian problem, involves constructing a cube with twice the volume of a given cube

Impact on Mathematics

- For centuries, mathematicians attempted to solve these problems using only a compass and straightedge, but no general solutions were found
- The attempts to solve these problems led to significant advancements in geometry and algebra
- Mathematicians developed new techniques and concepts in their pursuit of solutions
- The inability to solve these problems using the given tools led to the development of new mathematical concepts and theories
- The study of these problems contributed to the foundation of modern algebra and number theory
- The impossibility results demonstrated the limitations of compass and straightedge constructions and motivated the exploration of abstract algebraic concepts

Impossibility of Angle Trisection

Theoretical Foundation

- The proof relies on the fundamental theorem of algebra and the properties of field extensions
- Suppose we have an arbitrary angle θ , and we want to construct an angle $\theta/3$ using only a compass and straightedge
- The key idea is to show that the cosine of $\theta/3$ cannot be constructed from the cosine of θ using only the operations allowed in a compass and straightedge construction

Algebraic Representation

- The cosine of $\theta/3$ can be expressed as a cubic equation in terms of the cosine of θ using the triple angle formula: $4\cos^3(\theta/3) - 3\cos(\theta/3) - \cos(\theta) = 0$
- This equation relates the cosine of the trisected angle to the cosine of the original angle
- If the cosine of θ is a constructible number (i.e., it can be obtained from rational numbers using only the operations allowed in a compass and straightedge construction), then the cubic equation must be solvable by radicals

Impossibility Proof

- Using the theory of field extensions and Galois theory, it can be shown that the cubic equation is not always solvable by radicals, depending on the value of $\cos(\theta)$
- For example, if $\cos(\theta) = 1/2$, the cubic equation becomes $8x^3 - 6x - 1 = 0$, which is not solvable by radicals
- Therefore, there exist angles θ for which the cosine of $\theta/3$ cannot be constructed using only a compass and straightedge, proving the impossibility of trisecting an arbitrary angle
- This result demonstrates that not all geometric problems can be solved using the classical tools of compass and straightedge

Impossibility of Cube Duplication

Problem Statement

- Suppose we have a cube with side length 1, and we want to construct a cube with volume 2 using only a compass and straightedge
- The side length of the doubled cube must be the cube root of 2 ($\sqrt[3]{2}$) since the volume of a cube is proportional to the cube of its side length

Constructible Numbers

- To prove the impossibility, we need to show that $\sqrt[3]{2}$ is not a constructible number
- Constructible numbers are those that can be obtained from rational numbers using only the operations allowed in a compass and straightedge construction: addition, subtraction, multiplication, division, and taking square roots
- For example, $\sqrt{2}$ is a constructible number because it can be obtained by taking the square root of the rational number 2

Field Extensions

- The field of constructible numbers is a subfield of the complex numbers, and its degree over the rational numbers must be a power of 2
- The degree of a field extension is the dimension of the larger field as a vector space over the smaller field
- However, the degree of the extension field $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is 3, which is not a power of 2
- $\mathbb{Q}(\sqrt[3]{2})$ is the smallest field containing both the rational numbers and $\sqrt[3]{2}$
- Therefore, $\sqrt[3]{2}$ is not a constructible number, and it is impossible to double the volume of a cube using only a compass and straightedge

Field Extensions and Geometric Impossibilities

Connection between Algebra and Geometry

- The impossibility proofs for angle trisection and cube duplication rely on the properties of field extensions and the limitations of compass and straightedge constructions

- Compass and straightedge constructions can only generate numbers that lie in a field extension of the rational numbers with a degree that is a power of 2
- This limitation is due to the fact that each construction step corresponds to solving a linear or quadratic equation
- The cosine of the trisected angle and the cube root of 2 (for cube duplication) are elements of field extensions that do not satisfy this property
- The cosine of the trisected angle is a root of a cubic equation, and the cube root of 2 generates a field extension of degree 3 over the rational numbers

Impact on the Development of Mathematics

- The impossibility results demonstrate the limitations of compass and straightedge constructions and the connection between these geometric problems and abstract algebraic concepts like field extensions
- The study of these impossibility results led to the development of Galois theory, which provides a framework for understanding the solvability of polynomial equations and the properties of field extensions
- Galois theory establishes a correspondence between the structure of a field extension and the properties of the associated Galois group
- The exploration of these geometric problems and their algebraic underpinnings contributed to the growth of modern algebra and the unification of various branches of mathematics

11.3 Transcendence of π and e

Transcendental numbers like π and e can't be roots of polynomial equations with rational coefficients. This makes them uncountable and dense in the real numbers. They're key players in the realm of numbers we can't construct with just a compass and straightedge.

Proving π and e are transcendental involves clever uses of Galois theory and contradiction. These proofs show how tricky these numbers are and why they're so special in math. They also connect to big questions about geometry and number theory.

Transcendental Numbers and Their Properties

Definition and Characteristics

- Define transcendental numbers as real or complex numbers that are not algebraic, meaning they are not roots of any non-zero polynomial equation with rational coefficients
- Highlight the uncountability of transcendental numbers, implying there are infinitely more transcendental numbers than algebraic numbers
- Explain the density of the set of transcendental numbers in the real numbers, meaning between any two real numbers, there exists a transcendental number (π , e)
- Mention that transcendental numbers are not constructible with a compass and straightedge, meaning they cannot be constructed using a finite number of steps involving only a compass and straightedge

Algebraic Operations with Transcendental Numbers

- State that the sum, difference, product, and quotient of a transcendental number and an algebraic number is always transcendental
- Provide examples demonstrating the closure of transcendental numbers under these operations ($\pi + 1$, $e - 2$, 3π , $e/4$)
- Explain that these properties help identify new transcendental numbers based on known ones
- Discuss the implications of these properties in the study of transcendental number theory and its applications

Proving the Transcendence of π

Proof by Contradiction

- Assume π is algebraic and let K be the splitting field of the minimal polynomial of π over $\mathbb{Q}$
- Explain that the field extension $K/\mathbb{Q}$ is a Galois extension and its Galois group $G = \text{Gal}(K/\mathbb{Q})$ is a finite group
- Consider the field extension $K(e^{2\pi i/n})/K$ for some positive integer n and note that this extension is cyclotomic and has degree $\phi(n)$, where ϕ is Euler's totient function
- Show that the compositum of K and $\mathbb{Q}(e^{2\pi i/n})$ is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to a subgroup of $G \times (\mathbb{Z}/n\mathbb{Z})^\times$, which is finite

Contradiction and Conclusion

- Demonstrate that as n increases, the degree of the cyclotomic extension grows without bound, contradicting the finiteness of the Galois group
- Conclude that the assumption of π being algebraic leads to a contradiction, proving that π is transcendental
- Discuss the significance of this proof in establishing the transcendental nature of π
- Highlight the role of Galois theory in the proof and its importance in solving problems related to transcendental numbers

Transcendence of e

Proof by Contradiction

- Assume e is algebraic and let L be the splitting field of the minimal polynomial of e over $\mathbb{Q}$
- Explain that the field extension $L/\mathbb{Q}$ is a Galois extension and its Galois group $H = \text{Gal}(L/\mathbb{Q})$ is a finite group
- Consider the field extension $L(2^{1/n})/L$ for some positive integer n and note that this extension is radical and has degree n
- Show that the compositum of L and $\mathbb{Q}(2^{1/n})$ is a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to a subgroup of $H \times (\mathbb{Z}/n\mathbb{Z})$, which is finite

Contradiction and Conclusion

- Demonstrate that as n increases, the degree of the radical extension grows without bound, contradicting the finiteness of the Galois group
- Conclude that the assumption of e being algebraic leads to a contradiction, proving that e is transcendental
- Discuss the significance of this proof in establishing the transcendental nature of e
- Compare and contrast the proofs of transcendence for π and e , highlighting their similarities and differences

Implications of Transcendental Numbers in Mathematics

Geometric Consequences

- Discuss the impact of the transcendence of π and e on the solvability of certain geometric problems, such as squaring the circle or constructing regular polygons with a compass and straightedge
- Explain how the transcendental nature of these numbers limits the possibilities of constructing certain geometric objects using classical tools
- Provide historical context for these geometric problems and their significance in the development of mathematics

Connections to Other Mathematical Concepts

- Explore the relationship between the transcendence of π and e and the concept of periods, which are complex numbers that can be expressed as definite integrals of algebraic functions over algebraic domains
- Discuss the connections between the transcendence of π and e and the study of special functions, such as the gamma function and the zeta function, which have important applications in number theory and mathematical physics
- Highlight the interdisciplinary nature of transcendental number theory and its relevance to various branches of mathematics

Further Research and Open Questions

- Emphasize the power and versatility of Galois theory in solving problems related to transcendental numbers, as demonstrated by the proofs of the transcendence of π and e
- Discuss how the existence of transcendental numbers, exemplified by π and e , highlights the richness and complexity of the real number system and its extensions
- Identify open questions and areas for further research in transcendental number theory, such as the transcendence of other mathematical constants ($\ln 2$, $\zeta(3)$) and the development of new techniques for proving transcendence
- Encourage the exploration of the implications of transcendental numbers in other areas of mathematics and their potential applications in science and engineering

Unit 12 – Galois Theory: Modern Math Applications

12.1 Inverse Galois problem

The inverse Galois problem asks if every finite group is the Galois group of a field extension over the rationals. It's a key open question in modern Galois theory, connecting group theory, field theory, and algebraic geometry.

Solving this problem would fully characterize which finite groups can be Galois groups over the rationals. While progress has been made for specific group types, a complete solution remains elusive, making it an active area of research in mathematics.

The Inverse Galois Problem

Definition and Significance

- The inverse Galois problem asks whether every finite group appears as the Galois group of some Galois extension of the rational numbers
- Named after Évariste Galois, who laid the foundations of Galois theory in the early 19th century
- Solving the inverse Galois problem would provide a complete characterization of the finite groups that can arise as Galois groups over the rationals
- One of the central open problems in modern Galois theory
- Has connections to various areas of mathematics (number theory, algebraic geometry, representation theory)
- A complete solution would have significant implications for understanding the structure and properties of finite groups and their realizations as Galois groups

Open Problem in Modern Mathematics

- The inverse Galois problem remains unsolved despite significant progress in specific cases
- Affirmative solutions for abelian groups, symmetric groups, alternating groups, and many simple groups
- Open for many classes of finite groups, particularly non-solvable groups and groups with complex structure
- Connections to other areas of mathematics make the inverse Galois problem a central question in modern Galois theory
- Number theory: relates to the study of algebraic number fields and their Galois groups
- Algebraic geometry: techniques from algebraic geometry (Belyi's theorem, Riemann surfaces) are used to construct Galois extensions
- Representation theory: regular inverse Galois problem involves the study of group representations and their realizations over the rationals

Inverse Galois Problem and Field Extensions

Equivalent Formulation

- The inverse Galois problem is equivalent to determining whether every finite group can be realized as the Galois group of a Galois extension of the rational numbers
- Constructing a Galois extension with a prescribed Galois group involves finding a polynomial over the rationals whose splitting field has the desired group as its Galois group
- Example: constructing a Galois extension with Galois group isomorphic to the symmetric group S_n requires finding an irreducible polynomial of degree n with prescribed properties

Tools and Techniques

- Hilbert's irreducibility theorem provides a tool for constructing Galois extensions with prescribed Galois groups
- Shows that irreducible polynomials with certain properties exist over the rationals
- Used to construct Galois extensions with Galois groups isomorphic to symmetric groups and alternating groups
- The Shafarevich conjecture, which states that every finite solvable group is the Galois group of some Galois extension of the rationals, is a partial solution to the inverse Galois problem for solvable groups
- Proved by Shafarevich using techniques from algebraic number theory and class field theory
- Constructing Galois extensions with prescribed non-solvable Galois groups (Monster group, Mathieu groups) remains a challenging open problem in inverse Galois theory
- Requires advanced techniques from algebraic geometry, representation theory, and group theory

Progress Towards Solving the Inverse Galois Problem

Affirmative Results for Specific Classes of Groups

- The inverse Galois problem has been solved affirmatively for various classes of finite groups
- Abelian groups: every finite abelian group is the Galois group of a Galois extension of the rationals (Kronecker-Weber theorem)
- Symmetric groups: every symmetric group S_n is the Galois group of a Galois extension of the rationals (Hilbert's irreducibility theorem)
- Alternating groups: every alternating group A_n is the Galois group of a Galois extension of the rationals (Hilbert's irreducibility theorem)
- Many simple groups: the rigidity method has been used to construct Galois extensions with Galois groups isomorphic to various simple groups (sporadic simple groups, finite simple groups of Lie type)
- Shafarevich's theorem proves that every finite solvable group is the Galois group of some Galois extension of the rationals
- Provides a complete solution to the inverse Galois problem for solvable groups
- Uses techniques from algebraic number theory and class field theory

Regular Inverse Galois Problem

- The regular inverse Galois problem asks whether every finite group appears as the Galois group of a regular extension of the rationals
- A regular extension is a Galois extension where the Galois group acts freely on the roots of a generating polynomial
- The regular inverse Galois problem has been solved affirmatively for various classes of groups
- Abelian groups: every finite abelian group is the Galois group of a regular extension of the rationals (Kummer theory)
- Symmetric groups: every symmetric group S_n is the Galois group of a regular extension of the rationals (Noether's theorem)
- Many simple groups: techniques from algebraic geometry and representation theory have been used to construct regular extensions with Galois groups isomorphic to various simple groups
- The regular inverse Galois problem provides a stronger version of the inverse Galois problem and has important applications in algebraic geometry and arithmetic geometry

Open Problems and Challenges

- Despite significant progress, the inverse Galois problem remains open for many classes of finite groups
- Non-solvable groups: constructing Galois extensions with prescribed non-solvable Galois groups is a major challenge
- Groups with complex structure: groups with intricate subgroup structure or representation-theoretic properties pose difficulties for current techniques
- The inverse Galois problem for specific groups, such as the Monster group or the Mathieu groups, remains unresolved
- Constructing Galois extensions with these groups as Galois groups requires advanced techniques from algebraic geometry, representation theory, and group theory
- The development of new methods and techniques to tackle the inverse Galois problem for challenging classes of groups is an active area of research in modern Galois theory

Implications of a Complete Solution

Characterization of Galois Groups

- A complete solution to the inverse Galois problem would provide a full characterization of the finite groups that can arise as Galois groups over the rational numbers
- Would answer the question of which finite groups can be realized as automorphism groups of field extensions
- Would establish a deep connection between the structure of finite groups and the Galois theory of field extensions

Encoding Groups into Polynomial Equations

- A positive solution to the inverse Galois problem would imply that every finite group can be "encoded" into a polynomial equation over the rationals
- The Galois group of the splitting field of the polynomial would be isomorphic to the given finite group
- This encoding would establish a profound link between group theory and field theory
- Would allow for the study of finite groups using techniques from Galois theory and algebraic geometry

Implications for Related Problems

- A complete solution to the inverse Galois problem would have implications for related problems in Galois theory
- The Noether problem: asks about the rationality of fixed fields under group actions
- The Shafarevich conjecture: states that every finite solvable group is the Galois group of a Galois extension of the rationals (proved by Shafarevich)
- The regular inverse Galois problem: asks whether every finite group appears as the Galois group of a regular extension of the rationals
- The techniques and methods developed to solve the inverse Galois problem would likely have applications in other areas of mathematics
- Algebraic geometry: techniques from algebraic geometry (Belyi's theorem, Riemann surfaces) have been crucial in constructing Galois extensions
- Representation theory: the regular inverse Galois problem involves the study of group representations and their realizations over the rationals
- Number theory: the inverse Galois problem is closely related to the study of algebraic number fields and their Galois groups

Landmark Achievement in Mathematics

- The resolution of the inverse Galois problem would be a landmark achievement in modern mathematics
- Would represent a major advance in our understanding of the structure and properties of finite groups
- Would establish deep connections between group theory, field theory, and algebraic geometry
- Would open up new avenues for research in Galois theory, number theory, and related areas
- A complete solution to the inverse Galois problem would be a testament to the power and depth of modern algebraic methods and would showcase the importance of interdisciplinary approaches in mathematics

12.2 Galois theory in algebraic number theory

Galois theory in algebraic number theory unveils the hidden symmetries of number fields. It connects field extensions to group structures, offering a powerful toolkit for analyzing prime factorization, ideal class groups, and field properties.

This framework illuminates the arithmetic of algebraic integers and prime splitting. By linking Galois groups to field properties, it enables deeper insights into number fields and paves the way for advanced results in class field theory.

Galois theory in number fields

Fundamentals of Galois theory in algebraic number fields

- Galois theory offers a robust framework for analyzing symmetries and structural properties of algebraic number fields, which are finite extensions of the rational numbers $\mathbb{Q}$
- The Galois group of an algebraic number field captures essential information about the field, including its degree, subfields, and prime splitting behavior
- Galois theory enables the classification of algebraic number fields based on their Galois groups, giving rise to important concepts such as Galois extensions, abelian extensions, and solvable extensions
- The Galois correspondence establishes a one-to-one correspondence between the subfields of an algebraic number field and the subgroups of its Galois group, revealing a profound connection between field theory and group theory

Applications of Galois theory to arithmetic properties

- Galois theory facilitates the study of arithmetic properties of algebraic number fields, such as the structure of their ring of integers and ideal factorization
- The ring of integers of an algebraic number field is a fundamental object of study, and Galois theory provides insights into its properties and symmetries
- Ideal factorization in algebraic number fields is a central topic in algebraic number theory, and Galois theory offers powerful tools for understanding the splitting behavior of ideals
- Galois theory can be used to analyze the class group of an algebraic number field, which measures the failure of unique factorization in its ring of integers

Galois theory for algebraic integers

Properties of algebraic integers under Galois action

- Galois theory can be applied to investigate the properties of algebraic integers, which are elements of an algebraic number field that are roots of monic polynomials with integer coefficients
- The Galois group of an algebraic number field acts on its ring of integers, and the fixed points under this action are precisely the rational integers ($\mathbb{Z}$)
- The action of the Galois group on algebraic integers reveals important structural and symmetry properties of the ring of integers
- Studying the Galois action on algebraic integers leads to a deeper understanding of the arithmetic and algebraic properties of number fields

Galois theory and ideal class groups

- The ideal class group of an algebraic number field quantifies the failure of unique factorization in its ring of integers, and Galois theory provides tools for computing and analyzing this group

- The Hilbert class field of an algebraic number field, which is its maximal unramified abelian extension, has a Galois group isomorphic to the ideal class group of the field
- Galois cohomology can be employed to study the structure of ideal class groups and their relationships with other arithmetic invariants of algebraic number fields
- The connection between Galois groups and ideal class groups is a fundamental aspect of algebraic number theory and has far-reaching consequences in the study of number fields

Galois groups and prime ideal splitting

Relationship between Galois groups and prime splitting

- The splitting behavior of prime ideals in an algebraic number field extension is intimately connected to the structure of its Galois group
- When a prime ideal of the base field (usually $\mathbb{Q}$) is extended to an algebraic number field, it may remain prime, split into distinct prime ideals, or ramify, depending on the Galois group of the extension
- The Dedekind-Kummer theorem describes the splitting of primes in a Galois extension of algebraic number fields in terms of the factorization of certain polynomials associated with the extension
- Understanding the connection between Galois groups and prime splitting is crucial for studying the arithmetic properties of algebraic number fields

Frobenius elements and Chebotarev density theorem

- The Frobenius element of a prime ideal in a Galois extension encodes information about the splitting behavior of the prime and generates a conjugacy class in the Galois group
- The conjugacy class of the Frobenius element in the Galois group provides a way to classify prime ideals based on their splitting behavior
- The Chebotarev density theorem is a powerful generalization of Dirichlet's theorem on primes in arithmetic progressions, relating the density of primes with a given splitting behavior to the size of the corresponding conjugacy class in the Galois group
- The Chebotarev density theorem has numerous applications in algebraic number theory, including the study of prime distribution and the construction of number fields with prescribed properties

Galois theory in algebraic number theory results

Kronecker-Weber theorem and cyclotomic fields

- The Kronecker-Weber theorem asserts that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field, which is generated by roots of unity, and Galois theory plays a pivotal role in its proof
- The proof of the Kronecker-Weber theorem utilizes the fact that the Galois group of a cyclotomic field is isomorphic to the multiplicative group of integers modulo the order of the root of unity $(\mathbb{Z}/n\mathbb{Z})^\times$
- Galois theory is employed to demonstrate that every subfield of a cyclotomic field is itself a cyclotomic field, corresponding to a subgroup of the Galois group
- The Kronecker-Weber theorem is a cornerstone result in the theory of abelian extensions and has significant implications for the study of cyclotomic fields and their subfields

Class field theory and conductor-discriminant formula

- Class field theory is a major branch of algebraic number theory that describes the abelian extensions of an algebraic number field in terms of its ideal class group and idele class group, heavily relying on Galois-theoretic techniques
- The conductor-discriminant formula, which relates the conductor of an abelian extension to the discriminant of its ring of integers, is another important result in algebraic number theory that depends on Galois theory
- Galois theory provides the necessary tools and framework for proving key results in class field theory, such as the existence and uniqueness of class fields and the Artin reciprocity law
- The interplay between Galois theory and class field theory has led to significant advances in our understanding of abelian extensions and their arithmetic properties

12.3 Galois representations and modular forms

Galois representations and modular forms are powerful tools in modern number theory. They connect abstract algebra with complex analysis, providing insights into fundamental mathematical structures and relationships.

These concepts have led to groundbreaking results, including the proof of Fermat's Last Theorem. The Langlands program, which links Galois representations and automorphic forms, continues to drive research and shape our understanding of arithmetic geometry.

Galois representations and modular forms

Definition and connection

- Galois representation: continuous homomorphism from the absolute Galois group of a field to the general linear group of a vector space over a field
- Modular forms: complex analytic functions on the upper half-plane that satisfy certain transformation properties under the action of the modular group
- Transformation properties include invariance under specific subgroups of the modular group and holomorphicity at cusps
- Galois representations associated with modular forms obtained by studying the action of the absolute Galois group on the étale cohomology of modular curves
- Étale cohomology is a cohomology theory for algebraic varieties that takes into account the arithmetic properties of the variety
- Modular curves are algebraic curves that parametrize elliptic curves with additional structure (level structure)

Key results and conjectures

- Langlands correspondence predicts a bijection between certain Galois representations and automorphic representations of the adelic points of a reductive group
- Automorphic representations are representations of reductive groups over adeles that satisfy certain analytic and algebraic properties

- Adeles are a ring of "local" fields that contain information about all completions of a global field
- Taniyama-Shimura conjecture (now a theorem) states that every elliptic curve over the rational numbers is modular, i.e., its L-function agrees with the L-function of a modular form
- L-functions are complex analytic functions associated with arithmetic objects that encode important information about their properties
- Proof of Fermat's Last Theorem by Andrew Wiles relied on establishing the modularity of semistable elliptic curves, connecting Galois representations and modular forms
- Semistable elliptic curves have a specific type of reduction at primes of bad reduction (multiplicative reduction)

Significance of the Langlands program

Overview and scope

- Langlands program is a series of far-reaching conjectures that relate Galois representations and automorphic forms
- Seeks to establish a correspondence between ℓ -adic Galois representations of the absolute Galois group of a number field and automorphic representations of the adelic points of a reductive group
- ℓ -adic Galois representations are Galois representations on vector spaces over the field of ℓ -adic numbers (completions of the algebraic closure of the rational numbers with respect to a prime ℓ)
- Langlands correspondence proven in special cases ($GL(1)$, $GL(2)$) but remains open in general
- $GL(n)$ denotes the general linear group of degree n , consisting of invertible $n \times n$ matrices

Global and local Langlands correspondence

- Global Langlands correspondence relates global Galois representations to automorphic representations
- Global Galois representations are representations of the absolute Galois group of a number field
- Local Langlands correspondence deals with local Galois representations and local automorphic representations
- Local Galois representations are representations of the absolute Galois group of a local field (completion of a number field with respect to a prime)
- Local automorphic representations are representations of the points of a reductive group over a local field
- Langlands program has deep connections with number theory, representation theory, and harmonic analysis
- Proof of the Taniyama-Shimura conjecture can be viewed as a special case of the Langlands correspondence for $GL(2)$ over the rational numbers

Galois representations in elliptic curves

Galois representations and L-functions

- Elliptic curves are algebraic curves defined by a cubic equation in two variables, and their L-functions encode important arithmetic information
- Galois representation associated with an elliptic curve obtained by studying the action of the absolute Galois group on the Tate module of the curve
- Tate module is the inverse limit of the torsion points of an elliptic curve
- Taniyama-Shimura conjecture (now a theorem) states that the L-function of an elliptic curve over the rational numbers agrees with the L-function of a modular form
- Proof of the Taniyama-Shimura conjecture by Andrew Wiles and Richard Taylor relied on establishing the modularity of semistable elliptic curves using Galois representations

Applications and related conjectures

- Birch and Swinnerton-Dyer conjecture relates the rank of an elliptic curve to the order of vanishing of its L-function at $s=1$, and Galois representations play a crucial role in its study
- Rank of an elliptic curve is the number of independent rational points of infinite order
- Galois representations have been used to prove important results about the torsion points and isogenies of elliptic curves
- Torsion points are points of finite order on an elliptic curve
- Isogenies are morphisms between elliptic curves that preserve the group structure

Impact on modern number theory

Breakthroughs and new directions

- Galois representations have revolutionized number theory by providing a powerful tool for studying arithmetic objects (elliptic curves, modular forms)
- Proof of Fermat's Last Theorem by Andrew Wiles relied heavily on Galois representations to establish the modularity of semistable elliptic curves
- Langlands program, relating Galois representations and automorphic forms, has become a central focus of research in modern number theory
- Galois representations used to prove important results in Iwasawa theory, which studies the behavior of arithmetic objects in towers of number fields
- Iwasawa theory investigates the growth of arithmetic invariants (class groups, unit groups) in infinite extensions of number fields

Connections with other fields

- Study of p-adic Galois representations has led to significant advances in understanding p-adic L-functions and p-adic Hodge theory
- p-adic L-functions are analogues of complex L-functions that take values in p-adic fields

- p-adic Hodge theory studies the relationship between p-adic Galois representations and p-adic differential equations
- Galois representations have played a key role in the development of the theory of motives, which aims to provide a unified framework for studying arithmetic and geometric objects
- Motives are abstract objects that capture the essential properties of algebraic varieties and their cohomology
- Use of Galois representations has opened up new avenues for collaboration between number theory and other areas of mathematics (representation theory, algebraic geometry)

12.4 Differential Galois theory

Differential Galois theory extends classical Galois theory to tackle differential equations. It replaces the base field with a differential field and uses the differential Galois group to decode solution symmetries, much like the Galois group in classical theory.

This theory helps study linear differential equations' algebraic properties. The differential Galois group's structure reveals solution nature, algebraic relations, and symmetries. It also determines if equations are solvable by quadratures, connecting to broader applications in mathematics and physics.

Fundamental Concepts of Differential Galois Theory

Extension of Classical Galois Theory

- Differential Galois theory extends classical Galois theory to deal with differential equations and their solutions
- The base field is replaced by a differential field, a field equipped with a derivation operator satisfying certain properties
- The differential Galois group of a linear differential equation encodes information about the symmetries and structure of the solution space, analogous to the Galois group in classical Galois theory

Key Concepts and Structures

- The Picard-Vessiot extension of a differential field contains all the solutions of a given linear differential equation, similar to the splitting field in classical Galois theory
- It is the smallest extension containing all the solutions
- The differential Galois group acts on the solution space of the Picard-Vessiot extension
- The fundamental theorem of differential Galois theory establishes a correspondence between differential field extensions and closed subgroups of the differential Galois group
- The Galois correspondence in differential Galois theory relates intermediate differential fields to closed subgroups of the differential Galois group, analogous to the classical Galois correspondence

Differential Galois Theory for Linear Equations

Studying Solutions of Linear Differential Equations

- Differential Galois theory provides a framework for studying the algebraic properties of solutions to linear differential equations

- The structure of the differential Galois group provides information about the nature of the solutions
- Algebraic relations and symmetries among the solutions can be determined from the differential Galois group
- The solvability of a linear differential equation by quadratures (integrals, exponentials, and algebraic operations) is related to the solvability of the corresponding differential Galois group
- Differential Galois theory can determine the existence of liouvillian solutions, which are solutions expressible in terms of quadratures

Algorithms and Techniques

- Algorithms and techniques of differential Galois theory can be applied to find closed-form solutions or prove the non-existence of such solutions for certain classes of linear differential equations
- Kovacic's algorithm is a notable example for second-order linear differential equations
- The differential Galois group can be used to determine the minimal number of quadratures required to express the solutions of a linear differential equation
- Computational methods in differential Galois theory, such as factorization algorithms for linear differential operators, aid in the study of linear differential equations

Solvability of Differential Equations vs Differential Galois Groups

Relationship between Solvability and Differential Galois Groups

- The solvability of a linear differential equation by quadratures is closely related to the structure and properties of its differential Galois group
- If the differential Galois group is solvable (has a subnormal series with abelian quotients), then the equation is solvable by quadratures
- The Lie-Kolchin theorem characterizes solvable connected linear algebraic groups, providing a criterion for determining the solvability of differential equations by quadratures

Liouville Extensions and Solvability

- The Liouville extension of a differential field is obtained by adjoining integrals, exponentials, and algebraic elements
- It plays a crucial role in the solvability of differential equations
- The Liouville-Ritt theorem states that if the differential Galois group of a linear differential equation is solvable, then all its solutions lie in a Liouville extension of the base field
- The structure of the differential Galois group determines the minimal Liouville extension containing the solutions of a linear differential equation

Applications of Differential Galois Theory

Dynamical Systems and Integrability

- Differential Galois theory has applications in studying integrability and symmetries of dynamical systems

- The Morales-Ramis theorem uses differential Galois theory to provide a necessary condition for the integrability of Hamiltonian systems
- It relates the integrability to the solvability of the differential Galois group of the variational equations along a particular solution
- Differential Galois theory can provide information about the existence of first integrals and conservation laws for dynamical systems

Mathematical Physics

- In mathematical physics, differential Galois theory has been applied to study the integrability and symmetries of various equations (Schrödinger equation, Korteweg-de Vries equation)
- Differential Galois theory has connections with the theory of Lie algebras and Lie groups, fundamental tools in studying symmetries and conservation laws in physics
- The techniques of differential Galois theory have been applied to the study of isomonodromic deformations and the Riemann-Hilbert problem, with applications in integrable systems and mathematical physics
- Differential Galois theory has been used to study the integrability of non-linear differential equations, such as the Painlevé equations, which arise in various areas of mathematical physics