MATS UNIVERSITY

NAAC GRADE A+ ACCREDITED UNIVERSITY

# MATS CENTRE FOR DISTANCE & ONLINE EDUCATION

## Algebra

**Master of Science (M.Sc.)**
**Semester - 1**


SELF LEARNING MATERIAL

MATS UNIVERSITY
www.matsuniversity.ac.in
NAAC GRADE A+
ACCREDITED UNIVERSITY

# MSCMODL101
# ALGEBRA

COURSE DEVELOPMENTEXPERT COMMITTEE

| | |
|---|---|
| Prof (Dr) K P Yadav | Vice Chancellor, MATS University |
| Prof (Dr) A J Khan | Professor Mathematics, MATS University |
| Prof (Dr) D K Das | Professor Mathematics, CCET, Bhilai |

COURSE COORDINATOR

| | |
|---|---|
| Prof (Dr.) A. J. Khan | Professor, MATS University |

COURSE /BLOCK PREPARATION

| | |
|---|---|
| Dr Vinita Dewangan | Associate Professor, MATS University |

March 2025

ISBN: 978-81-987774-0-9



Printed &Published on behalf of MATS University, Village-Gullu, Aarang, RaipurbyMr. MeghanadhuduKatabathuni, Facilities & Operations, MATS University,Raipur(C.G.)


Printed at: The Digital Press, Krishna Complex, Raipur-492001(Chhattisgarh)

## Acknowledgement

The material (pictures and passages) we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book.

Notes

# COURSE INTRODUCTION

Algebra forms the foundation of many areas in mathematics and its applications in science and engineering. This course explores essential algebraic structures, linear transformations, vector spaces, eigenvalue problems, and their applications to differential equations and coding theory. The course aims to build strong conceptual and problem-solving skills through a structured modular approach.

**Module 1: Group Theory**

This module introduces key concepts in group theory, including direct products and group actions on a set. Topics covered include isotropy subgroups, orbits, and applications of G-sets to counting. The module also explores counting theorems, p-groups, and the fundamental Sylow theorems.

**Module 2: Applications of Sylow Theory and Ring Theory**

Building on the Sylow theorems, this module examines their applications to p-groups and the class equation. Further applications will be explored in relation to ring theory, covering rings of polynomials, polynomials in an indeterminate, the evaluation homomorphism, and the factorization of polynomials over a field.

**Module 3: Field Theory**

This module covers extension fields, distinguishing between algebraic and transcendental elements. Topics include irreducible polynomials over a field, simple extensions, algebraic extensions, finite extensions, and the structure of finite fields.

**Module 4: Automorphisms and Splitting Fields**

Students will explore automorphisms of fields, conjugation isomorphisms, and the connection between automorphisms and fixed fields. This module introduces the Frobenius automorphism and splitting fields, providing insight into the structure of field extensions.

**Module 5: Galois Theory**

This module introduces separable extensions, normal extensions, and the main theorem of Galois theory. Illustrations of Galois theory include applications to symmetric functions and their significance in modern algebra.

# MODULE 1

## UNIT 1.1

## GROUP THEORY

### Objectives

- Understand the concept of direct products in group theory.
- Explore group actions on a set and their applications.
- Learn about isotropy subgroups and orbits.
- Study counting theorems and their significance in combinatorial group theory.
- Analyze p-groups and the Sylow theorems.

### 1.1.1: Introduction to Group Theory

A group is one of the fundamental structures in abstract algebra. It consists of a set of elements together with an operation that combines any two elements to form a third element, satisfying four conditions called the group axioms.

### Definition of a Group

A group (G, •) consists of a set G together with a binary operation • that satisfies the following axioms:

1. **Closure**: For all a, b in G, the result of a • b is also in G.
2. **Associativity**: For all a, b, c in G, (a • b) • c = a • (b • c).
3. **Identity element**: There exists an element e in G such that for every element a in G, e • a = a • e = a.
4. **Inverse element**: For each a in G, there exists an element b in G such that a • b = b • a = e, where e is the identity element.

Notes

If the operation is also commutative, meaning a • b = b • a for all a, b in G, then the group is called an **abelian group** or a **commutative group**.

**Examples of Groups**

a. **The integers Z under additionform a group:**

- Closure: The sum of two integers is an integer.
- Associativity: (a + b) + c = a + (b + c) for all integers a, b, and c.
- Identity: The integer 0 serves as the identity element.
- Inverse: For any integer a, its inverse is -a.
- This is an abelian group.

**b.** ***The non-zero real numbers R under multiplication*** **form a group:**

- Closure: The product of two non-zero real numbers is a non-zero real number.
- Associativity: (a × b) × c = a × (b × c) for all non-zero real numbers a, b, and c.
- Identity: The number 1 serves as the identity element.
- Inverse: For any non-zero real number a, its inverse is 1/a.
- This is an abelian group.

c. **The set of nxn invertible matrices with real entries under matrix multiplication** forms a group denoted by GL(n, R) (General Linear Group):

- Closure: The product of two invertible matrices is invertible.

- Associativity: matrix multiplication is associative.
- Identity: The identity matrix serves as the identity element.
- Inverse: Every invertible matrix has an inverse matrix.
- This is generally a non-abelian group for $n \geq 2$.

### 1.1.2 : Order of a Group and Order of an Element

The **order of a group** G, denoted by |G|, is the number of elements in G. If G has infinitely many elements, we say G has infinite order.

The **order of an element** a in a group G, denoted by |a|, is the smallest positive integer n such that a^n = e, where e is the identity element. If no such n exists, a has infinite order.

### 1.1.3: Subgroups

A **subgroup** H of a group G is a subset of G that is itself a group under the operation of G. For H to be a subgroup, it must:

- Contain the identity element of G.
- Be closed under the group operation.
- Contain the inverse of each of its elements.

### 1.1.4: Cyclic Groups

A group G is **cyclic** if there exists an element a in G such that every element in G can be written as a^n for some integer n. In this case, a is called a generator of G, and we write G = ⟨a⟩.

### Lagrange's Theorem

If H is a subgroup of a finite group G, then the order of H divides the order of G. That is, |H| divides |G|.

### 1.1.5: Cosets and Normal Subgroups

Notes

For a subgroup H of a group G and an element a in G, the set aH = {ah | h ∈ H} is called the **left coset** of H in G with respect to a. Similarly, Ha = {ha | h ∈ H} is the **right coset**.

A subgroup N of G is **normal** if, for every a in G, aN = Na. This is equivalent to saying that all left cosets of N are equal to their corresponding right cosets.

### 1.1.6: Quotient Groups

If N is a normal subgroup of G, then the set G/N of all left cosets of N in G forms a group under the operation (aN)(bN) = (ab)N. This group is called the **quotient group** of G by N.

### 1.1.7: Homomorphisms and Isomorphisms

A **group homomorphism** is a function f: G → H between two groups that preserves the group operation: f(a • b) = f(a) * f(b) for all a, b in G, where • is the operation in G and * is the operation in H.

An **isomorphism** is a bijective homomorphism. Two groups are **isomorphic** if there exists an isomorphism between them, meaning they have the same abstract structure.

**The First Isomorphism Theorem**

If φ: G → H is a group homomorphism, then:

1. The kernel of φ, Ker(φ) = {a ∈ G | φ(a) = e_H}, is a normal subgroup of G.
2. The image of φ, Im(φ) = {φ(a) | a ∈ G}, is a subgroup of H.
3. G/Ker(φ) is isomorphic to Im(φ).

### 1.1.8: Direct Products of Groups

The direct product is a way to construct a new group from existing groups. It allows us to build complex groups from simpler ones.

**Definition of Direct Product**

Notes

Given two groups (G, •) and (H, *), their **direct product** G × H is the set of all ordered pairs (g, h) where g ∈ G and h ∈ H, with the operation defined componentwise:

$(g_1, h_1) \odot (g_2, h_2) = (g_1 \bullet g_2, h_1 * h_2)$

**Properties of Direct Products**

1. **Identity**: The identity element of G × H is $(e_G, e_H)$, where $e_G$ and $e_H$ are the identity elements of G and H, respectively.

2. **Inverse**: The inverse of an element (g, h) in G × H is $(g^{-1}, h^{-1})$, where $g^{-1}$ is the inverse of g in G and $h^{-1}$ is the inverse of h in H.

3. **Order**: If G and H are finite groups, then |G × H| = |G| × |H|.

4. **Abelian**: G × H is abelian if and only if both G and H are abelian.

**Examples of Direct Products**

1. **$Z_2 \times Z_3$**: Consider the cyclic group $Z_2 = \{0, 1\}$ under addition modulo 2 and the cyclic group $Z_3 = \{0, 1, 2\}$ under addition modulo 3. Their direct product $Z_2 \times Z_3$ consists of the elements: {(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)}

For example, (1,2) + (1,1) = (1+1 mod 2, 2+1 mod 3) = (0,0).

2. **R × R**: The direct product of the real numbers under addition with itself is the Cartesian plane $R^2$ under component-wise addition.

**1.1.9: Subgroups of Direct Products**

A subgroup of G × H need not be a direct product of subgroups of G and H. However, there are two important types of subgroups:

1. For any subgroup K of G, K × H is a subgroup of G × H.

Notes

2. For any subgroup L of H, $G \times L$ is a subgroup of $G \times H$.

### 1.1.10: Projections and Embeddings

For a direct product $G \times H$, there are natural **projection homomorphisms**:

- $\pi_1: G \times H \to G$ defined by $\pi_1(g, h) = g$
- $\pi_2: G \times H \to H$ defined by $\pi_2(g, h) = h$

There are also natural **embedding homomorphisms**:

- $\iota_1: G \to G \times H$ defined by $\iota_1(g) = (g, e_H)$
- $\iota_2: H \to G \times H$ defined by $\iota_2(h) = (e_G, h)$

### 1.1.11: Internal Direct Products

A group G is an **internal direct product** of its subgroups $N_1$ and $N_2$ if:

1. $N_1$ and $N_2$ are normal subgroups of G.
2. $N_1 \cap N_2 = \{e\}$.
3. $G = N_1N_2 = \{n_1n_2 \mid n_1 \in N_1, n_2 \in N_2\}$.

When G is an internal direct product of $N_1$ and $N_2$, G is isomorphic to the external direct product $N_1 \times N_2$.

### 1.1.12: Direct Product of Multiple Groups

The direct product can be extended to any finite number of groups. For groups $G_1$, $G_2$, ..., $G_n$, their direct product $G_1 \times G_2 \times ... \times G_n$ consists of n-tuples $(g_1, g_2, ..., g_n)$ with component-wise operations.

### 1.1.13: Direct Sum

For abelian groups written additively, the direct product is sometimes called the **direct sum** and denoted by $G_1 \oplus G_2 \oplus ... \oplus G_n$. The operation is component-wise addition.

### The Fundamental Theorem of Finitely Generated Abelian Groups

Every finitely generated abelian group is isomorphic to a direct product of cyclic groups:

$$G \cong Z^r \oplus Z_{p_1}^{\{a_1\}} \oplus Z_{p_2}^{\{a_2\}} \oplus \ldots \oplus Z_{p_n}^{\{a_n\}}$$

where r is a non-negative integer, Z is the group of integers, and $Z_{p^a}$ is the cyclic group of order $p^a$ with p prime.

### 1.1.14: Group Actions and Orbits

Group actions allow us to understand how a group can act on a set, providing a powerful framework for analyzing symmetry and other properties.

#### Definition of a Group Action

A **group action** of a group G on a set X is a function $\varphi: G \times X \to X$ (often written as $g \cdot x$ instead of $\varphi(g,x)$) that satisfies:

1. **Identity**: $e \cdot x = x$ for all $x \in X$, where e is the identity element of G.
2. **Compatibility**: $(g \cdot h) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$ and all $x \in X$.

#### Examples of Group Actions

1. **The symmetric group $S_n$ acts on the set {1, 2, ..., n}** by permutation: $\sigma \cdot i = \sigma(i)$ for $\sigma \in S_n$ and $i \in \{1, 2, ..., n\}$.
2. **A group G acts on itself by conjugation**: $g \cdot x = gxg^{-1}$ for all $g, x \in G$.
3. **A group G acts on the set of its subgroups** by conjugation: $g \cdot H = gHg^{-1}$ for all $g \in G$ and all subgroups H of G.
4. **The dihedral group $D_n$ acts on the vertices of a regular n-gon** by rotation and reflection.

### 1.1.15: Orbits and Stabilizers

For a group action of G on X and an element $x \in X$:

Notes

The **orbit** of x, denoted by Orb(x), is the set of all elements in X to which x can be moved by elements of G: $Orb(x) = \{g \cdot x \mid g \in G\}$

The **stabilizer** of x, denoted by Stab(x), is the subgroup of G consisting of all elements that fix x: $Stab(x) = \{g \in G \mid g \cdot x = x\}$

**Orbit-Stabilizer Theorem**

For a group G acting on a set X and an element $x \in X$, if G is finite, then: $|Orb(x)| \times |Stab(x)| = |G|$

In other words, the size of the orbit of x multiplied by the size of the stabilizer of x equals the size of the group.

**1.1.16: Fixed Points and the Class Equation**

A **fixed point** of an element $g \in G$ is an element $x \in X$ such that $g \cdot x = x$.

For a finite group G acting on a finite set X, the **class equation** is: $|X| = |X^G| + \Sigma |Orb(x)|$

where $X^G = \{x \in X \mid g \cdot x = x \text{ for all } g \in G\}$ is the set of elements of X fixed by all elements of G, and the sum is taken over representatives x of the distinct orbits with $|Orb(x)| > 1$.

**Burnside's Lemma**

For a finite group G acting on a finite set X, the number of orbits equals the average number of fixed points: Number of orbits = $(1/|G|) \times \Sigma |X^g|$

where $X^g = \{x \in X \mid g \cdot x = x\}$ is the set of fixed points of g, and the sum is taken over all $g \in G$.

**1.1.17: Group Actions and Counting**

Group actions provide powerful tools for counting in combinatorics:

1. **Counting orbits** gives the number of essentially different configurations.

2. **Pólya's enumeration theorem** extends Burnside's lemma to count configurations by their "types."

### 1.1.18: Transitive and Regular Actions

A group action of G on X is transitive if for any x, y ∈ X, there exists g ∈ G such that g·x = y. In other words, there is exactly one orbit.

A group action is regular (or simply transitive) if it is transitive and the stabilizer of every point is trivial (i.e., contains only the identity element).

### The Orbit Decomposition

Under a group action, the set X is partitioned into orbits. Each orbit is an equivalence class under the relation x ~ y if and only if there exists g ∈ G such that g·x = y.

### Homomorphic Actions

If φ: G → Sym(X) is the homomorphism corresponding to an action of G on X (where Sym(X) is the symmetric group on X), then:

1. The kernel of φ is the set of elements that fix every point in X.
2. The image of φ is a subgroup of Sym(X) that represents the effective symmetries of X under the action.

### Solved Problems

**Problem 1: Determine whether the set of 2×2 matrices of the form [[a, b], [0, a]] where a ≠ 0 forms a group under matrix multiplication.**

**Solution:**

Let's call this set G. We need to check all four group axioms:

1. **Closure**: For any two matrices in G: [[a, b], [0, a]] × [[c, d], [0, c]] = [[ac, ad+bc], [0, ac]]

Notes

Since $ac \neq 0$ when $a \neq 0$ and $c \neq 0$, the result is in G. So G is closed under matrix multiplication.

2. **Associativity**: Matrix multiplication is always associative, so this axiom is satisfied.
3. **Identity**: The identity matrix [[1, 0], [0, 1]] is in G (take a = 1 and b = 0), and it serves as the identity element.
4. **Inverse**: For a matrix [[a, b], [0, a]] in G, we need its inverse to be in G as well. The inverse is $[[1/a, -b/a^2], [0, 1/a]]$, which has the required form with non-zero values on the diagonal.

Since all four axioms are satisfied, G is indeed a group under matrix multiplication.

**Problem 2: Find all subgroups of $Z_4 \times Z_2$, where $Z_4$ is the cyclic group of order 4 and $Z_2$ is the cyclic group of order 2.**

**Solution:**

First, let's enumerate the elements of $Z_4 \times Z_2$:

- $Z_4 = \{0, 1, 2, 3\}$ with addition modulo 4
- $Z_2 = \{0, 1\}$ with addition modulo 2
- $Z_4 \times Z_2 = \{(0,0), (0,1), (1,0), (1,1), (2,0), (2,1), (3,0), (3,1)\}$

The order of $Z_4 \times Z_2$ is 8. By Lagrange's theorem, the possible orders of subgroups are 1, 2, 4, and 8.

1. The trivial subgroup $\{(0,0)\}$ is the only subgroup of order 1.
2. Subgroups of order 2:
    - $\langle(2,0)\rangle = \{(0,0), (2,0)\}$
    - $\langle(0,1)\rangle = \{(0,0), (0,1)\}$
    - $\langle(2,1)\rangle = \{(0,0), (2,1)\}$
3. Subgroups of order 4:

- ⟨(1,0)⟩ = {(0,0), (1,0), (2,0), (3,0)} ≅ $Z_4$
- ⟨(0,1), (2,0)⟩ = {(0,0), (0,1), (2,0), (2,1)} ≅ $Z_2 \times Z_2$
- ⟨(1,1)⟩ = {(0,0), (1,1), (2,0), (3,1)}
- ⟨(3,1)⟩ = {(0,0), (1,0), (2,1), (3,0)}

4. The entire group $Z_4 \times Z_2$ is the only subgroup of order 8.

In total, $Z_4 \times Z_2$ has 9 subgroups.

**Problem 3: Let G be a group acting on a set X. Prove that if x and y are in the same orbit, then Stab(x) and Stab(y) are conjugate subgroups.**

**Solution:**

If x and y are in the same orbit, then there exists some $g \in G$ such that $g \cdot x = y$.

We want to show that $Stab(y) = g \cdot Stab(x) \cdot g^{-1}$, where $g \cdot Stab(x) \cdot g^{-1} = \{ghg^{-1} \mid h \in Stab(x)\}$.

Let $h \in Stab(x)$. Then $h \cdot x = x$.

Consider $ghg^{-1} \in g \cdot Stab(x) \cdot g^{-1}$. We need to show that $ghg^{-1} \in Stab(y)$, i.e., $(ghg^{-1}) \cdot y = y$.

$(ghg^{-1}) \cdot y = (ghg^{-1}) \cdot (g \cdot x) = g \cdot (h \cdot (g^{-1} \cdot (g \cdot x))) = g \cdot (h \cdot x) = g \cdot x = y$

Therefore, $ghg^{-1} \in Stab(y)$, so $g \cdot Stab(x) \cdot g^{-1} \subseteq Stab(y)$.

Conversely, let $k \in Stab(y)$. Then $k \cdot y = y$.

Consider $g^{-1}kg \in G$. We have: $(g^{-1}kg) \cdot x = g^{-1} \cdot (k \cdot (g \cdot x)) = g^{-1} \cdot (k \cdot y) = g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = x$

Thus, $g^{-1}kg \in Stab(x)$, which implies $k \in g \cdot Stab(x) \cdot g^{-1}$.

Therefore, $Stab(y) \subseteq g \cdot Stab(x) \cdot g^{-1}$.

Combining both inclusions, we get $Stab(y) = g \cdot Stab(x) \cdot g^{-1}$, meaning Stab(x) and Stab(y) are conjugate subgroups.

Notes

**Problem 4: Calculate the number of distinct necklaces that can be made with 4 beads, each of which can be either red or blue.**

**Solution:**

This is a problem of counting orbits under a group action. We can use Burnside's lemma.

The cyclic group $C_4$ (of order 4) acts on the set of all possible colorings of 4 beads by rotation. There are $2^4 = 16$ possible colorings (for each bead, we can choose either red or blue).

By Burnside's lemma, the number of orbits (distinct necklaces) is: Number of orbits = $(1/|G|) \times \Sigma |X^g|$

where $X^g$ is the set of colorings fixed by element g of the group.

The group $C_4$ has 4 elements: the identity e, and rotations by 90°, 180°, and 270°.

1. For the identity e, all 16 colorings are fixed: $|X^e| = 16$.
2. For a 90° rotation (call it r), a coloring is fixed only if all beads have the same color. So $|X^r| = 2$ (all red or all blue).
3. For a 180° rotation ($r^2$), a coloring is fixed if beads 1 and 3 have the same color, and beads 2 and 4 have the same color. So $|X^{r^2}| = 2^2 = 4$.
4. For a 270° rotation ($r^3$), like the 90° rotation, only the 2 solid-colored necklaces are fixed. So $|X^{r^3}| = 2$.

Using Burnside's lemma: Number of orbits = $(1/4) \times (16 + 2 + 4 + 2) = (1/4) \times 24 = 6$

Thus, there are 6 distinct necklaces possible.

**Problem 5: Let G be a group of order 15. Prove that G is cyclic.**

**Solution:**

By Lagrange's theorem, the order of any element in G divides the order of G. So the possible orders for elements are 1, 3, 5, and 15.

The only element of order 1 is the identity element e.

Let's consider the number of elements of each possible order:

1. For elements of order 3, they must satisfy $a^3 = e$. Each such element generates a cyclic subgroup of order 3.
2. For elements of order 5, they must satisfy $a^5 = e$. Each such element generates a cyclic subgroup of order 5.

The Sylow theorems tell us that G has a Sylow 3-subgroup (a subgroup of order 3) and a Sylow 5-subgroup (a subgroup of order 5).

The number of Sylow p-subgroups, $n_p$, satisfies:

- $n_p \equiv 1 \pmod{p}$
- $n_p$ divides the order of G divided by $p^k$, where $p^k$ is the highest power of p dividing |G|.

For p = 3, $n_3 \equiv 1 \pmod{3}$ and $n_3$ divides 5. The only possibility is $n_3 = 1$. For p = 5, $n_5 \equiv 1 \pmod{5}$ and $n_5$ divides 3. The only possibility is $n_5 = 1$.

So G has exactly one Sylow 3-subgroup (call it H) and one Sylow 5-subgroup (call it K).

Since both H and K are unique, they are normal in G. Also, $H \cap K = \{e\}$ because gcd(3,5) = 1.

Since $|H| \times |K| = 3 \times 5 = 15 = |G|$, we have $G = H \times K$ (internal direct product).

Since H is a group of order 3 and K is a group of order 5, both are cyclic (all groups of prime order are cyclic). Say $H = \langle a \rangle$ and $K = \langle b \rangle$.

Now, consider the element ab in G. We have:

- $(ab)^3 = a^3b^3 = eb^3 = b^3$

Notes

- $(ab)^5 = a^5b^5 = a^{5e} = a^5$
- $(ab)^{15} = a^{15}b^{15} = (a^3)^5(b^5)^3 = e^5e^3 = e$

We need to find the order of ab. Since a has order 3 and b has order 5, and 3 and 5 are coprime, the order of ab is lcm(3,5) = 15.

Thus, G = ⟨ab⟩ is cyclic of order 15.

**Unsolved Problems**

Problem 1: Prove that every subgroup of a cyclic group is cyclic.

Problem 2: Let G be a group and let H and K be normal subgroups of G such that $H \cap K = \{e\}$. Prove that for all $h \in H$ and $k \in K$, $hk = kh$.

Problem 3: Determine the number of non-isomorphic groups of order 8.

Problem 4: For a finite group G, prove that if for every proper subgroup H of G, there exists an element $g \in G$ such that $g^2 \notin H$, then G is a 2-group (i.e., $|G| = 2^n$ for some n).

Problem 5: Find all elements of the dihedral group $D_4$ (the group of symmetries of a square) that commute with a 90-degree rotation.

### 1.2.1: Isotropy Subgroups

The isotropy subgroup (also called the stabilizer) is a fundamental concept in group action theory that helps us understand how group elements interact with specific points in a set.

**Definition of Isotropy Subgroup**

Let G be a group acting on a set X. For any element x in X, the isotropy subgroup (or stabilizer) of x, denoted $G_x$, is defined as:

$G_x = \{g \in G \mid g \cdot x = x\}$

In other words, $G_x$ consists of all elements of G that fix the point x.It is straightforward to verify that $G_x$ is indeed a subgroup of G.

**Properties of Isotropy Subgroups**

1. **Subgroup Property**: For any x in X, $G_x$ is a subgroup of G.

Proof:

- Identity: The identity element $e \in G$ satisfies $e \cdot x = x$, so $e \in G\_x$.
- Closure: If $g, h \in G_x$, then $g \cdot x = x$ and $h \cdot x = x$. So $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$, which means $gh \in G_x$.
- Inverse: If $g \in G_x$, then $g \cdot x = x$. Applying $g^{(-1)}$ to both sides: $g^{(-1)} \cdot (g \cdot x) = g^{(-1)} \cdot x$, which gives $x = g^{(-1)} \cdot x$, so $g^{(-1)} \in G_x$.

2. **Conjugacy Relation**: For any $g \in G$ and $x \in X$, the isotropy subgroup of $g \cdot x$ is conjugate to the isotropy subgroup of x:

$G_{(g \cdot x)} = g G_x g^{(-1)}$

Proof: An element h belongs to $G_{(g \cdot x)}$ if and only if $h \cdot (g \cdot x) = g \cdot x$. This is equivalent to $g^{(-1)} \cdot h \cdot g \cdot x = x$, which means $g^{(-1)} hg \in G_x$.Thus, $h \in g G_x g^{(-1)}$.

Notes

3. **Fixed Points**: The set of all points fixed by a specific group element $g \in G$ is:

$X^g = \{x \in X \mid g \cdot x = x\}$

This is the set of all points x such that g belongs to the isotropy subgroup $G_x$.

**Example 1: Dihedral Group Action**

Consider the dihedral group $D_4$ acting on the vertices of a square. Label the vertices 1, 2, 3, and 4 in clockwise order.

Let's find the isotropy subgroup for vertex 1:

$D_4$ consists of:

- Identity (e): leaves all vertices in place
- Rotations: r (90° clockwise), $r^2$ (180°), $r^3$ (270°)
- Reflections: s (across horizontal axis), sr (across vertical axis), $sr^2$ (across diagonal from vertex 1 to 3), $sr^3$ (across diagonal from 2 to 4)

The elements that fix vertex 1 are:

- e (identity): leaves all vertices in place
- $sr^2$ (reflection across diagonal 1-3): fixes vertices 1 and 3

Therefore, $G_1 = \{e, sr^2\}$, which is isomorphic to $Z_2$.

**Example 2: Symmetric Group Action**

Consider $S_4$ acting on the set X = {1, 2, 3, 4} by the standard permutation action.

The isotropy subgroup of element 1 is: $G_1 = \{\sigma \in S_4 \mid \sigma(1) = 1\}$

This consists of all permutations that fix 1, which is isomorphic to $S_3$ as they freely permute {2, 3, 4}.

So $G_1 \cong S_3$, with order $|G_1| = 6$.

**Relationship with Orbits**

One of the most important results connecting isotropy subgroups with orbits is:

**Orbit-Stabilizer Theorem**: For a group G acting on a set X and an element $x \in X$:

$|G| = |Orb(x)| \times |G_x|$

where $|G|$ is the order of the group, $|Orb(x)|$ is the size of the orbit of x, and $|G_x|$ is the order of the isotropy subgroup of x.

This theorem provides a powerful method for counting orbit sizes when we know the isotropy subgroups.

**1.2.2: Applications of Group Actions**

Group actions provide a unifying framework for various mathematical problems. Here are several important applications:

**Counting Problems and Burnside's Lemma**

Burnside's Lemma (also known as the Cauchy-Frobenius Lemma) is a powerful tool for counting orbits under a group action.

**Burnside's Lemma**: Let G be a finite group acting on a finite set X. The number of orbits, denoted $|X/G|$, is given by:

$|X/G| = (1/|G|) \times \Sigma_{\{g \in G\}} |X^g|$

where $X^g = \{x \in X \mid g \cdot x = x\}$ is the set of elements fixed by g.

**Example: Necklaces with Colored Beads**

Consider necklaces made of n beads, each colored with one of k colors. Two necklaces are considered equivalent if one can be rotated to obtain the other.

This problem can be modeled as the cyclic group $C_n$ acting on the set X of all possible colorings ($k^n$ in total). By Burnside's Lemma, the number of distinct necklaces is:

Notes

Number of distinct necklaces = $(1/n) \times \Sigma_{\{d|n\}} \varphi(d) \times k^{(n/d)}$

where φ is Euler's quotient function and the sum is over all divisors d of n.

**Simplification of Symmetric Structures**

Group actions help identify symmetries in mathematical structures, simplifying their analysis.

**Example: Platonic Solids**

The rotational symmetry groups of the Platonic solids are:

- Tetrahedron: $A_4$ (alternating group on 4 elements)
- Cube/Octahedron: $S_4$ (symmetric group on 4 elements)
- Dodecahedron/Icosahedron: $A_5$ (alternating group on 5 elements)

These group actions explain why there are exactly five Platonic solids.

**Normal Subgroups and Quotient Groups**

Group actions provide a geometric interpretation of normal subgroups and quotient groups.

If N is a normal subgroup of G, then G acts on itself by conjugation: $g \cdot x = gxg^{(-1)}$. The orbits under this action are precisely the conjugacy classes of G. The isotropy subgroup of the identity element e is the centralizer of G.

**Sylow Theorems**

Group actions play a crucial role in proving Sylow's theorems, which are fundamental results in group theory concerning the existence and properties of subgroups whose orders are powers of prime numbers.

**First Sylow Theorem**: If G is a finite group and p is a prime dividing |G|, then G has a subgroup of order $p^k$, where $p^k$ is the highest power of p dividing |G|.

The proof uses the action of G on the set of all subsets of G of size $p^k$ by left multiplication.

**Galois Theory**

In Galois theory, the Galois group of a polynomial acts on its roots. This action reveals deep connections between field extensions and solvability of polynomial equations.

For a polynomial f(x) with Galois group G, the orbits of the roots under the action of G correspond to the irreducible factors of f(x).

**Representation Theory**

Group actions on vector spaces lead to representation theory, which studies how groups can be represented as linear transformations of vector spaces.

A representation of a group G on a vector space V is a homomorphism $\rho: G \to GL(V)$, where GL(V) is the general linear group of V.

**Crystallography**

The classification of crystal structures relies heavily on group actions. The 230 space groups in three dimensions describe all possible symmetric arrangements of atoms in crystals.

**UNIT 1.3**

### 1.3.1: Counting Theorems

Counting theorems in group theory provide powerful tools for enumeration problems involving symmetry. Here are the key results:

**Orbit-Counting Formula (Burnside's Lemma)**

As mentioned earlier, Burnside's Lemma gives us a way to count the number of orbits:

$|X/G| = (1/|G|) \times \Sigma_{\{g \in G\}} |X^g|$

**Pólya Enumeration Theorem**

Pólya's enumeration theorem extends Burnside's Lemma to situations where we not only want to count orbits but also need to classify them according to some property.

Let G be a group acting on a set X, and let w be a weight function that assigns weights to elements of X. The Pólya enumeration theorem gives a generating function for the weights of the orbits:

$Z_{G(w)} = (1/|G|) \times \Sigma_{\{g \in G\}} w^{\{cycle(g)\}}$

where cycle(g) represents the cycle structure of the permutation g, and $w^{\{cycle(g)\}}$ is a monomial determined by this cycle structure.

**Example: Colored Cubes**

Consider coloring the faces of a cube with k colors. The symmetry group of the cube, $S_4$, acts on the 6 faces.

Using Pólya's theorem, the generating function for the number of distinct colorings is:

$Z_G(x_1 + x_2 + ... + x_k) = (1/24) \times (x_1 + x_2 + ... + x_k)^6 + ...$(additional terms based on cycle structures)

**Orbit-Stabilizer Theorem**

As introduced earlier, the Orbit-Stabilizer theorem relates the size of an orbit to the order of the group and the order of an isotropy subgroup:

$|G| = |Orb(x)| \times |G_x|$

This immediately gives:

$|Orb(x)| = |G| / |G_x|$

This theorem is particularly useful for calculating orbit sizes when the isotropy subgroups are known.

**Class Equation**

The class equation is a fundamental result that divides the elements of a group into conjugacy classes:

$|G| = |Z(G)| + \Sigma |Cl(g_i)|$

where Z(G) is the center of G, and the sum is taken over representatives $g_i$ of non-singleton conjugacy classes $Cl(g_i)$.

This can be derived by considering the action of G on itself by conjugation.

**The Cauchy-Frobenius-Burnside Formula**

This is a generalized version of Burnside's Lemma that takes into account a weight function:

$\Sigma_{\{[x]\in X/G\}} w([x]) = (1/|G|) \times \Sigma_{\{g\in G\}} \Sigma_{\{x\in X^g\}} w(x)$

where w([x]) is the weight of the orbit [x].

**Solved Problems**

**Problem 1: Find the number of distinct necklaces with 4 beads, each colored either red or blue.**

**Solution:** This problem can be solved using Burnside's Lemma. We have the cyclic group $C_4$ acting on the set of all possible colorings.

- Total number of colorings: $2^4 = 16$

Notes

- We need to find $|X^g|$ for each $g \in C_4$:
    - For the identity e, all 16 colorings are fixed: $|X^e| = 16$
    - For a 90° rotation ($g_1$), a coloring is fixed if all beads have the same color: $|X^{g1}| = 2$
    - For a 180° rotation ($g_2$), a coloring is fixed if opposite beads have the same color: $|X^{g2}| = 2^2 = 4$
    - For a 270° rotation ($g_3$), same as 90°: $|X^{g3}| = 2$

By Burnside's Lemma: $|X/G| = (1/4) \times (16 + 2 + 4 + 2) = (1/4) \times 24 = 6$

Therefore, there are 6 distinct necklaces with 4 beads colored red or blue.

**Problem 2: In the symmetric group $S_4$, find the isotropy subgroup of the element 1 under the natural action of $S_4$ on {1, 2, 3, 4}.**

**Solution:** The isotropy subgroup $G_1$ consists of all permutations $\sigma \in S_4$ such that $\sigma(1) = 1$.These are precisely the permutations that fix 1 while permuting theelements 2, 3, and 4 in any way.The number of such permutations is 3! = 6, corresponding to allpossible ways to arrange {2, 3, 4}.Explicitly, $G_1$ = {e, (2 3), (2 4), (3 4), (2 3 4), (2 4 3)}, where e is theidentity and the other elements are written in cycle notation.This subgroup is isomorphic to $S_3$, the symmetric group on 3 elements.

**Problem 3: Find the number of different ways to color the vertices of a regular hexagon using 3 colors, where two colorings are considered the same if one can be obtained from the other by a rotation.**

**Solution:** This is a group action problem with the cyclic group C_6 acting on the set X of all possible colorings.

Notes

- Total number of colorings: $|X| = 3^6 = 729$
- We need to find $|X^g|$ for each $g \in C_6$:
    - For the identity (e), all 729 colorings are fixed: $|X^e| = 729$
    - For a 60° rotation ($g_1$), a coloring is fixed if all vertices have the same color: $|X^{g_1}| = 3$
    - For a 120° rotation ($g_2$), a coloring is fixed if vertices at positions i, i+2, i+4 have the same color: $|X^{g_2}| = 3^2 = 9$
    - For a 180° rotation ($g_3$), a coloring is fixed if vertices at positions i and i+3 have the same color: $|X^{g_3}| = 3\text{^}3 = 27$
    - For a 240° rotation ($g_4$), same as 120°: $|X^{g_4}| = 9$
    - For a 300° rotation ($g_5$), same as 60°: $|X^{g_5}| = 3$

By Burnside's Lemma: $|X/G| = (1/6) \times (729 + 3 + 9 + 27 + 9 + 3) = (1/6) \times 780 = 130$

Therefore, there are 130 different ways to color the vertices of a regular hexagon using 3 colors, up to rotation.

**Problem 4: Find the class equation for the dihedral group $D_8$ (the symmetry group of a regular square).**

**Solution:** $D_8$ consists of 8 elements: the identity e, rotations r, $r^2$, $r^3$ by 90°, 180°, and 270°, and reflections s, sr, $sr^2$, $sr^3$ across various axes.To find the conjugacy classes, we use the fact that two elements a, bare conjugate if there exists $g \in D_8$ such that $g^{-1}ag = b$. The center $Z(D_8)$ consists of elements that commute with all elements of $D_8$. These are e and $r^2$, so $|Z(D_8)| = 2$.For the remaining elements:

- r and $r^3$ form one conjugacy class of size 2
- The reflections s and $sr^2$ form one conjugacy class of size 2
- The reflections sr and $sr^3$ form another conjugacy class of size 2

Therefore, the class equation is: $|D_8| = |Z(D_8)| + |Cl(r)| + |Cl(s)| + |Cl(sr)|$ $8 = 2 + 2 + 2 + 2$

**Problem 5: Use the Orbit-Stabilizer theorem to find the number of different ways to place 2 identical rooks on a 3×3 chessboard, where configurations are considered the same if one can be obtained from the other by a rotation or reflection of the board.**

**Solution:** The dihedral group $D_4$ acts on the set X of all possible placements of 2 identical rooks on a 3×3 board.

First, let's count the total number of possible placements:

- We need to choose 2 positions from 9 possible positions
- Number of ways = C(9,2) = 36

Let's consider a specific configuration x where the rooks are at positions (1,1) and (2,2).

To find the isotropy subgroup $G_x$, we need elements of $D_4$ that keep these positions fixed:

- The identity e keeps all positions fixed
- The 180° rotation $r^2$ maps (1,1) to (3,3) and (2,2) to (2,2), so it doesn't fix our configuration
- None of the other rotations or reflections fix this configuration

Therefore, $G_x = \{e\}$, and $|G_x| = 1$.

By the Orbit-Stabilizer theorem: $|Orb(x)| = |D_4| / |G_x| = 8 / 1 = 8$

This means the orbit of our specific configuration has 8 elements.

However, this is just one orbit. To find the total number of distinct configurations, we need to compute all orbits.

Using Burnside's Lemma:

- For the identity e, all 36 configurations are fixed: $|X^e| = 36$
- For 90° rotation r, none of the configurations are fixed: $|X^r| = 0$
- For 180° rotation $r^2$, configurations where rooks are placed symmetrically across the center are fixed: $|X^{r^2}| = 0$ (since we need 2 rooks)
- For 270° rotation $r^3$, same as 90°: $|X^{r^3}| = 0$
- For horizontal reflection s, configurations symmetric about the horizontal axis are fixed: $|X^s| = 3$
- For vertical reflection $sr^2$, configurations symmetric about the vertical axis are fixed: $|X^{sr^2}| = 3$
- For diagonal reflection sr, configurations symmetric about the main diagonal are fixed: $|X^{sr}| = 3$
- For diagonal reflection $sr^3$, configurations symmetric about the other diagonal are fixed: $|X^{sr^3}| = 3$

By Burnside's Lemma: $|X/D_4| = (1/8) \times (36 + 0 + 0 + 0 + 3 + 3 + 3 + 3) = (1/8) \times 48 = 6$

Therefore, there are 6 different ways to place 2 identical rooks on a 3×3 chessboard, up to rotation and reflection.

**Unsolved Problems**

**Problem 1**

Let G be the alternating group A_4 acting on the set X = {1, 2, 3, 4} by the standard permutation action. Find all the isotropy subgroups and determine which of them are conjugate to each other.

Notes

**Problem 2**

Consider the action of the symmetric group $S_5$ on the set of all 2-element subsets of {1, 2, 3, 4, 5} by the natural action. Find the orbit and isotropy subgroup of the subset {1, 2}.

**Problem 3**

Using Burnside's Lemma, determine the number of distinct ways to color the faces of a cube using 3 colors (red, blue, green), where two colorings are considered the same if one can be obtained from the other by a rotation of the cube.

**Problem 4**

Let the dihedral group $D_6$ act on the set of all functions from the vertices of a regular hexagon to {0, 1}. If this action is by composition (i.e., for $g \in D_6$ and a function f, $g \cdot f = f \circ g^{-1}$), find the number of orbits.

**Problem 5**

For the group $G = Z_2 \times Z_2 \times Z_2$, consider its action on itself by conjugation. Find the class equation of G and explain what this tells you about the structure of the group.

**Formulas and Key Results**

1. **Isotropy Subgroup (Stabilizer)**: $G_x = \{g \in G \mid g \cdot x = x\}$
2. **Orbit-Stabilizer Theorem**: $|G| = |Orb(x)| \times |G\_x|$
3. **Burnside's Lemma**: $|X/G| = (1/|G|) \times \Sigma_{\{g \in G\}} |X^g|$
4. **Conjugacy of Isotropy Subgroups**: $G_{(g \cdot x)} = gG_x\, g^{(-1)}$
5. **Class Equation**: $|G| = |Z(G)| + \Sigma\, |Cl(g_i)|$
6. **Pólya Enumeration Theorem**: $Z_{G(w)} = (1/|G|) \times \Sigma_{\{g \in G\}} w^{\{cycle\ (g)\}}$
7. **Fixed Points Set**: $X^g = \{x \in X \mid g \cdot x = x\}$

8. **Number of Distinct Necklaces with n Beads and k Colors**: $(1/n) \times \Sigma\{d|n\} \varphi(d) \times k^{(n/d)}$
9. **Cauchy-Frobenius-Burnside Formula**: $\Sigma_{\{[x]\in X/G\}} w([x]) = (1/|G|) \times \Sigma_{\{g\in G\}} \Sigma_{\{x\in X^g\}} w(x)$
10. **Orbit Size Formula**: $|Orb(x)| = |G| / |G_x|$

This comprehensive overview of isotropy subgroups, applications of group actions, and counting theorems provides both theoretical foundations and practical applications. The solved problems demonstrate how these concepts can be applied to specific scenarios, while the unsolved problems offer opportunities for further practice and deeper understanding of the material.

**p-Groups and their Properties**

**Definition and Basic Properties of p-Groups**

A p-group is a group in which every element has order that is a power of a prime number p. In other words, if G is a p-group, then for every element g in G, there exists a non-negative integer n such that $g^{pn} = e$ (where e is the identity element).

Important characteristics of p-groups include:

1. Finite p-groups have order $p^n$ for some positive integer n.
2. Every non-trivial p-group has a non-trivial center.
3. The order of any subgroup and any quotient group of a p-group is also a power of p.

**Center of p-Groups**

**Theorem 1: If G is a non-trivial finite p-group, then the center Z(G) of G is non-trivial.**

*Proof*: Let G act on itself by conjugation. For each element g in G, we define the class equation:

$|G| = |Z(G)| + \sum|Cl(g)|$

Notes

Where Cl(g) is the conjugacy class of g, and the sum is taken over representatives of distinct non-central conjugacy classes.

For any non-central element g, the size of its conjugacy class is: $|Cl(g)| = [G : C_{G(g)}]$

Where $C_{G(g)}$ is the centralizer of g in G. Since $C_{G(g)}$ is a proper subgroup of G, its index $[G : C_{G(g)}]$ is divisible by p. This means each term in the sum is divisible by p.

Since $|G| = p^n$ for some $n > 0$, and the sum is divisible by p, the center |Z(G)| must also be divisible by p to satisfy the class equation. This implies that $|Z(G)| \geq p$, which means Z(G) is non-trivial.

**Normal Subgroups in p-Groups**

**Theorem 2: Every non-trivial finite p-group has a normal subgroup of order p.**

*Proof*: We already showed that the center Z(G) of a non-trivial p-group G is non-trivial. Since Z(G) is a p-group itself, it contains an element g of order p. The subgroup H = <g> generated by g has order p and is contained in Z(G). Since any subgroup of the center is normal in G, H is a normal subgroup of G with order p.

**Maximal Subgroups of p-Groups**

**Theorem 3: Let G be a finite p-group. Then every maximal subgroup of G has index p in G.**

*Proof*: Let M be a maximal subgroup of G. The quotient group G/M is a p-group with no proper non-trivial subgroups (by maximality of M). Such a group must be cyclic of prime order, which means G/M has order p. Therefore, [G : M] = p.

**Frattini Subgroup**

The Frattini subgroup Φ(G) of a group G is defined as the intersection of all maximal subgroups of G.

Theorem 4: If G is a finite p-group, then Φ(G) is the set of non-generators of G. Moreover, G/Φ(G) is an elementary abelian p-group.

*Proof*: An element g in G is called a non-generator if whenever G = <X, g> for some subset X of G, we also have G = <X>. It can be shown that the set of all non-generators forms a characteristic subgroup of G, which coincides with Φ(G).

Since every maximal subgroup of G has index p, each factor group G/M (where M is maximal) is cyclic of order p. Therefore, for any two elements g, h in G, we have g^p and h^p in every maximal subgroup, hence in Φ(G). Also, [g,h] (the commutator) is in every maximal subgroup. This implies that G/Φ(G) is an elementary abelian p-group, i.e., a direct product of cyclic groups of order p.

**Sylow Theorems and Their Applications**

The Sylow theorems, formulated by Norwegian mathematician Peter Ludwig Sylow in 1872, are fundamental results concerning the existence and properties of certain subgroups in finite groups. These theorems provide crucial insights into the structure of finite groups.

**Sylow Theorems**

**First Sylow Theorem: Let G be a finite group with order |G| = p^n · m, where p is a prime and p does not divide m. Then G contains at least one subgroup of order $p^n$.**

*Proof Sketch*: The proof uses group actions on sets of fixed size. Let G act on the set of all subsets of G of size p^n by left multiplication. This action induces orbits whose sizes divide |G|. By analyzing these orbits and using properties of binomial coefficients modulo p, we can show that at least one such orbit has a size not divisible by p. The stabilizer of an element in such an orbit gives us the desired Sylow p-subgroup.

**Second Sylow Theorem: All Sylow p-subgroups of a finite group G are conjugate to each other. That is, if P and Q are Sylow p-**

Notes

**subgroups of G, then there exists an element g in G such that Q = $g^{(-1)}$Pg.**

*Proof Sketch*: Let P be a Sylow p-subgroup of G and let Q be another Sylow p-subgroup. Consider the action of Q on the set of left cosets G/P by left multiplication. The number of fixed points under this action is congruent to |G/P| modulo p. Since |G/P| is not divisible by p, there must be a fixed point, say gP. This means that for some q in Q, we have qgP = gP, which implies $g^{(-1)}$qg is in P. By extending this argument, we can show that $g^{(-1)}$Qg is contained in P. Since both are Sylow p-subgroups, they must be equal, giving us Q = hP$h^{(-1)}$ for some h in G.

**Third Sylow Theorem: Let G be a finite group and p be a prime. If $n_p$ denotes the number of Sylow p-subgroups of G, then:**

1. $n_p \equiv 1 \pmod{p}$
2. $n_p$ divides |G|
3. $n_p$ = [G : N_G(P)], where P is any Sylow p-subgroup and $N_{G(P)}$ is its normalizer in G.

*Proof Sketch*: Let P be a Sylow p-subgroup of G. The group P acts on the set of all Sylow p-subgroups by conjugation. The orbit-stabilizer theorem gives us that the orbit sizes divide |P|. The only fixed point of this action is P itself, so the other orbit sizes are divisible by p. This gives us $n_p \equiv 1 \pmod{p}$.

The second part follows from the fact that $n_p$ = [G : $N_{G(P)}$] and$N_{G(P)}$ is a subgroup of G.

**Applications of Sylow Theorems**

The Sylow theorems have numerous applications in group theory. Here are some significant ones:

**Application 1: Determining possible group structures.**

By analyzing the number of Sylow subgroups, we can often determine whether non-isomorphic groups of a given order can exist.

**Application 2: Proving groups of certain orders are not simple.**

A group is simple if it has no proper non-trivial normal subgroups. By using the Sylow theorems, we can often prove that groups of certain orders must have proper normal subgroups.

Example: Show that any group of order 15 has a normal subgroup of order 5.

*Solution*: Let G be a group of order $15 = 3 \cdot 5$. By the first Sylow theorem, G has at least one Sylow 5-subgroup P of order 5. By the third Sylow theorem, the number of Sylow 5-subgroups $n_5$ satisfies:

- $n_5 \equiv 1 \pmod 5$
- $n_5$ divides 15 The only positive integer that is congruent to 1 modulo 5 and divides 15 is 1. Therefore, $n_5 = 1$, meaning G has exactly one Sylow 5-subgroup. Since there is only one Sylow 5-subgroup and all Sylow 5-subgroups are conjugate (by the second Sylow theorem), this unique Sylow 5-subgroup must be normal in G.

**Application 3: Classification of groups of specific orders.**

The Sylow theorems are instrumental in classifying groups of specific orders. For example, they help determine that there are exactly two non-isomorphic groups of order 6: the cyclic group $C_6$ and the dihedral group $D_6$.

**Solved Problems**

**Problem 1: Prove that a group of order $p^2$ (p prime) is abelian.**

Solution: Let G be a group of order $p^2$. We need to prove that G is abelian, i.e., gh = hg for all g, h in G.

There are two possibilities for G:

Notes

1. G is cyclic of order $p^2$
2. G is not cyclic

If G is cyclic, then G is automatically abelian.

If G is not cyclic, then its elements (except the identity) have order p. Let g be a non-identity element of G. Then |g| = p, so the subgroup <g> has p elements.

By Lagrange's theorem, G has p + 1 distinct subgroups of order p (including <g>). Let h be an element not in <g>. Then <h> is another subgroup of order p, and <g> ∩ <h> = {e} (the identity).

Every element in G can be uniquely written as $g^ih^j$ where $0 \leq i, j < p$. Now we need to show that gh = hg.

Consider the center Z(G) of G. We know that in p-groups, the center is non-trivial. Since G has order $p^2$, either Z(G) = G (meaning G is abelian) or |Z(G)| = p.

If |Z(G)| = p, then G/Z(G) has order p, which means G/Z(G) is cyclic. But if G/Z(G) is cyclic, then G must be abelian (this is a known result in group theory).

Therefore, in all cases, G must be abelian.

**Problem 2: Find all Sylow subgroups in $S^4$ (the symmetric group on 4 elements).**

Solution: The order of $S^4$ is 4! = 24 = $2^3 \cdot 3$.

Sylow 2-subgroups: These are subgroups of order $2^3 = 8$. By the third Sylow theorem, the number of Sylow 2-subgroups $n_2$ satisfies:

- $n_2 \equiv 1 \pmod 2$
- $n_2$ divides $24 = 2^3 \cdot 3$
- $n_2$ divides 3

So $n_2 = 1$ or $n_2 = 3$.

Notes

Let's identify these subgroups. Consider the subgroup generated by the permutations (1,2), (3,4), and (1,3)(2,4). This forms a Sylow 2-subgroup isomorphic to $D_8$ (the dihedral group of order 8).

Other Sylow 2-subgroups can be obtained through conjugation. For example:

- The subgroup generated by (1,3), (2,4), and (1,2)(3,4)
- The subgroup generated by (1,4), (2,3), and (1,2)(3,4)

Therefore, $S_4$ has exactly 3 Sylow 2-subgroups.

Sylow 3-subgroups: These are subgroups of order $3^1 = 3$. By the third Sylow theorem, the number of Sylow 3-subgroups $n_3$ satisfies:

- $n_3 \equiv 1 \pmod 3$
- $n_3$ divides $24 = 2^3 \cdot 3$
- $n_3$ divides 8

So $n^3 = 1$, 4, or 7. But since $n^3 \equiv 1 \pmod 3$, we have $n^3 = 1$, 4.

The Sylow 3-subgroups are cyclic of order 3. One such subgroup is generated by the 3-cycle (1,2,3). Through conjugation, we can find that there are exactly 4 Sylow 3-subgroups:

- <(1,2,3)>
- <(1,2,4)>
- <(1,3,4)>
- <(2,3,4)>

Therefore, $S_4$ has exactly 4 Sylow 3-subgroups.

**Problem 3: Prove that any group of order 20 has a normal subgroup of order 5.**

Solution: Let G be a group of order $20 = 2^2 \cdot 5$.

Notes

By the first Sylow theorem, G has at least one Sylow 5-subgroup P of order 5.

By the third Sylow theorem, the number of Sylow 5-subgroups $n_5$ satisfies:

- $n_5 \equiv 1 \pmod 5$
- $n_5$ divides $20 = 2^2 \cdot 5$
- $n_5$ divides 4

The only positive integer that is congruent to 1 modulo 5 and divides 4 is 1.

Therefore, $n_5 = 1$, meaning G has exactly one Sylow 5-subgroup.

Since there is only one Sylow 5-subgroup and all Sylow 5-subgroups are conjugate (by the second Sylow theorem), this unique Sylow 5-subgroup must be normal in G.

**Problem 4: Let G be a group of order p^n where p is prime and n ≥ 1. Prove that G has a normal subgroup of order p^(n-1).**

Solution: We'll use induction on n.

Base case: n = 1 If n = 1, then |G| = p. The only proper subgroup is the trivial subgroup {e} with order $p^0 = 1$, which is obviously normal.

Inductive hypothesis: Assume that for some $k \geq 1$, any group of order $p^k$ has a normal subgroup of order $p^{(k-1)}$.

Inductive step: Let G be a group of order $p^{(k+1)}$.We know that the center Z(G) of G is non-trivial (a fundamental property of p-groups). Let z be a non-identity element in Z(G). Sincez is in Z (G), the subgroup <z> is normal in G.Let H = G/<z>. Then |H| = $|G|/|\langle z\rangle| = p^{(k+1)}/p = p^k$.By the inductive hypothesis, H has a normal subgroup K of order$p^{(k-1)}$.

Notes

Let $\pi: G \to H$ be the natural projection. Consider $N = \pi^{(-1)}(K)$. This is a subgroup of G, and by the properties of quotient groups, N is normal in G.

The order of N is $|N| = |K| \cdot |\langle z \rangle| = p^{(k-1)} \cdot p = p^k$.

Thus, G has a normal subgroup N of order $p^k = p^{((k+1)-1)}$.

By the principle of mathematical induction, the result holds for all $n \geq 1$.

**Problem 5: Prove that every group of order 12 has a normal subgroup of order 3 or 4.**

Solution: Let G be a group of order $12 = 2^2 \cdot 3$.

By the first Sylow theorem, G has at least one Sylow 3-subgroup P of order 3, and at least one Sylow 2-subgroup Q of order 4.

By the third Sylow theorem, the number of Sylow 3-subgroups $n^3$ satisfies:

- $n^3 \equiv 1 \pmod 3$
- $n^3$ divides $12 = 2^2 \cdot 3$
- $n^3$ divides 4

The only positive integer that is congruent to 1 modulo 3 and divides 4 is 1 or 4.

Case 1: $n_3 = 1$ If there is only one Sylow 3-subgroup, then it must be normal in G. Thus, G has a normal subgroup of order 3.

Case 2: $n_3 = 4$ Now let's consider the Sylow 2-subgroups. By the third Sylow theorem, the number of Sylow 2-subgroups n_2 satisfies:

- $n_2 \equiv 1 \pmod 2$
- $n_2$ divides $12 = 2^2 \cdot 3$
- $n_2$ divides 3

Notes

The only positive integer that is congruent to 1 modulo 2 and divides 3 is 1 or 3.

Subcase 2.1: $n_2 = 1$ If there is only one Sylow 2-subgroup, then it is normal in G. Thus, G has a normal subgroup of order 4.

Subcase 2.2: $n_2 = 3$ Here we need to use additional group theory results. We can show that in this case, G must be isomorphic to $A_4$ (the alternating group on 4 elements).

In $A_4$, there are four Sylow 3-subgroups, and the union of these subgroups (minus the identity) gives us 8 elements of order 3. The remaining 3 non-identity elements form a subgroup called the Klein four-group, which is normal in $A_4$.

Therefore, even in this case, G has a normal subgroup of order 4.

**Unsolved Problems**

Problem 1: Prove that in a finite p-group G (p prime), every maximal subgroup has index p in G.

Problem 2: Let G be a p-group of order $p^n$ with $n \geq 2$. Prove that G has at least $p + 1$ subgroups of order $p^{(n-1)}$.

Problem 3: Let G be a group of order 2023. Determine the number of Sylow 7-subgroups and Sylow 17-subgroups in G.

Problem 4: Let G be a group of order 30. Prove that G is not simple.

Problem 5: Let G be a group of order 60. Prove that either G has a normal Sylow 5-subgroup or G has a normal Sylow 3-subgroup.

**Special Topics in p-Groups**

**Burnside's Basis Theorem**

Burnside's Basis Theorem states that if G is a finite p-group, then any minimal generating set of G has the same number of elements, which equals the rank of the elementary abelian group $G/\Phi(G)$.

**Nilpotency of p-Groups**

Every p-group is nilpotent. This means there exists a finite sequence of subgroups:

$G = G_0 > G_1 > ... > G_n = \{e\}$

Such that $[G, G_i] \leq G_{(i+1)}$ for all i.

**p-Groups and Representation Theory**

p-groups have special properties in representation theory. For example, if G is a p-group and V is a finite-dimensional vector space over a field of characteristic not equal to p, then any linear representation of G on V has a non-zero fixed point.

**Counting Subgroups in p-Groups**

For p-groups, there are formulas that give the number of subgroups of each possible order. These formulas involve sophisticated combinatorial techniques and can be quite complex.

**p-Groups in Computational Group Theory**

p-groups play an important role in computational group theory. Many algorithms exploit the special properties of p-groups to efficiently compute group-theoretic information.

**Advanced Applications of Sylow Theorems**

**Classification of Simple Groups**

The Sylow theorems are fundamental tools in the classification of simple groups. They provide criteria for when a group cannot be simple, which was crucial in the monumental effort to classify all finite simple groups.

**Semidirect Products and Group Extensions**

The Sylow theorems help in determining the structure of groups as semidirect products or extensions of smaller groups. This is particularly useful in classifying groups of certain orders.

**Group Actions and Fixed-Point Theorems**

Notes

The proofs of the Sylow theorems use group actions in an essential way. This connection between group actions and subgroup structure has led to various fixed-point theorems in group theory.

**Fusion Theory**

Fusion in group theory deals with how conjugacy in a larger group affects the structure of a subgroup. The Sylow theorems are the starting point for much of fusion theory, which has applications in modular representation theory.

**Historical Context and Development**

The development of p-group theory and the Sylow theorems represents a significant milestone in the history of abstract algebra. These concepts were initially formulated in the late 19th century and have continued to evolve and find new applications. The study of p-groups was further developed in the 20th century, with contributions from many mathematicians, including Burnside, Hall, Thompson, and others. The theory has connections to various other areas of mathematics, including number theory, topology, and representation theory. The Sylow theorems, in particular, stand as fundamental results that every student of group theory must master. They exemplify the power of abstract reasoning in uncovering deep structural properties of mathematical objects.

**Multiple Choice Questions (MCQs)**

1. **The order of a direct product of two finite groups is:**
   a) Sum of the orders of individual groups
   b) Product of the orders of individual groups
   c) Maximum of the orders of the two groups
   d) Minimum of the orders of the two groups

2. **A group action on a set satisfies which of the following properties?**
   a) Associativity and identity properties
   b) Distributivity and commutativity

c) Symmetry and transitivity

d) None of the above

3. **The orbit of an element under a group action is:**

   a) A subset of the group

   b) The set of elements obtained by applying group elements to it

   c) Always equal to the entire set

   d) None of the above

4. **Sylow's theorems provide information about:**

   a) Normal subgroups

   b) Prime-power order subgroups

   c) Commutative properties of groups

   d) None of the above

5. **The number of Sylow p-subgroups in a group is:**

   a) Any integer greater than 1

   b) A power of p

   c) Congruent to 1 modulo p

   d) Always 1

6. **Which of the following statements about p-groups is true?**

   a) Every element has order p

   b) They always have a normal subgroup

   c) They are abelian groups

   d) They have a unique Sylow subgroup

7. **The isotropy subgroup of an element is:**

   a) The set of all elements in the group that fix the element

   b) The orbit of the element

   c) The direct product of two subgroups

   d) A normal subgroup of the group

8. **The number of orbits in a group action is found using:**

   a) Lagrange's Theorem

   b) Sylow's Theorem

c) Orbit-Stabilizer Theorem

d) Cayley's Theorem

9. **In a finite group, the order of an element must:**

a) Divide the order of the group

b) Be a prime number

c) Be equal to the order of the group

d) None of the above

10. **The center of a p-group is:**

a) Trivial

b) Always nontrivial

c) Equal to the group itself

d) None of the above

**Short Answer Questions**

1. Define the direct product of two groups with an example.
2. Explain group actions with a real-life example.
3. What is an orbit in the context of group actions?
4. State and prove the Orbit-Stabilizer Theorem.
5. What is a p-group? Give an example.
6. State and prove Sylow's First Theorem.
7. What is an isotropy subgroup?
8. Explain the significance of counting theorems in combinatorial mathematics.
9. How do p-groups relate to Sylow's Theorems?
10. Why are Sylow subgroups important in the classification of finite groups?

**Long Answer Questions**

1. Explain the concept of direct product in groups with detailed examples and proofs.
2. Derive the Orbit-Stabilizer Theorem and give its applications.
3. Discuss in detail the applications of counting theorems in group theory.
4. Prove and explain all three Sylow theorems with examples.
5. Describe the significance of p-groups in the study of finite groups.
6. How do isotropy subgroups help in understanding group structures?
7. Explain how Sylow's theorems can be used to determine the number of subgroups of a given order.
8. Discuss the importance of group actions in modern algebra and their real-life applications.
9. Derive the class equation and explain its applications in group theory.
10. How does the Sylow theory contribute to the classification of finite simple groups?

Answer Key MCQ :

1. b

2. a

3. b

4. b

5. c

6. b

7. a

8. c

9. a

10. b

# MODULE 2

## UNIT 2.1

## APPLICATIONS OF THE SYLOW THEORY AND RING THEORY

**Objectives**

- Apply Sylow theorems to p-groups and the class equation.
- Understand further applications of Sylow's theorems in finite group classification.
- Study rings of polynomials and their properties.
- Explore the concept of polynomials in an indeterminate.
- Learn about the evaluation homomorphism and its significance.
- Understand factorization of polynomials over a field.

### 2.1.1: Applications of Sylow Theory

Sylow theory is one of the most powerful tools in finite group theory, providing critical information about the structure of groups through their subgroups of prime power order. The fundamental theorems, developed by Norwegian mathematician Ludwig Sylow in 1872, allow us to draw significant conclusions about finite groups by examining these special subgroups.

**Fundamental Concepts of Sylow Theory**

A p-Sylow subgroup (or Sylow p-subgroup) of a finite group G is a maximal p-subgroup of G, where p is a prime number. In other words, it's a subgroup whose order is the highest power of p that divides the order of G.

The Sylow theorems state:

1. Existence: If G is a finite group and $p^n$ divides |G| (where p is prime and $n \geq 1$), then G contains at least one subgroup of order $p^n$.
2. Number: If $n_p$ denotes the number of Sylow p-subgroups of G, then:
    - $n_p$ divides $|G|/p^s$ (where p^s is the highest power of p dividing |G|)
    - $n_p \equiv 1 \pmod{p}$
3. Conjugacy: All Sylow p-subgroups of G are conjugate to each other.

**Applications of Sylow Theory**

**1. Classification of Groups of Small Order**

Sylow theory is particularly effective in classifying groups of small order. Let's consider some examples:

Example: Groups of Order 15

If $|G| = 15 = 3 \times 5$, then:

- The number of Sylow 3-subgroups $n_3$ must divide 5 and satisfy $n_3 \equiv 1 \pmod{3}$.
- The only possibility is $n_3 = 1$.
- Similarly, $n_5 = 1$.

Since both Sylow subgroups are normal, G is isomorphic to $Z_{15}$ (cyclic group of order 15).

Example: Groups of Order 12

If $|G| = 12 = 2^2 \times 3$, then:

- For Sylow 3-subgroups, $n_3$ divides 4 and $n_3 \equiv 1 \pmod{3}$. So $n_3 = 1$ or 4.

- For Sylow 2-subgroups, $n_2$ divides 3 and $n_2 \equiv 1 \pmod 2$. So $n_2 = 1$ or 3.

This gives us different possibilities to analyze, leading to the classification of all groups of order 12: $Z_{12}$, $Z_6 \times Z_2$, $A_4$, $D_6$,and Q (the quaternion group).

**2. Proving Simplicity of Groups**

Sylow theory provides powerful tools for proving that certain groups are simple.

Example: Simplicity of $A_5$

To show that $A_5$ (the alternating group on 5 elements) is simple:

- $|A_5| = 60 = 2^2 \times 3 \times 5$
- By Sylow's theorems, $n_5$ divides 12 and $n_5 \equiv 1 \pmod 5$, so $n_5 = 6$
- If N is a normal subgroup, it must contain either all or none of the Sylow 5-subgroups
- Similar analysis for Sylow 2-subgroups and Sylow 3-subgroups shows that any non-trivial normal subgroup must be $A_5$ itself

**3. Proving Non-Simplicity**

Sylow theory can also be used to prove that certain groups cannot be simple.

Example: Non-Simplicity of Groups of Order 56

If $|G| = 56 = 2^3 \times 7$, then:

- $n_7$ divides 8 and $n_7 \equiv 1 \pmod 7$
- The only possibility is $n_7 = 8$
- Each Sylow 7-subgroup has 6 elements of order 7

- Total number of elements of order 7 is 8 × 6 = 48
- This leaves 56 - 48 - 1 = 7 elements (excluding the identity)
- These 7 elements must form a normal subgroup of G, proving G is not simple

**4. Proving Group Properties**

Example: Groups of Order $p^n$ q (p, q prime, n ≥ 1) Have Normal Subgroups

For a group G with |G| = $p^n$ × q where p, q are distinct primes:

- The number of Sylow q-subgroups $n_q$ divides $p^n$ and $n_q \equiv 1 \pmod q$
- If $n_q = 1$, then the unique Sylow q-subgroup is normal
- If $n_q > 1$, then $n_q = p^m$ for some $1 \leq m \leq n$
- The number of elements in all Sylow q-subgroups combined is $p^m(q-1) + 1$
- This leaves p^n × q - [$p^m$(q-1) + 1] elements
- These remaining elements form a normal subgroup

**5. Burnside's $p^aq^b$ Theorem**

One of the most important applications of Sylow theory is Burnside's theorem, which states that any group of order $p^aq^b$ (where p and qare distinct primes) is solvable.

The proof uses Sylow theory to establish that such groups must have normal subgroups, and builds from there to establish solvability.

**Advanced Applications**

**The Frobenius Groups**

Notes

A Frobenius group is a transitive permutation group on a finite set such that no non-identity element fixes more than one point and some non-identity element fixes exactly one point.

Sylow theory helps in analyzing the structure of Frobenius groups through their Sylow subgroups.

**Recognition Theorems**

Sylow theory is crucial in group recognition theorems, which identify groups based on specific properties. For example, any group of order 168 satisfying certain conditions must be isomorphic to PSL(2,7).

**Transfer Theory**

The transfer homomorphism extends Sylow theory, providing a way to map a group G to an abelian quotient of a specific subgroup. This becomes powerful when combined with Sylow theory for analyzing the structure of finite groups.

### 2.1.2: p-Groups and the Class Equation

**Definition and Basic Properties of p-Groups**

A p-group is a group in which every element has order $p^k$ for some non-negative integer k, where p is a prime number. Equivalently, a finite group G is a p-group if and only if $|G| = p^n$ for some positive integer n.

Key properties of p-groups include:

1. Every non-trivial p-group has a non-trivial center.
2. If H is a proper subgroup of a finite p-group G, then H is properly contained in its normalizer.
3. The order of any maximal subgroup of a finite p-group G is $|G|/p$.
4. Any finite p-group is nilpotent.

**The Class Equation**

Notes

The class equation (also called the conjugacy class equation) is a fundamental tool in group theory, particularly useful for analyzing p-groups.

For a finite group G, the class equation is expressed as:

$|G| = |Z(G)| + \sum|G:C_G(x_i)|$

where:

- Z(G) is the center of G
- The sum runs over representatives $x_i$ of non-central conjugacy classes
- $C_G(x_i)$ is the centralizer of $x_i$ in G

In other words, the order of the group equals the size of its center plus the sum of the sizes of all non-central conjugacy classes.

Applications of the Class Equation to p-Groups

**1. Non-Trivial Center in p-Groups**

One of the most important applications of the class equation is proving that every non-trivial p-group has a non-trivial center.

Proof: Let G be a p-group with $|G| = p^n > 1$. From the class equation:

$|G| = |Z(G)| + \sum|G:C_G(x_i)|$

Each term $|G:C_G(x_i)|$ is the size of the conjugacy class of $x_i$, which equals $[G:C_G(x_i)]$. Since $x_i$ is not in the center, $C_G(x_i)$ is a proper subgroup of G, so $[G:C_G(x_i)] > 1$.

For a p-group, any index greater than 1 must be divisible by p. Thus, each $|G:C_G(x_i)|$ is divisible by p.

So we have: |G| = |Z(G)| + (a sum of multiples of p)

Since $|G| = p^n$ is itself divisible by p, the only way this equation can hold is if |Z(G)| is also divisible by p. This means $|Z(G)| \geq p$, so the center is non-trivial.

Notes

**2. Structure of Groups of Order $p^2$**

The class equation helps us classify groups of order $p^2$.

For any group G of order $p^2$:

- Either $|Z(G)| = p^2$, which means G is abelian
- Or $|Z(G)| = p$, which means G has a non-trivial center

From the class equation, if $|Z(G)| = p$, then G has p conjugacy classes, each containing p elements except for the conjugacy class of the identity. This structure information helps prove that there are only two isomorphism classes of groups of order $p^2$: $Z_{\{p2\}}$ and $Z_p \times Z_p$.

**3. Nilpotency of p-Groups**

The class equation is instrumental in proving that all finite p-groups are nilpotent.

Since every non-trivial p-group G has a non-trivial center Z(G), we can form the quotient group G/Z(G). This is again a p-group (of smaller order), so it also has a non-trivial center. Continuing this process, we get a sequence:

$G \supset Z(G) \supset Z_2(G) \supset ... \supset Z_k(G) = G$

where $Z_i(G)$ is the $i^{th}$ center. This establishes a central series for G, proving it is nilpotent.

**4. Counting Conjugacy Classes**

The class equation allows us to count conjugacy classes in p-groups and relate this count to structural properties.

If G is a p-group of order $p^n$, and G has k conjugacy classes, then:

$k \equiv |G| \pmod p$

This congruence relation comes from analyzing the class equation modulo p.

**5. Analyzing Normal Subgroups**

For a p-group G, the class equation helps identify normal subgroups. If N is a normal subgroup of G, then $N \cap Z(G) \neq \{e\}$ (unless N is trivial).

This means every normal subgroup of a p-group intersects the center non-trivially, a powerful structural insight derived from the class equation.

**Connection Between Sylow Theory and p-Groups**

Sylow theory and p-groups are deeply connected, as Sylow p-subgroups are themselves p-groups. The structural properties of p-groups (established using the class equation) inform our understanding of Sylow subgroups in general groups.

Key connections include:

1. Normalizers Grow in p-Groups: If H is a proper subgroup of a p-group G, then H is properly contained in its normalizer $N_G(H)$. This property, established using the class equation, is crucial in proving the third Sylow theorem.

2. Center-Focused Analysis: The non-trivial center of p-groups (established via the class equation) allows for inductive arguments in analyzing Sylow subgroups.

3. Transfer Theory: The class equation informs transfer theory, which extends Sylow theory by providing homomorphisms that reveal information about the structure of a group based on its Sylow subgroups.

**Solved Problems**

**Problem 1: Classify all groups of order 20**

**Solution:**

Let G be a group of order $20 = 2^2 \times 5$.

Step 1: Find the number of Sylow 5-subgroups.

Notes

- By Sylow's theorems, the number of Sylow 5-subgroups ($n_5$) divides 4 and $n_5 \equiv 1 \pmod 5$.
- The only possibility is $n_5 = 1$.
- Let P be the unique Sylow 5-subgroup. Since it's unique, P is normal in G.
- P is isomorphic to $Z_5$ (cyclic group of order 5).

Step 2: Find the number of Sylow 2-subgroups.

- By Sylow's theorems, the number of Sylow 2-subgroups ($n_2$) divides 5 and $n_2 \equiv 1 \pmod 2$.
- The only possibility is $n_2 = 1$ or $n_2 = 5$.

**Case 1: $n_2 = 1$**

- Let Q be the unique Sylow 2-subgroup of order 4.
- Q is normal in G.
- G is the direct product of P and Q (since they have coprime orders and are both normal).
- Q can be either $Z_4$ or $Z_2 \times Z_2$. a) If Q ≅ Z_4, then G ≅ $Z_4 \times Z_5 \cong Z_{20}$. b) If Q ≅ $Z_2 \times Z_2$, then G ≅ $(Z_2 \times Z_2) \times Z_5 \cong Z_2 \times Z_2 \times Z_5$.

**Case 2: $n_2 = 5$**

- Let Q be a Sylow 2-subgroup of order 4.
- Since $n_2 = 5$, Q is not normal in G.
- G must have the structure of a semidirect product $Z_5 \rtimes Q$.
- Since $\mathrm{Aut}(Z_5) \cong Z_4$, and Q acts non-trivially on $Z_5$, we must have Q ≅ $Z_4$.
- This gives us the dihedral group of order 20: $D_{10}$.

Therefore, there are three isomorphism classes of groups of order 20: Notes

1. $Z_{20}$ (cyclic group of order 20)
2. $Z_2 \times Z_2 \times Z_5$
3. $D_{10}$ (dihedral group of order 20)

**Problem 2: Prove that a group of order 255 = 3 × 5 × 17 must be cyclic**

**Solution:**

Let G be a group of order 255 = 3 × 5 × 17.

Step 1: Find the number of Sylow 3-subgroups (n_3).

- By Sylow's theorem, $n_3$ divides 85 (= 5 × 17) and $n_3 \equiv 1 \pmod 3$.
- The possible values for $n_3$ are 1, 5, 17, or 85.
- If $n_3 = 5$, then there are 5 subgroups of order 3, each with 2 non-identity elements. This gives 10 elements of order 3.
- If $n_3 = 17$, this gives 34 elements of order 3.
- If $n_3 = 85$, this gives 170 elements of order 3.
- But $n_3$ can't be 5, 17, or 85 because the total order of G is 255, and we would need room for elements of orders 5 and 17 as well.
- Therefore, $n_3 = 1$.

Step 2: Find the number of Sylow 5-subgroups ($n_5$).

- By Sylow's theorem, $n_5$ divides 51 (= 3 × 17) and $n_5 \equiv 1 \pmod 5$.
- The possible values for $n_5$ are 1, 6, 11, 16, 21, 26, 31, 36, 41, 46, or 51.

Notes

- But $n_5 \equiv 1 \pmod 5$ means $n_5$ can only be 1, 6, 11, 16, 21, 26, 31, 36, 41, 46, or 51.
- The intersection of these constraints gives $n_5 = 1$.

Step 3: Find the number of Sylow 17-subgroups ($n_{17}$).

- By Sylow's theorem, $n_{17}$ divides 15 ($= 3 \times 5$) and $n_{17} \equiv 1 \pmod{17}$.
- The only value that satisfies both conditions is $n_{17} = 1$.

Step 4: Determine the structure of G.

- Let $P_3$, $P_5$, and $P_{17}$ be the unique Sylow subgroups of orders 3, 5, and 17 respectively.
- Since each is unique, all three are normal in G.
- $P_3 \cong Z_3$, $P_5 \cong Z_5$, and $P_{17} \cong Z_{17}$ (since groups of prime order are cyclic).
- $G = P_3 \times P_5 \times P_{17} \cong Z_3 \times Z_5 \times Z_{17} \cong Z_{255}$ (by the Chinese Remainder Theorem).

Therefore, G must be isomorphic to $Z_{255}$, the cyclic group of order 255.

**Problem 3: Use the class equation to prove that every p-group of order $p^2$ is abelian**

**Solution:**

Let G be a p-group of order $p^2$.

Step 1: Apply the class equation. The class equation states: $|G| = |Z(G)| + \sum|G:C_G(x_i)|$

where Z(G) is the center of G, and the sum runs over representatives x_i of non-central conjugacy classes.

Notes

Step 2: Analyze possible values for |Z(G)|. Since G is a p-group, we know |Z(G)| > 1 (by a property of p-groups established using the class equation). |Z(G)| divides $|G| = p^2$, so |Z(G)| = p or $|Z(G)| = p^2$.If $|Z(G)| = p^2$, then Z(G) = G, which means G is abelian, and we'redone.

Step 3: Consider the case |Z(G)| = p. In this case, the class equation becomes: $p^2 = p + \sum|G:C_G(x_i)|$Each index $|G:C_G(x_i)|$ must be a divisor of $|G| = p^2$, so it equalseither p or $p^2$.If $|G:C_G(x_i)| = p^2$, then $C_G(x_i) = \{e\}$, which means only theidentity commutes with $x_i$. This is impossible in a group, as $x_i$ always commutes with itself. Therefore, all $|G:C_G(x_i)| = p$.

The class equation becomes: $p^2 = p + kp$ where k is the number of non-central conjugacy classes.

Solving for k: $p^2 = p + kp$ $p^2 - p = kp$ $p(p-1) = kp$ $k = p-1$

Step 4: Calculate the size of Z(G) from another perspective. If |Z(G)| = p, then G/Z(G) has order $p^2/p = p$.Any group of prime order is cyclic, so $G/Z(G) \cong Z_p$.Let's denote the elements of G/Z(G) as {Z(G), aZ(G), $a^2Z(G)$, ...,$a^{(p-1)}Z(G)$} where a is some element of G not in Z(G).For any $g \in G$, there exists some j such that $gZ(G) = a^jZ(G)$, whichmeans $g = a^jz$ for some $z \in Z(G)$.

Step 5: Show that G is abelian. For any two elements $g, h \in G$, we can write: $g = a^jz_1$ and $h = a^kz_2$ for some $z_1, z_2 \in Z(G)$.

Then: $gh = (a^jz_1)(a^kz_2) = a^ja^kz_1z_2 = a^{j+k}z_1z_2$

and: $hg = (a^kz_2)(a^jz_1) = a^ka^jz_2z_1 = a^{k+j}z_2z_1 = a^{j+k}z_1z_2 = gh$

Therefore, G is abelian.

**Problem 4: Determine all possible orders of a non-abelian group with exactly 5 conjugacy classes**

**Solution:**

Step 1: Establish a relationship between conjugacy classes and center. For any finite group G, the number of conjugacy classes equals the number of irreducible complex representations.

From representation theory, if G has k conjugacy classes, then: $\sum(d_i^2) = |G|$

where d_i are the dimensions of the irreducible representations.

Step 2: Analyze the constraints. If G has exactly 5 conjugacy classes, we need to find the possible dimensions $d_i$.

The trivial representation always exists with $d_1 = 1$.

If G is non-abelian, it must have at least one irreducible representation with dimension greater than 1.

For a non-abelian group, the center Z(G) is in one-to-one correspondence with the 1-dimensional representations.

Step 3: List possible dimension patterns. With 5 conjugacy classes, we need 5 irreducible representations. Let's list possible patterns of dimensions:

1. (1, 1, 1, 1, n) where n > 1
2. (1, 1, 1, m, n) where m, n > 1
3. (1, 1, m, n, p) where m, n, p > 1

Step 4: Examine pattern 1: (1, 1, 1, 1, n). If the dimensions are (1, 1, 1, 1, n), then: $1^2 + 1^2 + 1^2 + 1^2 + n^2 = |G|$ $4 + n^2 = |G|$

Since G is non-abelian, its center has order 4 (corresponding to the four 1-dimensional representations).

Notes

For any finite group, the order of the center divides the order of the group, so $|G| = 4k$ for some integer k.

Substituting: $4 + n^2 = 4k$ $n^2 = 4k - 4$ $n^2 = 4(k - 1)$

For n to be an integer, k - 1 must be a perfect square times a power of 2.

Let $k - 1 = m^2 \times 2^r$ where $2^r$ is the highest power of 2 dividing k -1.

- If $r \geq 2$, then $n^2 = 4m^2 \times 2^r$, which means $n = 2m \times 2^{(r/2)}$ is even.
- If $r = 1$, then $n^2 = 4m^2 \times 2$, which means $n = 2m \times \sqrt{2}$, which is not an integer.
- If $r = 0$, then $n^2 = 4m^2$, which means $n = 2m$.

So for pattern 1, $|G| = 4k$ where k - 1 is a perfect square times a power of 4, or simply a perfect square.

The smallest examples are:

- $k = 2$ gives $|G| = 8$ (the quaternion group or dihedral group $D_4$)
- $k = 5$ gives $|G| = 20$ (no non-abelian group of order 20 has 5 conjugacy classes)
- $k = 10$ gives $|G| = 40$ (certain non-abelian groups of order 40)

Step 5: Examine patterns 2 and 3. Similar analysis of patterns 2 and 3 leads to other possible orders.

For pattern 2: (1, 1, 1, m, n): $1^2 + 1^2 + 1^2 + m^2 + n^2 = |G|$ $3 + m^2 + n^2 = |G|$

For pattern 3: (1, 1, m, n, p): $1^2 + 1^2 + m^2 + n^2 + p^2 = |G|$ $2 + m^2 + n^2 + p^2 = |G|$

Notes

Analysis of these patterns yields additional possible orders, including 8, 16, 21, 24, 27, 32, and 40.

Therefore, the possible orders of a non-abelian group with exactly 5 conjugacy classes include 8, 16, 21, 24, 27, 32, 40, and others.

**Problem 5: Prove that a finite p-group with exactly $p^2$ elementsof order p must have order $p^3$**

**Solution:**

Step 1: Set up what we know. Let G be a finite p-group with exactly $p^2$ elements of order p. Let's denote the order of G as $p^n$.

Step 2: Use the structure of p-groups. In a p-group, every element has order a power of p. The elements of order p, together with the identity, form a set that's not necessarily a subgroup.

Step 3: Apply the class equation. The class equation gives us: $|G| = |Z(G)| + \sum|G:C_G(x_i)|$where Z(G) is the center and the sum runs over representatives ofnon-central conjugacy classes.

Step 4: Consider the elements of order p in Z(G). In a p-group, Z(G) is non-trivial. Let $|Z(G)| = p^m$ where $m \geq 1$.The center Z(G) is an abelian p-group, so it can be written as a directproduct of cyclic p-groups.If Z(G) contains k cyclic factors, then the number of elements of orderp in Z(G) is $(p^{k-1})$.

Step 5: Find the possible structure for Z(G). Given that we have exactly $p^2$ elements of order p in G, and some of these are in Z(G), we need to determine the possible structures for Z(G).

Case 1: If Z(G) is cyclic of order $p^m$, it contains exactly p-1 elements of order p.

Case 2: If $Z(G) = Z_p \times Z_p$, it contains $p^2$-1 elements of order p.

Case 3: If Z(G) has more cyclic factors or higher powers, it would contain more elements of order p.

Notes

Step 6: Analyze the non-central elements of order p. If there are exactly $p^2$ elements of order p in G, and Z(G) contains some of them, then the remaining elements of order p must occur in non-central conjugacy classes.

For a non-central element x of order p, its conjugacy class has size $|G:C_G(x)|$. This size must be a power of p since G is a p-group.

Step 7: Determine the structure of G. The only way to have exactly p2 elements of order p is if:

1. $Z(G) = Z_p$ (containing p-1 elements of order p), and
2. There is exactly one non-central conjugacy class of elements of order p, with size p(p-1).

The total number of elements of order p is then: (p-1) + p(p-1) = p(p-1) + (p-1) = (p+1)(p-1) = p2-1

But we assumed G has $p^2$ elements of order p, which contradicts our calculation.

The problem likely misstated the constraint. If G has exactly $p^2$-1 elements of order p, then our analysis shows $|G| = p^3$.

For a group of order $p^3$ with $Z(G) = Z_p$ and one non-central conjugacy class of elements of order p of size p(p-1), the total number of elements of order p is (p-1) + p(p-1) = $p^2$-1.

Therefore, a finite p-group with exactly $p^2$-1 elements of order p must have order $p^3$.

**Unsolved Problems**

**Problem 1**

Prove that if G is a group of order $56 = 2^3 \times 7$, then G is not simple.

**Problem 2**

Notes

Let G be a group of order $351 = 3^3 \times 13$. Prove that G has a normal subgroup of order 27 or a normal subgroup of order 13.

**Problem 3**

Use the class equation to prove that if G is a p-group of order $p^n$, and $|Z(G)| = p$, then G has a normal subgroup of order $p^2$.

**Problem 4**

Prove that any group of order $105 = 3 \times 5 \times 7$ has a normal Sylow subgroup.

**Problem 5**

Let G be a p-group of order $p^4$. Prove that if G has more than p+1 elements of order p, then G has a subgroup isomorphic to the elementary abelian group of order $p^2$ (i.e., $Z_p \times Z_p$).

### 2.1.3: Further Applications of Sylow's Theorems

Sylow's theorems are powerful tools in group theory that allow us to analyze the structure of finite groups by examining their subgroups of prime power order. Having established the fundamental theorems, we can now explore various applications that demonstrate their utility in solving complex group-theoretical problems.

**The Structure of Groups of Specific Orders**

One of the most common applications of Sylow's theorems is determining the possible structures of groups with a specific order. Let's explore some important examples.

**Groups of Order pq**

Let's consider groups of order pq, where p and q are distinct primes with $p > q$.

By Sylow's first theorem, a group G of order pq has a Sylow p-subgroup P of order p and a Sylow q-subgroup Q of order q. Since $p > q$, Sylow's third theorem tells us that the number of Sylow p-subgroups, denoted $n_p$, must satisfy:

- np divides q (the other factor in the group order)
- np ≡ 1 (mod p)

The only value of np that can satisfy both conditions is np = 1, since any other divisor of q would be greater than 1 but less than q, and cannot be congruent to 1 modulo p when p > q.

This means G has a unique Sylow p-subgroup P, which implies P is normal in G. Similarly, let's determine nq:

- nq divides p
- nq ≡ 1 (mod q)

Here, we have two possibilities:

1. nq = 1, which means Q is normal in G
2. nq = p, which means there are p distinct Sylow q-subgroups

If nq = 1, then both P and Q are normal in G. Since P ∩ Q = {e} (as their orders are coprime) and |P|·|Q| = |G|, we have G = P × Q, which is isomorphic to the cyclic group Zpq.

If nq = p, then Q is not normal in G. In this case, G is isomorphic to a semidirect product P ⋊ Q, specifically Zp⋊Zq, which is non-abelian.

For nq = p to be possible, we need p ≡ 1 (mod q), meaning p = kq + 1 for some integer k.

Therefore:

- If p ≡ 1 (mod q), there are exactly two groups of order pq up to isomorphism: Zpq and Zp⋊Zq
- If p ≢ 1 (mod q), there is exactly one group of order pq up to isomorphism: Zpq

**Groups of Order $p^2q$**

Now let's analyze groups of order $p^2q$, where p and q are distinct primes.

Notes

By Sylow's theorems:

- There exists a Sylow p-subgroup P of order $p^2$
- There exists a Sylow q-subgroup Q of order q
- The number of Sylow p-subgroups np divides q and $np \equiv 1 \pmod{p}$
- The number of Sylow q-subgroups nq divides $p^2$ and $nq \equiv 1 \pmod{q}$

For np, the possibilities are $np = 1$ or $np = q$, but $np \equiv 1 \pmod{p}$ means $np = 1$ is the only possibility when $q < p$. If $q > p$, we need to check if $q \equiv 1 \pmod{p}$.

For nq, the possibilities are $nq = 1$, $nq = p$, or $nq = p^2$. We need $nq \equiv 1 \pmod{q}$, so:

- If $p \not\equiv 1 \pmod{q}$ and $p^2 \not\equiv 1 \pmod{q}$, then $nq = 1$
- Otherwise, we need to determine if $nq = p$ or $nq = p^2$ is possible

When $np = 1$ and $nq = 1$, both P and Q are normal, leading to a direct product structure.

The classification becomes more complex depending on the structure of the Sylow p-subgroup P, which can be either cyclic ($Zp^2$) or elementary abelian ($Zp \times Zp$). Each case leads to different possibilities for the group structure.

**Simplicity and Sylow Subgroups**

Another important application of Sylow's theorems is determining whether a group is simple or not. Recall that a group is simple if it has no proper normal subgroups except the trivial subgroup.

A Group of Order 60

Let's determine if a group of order $60 = 2^2 \times 3 \times 5$ can be simple.

The numbers of Sylow subgroups are:

- $n_2$ divides 15 and $n_2 \equiv 1 \pmod 2$, so $n_2 \in \{1, 3, 5, 15\}$
- $n_3$ divides 20 and $n_3 \equiv 1 \pmod 3$, so $n_3 \in \{1, 4, 10\}$
- $n_5$ divides 12 and $n_5 \equiv 1 \pmod 5$, so $n_5 \in \{1, 6\}$

If any of these are 1, then the corresponding Sylow subgroup is normal, and the group is not simple.

For a group of order 60 to be simple, we need $n_2 > 1$, $n_3 > 1$, and $n_5 > 1$.

Let's consider A5, the alternating group on 5 symbols. In A5:

- $n_2 = 5$ (the Sylow 2-subgroups have order 4)
- $n_3 = 10$ (the Sylow 3-subgroups have order 3)
- $n_5 = 6$ (the Sylow 5-subgroups have order 5)

Since none of these Sylow subgroups are normal, A5 is a candidate for being simple. In fact, A5 is the only simple group of order 60, and this can be proven using more advanced techniques in group theory.

**Burnside's $p^aq^b$ Theorem**

A powerful result derived from Sylow's theorems is Burnside's $p^aq^b$ theorem, which states that any group whose order is divisible by at most two distinct primes is solvable, hence not simple (unless it's of prime order).This means groups of order $p^aq^b$, where p and q are primes and a, b are non-negative integers, are never simple if both a and b are positive.

**Automorphism Groups and Sylow Subgroups**

The automorphism group Aut(G) of a group G consists of all isomorphisms from G to itself. Sylow's theorems provide insights into the structure of Aut(G).

Notes

For a p-group P (a group whose order is a power of a prime p), the automorphism group Aut(P) has interesting properties:

- The order of Aut(P) is divisible by p if P is not elementary abelian
- There is a subgroup of Aut(P) consisting of automorphisms that fix the elements of the center of P modulo the commutator subgroup

For Sylow p-subgroups in general, conjugation by elements of the normalizer of a Sylow p-subgroup gives rise to automorphisms of the Sylow p-subgroup, connecting the normalizer structure with the automorphism group.

**Frobenius Groups and Sylow's Theorems**

A Frobenius group is a group G with a proper subgroup H (called the Frobenius complement) such that $H \cap H^g = \{e\}$ for all $g \in G - H$, where $H^g = g^{(-1)}Hg$.

Sylow's theorems help in analyzing the structure of Frobenius groups. For instance, if G is a Frobenius group with complement H, and P is a Sylow p-subgroup of H, then $N_G(P) \subseteq H$. This result helps in understanding the distribution of Sylow subgroups in Frobenius groups.

**Solved Problems on Sylow's Theorems**

**Problem 1: Determine all groups of order 15 up to isomorphism.**

Solution: We have $15 = 3 \times 5$, where 3 and 5 are distinct primes.

Step 1: Identify the Sylow subgroups.

- By Sylow's first theorem, there exists a Sylow 3-subgroup P of order 3 and a Sylow 5-subgroup Q of order 5.

Step 2: Determine the number of Sylow subgroups.

- The number of Sylow 3-subgroups $n_3$ must divide 5 and satisfy $n_3 \equiv 1 \pmod 3$
- The possible values for n3 are 1 and 5, but only 1 satisfies $n_3 \equiv 1 \pmod 3$
- So $n_3 = 1$, which means the Sylow 3-subgroup is normal in G
- The number of Sylow 5-subgroups n5 must divide 3 and satisfy $n_5 \equiv 1 \pmod 5$
- The possible values for $n_5$ are 1 and 3, but since $3 \not\equiv 1 \pmod 5$, we have $n_5 = 1$
- So the Sylow 5-subgroup is also normal in G

Step 3: Determine the group structure.

- Both the Sylow 3-subgroup P and the Sylow 5-subgroup Q are normal in G
- $P \cap Q = \{e\}$ because $\gcd(3, 5) = 1$
- $|P| \cdot |Q| = 3 \cdot 5 = 15 = |G|$
- Therefore, $G = P \times Q \cong Z_3 \times Z_5 \cong Z_{15}$

Thus, there is exactly one group of order 15 up to isomorphism, namely the cyclic group Z15.

**Problem 2: Prove that any group of order 20 has a normal subgroup of order 5 or a normal subgroup of order 4.**

Solution: We have $20 = 2^2 \times 5$, so a group G of order 20 has Sylow 2-subgroups of order $2^2 = 4$ and Sylow 5-subgroups of order 5.

Step 1: Determine the possible numbers of Sylow subgroups.

- The number of Sylow 2-subgroups $n_2$ must divide 5 and satisfy $n_2 \equiv 1 \pmod 2$
- The possible values are $n_2 = 1$ or $n_2 = 5$

- The number of Sylow 5-subgroups $n_5$ must divide 4 and satisfy $n_5 \equiv 1 \pmod 5$)
- The only possible value is $n_5 = 1$ since no number dividing 4 is congruent to 1 modulo 5 except 1

Step 2: Analyze the cases.

- If $n_2 = 1$, then the Sylow 2-subgroup is normal and has order 4
- If $n_5 = 1$ (which must be true), then the Sylow 5-subgroup is normal and has order 5

In either case, G has a normal subgroup of order 4 or a normal subgroup of order 5 (or both).

Therefore, any group of order 20 has a normal subgroup of order 5, and it may also have a normal subgroup of order 4.

**Problem 3: Prove that no group of order 30 is simple.**

Solution: We have $30 = 2 \times 3 \times 5$, so a group G of order 30 has Sylow 2-subgroups of order 2, Sylow 3-subgroups of order 3, and Sylow 5-subgroups of order 5.

Step 1: Determine the possible numbers of Sylow subgroups.

- The number of Sylow 2-subgroups $n_2$ must divide 15 and satisfy $n_2 \equiv 1 \pmod 2$)
- The possible values are $n_2 = 1, 3, 5,$ or 15
- The number of Sylow 3-subgroups $n_3$ must divide 10 and satisfy $n_3 \equiv 1 \pmod 3$)
- The possible values are $n_3 = 1$ or 10
- The number of Sylow 5-subgroups $n_5$ must divide 6 and satisfy $n_5 \equiv 1 \pmod 5$)
- The possible values are $n_5 = 1$ or 6

Step 2: Count elements in the Sylow subgroups.

- Each Sylow 2-subgroup has 1 element of order 1 and 1 element of order 2
- Each Sylow 3-subgroup has 1 element of order 1 and 2 elements of order 3
- Each Sylow 5-subgroup has 1 element of order 1 and 4 elements of order 5

Step 3: Use counting arguments to find a contradiction. Suppose G is simple. Then none of the Sylow subgroups are normal, so $n_2 > 1$, $n_3 > 1$, and $n_5 > 1$.

If $n_5 = 6$, there are $6 \times 4 = 24$ elements of order 5. If $n_3 = 10$, there are $10 \times 2 = 20$ elements of order 3. The identity element accounts for 1 more element.

This gives at least $24 + 20 + 1 = 45$ elements, which exceeds the order of G (30).

Therefore, at least one of the Sylow subgroups must be normal, which means G is not simple.

**Problem 4: Classify all groups of order 12 up to isomorphism.**

Solution: We have $12 = 2^2 \times 3$, so a group G of order 12 has Sylow 2-subgroups of order 4 and Sylow 3-subgroups of order 3.

Step 1: Determine the possible numbers of Sylow subgroups.

- The number of Sylow 2-subgroups $n_2$ must divide 3 and satisfy $n_2 \equiv 1 \pmod 2$
- The possible values are $n_2 = 1$ or $n_2 = 3$
- The number of Sylow 3-subgroups $n_3$ must divide 4 and satisfy $n_3 \equiv 1 \pmod 3$
- The possible values are $n_3 = 1$ or $n_3 = 4$

Notes

Step 2: Analyze the possible structures based on these values.

Case 1: $n_2 = 1$ and $n_3 = 1$ Both Sylow subgroups are normal. Let P be the Sylow 2-subgroup and Q be the Sylow 3-subgroup.

- $P \cap Q = \{e\}$ since $\gcd(4, 3) = 1$
- $|P| \cdot |Q| = 4 \cdot 3 = 12 = |G|$
- $G = P \times Q \cong P \times Z3$
- P can be either $Z_4$ or $Z_2 \times Z_2$ So we get $Z_4 \times Z_3 \cong Z_{12}$ or $(Z_2 \times Z_2) \times Z_3 \cong Z_2 \times Z_2 \times Z_3 \cong Z_2 \times Z_6$

Case 2: $n_2 = 1$ and $n_3 = 4$ The Sylow 2-subgroup P is normal, and there are 4 Sylow 3-subgroups.

- If $P \cong Z_4$, we get $A_4$ (the alternating group on 4 symbols)
- If $P \cong Z_2 \times Z_2$, we get $D_{12}$ (the dihedral group of order 12)

Case 3: n2 = 3 and n3 = 1 The Sylow 3-subgroup Q is normal, and there are 3 Sylow 2-subgroups. This gives us a semi-direct product structure.

- If the action of Q on P is trivial, we get $P \times Q$
- If the action is non-trivial, we get a different group, which is a semi-direct product $Z_3 \rtimes Z_4$ or $Z_3 \rtimes (Z_2 \times Z_2)$

Case 4: $n_2 = 3$ and $n_3 = 4$ This is not possible by a counting argument: 3 Sylow 2-subgroups contain 9 distinct elements, and 4 Sylow 3-subgroups contain 8 distinct elements, plus the identity gives 18 elements, which exceeds 12.

Therefore, the groups of order 12 up to isomorphism are:

1. $Z_{12}$ (cyclic group)
2. $Z_2 \times Z_6$ (direct product)
3. $A_4$ (alternating group on 4 symbols)

4. $D_{12}$ (dihedral group of order 12)
5. $Z_3 \rtimes Z_4$ (semi-direct product)

**Problem 5: Show that a group of order $56 = 2^3 \times 7$ has a normal Sylow 7-subgroup.**

Solution: We have $56 = 2^3 \times 7$, so a group G of order 56 has Sylow 2-subgroups of order $2^3 = 8$ and Sylow 7-subgroups of order 7.

Step 1: Determine the number of Sylow 7-subgroups.

- The number of Sylow 7-subgroups n7 must divide 8 and satisfy $n_7 \equiv 1 \pmod 7$
- The possible values are $n_7 = 1$ or $n_7 = 8$

Step 2: Show that $n_7 = 8$ is impossible. If $n_7 = 8$, then there are 8 distinct Sylow 7-subgroups. Each Sylow 7-subgroup has 6 elements of order 7, plus the identity.

Let's count the elements in these Sylow 7-subgroups:

- The identity element is in all Sylow 7-subgroups
- Each of the 8 Sylow 7-subgroups has 6 elements of order 7
- Different Sylow 7-subgroups intersect only at the identity (by a property of Sylow p-subgroups when p is the largest prime dividing |G|)

So we have $1 + 8 \times 6 = 1 + 48 = 49$ distinct elements. But this leaves only 56 - 49 = 7 elements for the Sylow 2-subgroups, which is impossible since each Sylow 2-subgroup has 8 elements.

Therefore, $n_7 = 1$, which means there is a unique Sylow 7-subgroup, and it must be normal in G.

Unsolved Problems on Sylow's Theorems

1. Determine all groups of order $42 = 2 \times 3 \times 7$ up to isomorphism.

Notes

2. Prove that any group of order $36 = 2^2 \times 3^2$ has a normal subgroup.
3. Show that a group of order $255 = 3 \times 5 \times 17$ is not simple.
4. Classify all groups of order $21 = 3 \times 7$ up to isomorphism.
5. Prove that any group of order $100 = 2^2 \times 5^2$ has a normal Sylow subgroup.

## 2.2.1: Introduction to Ring Theory

### Definition and Basic Properties of Rings

A ring is an algebraic structure that generalizes the familiar properties of integers with respect to addition and multiplication. Formally, a ring is a set R together with two binary operations, usually denoted as addition (+) and multiplication (·), satisfying the following axioms:

1. (R, +) is an abelian group:
    - Closure: For all a, b ∈ R, a + b ∈ R
    - Associativity: For all a, b, c ∈ R, (a + b) + c = a + (b + c)
    - Identity: There exists an element 0 ∈ R such that a + 0 = 0 + a = a for all a ∈ R
    - Inverse: For each a ∈ R, there exists -a ∈ R such that a + (-a) = (-a) + a = 0
    - Commutativity: For all a, b ∈ R, a + b = b + a
2. Multiplication is associative:
    - For all a, b, c ∈ R, (a · b) · c = a · (b · c)
3. Multiplication distributes over addition:
    - Left distributivity: For all a, b, c ∈ R, a · (b + c) = (a · b) + (a · c)
    - Right distributivity: For all a, b, c ∈ R, (a + b) · c = (a · c) + (b · c)

Note that multiplication in a ring is not required to be commutative. A ring in which multiplication is commutative (a · b = b · a for all a, b ∈ R) is called a commutative ring.

Examples of Rings

1. The integers Z with ordinary addition and multiplication form a commutative ring.
2. The set of n × n matrices over a field F, denoted $M_n(F)$, forms a non-commutative ring when n > 1.
3. The set of polynomials with coefficients from a ring R, denoted R[x], forms a ring.
4. The set of continuous functions from R to R forms a commutative ring under pointwise addition and multiplication.
5. The set Zn of integers modulo n forms a commutative ring.

Units, Zero Divisors, and Integral Domains

In a ring R, we define:

- A unit is an element a ∈ R for which there exists an element b ∈ R such that a · b = b · a = 1, where 1 is the multiplicative identity if it exists. The element b is called the multiplicative inverse of a and is denoted $a^{(-1)}$.
- A zero divisor is a non-zero element a ∈ R for which there exists a non-zero element b ∈ R such that a · b = 0 or b · a = 0.
- An integral domain is a commutative ring with a multiplicative identity where there are no zero divisors.

Example: In $Z_6$, the element 2 is a zero divisor because 2 · 3 = 0. The units in $Z_6$ are 1 and 5, as 1 · 1 = 1 and 5 · 5 = 25 ≡ 1 (mod 6).

**Subrings and Ideals**

A subring of a ring R is a subset S of R that forms a ring under the same operations as R. For S to be a subring, it must:

1. Be non-empty
2. Be closed under addition

3. Be closed under negation
4. Be closed under multiplication

An ideal of a ring R is a subring I with the additional property that for all r ∈ R and all a ∈ I, both r · a and a · r are in I. In other words, I "absorbs" multiplication by any element of R.

For a commutative ring R, a subset I is an ideal if and only if:

1. I is non-empty
2. I is closed under addition
3. For all a ∈ I and r ∈ R, r · a ∈ I

**Types of Ideals**

1. Trivial Ideals: The set {0} (containing only the additive identity) and the entire ring R are always ideals of R, called the trivial ideals.
2. Principal Ideal: An ideal generated by a single element a ∈ R, denoted (a) or Ra, is called a principal ideal. In a commutative ring, (a) = {r · a | r ∈ R}.
3. Prime Ideal: In a commutative ring, an ideal P is prime if whenever a · b ∈ P for a, b ∈ R, then either a ∈ P or b ∈ P.
4. Maximal Ideal: An ideal M is maximal if M ≠ R and there is no ideal I such that M ⊂ I ⊂ R.

**Ring Homomorphisms and Isomorphisms**

A ring homomorphism is a function φ: R → S between rings R and S that preserves the ring operations:

1. φ(a + b) = φ(a) + φ(b) for all a, b ∈ R
2. φ(a · b) = φ(a) · φ(b) for all a, b ∈ R

Notes

If φ is bijective, it is a ring isomorphism, and R and S are said to be isomorphic, denoted $R \cong S$.

The kernel of a ring homomorphism $\varphi: R \to S$ is the set of elements in R that map to the additive identity in S: $\text{Ker}(\varphi) = \{r \in R \mid \varphi(r) = 0S\}$

The kernel of a ring homomorphism is always an ideal of R.

**Quotient Rings**

Given a ring R and an ideal I of R, we can form the quotient ring R/I, whose elements are the cosets of I: $R/I = \{r + I \mid r \in R\}$

The operations on R/I are defined as: $(r + I) + (s + I) = (r + s) + I$ $(r + I) \cdot (s + I) = (r \cdot s) + I$

The quotient ring R/I inherits many properties from R. For example, if R is commutative, then R/I is commutative.

**The First Isomorphism Theorem for Rings**

If $\varphi: R \to S$ is a ring homomorphism with kernel K, then: $R/K \cong \text{Im}(\varphi)$

where $\text{Im}(\varphi)$ is the image of φ.

**Polynomial Rings**

Given a ring R, the polynomial ring R[x] consists of polynomials with coefficients from R. A typical element of R[x] has the form: $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$

where $a_0, a_1, ..., a_n$ are elements of R.

Addition in R[x] is performed term by term, and multiplication follows the standard rule of multiplying polynomials.

**Properties of Polynomial Rings**

1. If R is a commutative ring, then R[x] is a commutative ring.
2. If R is an integral domain, then R[x] is an integral domain.

3. The degree of a product of polynomials equals the sum of the degrees of the factors when R is an integral domain.

**Irreducibility**

A polynomial $f(x) \in R[x]$ is irreducible over R if it cannot be expressed as a product of two polynomials of lower degree in R[x].

For example, $x^2 + 1$ is irreducible over R (the real numbers) but reducible over C (the complex numbers), where it can be factored as $(x + i)(x - i)$.

### 2.2.2: Fields

A field is a commutative ring in which every non-zero element has a multiplicative inverse. In other words, a field is a commutative ring where the non-zero elements form a group under multiplication.

Examples of fields include:

1. The rational numbers Q
2. The real numbers R
3. The complex numbers C
4. The finite field Zp when p is a prime number

**Field Extensions**

A field extension is a pair of fields E and F such that F is a subfield of E. We denote this as E/F.

The degree of the extension E/F, denoted [E:F], is the dimension of E as a vector space over F.

**Algebraic Elements and Extensions**

An element $\alpha \in E$ is algebraic over F if it is a root of a non-zero polynomial with coefficients in F. Otherwise, $\alpha$ is transcendental over F.

Notes

An extension E/F is algebraic if every element of E is algebraic over F.

Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

A Euclidean domain is an integral domain R with a function d: R - {0} → N (natural numbers) such that for any a, b ∈ R with b ≠ 0, there exist q, r ∈ R such that a = qb + r with either r = 0 or d(r) < d(b).

A principal ideal domain (PID) is an integral domain in which every ideal is principal.

A unique factorization domain (UFD) is an integral domain in which every non-zero non-unit element can be written as a product of irreducible elements, and this factorization is unique up to units and the order of factors.

The relationship between these domains is: Euclidean Domain ⇒ Principal Ideal Domain ⇒ Unique Factorization Domain

Examples:

- Z (integers) is a Euclidean domain, hence also a PID and a UFD.
- F[x] (polynomials over a field F) is a Euclidean domain.
- Z[x] (polynomials with integer coefficients) is a UFD but not a PID.

**Solved Problems on Ring Theory**

Problem 1: Determine whether $Z[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in Z\}$ is a unique factorization domain.

Solution: To determine whether $Z[\sqrt{-5}]$ is a UFD, we need to check if factorizations into irreducibles are unique.

Step 1: Consider the element $6 \in Z[\sqrt{-5}]$. We can factor 6 as $2 \times 3$.

Step 2: Consider the element $1 + \sqrt{-5}$ and its conjugate $1 - \sqrt{-5}$ in $Z[\sqrt{-5}]$. Their product is $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 1 - (\sqrt{-5})^2 = 1 - (-5) = 6$.

Step 3: Check if 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are irreducible in $Z[\sqrt{-5}]$.

Define the norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$, which satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$.

- $N(2) = 4$
- $N(3) = 9$
- $N(1 + \sqrt{-5}) = 1 + 5 = 6$
- $N(1 - \sqrt{-5}) = 1 + 5 = 6$

If any of these elements were reducible, they could be expressed as a product of two elements with smaller norms. But none of the norms 4, 9, or 6 can be expressed as a product of norms of elements in $Z[\sqrt{-5}]$ other than 1 times themselves. Therefore, all four elements are irreducible.

Step 4: Since $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, we have two distinct factorizations of 6 into irreducibles.

Therefore, $Z[\sqrt{-5}]$ is not a unique factorization domain.

**Problem 2: Show that in a commutative ring, maximal ideals are prime.**

Solution: Let R be a commutative ring and M a maximal ideal of R.

Step 1: Recall the definitions:

- An ideal M is maximal if $M \neq R$ and there is no ideal I such that $M \subset I \subset R$.
- An ideal P is prime if for all $a, b \in R$, $ab \in P$ implies $a \in P$ or $b \in P$.

Step 2: To show M is prime, assume $ab \in M$ for some $a, b \in R$.

Notes

Step 3: We need to show that either $a \in M$ or $b \in M$. Let's use a proof by contradiction. Suppose $a \notin M$ and $b \notin M$.

Step 4: Consider the ideal (M, a) generated by M and a: (M, a) = {m + ra | $m \in M$, $r \in R$}Since M is maximal and $a \notin M$, we must have (M, a) = R. Thus, thereexist $m1 \in M$ and $r1 \in R$ such that $m1 + r1a = 1$. Similarly, (M, b) = R, so there exist $m_2 \in M$ and $r_2 \in R$ such that $m_2 + r_2b = 1$.

### 2.2.3: Rings of Polynomials

**Introduction to Polynomial Rings**

A polynomial ring is a fundamental algebraic structure that extends the concept of a ring to include polynomials with coefficients from another ring. Polynomials are expressions consisting of variables, coefficients, and operations of addition, subtraction, and multiplication.

For a ring R, the polynomial ring R[x] consists of all polynomials with coefficients from R in the indeterminate x. These polynomials take the form:

$f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$

where $a_0$, $a_1$, $a_2$, ..., $a_n$ are elements of the ring R, and n is a non-negative integer. The element $a_n$ (if non-zero) is called the leading coefficient, and n is the degree of the polynomial, denoted by deg(f).

**Basic Properties of Polynomial Rings**

1. Ring Structure: R[x] forms a ring with the standard operations of polynomial addition and multiplication.
2. Addition: For polynomials $f(x) = a_0 + a_1x + ... + a_nx^n$ and $g(x) = b_0 + b_1x + ... + b_mx^m$:

$f(x) + g(x) = (a_0+b_0) + (a_1+b_1)x + ...$ + higher terms

Essentially, we add the coefficients of like terms.



3. Multiplication: For the same polynomials:

$f(x) \times g(x) = c_0 + c_1x + c_2x^2 + ... + c_{n+m}x^{n+m}$

where $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ for each k = 0, 1, 2, ..., n+m.

4. Degree Properties:
    - For non-zero polynomials f and g, deg(f·g) = deg(f) + deg(g)
    - For polynomials f and g, deg(f+g) ≤ max(deg(f), deg(g))
5. Zero Polynomial: The polynomial $0 + 0x + 0x^2 + ...$ is called the zero polynomial and is denoted by 0. Its degree is conventionally defined as $-\infty$.

**Integral Domains and Polynomial Rings**

If R is an integral domain (a ring with no zero divisors), then R[x] is also an integral domain. This means:

- If f(x) and g(x) are non-zero polynomials in R[x], then their product f(x)·g(x) is also non-zero.
- The leading coefficient of the product is the product of the leading coefficients of the factors.

**Units in Polynomial Rings**

A unit in a ring is an element that has a multiplicative inverse. In R[x]:

- If R is an integral domain, the only units in R[x] are the constant polynomials that are units in R.
- For example, in Z[x] (polynomials with integer coefficients), the only units are 1 and -1.

- In Q[x] (polynomials with rational coefficients), any non-zero rational number forms a unit.

**Irreducible Polynomials**

A non-constant polynomial f(x) in R[x] is irreducible over R if it cannot be factored as a product of two non-constant polynomials in R[x].

Examples:

- $x^2 + 1$ is irreducible over R (the real numbers)
- $x^2 + 1$ is reducible over C (the complex numbers) as (x+i)(x-i)
- $x^2 - 2$ is irreducible over Q (the rational numbers)

**Polynomial Division**

If R is a field, then there's a division algorithm for polynomials in R[x]:

For polynomials f(x) and g(x) ≠ 0 in R[x], there exist unique polynomials q(x) (quotient) and r(x) (remainder) such that:

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

where either r(x) = 0 or deg(r) <deg(g).

This leads to the important result that R[x] is a Euclidean domain when R is a field, meaning we can find greatest common divisors using the Euclidean algorithm.

**Evaluating Polynomials**

For a polynomial $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ in R[x] and an element r in R, the evaluation of f at r, denoted f(r), is:

$f(r) = a_0 + a_1r + a_2r^2 + ... + a_nr^n$

This is an element of R and is computed by substituting r for x in the polynomial.

**Polynomial Rings in Multiple Variables**

The concept extends naturally to multiple variables. For example, R[x,y] represents the ring of polynomials in two variables x and y with coefficients from R.

A polynomial in R[x,y] takes the form:

$$f(x,y) = \sum_{i=0}^{n} \sum_{i=0}^{m} a_{ij} x^i y^j$$

where $a_{ij}$ are elements of R.

**Solved Examples**

**Example 1: Addition and Multiplication in Z[x]**

Let $f(x) = 2x^3 + 3x^2 - 5x + 1$ and $g(x) = x^2 - 2x + 4$ in Z[x].

Calculate $f(x) + g(x)$ and $f(x) \cdot g(x)$.

**Solution:**

For addition, we combine like terms: $f(x) + g(x) = (2x^3 + 3x^2 - 5x + 1) + (x^2 - 2x + 4) = 2x^3 + (3+1)x^2 + (-5-2)x + (1+4) = 2x^3 + 4x^2 - 7x + 5$

For multiplication, we multiply each term of f(x) by each term of g(x): $f(x) \cdot g(x) = (2x^3 + 3x^2 - 5x + 1) \cdot (x^2 - 2x + 4)$

First, multiply $2x^3$ by each term in g(x): $2x^3(x^2 - 2x + 4) = 2x^5 - 4x^4 + 8x^3$

Next, multiply $3x^2$ by each term in g(x): $3x^2(x^2 - 2x + 4) = 3x^4 - 6x^3 + 12x^2$

Next, multiply $-5x$ by each term in g(x): $-5x(x^2 - 2x + 4) = -5x^3 + 10x^2 - 20x$

Finally, multiply 1 by each term in g(x): $1(x^2 - 2x + 4) = x^2 - 2x + 4$

Now combine like terms: $f(x) \cdot g(x) = 2x^5 + (-4+3)x^4 + (8-6-5)x^3 + (12+10)x^2 + (-20-2)x + 4 = 2x^5 - x^4 - 3x^3 + 22x^2 - 22x + 4$

**Example 2: Determining Irreducibility**

Determine whether $p(x) = x^3 - 3x + 1$ is irreducible over Q.

**Solution:**

Notes

To check if p(x) is irreducible over Q, we can use the Rational Root Theorem.

If p(x) has a rational root a/b in lowest terms, then a divides the constant term (1) and b divides the leading coefficient (1).

The possible rational roots are therefore: ±1.

Let's check: $p(1) = 1^3 - 3\cdot1 + 1 = 1 - 3 + 1 = -1 \neq 0$ $p(-1) = (-1)^3 - 3\cdot(-1) + 1 = -1 + 3 + 1 = 3 \neq 0$

So p(x) has no rational roots. Since p(x) is a cubic polynomial with no linear factors, it must be irreducible over Q (as any factorization would necessarily include a linear factor).

Therefore, $x^3 - 3x + 1$ is irreducible over Q.

**Example 3: Division Algorithm in Q[x]**

Use the polynomial division algorithm to find the quotient and remainder when $f(x) = 2x^4 - 3x^3 + x - 5$ is divided by $g(x) = x^2 - 2$.

**Solution:**

We need to find polynomials q(x) and r(x) such that $f(x) = g(x)\cdot q(x) + r(x)$ where deg(r) <deg(g) = 2.

Step 1: Divide the leading term of f(x) by the leading term of g(x): $2x^4 \div x^2 = 2x^2$

Step 2: Multiply g(x) by this term: $2x^2 \cdot (x^2 - 2) = 2x^4 - 4x^2$

Step 3: Subtract from f(x) and continue: $f(x) - (2x^4 - 4x^2) = -3x^3 + 4x^2 + x - 5$

Step 4: Divide the leading term of this result by the leading term of g(x): $-3x^3 \div x^2 = -3x$

Step 5: Multiply g(x) by this term: $-3x \cdot (x^2 - 2) = -3x^3 + 6x$

Step 6: Subtract and continue: $-3x^3 + 4x^2 + x - 5 - (-3x^3 + 6x) = 4x^2 + x - 6x - 5 = 4x^2 - 5x - 5$

The degree of this remainder is less than deg(g), so we're done.

Therefore, $q(x) = 2x^2 - 3x$ and $r(x) = 4x^2 - 5x - 5$.

Verification: $f(x) = g(x) \cdot q(x) + r(x) = (x^2 - 2)(2x^2 - 3x) + (4x^2 - 5x - 5) = 2x^4 - 4x^2 - 3x^3 + 6x + 4x^2 - 5x - 5 = 2x^4 - 3x^3 + 0x^2 + x - 5$

**Example 4: Finding GCD using the Euclidean Algorithm**

Find the greatest common divisor of $f(x) = x^3 - 1$ and $g(x) = x^2 - 1$ in $Q[x]$.

**Solution:**

We apply the Euclidean algorithm:

Step 1: Divide f(x) by g(x): $x^3 - 1 = (x^2 - 1) \cdot x + (x - 1)$

So the remainder $r_1(x) = x - 1$.

Step 2: Divide g(x) by $r_1(x)$: $x^2 - 1 = (x - 1) \cdot (x + 1) + 0$

Since the remainder is 0, the GCD is the last non-zero remainder, which is $r_1(x) = x - 1$.

Therefore, $\gcd(x^3 - 1, x^2 - 1) = x - 1$.

This makes sense because: $x^3 - 1 = (x - 1)(x^2 + x + 1)$ $x^2 - 1 = (x - 1)(x + 1)$

**Example 5: Evaluating a Polynomial at a Point**

Let $f(x) = 3x^4 - 2x^2 + 5x - 7$ be a polynomial in $Z[x]$. Evaluate f(2).

**Solution:**

$f(2) = 3(2^4) - 2(2^2) + 5(2) - 7 = 3(16) - 2(4) + 5(2) - 7 = 48 - 8 + 10 - 7 = 43$

Therefore, f(2) = 43.

**Unsolved Problems**

**Problem 1**

Notes

Let $f(x) = x^3 - 4x^2 + 3x + 1$ and $g(x) = x^2 - x - 2$ be polynomials in $Q[x]$. Find the quotient and remainder when $f(x)$ is divided by $g(x)$.

**Problem 2**

Determine whether the polynomial $p(x) = x^4 - 10x^2 + 1$ is irreducible over $Q$.

**Problem 3**

Find the greatest common divisor of $h(x) = x^4 - 16$ and $k(x) = x^2 - 4$ in $Z[x]$.

**Problem 4**

Let $R[x,y]$ be the ring of polynomials in two variables with real coefficients. If $f(x,y) = x^2y + 3xy^2 - y^3 + 2$, evaluate $f(1,2)$.

**Problem 5**

Prove that if $R$ is an integral domain, then the polynomial $f(x) = ax + b$ is irreducible in $R[x]$ if and only if it is not divisible by any non-unit element of $R$.

## 2.3.1: Polynomials in an Indeterminate

### Introduction to Indeterminates

An indeterminate in algebra is a symbol that does not stand for any fixed value, unlike a variable which can be assigned different values. The concept of an indeterminate is fundamental to the theory of polynomial rings.

When we write R[x], we are considering the ring of polynomials in the indeterminate x with coefficients from the ring R. The element x in R[x] is transcendental over R, meaning it doesn't satisfy any non-zero polynomial equation with coefficients in R.

### Formal Definition and Structure

A polynomial in an indeterminate x over a ring R is formally defined as an infinite sequence of elements from R:

$(a_0, a_1, a_2, ..., a_n, 0, 0, ...)$

where only finitely many terms are non-zero. This sequence represents the polynomial:

$a_0 + a_1x + a_2x^2 + ... + a_nx^n$

The set of all such sequences forms the polynomial ring R[x]. The operations in this ring are defined as follows:

- Addition: Component-wise addition of sequences
- Multiplication: Convolution product of sequences, where the kth component of the product is given by $\sum_{i=0}^{k} a_i b_{k-i}$

### Comparison with Function Rings

It's important to distinguish between polynomials as formal expressions and polynomial functions:

- A polynomial in R[x] is a formal algebraic expression

- A polynomial function maps elements of R to R by evaluation

When R is an infinite integral domain, the ring R[x] is isomorphic to a subring of the ring of functions from R to R. However, when R is a finite field, different polynomials may induce the same function.

For example, in $Z_2[x]$ (polynomials over the field with two elements), the polynomials $x^2$ and x induce the same function since $0^2 = 0$ and $1^2 = 1$.

**Monomials and Terms**

A monomial in the indeterminate x is an expression of the form ax^n where a is a coefficient from R and n is a non-negative integer. The degree of this monomial is n.

A term of a polynomial refers to each monomial that appears in the polynomial with a non-zero coefficient.

**Evaluating Polynomials at Points**

For a polynomial $f(x) = a_0 + a_1x + ... + a_nx^n$ in R[x] and an element r in R, the evaluation homomorphism $\varphi_r$: R[x] → R is defined by:

$\varphi_r(f) = f(r) = a_0 + a_1r + ... + a_nr^n$

This is a ring homomorphism, meaning it preserves the operations of addition and multiplication.

**The Universal Property**

The polynomial ring R[x] satisfies an important universal property: For any ring S and any ring homomorphism $\varphi$: R → S and any element s in S, there exists a unique ring homomorphism $\psi$: R[x] → S such that $\psi(r) = \varphi(r)$ for all r in R and $\psi(x) = s$.

This property characterizes R[x] up to isomorphism and highlights its fundamental role in algebra.

**Polynomial Identities and the Substitution Principle**

A polynomial identity is an equation between two polynomials that holds for all possible values of the indeterminates.

The substitution principle states that if an identity holds for all polynomials, then it holds when the indeterminates are replaced by any elements from the ring.

**Roots and Factors**

An element r in R is called a root of a polynomial f(x) in R[x] if f(r) = 0.

If r is a root of f(x), then (x - r) is a factor of f(x), meaning there exists a polynomial q(x) such that f(x) = (x - r)·q(x).

A polynomial of degree n over a field can have at most n roots unless it is the zero polynomial.

**Polynomials over Fields**

When R is a field, R[x] has several additional properties:

1. R[x] is a principal ideal domain, meaning every ideal is generated by a single element.
2. The division algorithm holds: for polynomials f(x) and g(x) ≠ 0, there exist unique q(x) and r(x) such that f(x) = g(x)·q(x) + r(x) where r(x) = 0 or deg(r) <deg(g).
3. Every non-constant polynomial can be factored uniquely (up to units) as a product of irreducible polynomials.

**The Remainder Theorem**

The Remainder Theorem states that when a polynomial f(x) is divided by (x - a), the remainder is equal to f(a).

Mathematically: f(x) = (x - a)q(x) + f(a)

This theorem provides a quick way to evaluate polynomials and is the basis for polynomial interpolation.

Notes

**The Factor Theorem**

The Factor Theorem is a direct consequence of the Remainder Theorem:

An element a is a root of f(x) if and only if (x - a) is a factor of f(x).

This follows because f(a) = 0 if and only if the remainder when dividing f(x) by (x - a) is zero.

**Multiple Indeterminates**

The construction of polynomial rings can be extended to multiple indeterminates. For example, R[x,y] is the ring of polynomials in two indeterminates x and y with coefficients in R.

A polynomial in R[x,y] can be written as:
$f(x,y) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x^i y^j$

where $a_{ij}$ are elements of R.

There are different ways to view R[x,y]:

- As (R[x])[y], polynomials in y with coefficients in R[x]
- As (R[y])[x], polynomials in x with coefficients in R[y]
- Directly as R[x,y], polynomials in x and y with coefficients in R

All these viewpoints are isomorphic.

**Homogeneous Polynomials**

A homogeneous polynomial (or form) is a polynomial whose terms all have the same total degree.

For example, in R[x,y], the polynomial $3x^2 + 5xy + 2y^2$ is homogeneous of degree 2 because each term has total degree 2.

Homogeneous polynomials have important applications in projective geometry and invariant theory.

**Multivariate Polynomial Division**

Division of multivariate polynomials is more complex than in the single-variable case. There's no unique quotient and remainder without specifying a monomial ordering.

Common monomial orderings include:

- Lexicographic ordering
- Graded lexicographic ordering
- Graded reverse lexicographic ordering

The theory of Gröbner bases extends the Euclidean algorithm to multivariate polynomials.

**Solved Examples**

**Example 1: The Evaluation Homomorphism**

Prove that the evaluation map $\varphi_r$: R[x] → R defined by $\varphi_r(f) = f(r)$ is a ring homomorphism.

**Solution:**

We need to show that $\varphi_r$ preserves addition and multiplication.

For addition, let $f(x) = a_0 + a_1x + ... + a_nx^n$ and $g(x) = b_0 + b_1x + ... + b_mx^m$ be polynomials in R[x].

$\varphi_r(f + g) = (f + g)(r) = (a_0 + b_0) + (a_1 + b_1)r + ...$ + higher terms evaluated at $r = (a_0 + a_1r + ... + a_nr^n) + (b_0 + b_1r + ... + b_mr^m) = f(r) + g(r) = \varphi_r(f) + \varphi_r(g)$

For multiplication:

$\varphi_r(f \cdot g) = (f \cdot g)(r) = (a_0 + a_1r + ... + a_nr^n)(b_0 + b_1r + ... + b_mr^m) = f(r) \cdot g(r) = \varphi_r(f) \cdot \varphi_r(g)$

Therefore, $\varphi_r$ is a ring homomorphism.

**Example 2: Application of the Remainder Theorem**

Notes

Use the Remainder Theorem to evaluate $f(x) = 2x^3 - 5x^2 + 3x - 7$ at $x = 3$.

**Solution:**

According to the Remainder Theorem, when f(x) is divided by (x - 3), the remainder equals f(3).

Let's divide f(x) by (x - 3) using synthetic division:

```
3 |  2   -5    3   -7
  |      6    3   18
  ----------------
     2    1    6   11
```

Working through the synthetic division:

- Bring down 2
- Multiply 2 by 3 to get 6, add to -5 to get 1
- Multiply 1 by 3 to get 3, add to 3 to get 6
- Multiply 6 by 3 to get 18, add to -7 to get 11

The remainder is 11, so f(3) = 11.

We can verify this by direct computation: $f(3) = 2(3^3) - 5(3^2) + 3(3) - 7 = 2(27) - 5(9) + 3(3) - 7 = 54 - 45 + 9 - 7 = 11$

**Example 3: Proving a Polynomial Identity**

Prove that $(x + y)^2 = x^2 + 2xy + y^2$ for all elements x and y in a commutative ring R.

**Solution:**

We can expand the left-hand side using the distributive property: $(x + y)^2 = (x + y)(x + y) = x(x + y) + y(x + y) = x^2 + xy + yx + y^2$

Since R is commutative, xy = yx, so: $(x + y)^2 = x^2 + xy + xy + y^2 = x^2 + 2xy + y^2$

This is a polynomial identity in R[x,y] and holds for all x, y in R.

**Example 4: Polynomial Division in Multiple Indeterminates**

Divide $f(x,y) = x^2y + xy^2 + y^3$ by $g(x,y) = x + y$ in Q[x,y] using the lexicographic ordering with $x > y$.

**Solution:**

We need to find polynomials q(x,y) and r(x,y) such that $f(x,y) = g(x,y) \cdot q(x,y) + r(x,y)$.

Step 1: Divide the leading term of f(x,y), which is $x^2y$, by the leading term of g(x,y), which is x: $x^2y \div x = xy$

Step 2: Multiply g(x,y) by xy: $xy(x + y) = x^2y + xy^2$

Step 3: Subtract from f(x,y): $f(x,y) - (x^2y + xy^2) = x^2y + xy^2 + y^3 - (x^2y + xy^2) = y^3$

Step 4: Divide $y^3$ by the leading term of g(x,y): $y^3 \div x$ cannot be divided further since $y^3$ doesn't contain x

Therefore, $q(x,y) = xy$ and $r(x,y) = y^3$.

Verification: $f(x,y) = g(x,y) \cdot q(x,y) + r(x,y) = (x + y) \cdot xy + y^3 = x^2y + xy^2 + y^3$

**Example 5: Using the Factor Theorem**

Use the Factor Theorem to completely factor the polynomial $f(x) = x^3 - 4x^2 - 7x + 10$ over the rational numbers, given that $x = 2$ is a root.

**Solution:**

Since $x = 2$ is a root, we know that $(x - 2)$ is a factor of f(x).

We can use synthetic division to find the quotient when f(x) is divided by $(x - 2)$:

```
2 |  1   -4   -7   10
  |      2   -4  -22
  ----------------
```

1 -2 -11 -12

So $f(x) = (x - 2)(x^2 - 2x - 11)$

Now we need to factor $x^2 - 2x - 11$. Using the quadratic formula: $x = (2 \pm \sqrt{(4 + 44)})/2 = (2 \pm \sqrt{48})/2 = (2 \pm 4\sqrt{3})/2 = 1 \pm 2\sqrt{3}$

Since these roots are irrational, the quadratic is irreducible over Q.

Therefore, the complete factorization of f(x) over Q is: $f(x) = (x - 2)(x^2 - 2x - 11)$

**Unsolved Problems**

**Problem 1**

Let $f(x) = x^4 - 5x^2 + 4$ be a polynomial in Z[x]. Show that f(x) can be written as a product of two quadratic polynomials with integer coefficients.

**Problem 2**

Let R be a commutative ring with unity. Prove that the center of the polynomial ring R[x] is Z(R)[x], where Z(R) is the center of R.

**Problem 3**

Let $f(x) = x^5 + 3x^3 - 2x^2 + 5$ be a polynomial in Q[x]. Use the Remainder Theorem to find the remainder when f(x) is divided by (x - 1).

**Problem 4**

Let $f(x,y) = x^3y^2 + 2x^2y^3 - 3xy^4 + y^5$ be a polynomial in R[x,y]. Find all terms of f(x,y) that are homogeneous of degree 5.

**Problem 5**

Prove that if R is an integral domain, then the polynomial ring R[x] is never a field.

**2.3.2: Evaluation Homomorphism**

The evaluation homomorphism is a fundamental concept in abstract algebra, particularly in the theory of polynomials. It provides a way to evaluate polynomials at specific values while preserving their algebraic structure.

**Definition and Basic Properties**

Let F be a field and F[x] be the ring of polynomials with coefficients in F. For any element a ∈ F, the evaluation homomorphism at a is the map:

$\varphi_a$: F[x] → F

defined by:

$\varphi_a(p(x)) = p(a)$

In other words, the evaluation homomorphism takes a polynomial p(x) and evaluates it at the point x = a.

**Properties of the Evaluation Homomorphism**

1. Homomorphism Property:
    - For any polynomials p(x) and q(x) in F[x]:
        - $\varphi_a(p(x) + q(x)) = \varphi_a(p(x)) + \varphi_a(q(x))$
        - $\varphi_a(p(x) \cdot q(x)) = \varphi_a(p(x)) \cdot \varphi_a(q(x))$
2. Kernel Determination:
    - The kernel of $\varphi_a$ consists of all polynomials p(x) such that p(a) = 0
    - This means $\ker(\varphi_a) = \{p(x) \in F[x] \mid p(a) = 0\}$
    - The kernel is precisely the ideal generated by (x - a)
    - $\ker(\varphi_a) = (x - a)$
3. Surjectivity:

- The evaluation homomorphism is surjective (onto), meaning every element in F is the image of some polynomial in F[x]
- For any b ∈ F, the constant polynomial p(x) = b satisfies $\varphi_a(p(x)) = b$

4. First Isomorphism Theorem Application:
   - By the First Isomorphism Theorem for rings, F[x]/(x - a) ≅ F
   - This means the quotient ring of F[x] by the ideal generated by (x - a) is isomorphic to F

**Polynomial Division and the Remainder Theorem**

One important application of the evaluation homomorphism is the Remainder Theorem.

**Remainder Theorem**

For any polynomial p(x) ∈ F[x] and any a ∈ F, when p(x) is divided by (x - a), the remainder is equal to p(a).

Proof: By the Division Algorithm, we can write: p(x) = q(x)(x - a) + r

where r is a constant (polynomial of degree 0).

Evaluating both sides at x = a: p(a) = q(a)(a - a) + r = 0 + r = r

Therefore, r = p(a), which means the remainder when p(x) is divided by (x - a) is p(a).

**Factor Theorem**

The Factor Theorem is a direct consequence of the Remainder Theorem:

Theorem: (x - a) is a factor of p(x) if and only if p(a) = 0.

Proof:

- If (x - a) is a factor of p(x), then p(x) = q(x)(x - a) for some q(x)
- Evaluating at x = a: p(a) = q(a)(a - a) = 0
- Conversely, if p(a) = 0, then by the Remainder Theorem, the remainder when p(x) is divided by (x - a) is 0
- Thus, p(x) = q(x)(x - a) for some q(x), meaning (x - a) is a factor of p(x)

**Multiple Evaluation Points and Chinese Remainder Theorem**

The concept of evaluation homomorphism extends to multiple points through the Chinese Remainder Theorem for polynomials.

If $a_1, a_2, ..., a_n$ are distinct elements in F, then the combined evaluation homomorphism:

$\varphi: F[x] \to F \times F \times ... \times F$ (n times) $\varphi(p(x)) = (p(a_1), p(a_2), ..., p(a_n))$

has the kernel: $\ker(\varphi) = ((x - a_1)(x - a_2)...(x - a_n))$

By the Chinese Remainder Theorem: $F[x]/((x - a_1)(x - a_2)...(x - a_n)) \cong F[x]/(x - a_1) \times F[x]/(x - a_2) \times ... \times F[x]/(x - a_n) \cong F^n$

This isomorphism allows us to solve systems of polynomial congruences.

**Lagrange Interpolation**

Lagrange interpolation uses the evaluation homomorphism concept to construct a polynomial that passes through a given set of points.

Given distinct points $a_1, a_2, ..., a_n \in F$ and corresponding values $b_1, b_2, ..., b_n \in F$, the Lagrange interpolation polynomial is:

$p(x) = \Sigma\, b_j\, L_j(x)$

where $L_j(x)$ are the Lagrange basis polynomials:

$L_j(x) = \Pi\, (x - a_k)/(a_j - a_k)\ k \neq j$

This polynomial satisfies $p(a_j) = b_j$ for all $j = 1, 2, ..., n$.

Notes

**Solved Problems**

**Problem 1**

Problem: Find the kernel of the evaluation homomorphism $\varphi_2$: $\mathbb{Q}[x] \rightarrow \mathbb{Q}$ where $\varphi_2(p(x)) = p(2)$.

Solution: The kernel of an evaluation homomorphism $\varphi_a$ consists of all polynomials p(x) such that p(a) = 0. In this case, a = 2, so: $\ker(\varphi_2) = \{p(x) \in \mathbb{Q}[x] \mid p(2) = 0\}$

By the theory of evaluation homomorphisms, we know that: $\ker(\varphi_2) = (x - 2)$

This means the kernel is the set of all polynomials that are divisible by (x - 2), which can be written as: $\{q(x)(x - 2) \mid q(x) \in \mathbb{Q}[x]\}$

Therefore, $\ker(\varphi_2) = (x - 2)$.

**Problem 2**

Problem: Use the Remainder Theorem to find the remainder when $p(x) = x^3 - 2x^2 + 4x - 7$ is divided by (x - 3).

Solution: According to the Remainder Theorem, when a polynomial p(x) is divided by (x - a), the remainder is equal to p(a).

In this case, we need to find p(3): $p(3) = 3^3 - 2(3)^2 + 4(3) - 7 = 27 - 2(9) + 12 - 7 = 27 - 18 + 12 - 7 = 14$

Therefore, the remainder when $p(x) = x^3 - 2x^2 + 4x - 7$ is divided by (x - 3) is 14.

**Problem 3**

Problem: Determine whether (x - 2) is a factor of $p(x) = x^4 - 5x^3 + 2x^2 + 8x - 16$.

Solution: According to the Factor Theorem, (x - a) is a factor of p(x) if and only if p(a) = 0.

So to determine if (x - 2) is a factor of p(x), we need to check if p(2) = 0.

$p(2) = 2^4 - 5(2)^3 + 2(2)^2 + 8(2) - 16 = 16 - 5(8) + 2(4) + 16 - 16 = 16 - 40 + 8 + 16 - 16 = -16$

Since $p(2) = -16 \neq 0$, $(x - 2)$ is not a factor of $p(x)$.

**Problem 4**

Problem: Use the Chinese Remainder Theorem to find a polynomial $p(x) \in \mathbb{Q}[x]$ of degree less than 3 such that:

- $p(1) = 2$
- $p(2) = -1$
- $p(3) = 4$

Solution: We'll use Lagrange interpolation to construct the polynomial. For each point, we define:

$L_1(x) = ((x-2)(x-3))/((1-2)(1-3)) = ((x-2)(x-3))/(-1)(-2) = (x-2)(x-3)/2$

$L_2(x) = ((x-1)(x-3))/((2-1)(2-3)) = ((x-1)(x-3))/(1)(-1) = -(x-1)(x-3)$

$L_3(x) = ((x-1)(x-2))/((3-1)(3-2)) = ((x-1)(x-2))/(2)(1) = (x-1)(x-2)/2$

Now, our polynomial is: $p(x) = 2L_1(x) + (-1)L_2(x) + 4L_3(x) = 2((x-2)(x-3)/2) + (-1)(-(x-1)(x-3)) + 4((x-1)(x-2)/2) = (x-2)(x-3) + (x-1)(x-3) + 2(x-1)(x-2)$

Let's expand: $(x-2)(x-3) = x^2 - 5x + 6$ $(x-1)(x-3) = x^2 - 4x + 3$ $2(x-1)(x-2) = 2(x^2 - 3x + 2) = 2x^2 - 6x + 4$

$p(x) = (x^2 - 5x + 6) + (x^2 - 4x + 3) + (2x^2 - 6x + 4) = 4x^2 - 15x + 13$

To verify: $p(1) = 4(1)^2 - 15(1) + 13 = 4 - 15 + 13 = 2$ ✓ $p(2) = 4(2)^2 - 15(2) + 13 = 16 - 30 + 13 = -1$ ✓ $p(3) = 4(3)^2 - 15(3) + 13 = 36 - 45 + 13 = 4$ ✓

Therefore, $p(x) = 4x^2 - 15x + 13$ is our solution.

**Problem 5**

Notes

Problem: Determine the quotient and remainder when $p(x) = x^4 + 2x^3 - 3x^2 + x - 5$ is divided by $(x - 2)$.

Solution: We can use the evaluation homomorphism and the Division Algorithm to solve this.

By the Remainder Theorem, the remainder when $p(x)$ is divided by $(x - 2)$ is $p(2)$.

$p(2) = 2^4 + 2(2)^3 - 3(2)^2 + 2 - 5 = 16 + 2(8) - 3(4) + 2 - 5 = 16 + 16 - 12 + 2 - 5 = 17$

So the remainder is 17.

To find the quotient $q(x)$, we use the Division Algorithm: $p(x) = q(x)(x - 2) + 17$

We can use synthetic division or polynomial long division:

Using synthetic division with divisor $(x - 2)$: 2 | 1 2 -3 1 -5 | 2 8 10 22 ---------- 1 4 5 11 17

The quotient is the coefficients above the line, excluding the remainder: $q(x) = x^3 + 4x^2 + 5x + 11$

To verify: $(x^3 + 4x^2 + 5x + 11)(x - 2) + 17 = x^4 - 2x^3 + 4x^3 - 8x^2 + 5x^2 - 10x + 11x - 22 + 17 = x^4 + 2x^3 - 3x^2 + x - 5$ ✓

Therefore, when $p(x) = x^4 + 2x^3 - 3x^2 + x - 5$ is divided by $(x - 2)$:

- Quotient: $q(x) = x^3 + 4x^2 + 5x + 11$
- Remainder: 17

**Unsolved Problems**

**Problem 1**

Find the kernel of the evaluation homomorphism $\varphi_{-1}$: $\mathbb{R}[x] \to \mathbb{R}$ where $\varphi_{-1}(p(x)) = p(-1)$.

**Problem 2**

Use the Remainder Theorem to find the remainder when $p(x) = 2x^5 - 3x^3 + 4x - 7$ is divided by $(x + 2)$.

**Problem 3**

Use the Factor Theorem to determine all values of k for which $(x - 3)$ is a factor of $p(x) = x^3 - kx^2 + 4x - 12$.

**Problem 4**

Find a polynomial $p(x) \in \mathbb{Q}[x]$ of degree less than 4 such that:

- $p(0) = 1$
- $p(1) = -2$
- $p(2) = 0$
- $p(3) = 4$

**Problem 5**

Let $\varphi: \mathbb{Z}_5[x] \to \mathbb{Z}_5 \times \mathbb{Z}_5$ be the evaluation homomorphism defined by $\varphi(p(x)) = (p(2), p(3))$. Find a polynomial $p(x)$ of degree less than 2 such that $\varphi(p(x)) = (4, 1)$.

### 2.3.3 Factorization of Polynomials over a Field

Polynomial factorization is a central topic in algebra, with applications ranging from solving polynomial equations to cryptography. This section explores the theory and techniques of factoring polynomials over fields.

**Irreducible Polynomials**

A polynomial $p(x) \in F[x]$ of degree at least 1 is called irreducible over F if it cannot be expressed as a product of two polynomials in F[x], each of degree at least 1.

Properties of Irreducible Polynomials

1. Prime Elements: Irreducible polynomials are the "prime elements" of the polynomial ring F[x].

2. Degree 1 Polynomials: Every polynomial of degree 1 is irreducible.
3. Field Extensions: If p(x) is irreducible over F, then F[x]/(p(x)) is a field extension of F.
4. Unique Factorization: Every polynomial in F[x] can be factored uniquely (up to units) as a product of irreducible polynomials.

**Unique Factorization Theorem**

The Fundamental Theorem of Algebra for polynomials states:

Theorem: Every non-constant polynomial $p(x) \in F[x]$ can be factored uniquely as:

$$p(x) = a \cdot p_1(x)^{e_1} \cdot p_2(x)^{e_2} \cdot ... \cdot p_n(x)^{e_n}$$

where $a \in F$ is a non-zero constant, each $p_i(x)$ is a monic irreducible polynomial over F, and each $e_i$ is a positive integer. This factorization is unique up to the order of the factors.

**Techniques for Factorization**

**1. Rational Root Theorem**

For a polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ with integer coefficients, if p/q is a rational root (with gcd(p,q) = 1), then:

- p divides $a_0$
- q divides $a_n$

This helps identify potential rational roots for testing.

**2. Eisenstein's Criterion**

Theorem: Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{Z}[x]$. If there exists a prime number p such that:

- p divides all coefficients except $a_n$

- $p^2$ does not divide $a_0$
- p does not divide $a_n$

Then p(x) is irreducible over $\mathbb{Q}$.

**3. Gauss's Lemma**

Lemma: A primitive polynomial in $\mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$.

This allows testing irreducibility over $\mathbb{Q}$ by examining factorizations over $\mathbb{Z}$.

**4. Reducibility Testing over Finite Fields**

For polynomials over finite fields, we can test all possible factorizations up to a certain degree, as there are only finitely many polynomials of a given degree.

Special Cases: Factorization over Specific Fields

Factorization over $\mathbb{R}$ (Real Numbers)

Over $\mathbb{R}$, irreducible polynomials are either of degree 1 or 2:

- Linear factors: $(x - a)$ where $a \in \mathbb{R}$
- Quadratic factors: $(x^2 + bx + c)$ where $b^2 - 4c < 0$

Factorization over $\mathbb{C}$ (Complex Numbers)

Over $\mathbb{C}$, every non-constant polynomial factors completely into linear factors by the Fundamental Theorem of Algebra:

$p(x) = a(x - z_1)(x - z_2)...(x - z_n)$

where $a \in \mathbb{C}$ is a constant and $z_1, z_2, ..., z_n \in \mathbb{C}$ are the roots of p(x).

Factorization over $\mathbb{Q}$ (Rational Numbers)

Over $\mathbb{Q}$, irreducible polynomials can have any degree. Some common techniques for factoring over $\mathbb{Q}$ include:

- The Rational Root Theorem

- Eisenstein's Criterion
- Gauss's Lemma
- Descartes' Rule of Signs (for information about the number of positive and negative roots)

Factorization over Finite Fields

For a finite field $F_q$ with q elements:

- Every irreducible polynomial of degree n over $F_q$ divides $x^{(qn)} - x$
- The number of monic irreducible polynomials of degree n over $F_q$ can be calculated using Möbius inversion formula

Cyclotomic Polynomials

The cyclotomic polynomial $\Phi_n(x)$ is the monic polynomial whose roots are the primitive nth roots of unity.

Properties:

- $\Phi_n(x)$ is irreducible over $\mathbb{Q}$
- $\Phi_n(x)$ has degree $\varphi(n)$, where $\varphi$ is Euler's totient function
- $x^n - 1 = \prod \Phi_p(x)$, where d ranges over all divisors of n

Applications of Polynomial Factorization

1. Solving Polynomial Equations: Factoring a polynomial allows us to find its roots.
2. Field Extensions: Irreducible polynomials are used to construct field extensions.
3. Error-Correcting Codes: Polynomial factorization plays a crucial role in coding theory.
4. Cryptography: Many cryptographic systems rely on the difficulty of factoring certain polynomials over finite fields.

5. Computer Algebra Systems: Efficient factorization algorithms are essential components of computer algebra systems.

**Solved Problems**

**Problem 1**

Problem: Determine whether the polynomial $p(x) = x^3 - 3x + 1$ is irreducible over $\mathbb{Q}$.

Solution: To determine if $p(x) = x^3 - 3x + 1$ is irreducible over $\mathbb{Q}$, we can apply the Rational Root Theorem.

The possible rational roots of p(x) are the divisors of the constant term (1) divided by the divisors of the leading coefficient (1). Possible rational roots: ±1

Let's check these candidates: $p(1) = 1^3 - 3(1) + 1 = 1 - 3 + 1 = -1 \neq 0$ $p(-1) = (-1)^3 - 3(-1) + 1 = -1 + 3 + 1 = 3 \neq 0$

Since p(x) has no rational roots, it has no linear factors in $\mathbb{Q}[x]$.

The only other possibility for reducibility would be a factorization into a linear and a quadratic factor, but since there are no linear factors, this is impossible.

Therefore, $p(x) = x^3 - 3x + 1$ is irreducible over $\mathbb{Q}$.

**Problem 2**

Problem: Factor the polynomial $p(x) = x^4 - 5x^2 + 4$ over $\mathbb{R}$.

Solution: Let's try to recognize this as a quadratic in $x^2$. Let's set $u = x^2$ and rewrite: $p(x) = x^4 - 5x^2 + 4 = u^2 - 5u + 4$

Now we can factor this quadratic: $u^2 - 5u + 4 = (u - 4)(u - 1) = (x^2 - 4)(x^2 - 1)$

We can factor these further: $x^2 - 4 = (x - 2)(x + 2)$ $x^2 - 1 = (x - 1)(x + 1)$

Therefore: $p(x) = x^4 - 5x^2 + 4 = (x - 2)(x + 2)(x - 1)(x + 1)$

Notes

To verify: $(x - 2)(x + 2)(x - 1)(x + 1) = (x^2 - 4)(x^2 - 1) = x^4 - x^2 - 4x^2 + 4 = x^4 - 5x^2 + 4$ ✓

So the factorization of $p(x) = x^4 - 5x^2 + 4$ over $\mathbb{R}$ is $(x - 2)(x + 2)(x - 1)(x + 1)$.

**Problem 3**

Problem: Use Eisenstein's Criterion to prove that $p(x) = 2x^3 + 6x^2 + 3x + 9$ is irreducible over $\mathbb{Q}$.

Solution: To apply Eisenstein's Criterion, we need to find a prime p such that:

1. p divides all coefficients except the leading coefficient
2. $p^2$ does not divide the constant term
3. p does not divide the leading coefficient

Let's examine the coefficients of $p(x) = 2x^3 + 6x^2 + 3x + 9$:

- Leading coefficient: 2
- $x^2$ coefficient: 6
- x coefficient: 3
- Constant term: 9

Let's try p = 3:

- 3 divides 6, 3, and 9
- 3 does not divide 2 (the leading coefficient)
- $3^2 = 9$ divides 9 (the constant term)

Since $3^2$ divides the constant term, Eisenstein's Criterion does not apply with p = 3.

Let's transform the polynomial to make Eisenstein's Criterion applicable. Let's substitute $x = y + 1$:

$p(y + 1) = 2(y + 1)^3 + 6(y + 1)^2 + 3(y + 1) + 9$ Notes

Expanding: $p(y + 1) = 2(y^3 + 3y^2 + 3y + 1) + 6(y^2 + 2y + 1) + 3(y + 1) + 9 = 2y^3 + 6y^2 + 6y + 2 + 6y^2 + 12y + 6 + 3y + 3 + 9 = 2y^3 + 12y^2 + 21y + 20$

Now let's check if Eisenstein's Criterion applies with the prime $p = 3$:

- 3 divides 12, 21, and 20 (all coefficients except the leading coefficient)
- 3 does not divide 2 (the leading coefficient)
- $3^2 = 9$ does not divide 20 (the constant term)

All conditions of Eisenstein's Criterion are satisfied for the transformed polynomial. Since irreducibility is preserved under the substitution $x = y + 1$, we conclude that the original polynomial $p(x) = 2x^3 + 6x^2 + 3x + 9$ is irreducible over $\mathbb{Q}$.

**Problem 4**

Problem: Factor the polynomial $p(x) = x^6 - 1$ over $\mathbb{Q}$.

Solution: We can use cyclotomic polynomials to factor $x^n - 1$. $x^n - 1 = \prod \Phi_p(x)$, where d ranges over all divisors of n.

For $n = 6$: $x^6 - 1 = \Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_3(x) \cdot \Phi_6(x)$

Now we need to compute these cyclotomic polynomials:

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = x + 1$
- $\Phi_3(x) = x^2 + x + 1$
- $\Phi_6(x) = x^2 - x + 1$

Therefore: $p(x) = x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$

Notes

To verify, we can multiply out: $(x - 1)(x + 1) = x^2 - 1$ $(x^2 - 1)(x^2 + x + 1) = x^4 + x^3 + x^2 - x^2 - x - 1 = x^4 + x^3 - x - 1$ $(x^4 + x^3 - x - 1)(x^2 - x + 1) = x^6 - x^5 + x^4 + x^5 - x^4 + x^3 - x^3 + x^2 - x - x^2 + x + 1 = x^6 - 1$ ✓

Therefore, the factorization of $p(x) = x^6 - 1$ over $\mathbb{Q}$ is: $(x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$

**Problem 5**

Problem: Factor the polynomial $p(x) = x^4 + 4$ over $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

Solution: Factorization over $\mathbb{Q}$: Let's check if $p(x) = x^4 + 4$ is irreducible over $\mathbb{Q}$.

By the Rational Root Theorem, any rational root would need to be a divisor of 4, so the candidates are: ±1, ±2, ±4.

Testing these values: $p(1) = 1^4 + 4 = 1 + 4 = 5 \neq 0$ $p(-1) = (-1)^4 + 4 = 1 + 4 = 5 \neq 0$ $p(2) = 2^4 + 4 = 16 + 4 = 20 \neq 0$ $p(-2) = (-2)^4 + 4 = 16 + 4 = 20 \neq 0$ $p(4) = 4^4 + 4 = 256 + 4 = 260 \neq 0$ $p(-4) = (-4)^4 + 4 = 256 + 4 = 260 \neq 0$

So $p(x)$ has no rational roots.

Let's check if it can be factored as a product of two quadratics: If $x^4 + 4 = (x^2 + ax + b)(x^2 + cx + d)$, then:

- $bd = 4$
- $ad + bc = 0$
- $b + d + ac = 0$
- $a + c = 0$

From the last equation, $c = -a$. Substituting into the third equation: $b + d - a^2 = 0$

Since $b \cdot d = 4$, there are limited options for b and d as integers or rational numbers: (b,d) = (1,4), (2,2), (4,1), (-1,-4), (-2,-2), (-4,-1)

Let's try (b,d) = (2,2): $b + d - a^2 = 2 + 2 - a^2 = 4 - a^2 = 0$ This gives $a^2 = 4$, so $a = \pm 2$

Notes

If $a = 2$, then $c = -2$, and we can check: $(x^2 + 2x + 2)(x^2 - 2x + 2) = x^4 - 4x^2 + 4 + 2x^3 - 4x^2 + 4x - 2x^3 + 4x^2 - 4x = x^4 - 4x^2 + 4 + 0 + 0 = x^4 + 4 \neq x^4 + 4$

So this factorization doesn't work. After trying other combinations, we can conclude that $x^4 + 4$ is irreducible over $\mathbb{Q}$.

Factorization over $\mathbb{R}$: Over $\mathbb{R}$, we can express $x^4 + 4$ as: $x^4 + 4 = x^4 + 4 \cdot 1^2 = x^4 + 4 \cdot 2^2/2^2 = (x^4 + 4 \cdot 2^2)/2^2 \cdot 2^2 = ((x^2)^2 + (2 \cdot \sqrt{2})^2)/2^2 \cdot 2^2 = (x^2 + 2\sqrt{2}i)(x^2 - 2\sqrt{2}i)$

So over $\mathbb{R}$: $x^4 + 4 = (x^2 + 2\sqrt{2}i)(x^2 - 2\sqrt{2}i)$

Factorization over $\mathbb{C}$: To factor further over $\mathbb{C}$, we can factor each of the quadratics: $x^2 + 2\sqrt{2}i = (x + \sqrt{2} \cdot e^{(\pi i/4)})(x + \sqrt{2} \cdot e^{(3\pi i/4)}) = (x + \sqrt{2} \cdot (1+i)/\sqrt{2})(x + \sqrt{2} \cdot (-1+i)/\sqrt{2}) = (x + (1+i))(x + (-1+i))$ $x^2 - 2\sqrt{2}i = (x + \sqrt{2} \cdot e^{(5\pi i/4)})(x + \sqrt{2} \cdot e^{(7\pi i/4)}) = (x + \sqrt{2} \cdot (-1-i)/\sqrt{2})(x + \sqrt{2} \cdot (1-i)/\sqrt{2}) = (x + (-1-i))(x + (1-i))$

Simplifying: $x^4 + 4 = (x + (1+i))(x + (-1+i))(x + (-1-i))(x + (1-i))$

Therefore:

- Over $\mathbb{Q}$: $x^4 + 4$ is irreducible
- Over $\mathbb{R}$: $x^4 + 4 = (x^2 + 2\sqrt{2}i)(x^2 - 2\sqrt{2}i)$
- Over $\mathbb{C}$: $x^4 + 4 = (x + (1+i))(x + (-1+i))(x + (-1-i))(x + (1-i))$

**Unsolved Problems**

**Problem 1**

Determine whether the polynomial $p(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$.

**Problem 2**

Factor the polynomial $p(x) = x^4 - 16$ over $\mathbb{R}$ and $\mathbb{C}$.

Notes

**Problem 3**

Use Eisenstein's Criterion to prove that the polynomial $p(x) = x^3 + 15x^2 + 5x + 10$ is irreduc

**Multiple Choice Questions (MCQs)**

1. **Which of the following is true about p-groups?**
   a) They always contain a normal subgroup.
   b) They have order divisible by p but not necessarily a power of p.
   c) They are always abelian.
   d) None of the above.

2. **The class equation of a finite group helps in:**
   a) Finding normal subgroups
   b) Counting the number of conjugacy classes
   c) Determining the number of elements in a group
   d) None of the above

3. **The Sylow theorems are particularly useful in studying:**
   a) Infinite groups
   b) Finite simple groups
   c) Abelian groups
   d) None of the above

4. **The set of all polynomials with real coefficients forms:**
   a) A group under addition
   b) A ring under addition and multiplication
   c) A field under addition and multiplication
   d) None of the above

5. **The evaluation homomorphism maps a polynomial to:**
   a) Its derivative
   b) Its integral
   c) A specific value by substituting an element from the field
   d) None of the above

6. **Which of the following is true about polynomial rings?**
   a) Every polynomial has a unique factorization over any ring.
   b) The degree of the product of two polynomials is the sum of their degrees.
   c) Polynomial rings are always commutative.
   d) None of the above.

7. **A polynomial f(x) over a field F is irreducible if:**
   a) It has a root in F.
   b) It cannot be factored into nontrivial polynomials in F[x].
   c) It has complex coefficients.
   d) It is of degree 1.

8. **The fundamental theorem of algebra states that every polynomial of degree n over the complex numbers has:**
   a) At most n roots
   b) At least one real root
   c) Exactly n roots (counting multiplicities)
   d) None of the above

9. **The ring of polynomials over a field is:**
   a) Always a division ring
   b) A commutative ring with unity
   c) A non-commutative ring
   d) None of the above

10. **A field F is said to be algebraically closed if:**
    a) Every polynomial over F has a root in F.
    b) It contains all real numbers.
    c) It has finite elements.
    d) It has an identity element.

**Short Answer Questions**

1. State and explain the class equation of a finite group.

2. How do Sylow's theorems help in studying the structure of finite groups?
3. Define a p-group and give an example.
4. What is the significance of polynomial rings in algebra?
5. Define the evaluation homomorphism and provide an example.
6. What is an irreducible polynomial? Provide an example over the field of real numbers.
7. How do you factorize polynomials over a field? Give an example.
8. Explain why every field has a polynomial ring.
9. What is the role of Sylow's theorems in classifying finite simple groups?
10. Give an example of a ring that is not a field and explain why.

**Long Answer Questions**

1. Discuss in detail the class equation and its significance in group theory.
2. How do Sylow's theorems provide insight into the structure of finite groups? Give detailed examples.
3. Explain the concept of polynomial rings and their applications in algebra.
4. Define irreducible polynomials and describe their importance in field theory.
5. Prove that the set of all polynomials over a field forms a commutative ring.

6. Explain the factorization of polynomials over a field and provide examples.
7. How does the fundamental theorem of algebra relate to polynomial factorization?
8. Discuss applications of polynomial rings in modern algebra and number theory.
9. Describe how the evaluation homomorphism works and illustrate with examples.
10. What are the differences between a field and a ring? Give examples to illustrate their properties.

Answer Key MCQ :

1. a

2. b

3. b

4. b

5. c

6. b

7. b

8. c

9. b

10. a

# MODULE 3

## UNIT 3.1

## FIELD THEORY

**Objectives**

- Understand the concept of extension fields.
- Differentiate between algebraic and transcendental elements.
- Learn about irreducible polynomials over a field.
- Explore simple extensions and algebraic extensions.
- Analyze finite extensions and their structure.
- Study the construction and properties of finite fields.

### 3.1.1: Introduction to Field Theory

Field theory is a branch of abstract algebra that studies the properties and structures of fields, which are sets equipped with operations of addition, subtraction, multiplication, and division. Fields are fundamental algebraic structures that appear throughout mathematics, particularly in areas like number theory, algebraic geometry, and cryptography.

A field is a set F together with two binary operations, addition (+) and multiplication (·), that satisfy the following axioms:

1. **Closure under addition**: For all a, b in F, a + b is in F.
2. **Associativity of addition**: For all a, b, c in F, (a + b) + c = a + (b + c).
3. **Commutativity of addition**: For all a, b in F, a + b = b + a.
4. **Additive identity**: There exists an element 0 in F such that a + 0 = a for all a in F.

5. **Additive inverse**: For each a in F, there exists an element -a in F such that a + (-a) = 0.
6. **Closure under multiplication**: For all a, b in F, a · b is in F.
7. **Associativity of multiplication**: For all a, b, c in F, (a · b) · c = a · (b · c).
8. **Commutativity of multiplication**: For all a, b in F, a · b = b · a.
9. **Multiplicative identity**: There exists an element 1 in F, with 1 ≠ 0, such that a · 1 = a for all a in F.
10. **Multiplicative inverse**: For each a ≠ 0 in F, there exists an element $a^{(-1)}$ in F such that a · $a^{(-1)}$ = 1.
11. **Distributivity**: For all a, b, c in F, a · (b + c) = (a · b) + (a · c).

The most familiar examples of fields include:

- The rational numbers Q
- The real numbers R
- The complex numbers C
- Finite fields such as Z_p (integers modulo p, where p is prime)

Fields provide a setting in which equations can be solved by the basic operations of arithmetic. For example, in a field, we can always divide by non-zero elements, which is not possible in other algebraic structures like rings.

Field theory investigates the relationships between different fields, particularly how larger fields can be constructed from smaller ones. This leads to the concept of field extensions, which we'll explore in the next section.

### 3.1.2 Extension Fields and Their Importance

Notes

An extension field is a larger field that contains a smaller field within it. If F is a field and E is a field containing F, then E is called an extension field of F, and we write $F \subseteq E$ or E/F.

Formally, an extension field E of a field F is a field E containing F as a subfield. This means that:

1. F is a subset of E
2. The operations of F coincide with those of E when restricted to elements of F

For example:

- The field of real numbers R is an extension of the field of rational numbers Q
- The field of complex numbers C is an extension of the field of real numbers R
- For a prime p, the field $F_{pn}$ is an extension of $F_p$

**Importance of Extension Fields**

Extension fields are fundamental in algebra for several reasons:

1. **Solving Equations**: Extension fields allow us to solve equations that have no solutions in the original field. For example, $x^2 = 2$ has no solution in Q, but in the extension field $Q(\sqrt{2})$, we can find solutions.
2. **Algebraic Closure**: Every field F has an algebraic closure, which is an extension field in which every polynomial with coefficients in F has a root.
3. **Field Theory Applications**: Extension fields are essential in Galois theory, which connects field theory with group theory to address questions about the solvability of polynomial equations.

4. **Algebraic Number Theory**: Extension fields of the rational numbers are fundamental in studying algebraic number theory.
5. **Finite Fields**: Extensions of finite fields are crucial in coding theory, cryptography, and computer science.

**Degree of an Extension**

If E is an extension of F, then E can be viewed as a vector space over F. The dimension of this vector space is called the degree of the extension, denoted by [E:F].

If [E:F] is finite, E is called a finite extension of F. Otherwise, it's an infinite extension.

For example:

- [R:Q] is infinite
- [C:R] = 2 (because C is a 2-dimensional vector space over R with basis {1, i})
- [Q(√2):Q] = 2 (with basis {1, √2})

**The Tower Law**

If F ⊆ K ⊆ E are fields, then [E:F] = [E:K][K:F].

This important property allows us to break down complex extensions into simpler ones, making them easier to analyze.

### 3.1.3 Algebraic vs. Transcendental Elements

When studying field extensions, an important distinction is made between algebraic and transcendental elements.

**Algebraic Elements**

Let E be an extension field of F, and let α be an element of E. We say α is **algebraic** over F if there exists a non-zero polynomial p(x) with coefficients in F such that p(α) = 0.

Notes

In other words, an element is algebraic if it is a root of some polynomial with coefficients in the base field.

**Examples of Algebraic Elements:**

1. $\sqrt{2}$ is algebraic over Q because it satisfies the polynomial $x^2 - 2 = 0$.
2. i (the imaginary unit) is algebraic over R because it satisfies $x^2 + 1 = 0$.
3. Every element of a finite field extension is algebraic over the base field.

**Minimal Polynomial**

For any algebraic element α over F, there exists a unique monic irreducible polynomial $m_\alpha(x)$ in F[x] such that $m_\alpha(\alpha) = 0$. This polynomial is called the **minimal polynomial** of α over F.

The minimal polynomial has the following properties:

- It is irreducible over F
- It is monic (the leading coefficient is 1)
- Any polynomial p(x) in F[x] such that $p(\alpha) = 0$ is divisible by $m_\alpha(x)$

The degree of the minimal polynomial of α is called the **degree** of α over F.

**Transcendental Elements**

An element α in E is **transcendental** over F if it is not algebraic over F. This means that α does not satisfy any non-zero polynomial equation with coefficients in F.

**Examples of Transcendental Elements:**

1. π (pi) is transcendental over Q (proved by Lindemann in 1882)

2. e (Euler's number) is transcendental over Q (proved by Hermite in 1873)

3. In general, "most" real numbers are transcendental over Q

**Algebraic and Transcendental Extensions**

An extension E/F is called **algebraic** if every element of E is algebraic over F. Otherwise, it is **transcendental**.

For an algebraic element α over F, the field F(α) (the smallest field containing both F and α) is: $F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{(n-1)}\alpha^{(n-1)} | a_i \in F\}$

where n is the degree of the minimal polynomial of α over F.

For a transcendental element τ over F, the field F(τ) is isomorphic to the field of rational functions F(x).

**Importance of the Distinction**

The distinction between algebraic and transcendental elements is crucial in field theory because:

1. Algebraic extensions are well-structured and can be studied using tools like minimal polynomials and Galois theory.

2. Transcendental extensions are less structured but are important in areas like transcendental number theory.

3. The classification of numbers as algebraic or transcendental is a fundamental problem in number theory.

4. Many important mathematical constants like π and e are transcendental, which has significant implications in various areas of mathematics.

## UNIT 3.2

### 3.2.1: Irreducible Polynomials over a Field

Irreducible polynomials play a crucial role in field theory, particularly in constructing field extensions. A polynomial is irreducible over a field if it cannot be factored into polynomials of lower degree over that field.

**Definition and Properties**

A non-constant polynomial p(x) in F[x] is **irreducible** over F if p(x) cannot be expressed as a product of two non-constant polynomials in F[x].

Key properties of irreducible polynomials:

1. Linear polynomials (degree 1) are always irreducible.
2. If p(x) is irreducible over F and α is a root of p(x) in some extension E, then p(x) is the minimal polynomial of α over F.
3. If p(x) is irreducible over F of degree n, and α is a root of p(x), then $[F(\alpha):F] = n$.
4. Irreducible polynomials play the role of "prime elements" in the ring F[x] of polynomials.

**Methods for Determining Irreducibility**

Several techniques can be used to determine whether a polynomial is irreducible:

1. **Eisenstein's Criterion**: Let $p(x) = a_n x^n + a_{(n-1)} x^{(n-1)} + ... + a_1 x + a_0$ be a polynomial with integer coefficients. If there exists a prime number p such that:
    - p divides $a_0, a_1, ..., a_{(n-1)}$
    - p does not divide $a_n$
    - $p^2$ does not divide $a_0$

Then p(x) is irreducible over Q.



2. **Reduction modulo p**: If the reduction of a polynomial f(x) with integer coefficients modulo a prime p yields an irreducible polynomial in $Z_p[x]$, then f(x) is irreducible over Q.

3. **Gauss's Lemma**: A polynomial with integer coefficients is irreducible over Q if and only if it is irreducible over Z and its content (the greatest common divisor of its coefficients) is 1.

4. **Rational Root Theorem**: If p(x)/q(x) is a rational root of a polynomial f(x) with integer coefficients (where p and q are coprime integers), then p divides the constant term of f(x) and q divides the leading coefficient of f(x).

**Examples of Irreducible Polynomials:**

1. $x^2 - 2$ is irreducible over Q (no rational root)
2. $x^2 + 1$ is irreducible over R (no real root)
3. $x^2 + 1$ is reducible over C as $(x + i)(x - i)$
4. $x^p - x - 1$ is irreducible over Q for any prime p
5. Cyclotomic polynomials $\Phi_n(x)$ are irreducible over Q

**Constructing Field Extensions Using Irreducible Polynomials**

One of the most important applications of irreducible polynomials is in constructing field extensions:

If p(x) is an irreducible polynomial of degree n over a field F, then the quotient ring F[x]/(p(x)) is a field extension of F of degree n.

This construction gives us a concrete way to build extension fields. For example:

- $Q[x]/(x^2 - 2)$ is isomorphic to $Q(\sqrt{2})$
- $R[x]/(x^2 + 1)$ is isomorphic to C

Notes

- $F_p[x]/(p(x))$ where p(x) is irreducible of degree n gives us a field with p^n elements

**Field Splitting**

An irreducible polynomial p(x) over F may become reducible in an extension field E. If E contains all the roots of p(x), we say that E is a **splitting field** of p(x) over F.

For example:

- $Q(\sqrt{2})$ is the splitting field of $x^2 - 2$ over Q
- C is the splitting field of $x^2 + 1$ over R

The concept of splitting fields is central to Galois theory, which studies the connection between field extensions and group theory.

**Solved Problems**

**Problem 1: Verify that $Q(\sqrt{2})$ is a field and determine its elements.**

**Solution:**

To verify that $Q(\sqrt{2})$ is a field, we need to ensure it satisfies all field axioms.

$Q(\sqrt{2})$ consists of all elements of the form $a + b\sqrt{2}$, where a, b are rational numbers.

First, let's verify that this set is closed under the field operations:

For addition: $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$, which is again of the form $p + q\sqrt{2}$ with $p, q \in Q$.

For multiplication: $(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + bd(\sqrt{2})^2 = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2}$, which is againof the form $p + q\sqrt{2}$ with $p, q \in Q$.

For additive inverse: The negative of $a + b\sqrt{2}$ is $-a - b\sqrt{2}$, which is in $Q(\sqrt{2})$.

For multiplicative inverse (where $a + b\sqrt{2} \neq 0$): $(a + b\sqrt{2})^{(-1)} = (a - b\sqrt{2})/(a^2 - 2b^2)$

Note that $a^2 - 2b^2 \neq 0$ when $a + b\sqrt{2} \neq 0$. This fraction gives us: $(a - b\sqrt{2})/(a^2 - 2b^2) = a/(a^2 - 2b^2) - b\sqrt{2}/(a^2 - 2b^2)$

This is of the form $p + q\sqrt{2}$ with $p, q \in Q$, so the multiplicative inverse exists in $Q(\sqrt{2})$.

The remaining field axioms (associativity, commutativity, distributivity, and existence of identities) are inherited from the properties of real numbers.

Therefore, $Q(\sqrt{2})$ is indeed a field.

The elements of $Q(\sqrt{2})$ are all numbers of the form $a + b\sqrt{2}$, where a and b are rational numbers. This creates an infinite field with a basis $\{1, \sqrt{2}\}$ over Q. This field is a simple algebraic extension of Q, and it has degree 2 over Q since $[Q(\sqrt{2}):Q] = 2$.

**Problem 2: Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over Q.**

**Solution:**

We need to find a polynomial p(x) with rational coefficients such that $p(\sqrt{2} + \sqrt{3}) = 0$, and p(x) is irreducible over Q.

Let $\alpha = \sqrt{2} + \sqrt{3}$. We'll try to find a polynomial by considering the powers of $\alpha$.

$\alpha = \sqrt{2} + \sqrt{3}$ $\alpha^2 = (\sqrt{2} + \sqrt{3})^2 = 2 + 3 + 2\sqrt{2}\sqrt{3} = 5 + 2\sqrt{6}$

Let's compute $\alpha^3$: $\alpha^3 = \alpha \cdot \alpha\text{^}2 = (\sqrt{2} + \sqrt{3})(5 + 2\sqrt{6}) = 5\sqrt{2} + 5\sqrt{3} + 2\sqrt{6}\sqrt{2} + 2\sqrt{6}\sqrt{3} = 5\sqrt{2} + 5\sqrt{3} + 2\sqrt{12} + 2\sqrt{18} = 5\sqrt{2} + 5\sqrt{3} + 4\sqrt{3} + 6\sqrt{2} = 11\sqrt{2} + 9\sqrt{3}$

Now let's compute $\alpha^4$: $\alpha^4 = \alpha^2 \cdot \alpha^2 = (5 + 2\sqrt{6})^2 = 25 + 20\sqrt{6} + 24 = 49 + 20\sqrt{6}$

Looking at these powers, we can see that $\alpha$ satisfies a 4th-degree polynomial. Let's try to construct it.

Notes

Let $p(x) = x^4 + ax^3 + bx^2 + cx + d$ be the minimal polynomial.

We need to find a, b, c, and d such that: $p(\alpha) = \alpha^4 + a\alpha^3 + b\alpha^2 + c\alpha + d = 0$

Substituting what we've calculated: $(49 + 20\sqrt{6}) + a(11\sqrt{2} + 9\sqrt{3}) + b(5 + 2\sqrt{6}) + c(\sqrt{2} + \sqrt{3}) + d = 0$

Collecting the terms: $49 + 20\sqrt{6} + 11a\sqrt{2} + 9a\sqrt{3} + 5b + 2b\sqrt{6} + c\sqrt{2} + c\sqrt{3} + d = 0$

For this equation to be true, the coefficients of each linearly independent term (1, √2, √3, √6) must be zero: 1: $49 + 5b + d = 0$ √2: $11a + c = 0$ √3: $9a + c = 0$ √6: $20 + 2b = 0$

From the last equation: $b = -10$ From the second and third equations: $11a + c = 9a + c$, so $2a = 0$, which means $a = 0$, and consequently $c = 0$ From the first equation with $a = 0$, $b = -10$, $c = 0$: $49 + 5(-10) + d = 0$, so $d = -49 + 50 = 1$

Therefore, the minimal polynomial is: $p(x) = x^4 - 10x^2 + 1$

We can verify this is irreducible over Q by checking that it has no rational roots (using the rational root theorem) and it cannot be factored as a product of two quadratics with rational coefficients.

The minimal polynomial of $\sqrt{2} + \sqrt{3}$ over Q is $x^4 - 10x^2 + 1$.

**Problem 3: Determine whether the polynomial $x^3 - 3x + 1$ is irreducible over Q.**

**Solution:**

To determine if $p(x) = x^3 - 3x + 1$ is irreducible over Q, we'll use several approaches:

First, by the Rational Root Theorem, if p(x) has a rational root p/q in lowest terms, then p divides the constant term (1) and q divides the leading coefficient (1). Therefore, the only possible rational roots are ±1.

Let's check: p(1) = 1 - 3 + 1 = -1 ≠ 0 p(-1) = -1 - 3(-1) + 1 = -1 + 3 + 1 = 3 ≠ 0

Notes

So p(x) has no rational roots. However, this doesn't immediately prove irreducibility because p(x) could potentially factor as a product of an irreducible quadratic and a linear term with irrational coefficients.

Since p(x) is a cubic polynomial, if it were reducible over Q, it would have to be a product of a linear factor and a quadratic factor, both with rational coefficients. Since we've established there are no rational roots, p(x) must be irreducible over Q.

Alternatively, we can use the Eisenstein criterion with a suitable transformation. Let's try substituting y = x + 1 to get: $p(y - 1) = (y - 1)^3 - 3(y - 1) + 1 = y^3 - 3y^2 + 3y - 1 - 3y + 3 + 1 = y^3 - 3y^2 + 0y + 3$

Applying the Eisenstein criterion with prime p = 3:

- 3 divides the constant term (3)
- 3 does not divide the leading coefficient (1)
- 3^2 = 9 does not divide the constant term (3)

Therefore, $y^3 - 3y^2 + 3$ is irreducible over Q by the Eisenstein criterion. Since this polynomial is obtained from our original polynomial through a change of variables, the original polynomial $x^3 - 3x + 1$ is also irreducible over Q.

**Problem 4: Show that the field extension Q(√2, √3)/Q has degree 4.**

**Solution:**

To find the degree of the extension Q(√2, √3)/Q, we can use the tower law: [Q(√2, √3):Q] = [Q(√2, √3):Q(√2)][Q(√2):Q]

We know that [Q(√2):Q] = 2 since √2 has minimal polynomial $x^2 - 2$ over Q.

Notes

Now we need to find $[Q(\sqrt{2}, \sqrt{3}):Q(\sqrt{2})]$.

Consider the minimal polynomial of $\sqrt{3}$ over $Q(\sqrt{2})$. Let's check if $\sqrt{3}$ satisfies a linear polynomial over $Q(\sqrt{2})$. That would happen if $\sqrt{3} \in Q(\sqrt{2})$, which means $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in Q$.

If $\sqrt{3} = a + b\sqrt{2}$, then by squaring both sides: $3 = a^2 + 2ab\sqrt{2} + 2b^2$

Since the left side is rational and $\sqrt{2}$ is irrational, we must have $ab = 0$. If $b = 0$, then $a^2 = 3$, which has no rational solution. If $a = 0$, then $2b^2 = 3$, which also has no rational solution.

Therefore, $\sqrt{3}$ is not in $Q(\sqrt{2})$, so its minimal polynomial over $Q(\sqrt{2})$ is at least quadratic.

The obvious candidate is $x^2 - 3$, and indeed this is a polynomial with coefficients in $Q(\sqrt{2})$ that has $\sqrt{3}$ as a root. Let's verify this is irreducible over $Q(\sqrt{2})$.

If $x^2 - 3$ were reducible over $Q(\sqrt{2})$, it would factor as $(x - \alpha)(x - \beta)$ where $\alpha, \beta \in Q(\sqrt{2})$. But the roots of $x^2 - 3$ are $\pm\sqrt{3}$, and we've just shown that $\sqrt{3} \notin Q(\sqrt{2})$. Therefore, $x^2 - 3$ is irreducible over $Q(\sqrt{2})$.

Since the minimal polynomial of $\sqrt{3}$ over $Q(\sqrt{2})$ has degree 2, we have $[Q(\sqrt{2}, \sqrt{3}):Q(\sqrt{2})] = 2$.

Now, applying the tower law: $[Q(\sqrt{2}, \sqrt{3}):Q] = [Q(\sqrt{2}, \sqrt{3}):Q(\sqrt{2})][Q(\sqrt{2}):Q] = 2 \times 2 = 4$

Therefore, the degree of the extension $Q(\sqrt{2}, \sqrt{3})/Q$ is 4.

This means that $Q(\sqrt{2}, \sqrt{3})$ is a 4-dimensional vector space over Q, with basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

**Problem 5: Determine if $Q(\sqrt{2})/Q$ is a normal extension.**

**Solution:**

A field extension E/F is normal if every irreducible polynomial p(x) in F[x] that has at least one root in E completely splits (factors into linear terms) in E[x].

In our case, we need to determine if Q(√2)/Q is a normal extension.

Notes

The minimal polynomial of √2 over Q is $f(x) = x^2 - 2$. This polynomial has roots √2 and -√2.

Let's check if both roots are in Q(√2):

- √2 is in Q(√2) by definition
- -√2 is also in Q(√2) since it's of the form a + b√2 where a = 0 and b = -1, which are both in Q

Since both roots of the minimal polynomial $x^2 - 2$ are in Q(√2), every irreducible polynomial over Q that has a root in Q(√2) splits completely in Q(√2).

In fact, any element of Q(√2) is of the form a + b√2 where a, b ∈ Q. Its minimal polynomial over Q will be either linear (if b = 0, so the element is already in Q) or quadratic (if b ≠ 0).

If the minimal polynomial is quadratic, it will be of the form (x - (a + b√2))(x - (a - b√2)), which splits completely in Q(√2).

Therefore, Q(√2)/Q is indeed a normal extension.

Another way to verify this is to note that Q(√2) is the splitting field of x^2 - 2 over Q, and splitting field extensions are always normal.

**Unsolved Problems**

Problem 1: Find a basis for the field extension Q(√2, √3, √5)/Q and determine its degree.

Problem 2: Prove that the polynomial $x^4 + 1$ is irreducible over Q but reducible over R.

Problem 3: Let F be a field and let p(x) be an irreducible polynomial in F[x]. Show that the field extension F[x]/(p(x)) is isomorphic to F(α), where α is a root of p(x) in some extension field of F.

Problem 4: Determine all elements α in the complex field C such that Q(α) = Q(i), where i is the imaginary unit.

Notes

Problem 5: Let $f(x) = x^3 - 2$ and let $\alpha$ be a root of f in some extension field. Determine the degree of the extension $Q(\alpha, \omega)/Q$, where $\omega$ is a primitive cube root of unity.

### 3.3.1: Simple Extensions and Their Properties

A simple extension is one of the most fundamental types of field extensions in abstract algebra. It occurs when we adjoin a single element to a field to create a larger field. This concept is essential for understanding how to build more complex field structures.

**Definition of a Simple Extension**

Let F be a field and α be an element not in F. A simple extension, denoted F(α), is the smallest field containing both F and the element α.

There are two main cases to consider:

1. Algebraic case: When α is algebraic over F
2. Transcendental case: When α is transcendental over F

**Properties of Simple Extensions**

**Property 1: Structure of F(α) when α is algebraic over F**

If α is algebraic over F with minimal polynomial p(x), then:

$F(\alpha) \cong F[x]/(p(x))$

This means that F(α) is isomorphic to the quotient ring of polynomials F[x] modulo the ideal generated by p(x).

Furthermore, elements of F(α) can be expressed as:

$F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1} \mid a_i \in F\}$

where n is the degree of the minimal polynomial p(x).

**Property 2: Structure of F(α) when α is transcendental over F**

If α is transcendental over F, then:

$F(\alpha) \cong F(x)$

Notes

which means F(α) is isomorphic to the field of rational functions in one variable over F.

Elements of F(α) can be expressed as:

$F(\alpha) = \{f(\alpha)/g(\alpha) \mid f(x), g(x) \in F[x], g(\alpha) \neq 0\}$

**Property 3: Degree of a Simple Extension**

For an algebraic element α over F, the degree of the extension [F(α):F] equals the degree of the minimal polynomial of α over F.

**Property 4: Tower Law for Simple Extensions**

If K = F(α) and L = K(β), then L = F(α,β). Furthermore, [L:F] = [L:K]·[K:F].

**Property 5: Primitive Element Theorem (Preview)**

If F is a field of characteristic 0 and K/F is a finite extension, then K = F(α) for some α ∈ K. In other words, K is a simple extension of F.

**Examples of Simple Extensions**

**Example 1: Q(√2)**

The extension Q(√2) is a simple extension of Q obtained by adjoining √2.

Since √2 is a root of the polynomial $p(x) = x^2 - 2$, which is irreducible over Q, the minimal polynomial of √2 over Q is $x^2 - 2$.

**Therefore:**

- **[Q(√2):Q] = 2**
- **Every element of Q(√2) can be written as a + b√2, where a, b ∈ Q**

**Example 2: Q(i)**

The extension Q(i) is a simple extension of Q obtained by adjoining i = √(-1).

Since i is a root of the polynomial $p(x) = x^2 + 1$, which is irreducible over Q, the minimal polynomial of i over Q is $x^2 + 1$.

**Therefore:**

- $[Q(i):Q] = 2$
- Every element of Q(i) can be written as $a + bi$, where $a, b \in Q$

**Example 3: Q(π)**

Since π is transcendental over Q (a famous result proved by Lindemann in 1882), the extension Q(π) is a transcendental extension.

**Therefore:**

- Q(π) consists of all rational functions in π with coefficients in Q
- Elements have the form $f(\pi)/g(\pi)$ where f, g are polynomials with coefficients in Q and $g(\pi) \neq 0$
- $[Q(\pi):Q]$ is infinite

**Applications of Simple Extensions**

Simple extensions are fundamental building blocks in field theory and have numerous applications:

1. Constructibility problems: Determining which numbers can be constructed using ruler and compass
2. Solving polynomial equations: Understanding when polynomial equations are solvable by radicals
3. Cyclotomic extensions: Creating fields that contain primitive roots of unity
4. Number theory: Studying algebraic numbers and their properties

**3.3.2: Algebraic Extensions: Definitions and Examples**

Notes

**Definition of an Algebraic Extension**

Let $F \subseteq K$ be a field extension. We say that K is an algebraic extension of F if every element of K is algebraic over F.

Recall that an element $\alpha \in K$ is algebraic over F if there exists a non-zero polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.

**Properties of Algebraic Extensions**

**Property 1: Transitivity of Algebraic Extensions**

If $F \subseteq K \subseteq L$ are fields such that K is algebraic over F and L is algebraic over K, then L is algebraic over F.

**Property 2: Algebraic Elements Form a Field**

If $F \subseteq K$ is a field extension, then the set of all elements in K that are algebraic over F forms a field.

**Property 3: Finite Extensions are Algebraic**

If $F \subseteq K$ is a field extension with [K:F] finite, then K is an algebraic extension of F.

**Property 4: Degree of an Algebraic Extension**

If K is an algebraic extension of F, then [K:F] equals the cardinality of a basis of K as a vector space over F (possibly infinite).

**Property 5: Products of Algebraic Extensions**

If $K_1$ and $K_2$ are algebraic extensions of F contained in some larger field, then the compositum $K_1K_2$ is also an algebraic extension of F.

**Examples of Algebraic Extensions**

**Example 1: $Q(\sqrt{2}, \sqrt{3})$**

The field $Q(\sqrt{2}, \sqrt{3})$ is obtained by adjoining both $\sqrt{2}$ and $\sqrt{3}$ to Q.

Since both $\sqrt{2}$ and $\sqrt{3}$ are algebraic over Q, this is an algebraic extension.

- $[Q(\sqrt{2}, \sqrt{3}):Q] = 4$
- A basis for $Q(\sqrt{2}, \sqrt{3})$ over Q is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\cdot\sqrt{3}\}$
- Every element can be written as $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\cdot\sqrt{3}$ where $a, b, c, d \in Q$

**Example 2: $Q(2^{(1/3)})$**

The field $Q(2^{(1/3)})$ is obtained by adjoining the real cube root of 2 toQ.

Since $2^{(1/3)}$ is a root of $x^3 - 2$, which is irreducible over Q, we have:

- $[Q(2^{(1/3)}):Q] = 3$
- A basis for $Q(2^{(1/3)})$ over Q is $\{1, 2^{(1/3)}, 2^{(2/3)}\}$
- Every element can be written as $a + b\cdot2^{(1/3)} + c\cdot2^{(2/3)}$ where $a, b, c \in Q$

**Example 3: The Algebraic Closure of Q**

The set of all complex numbers that are algebraic over Q, denoted $\bar{Q}$, forms an algebraic extension of Q.

This extension has the following properties:

- $\bar{Q}$ is algebraic over Q
- Every polynomial in Q[x] splits completely into linear factors over $\bar{Q}$
- $[\bar{Q}:Q]$ is infinite
- $\bar{Q}$ is countably infinite

**Example 4: Field of Algebraic Numbers**

The field of all algebraic numbers, A, is the set of all complex numbers that are algebraic over Q.

This is an algebraic extension of Q with infinite degree.

**Example 5: Finite Fields**

For a prime p and a positive integer n, the finite field $GF(p^n)$ is an algebraic extension of GF(p) of degree n.

**Algebraic vs. Transcendental Extensions**

An extension that is not algebraic is called transcendental. Here's a comparison:

**Algebraic Extensions:**

- Every element satisfies a polynomial equation with coefficients in the base field
- Can have finite or infinite degree
- Examples: $Q(\sqrt{2})$, Q(i), $Q(2^{(1/3)})$

**Transcendental Extensions:**

- Contain at least one element that doesn't satisfy any polynomial equation with coefficients in the base field
- Always have infinite degree
- Examples: $Q(\pi)$, Q(e), R(x) (rational functions)

**Algebraic Closure**

**Definition**

An algebraic closure of a field F, denoted $\bar{F}$, is an algebraic extension of F that is algebraically closed (meaning every non-constant polynomial in $\bar{F}[x]$ has a root in $\bar{F}$).

Properties of Algebraic Closures

1. Every field has an algebraic closure (requires Zorn's Lemma)
2. The algebraic closure is unique up to isomorphism
3. If F has characteristic 0, then $\bar{F}$ has characteristic 0

4. If F has characteristic $p > 0$, then $\bar{F}$ has characteristic p



Example: Algebraic Closure of the Real Numbers

The algebraic closure of R is C, the field of complex numbers.

**Solved Problems**

**Problem 1: Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over Q.**

Solution: Let $\alpha = \sqrt{2} + \sqrt{3}$. We need to find the minimal polynomial of $\alpha$ over Q.

Step 1: Calculate the powers of $\alpha$. $\alpha = \sqrt{2} + \sqrt{3}$ $\alpha^2 = (\sqrt{2} + \sqrt{3})^2 = 2 + 3 + 2\sqrt{2}\cdot\sqrt{3} = 5 + 2\sqrt{6}$

Step 2: Calculate $\alpha^2 - 5 = 2\sqrt{6}$, so $(\alpha^2 - 5)^2 = 24$ $(\alpha^2 - 5)^2 = 24$ $\alpha^4 - 10\alpha^2 + 25 = 24$ $\alpha^4 - 10\alpha^2 + 1 = 0$

Step 3: Check that this polynomial is irreducible over Q. If $p(x) = x^4 - 10x^2 + 1$ were reducible, it would factor as a product of two quadratic polynomials. We can verify that no such factorization exists using the rational root theorem and checking possible quadratic factors.

Therefore, the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over Q is $x^4 - 10x^2 + 1$.

**Problem 2: Determine the degree of the extension $Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over Q.**

Solution: Step 1: Consider the tower of extensions: $Q \subseteq Q(\sqrt{2}) \subseteq Q(\sqrt{2}, \sqrt{3}) \subseteq Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$

Step 2: Calculate the degrees of each extension. $[Q(\sqrt{2}):Q] = 2$ since the minimal polynomial of $\sqrt{2}$ over Q is $x^2 - 2$. $[Q(\sqrt{2}, \sqrt{3}):Q(\sqrt{2})] = 2$ since the minimal polynomial of $\sqrt{3}$ over $Q(\sqrt{2})$ is $x^2 - 3$. $[Q(\sqrt{2}, \sqrt{3}, \sqrt{5}):Q(\sqrt{2}, \sqrt{3})] = 2$ since the minimal polynomial of $\sqrt{5}$ over $Q(\sqrt{2}, \sqrt{3})$ is $x^2 - 5$.

Step 3: Apply the tower law. $[Q(\sqrt{2}, \sqrt{3}, \sqrt{5}):Q] = [Q(\sqrt{2}, \sqrt{3}, \sqrt{5}):Q(\sqrt{2}, \sqrt{3})] \times [Q(\sqrt{2}, \sqrt{3}):Q(\sqrt{2})] \times [Q(\sqrt{2}):Q]$ $[Q(\sqrt{2}, \sqrt{3}, \sqrt{5}):Q] = 2 \times 2 \times 2 = 8$

Notes

Therefore, the degree of Q(√2, √3, √5) over Q is 8.

**Problem 3: Determine if the extension Q(√2, 3√5) over Q is a simple extension.**

Solution: Step 1: Consider α = √2 + 3√5. Let's check if Q(√2, 3√5) = Q(α).

Step 2: Show that √2 and 3√5 can be expressed in terms of α and elements of Q. α = √2 + 3√5 $\alpha^2 = (\sqrt{2})^2 + 6\sqrt{2}\cdot\sqrt{5} + 9(\sqrt{5})^2 = 2 + 6\sqrt{10} + 45 = 47 + 6\sqrt{10}$

If we let $\beta = \alpha^2 - 47$, then $\beta = 6\sqrt{10}$. $\beta^2 = 36 \cdot 10 = 360$, so $\sqrt{10} = \beta/6$.

Now, $(\sqrt{2})(\sqrt{10}) = \sqrt{20} = 2\sqrt{5}$, so $\sqrt{5} = (\sqrt{2})(\sqrt{10})/2$. Therefore, $\sqrt{5} = (\sqrt{2})(\beta/6)/2 = (\sqrt{2})(\beta)/12$.

Since we know β in terms of α, we can express √5 in terms of α and elements of Q. Then, $3\sqrt{5} = 3(\sqrt{2})(\beta)/12 = (\sqrt{2})(\beta)/4$.

Also, $\sqrt{2} = \alpha - 3\sqrt{5} = \alpha - (\sqrt{2})(\beta)/4$. $4\sqrt{2} = 4\alpha - (\sqrt{2})(\beta)$. $4\sqrt{2} + (\sqrt{2})(\beta) = 4\alpha$. $\sqrt{2}(4 + \beta) = 4\alpha$. $\sqrt{2} = 4\alpha/(4 + \beta)$.

Step 3: Since both √2 and 3√5 can be expressed in terms of α and elements of Q, we have Q(√2, 3√5) = Q(α).

Therefore, Q(√2, 3√5) is a simple extension, specifically Q(√2 + 3√5).

**Problem 4: Find a basis for Q(√2, i) over Q and determine its degree.**

Solution: Step 1: Consider the tower of extensions: Q ⊆ Q(i) ⊆Q(i, √2)

Step 2: Calculate the degrees of each extension. [Q(i):Q] = 2 since the minimal polynomial of i over Q is $x^2 + 1$. [Q(i, √2):Q(i)] = 2 since the minimal polynomial of √2 over Q(i) is $x^2 - 2$.

Step 3: Apply the tower law. [Q(i, √2):Q] = [Q(i, √2):Q(i)] × [Q(i):Q] = 2 × 2 = 4

Step 4: Find a basis for Q(i, √2) over Q. Since [Q(i, √2):Q] = 4, we need four linearly independent elements. A basis for Q(i) over Q is {1, i}. A basis for Q(i, √2) over Q(i) is {1, √2}.

The complete basis for Q(i, √2) over Q is: {1, i, √2, i√2}

Any element of Q(i, √2) can be written uniquely as a + bi + c√2 + di√2, where a, b, c, d ∈ Q.

**Problem 5: Prove that if α is algebraic over F with minimal polynomial p(x), then F(α) ≅ F[x]/(p(x)).**

Solution: Step 1: Define a ring homomorphism φ: F[x] → F(α) by φ(f(x)) = f(α).

Step 2: Verify that φ is indeed a ring homomorphism.

- φ(f(x) + g(x)) = (f + g)(α) = f(α) + g(α) = φ(f(x)) + φ(g(x))
- φ(f(x) · g(x)) = (f · g)(α) = f(α) · g(α) = φ(f(x)) · φ(g(x))
- φ(1) = 1

Step 3: Determine the kernel of φ. The kernel of φ is the set of all polynomials f(x) ∈ F[x] such that f(α) = 0. Since p(x) is the minimal polynomial of α over F, any polynomial f(x) such that f(α) = 0 must be divisible by p(x). Therefore, ker(φ) = (p(x)), the ideal generated by p(x).

Step 4: By the First Isomorphism Theorem, we have: F[x]/ker(φ) ≅Im(φ) F[x]/(p(x)) ≅Im(φ)

Step 5: Show that Im(φ) = F(α). Clearly, Im(φ) ⊆ F(α) since φ maps into F(α). F(α) is the smallest field containing F and α, and Im(φ) contains F (as constants) and α (as φ(x)). Since Im(φ) is a ring and contains inverses for all non-zero elements (due to the fact that p(x) is irreducible), Im(φ) is a field. Therefore, F(α) ⊆Im(φ), and we have Im(φ) = F(α).

Step 6: Conclude that F(α) ≅ F[x]/(p(x)).

Notes

**Unsolved Problems**

**Problem 1:**

Determine whether the extension $Q(2^{(1/4)}, i)$ over Q is a simple extension. If it is, find an element α such that $Q(2^{(1/4)}, i) = Q(\alpha)$.

**Problem 2:**

Let $F = Q(\sqrt{2})$ and $K = F(\sqrt{3}, \sqrt{5})$. Find the degree [K:F] and determine a basis for K over F.

**Problem 3:**

Prove that if F is a field of characteristic 0 and α, β are algebraic elements over F that are not in F, then α + β, α - β, αβ, and α/β (if $\beta \neq 0$) are all algebraic over F.

**Problem 4:**

Find the minimal polynomial of $\alpha = \cos(2\pi/7)$ over Q.

**Problem 5:**

If $F \subseteq K$ is a field extension and $\alpha \in K$ is transcendental over F, prove that $[F(\alpha, \alpha^2):F(\alpha)] = 1$ and $[F(\alpha, 1/\alpha):F(\alpha)] = 1$.

Summary of Key Concepts

1. Simple Extensions:
    - $F(\alpha)$ is the smallest field containing F and the element α
    - If α is algebraic with minimal polynomial p(x), then $F(\alpha) \cong F[x]/(p(x))$
    - If α is transcendental, then $F(\alpha) \cong F(x)$, the field of rational functions
2. Algebraic Extensions:

- An extension K/F is algebraic if every element of K is algebraic over F
- Finite extensions are always algebraic
- Algebraic extensions are transitive
- The set of all algebraic elements over a field forms a field

3. Degree of Extensions:
   - For algebraic α, [F(α):F] equals the degree of the minimal polynomial
   - The tower law: [L:F] = [L:K] × [K:F]
   - The degree of a finite extension equals the dimension as a vector space
4. Basis Representation:
   - For algebraic α with minimal polynomial of degree n, elements of F(α) can be written as linear combinations of $\{1, \alpha, \alpha^2, ..., \alpha^{(n-1)}\}$
   - A basis allows us to represent and compute with elements of field extensions
5. Minimal Polynomials:
   - The minimal polynomial is the monic polynomial of least degree with coefficients in F that has α as a root
   - The minimal polynomial is always irreducible
   - Finding minimal polynomials is a key technique in studying field extensions

These concepts form the foundation for understanding more complex field extensions and their applications in various areas of

Notes

mathematics, including Galois theory, algebraic geometry, and number theory.

### 3.3.3 Finite Extensions and Their Structure

**Introduction to Finite Extensions**

A field extension L over a field K (denoted as L/K) is called a finite extension if L has finite dimension as a vector space over K. This dimension is called the degree of the extension, written as [L:K].

Finite extensions are fundamental objects in field theory and have numerous applications in algebra, number theory, and cryptography. In this section, we'll explore their structure and key properties.

Basic Properties of Finite Extensions

Degree of an Extension

For a field extension L/K, if L is a finite-dimensional vector space over K, then the dimension [L:K] is called the degree of the extension.

For example, if we consider $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, any element can be written as $a + b\sqrt{2}$ where $a,b \in \mathbb{Q}$. The set $\{1, \sqrt{2}\}$ forms a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$.

**Tower Law**

If $K \subseteq L \subseteq M$ are fields, then:

$[M:K] = [M:L][L:K]$

This multiplicative property is extremely useful in computing degrees of complicated extensions.

**Simple Extensions**

An extension L/K is called simple if $L = K(\alpha)$ for some element $\alpha \in L$. When $\alpha$ is algebraic over K, the degree $[K(\alpha):K]$ equals the degree of the minimal polynomial of $\alpha$ over K.

**Algebraic Extensions**

An element α is algebraic over K if it satisfies a non-zero polynomial with coefficients in K. An extension L/K is algebraic if every element of L is algebraic over K.

All finite extensions are algebraic, but not all algebraic extensions are finite.

**Properties of Algebraic Extensions**

1. If α is algebraic over K, then K(α)/K is a finite extension.
2. If L/K is a finite extension, then L/K is algebraic.
3. The composition of algebraic extensions is algebraic.

**Primitive Element Theorem**

A fundamental result about finite extensions is the Primitive Element Theorem:

If L/K is a finite separable extension, then $L = K(\alpha)$ for some $\alpha \in L$.

This means that any finite separable extension is simple.

**Separable and Inseparable Extensions**

**Separability**

An irreducible polynomial p(x) over a field K is separable if it has no repeated roots in its splitting field. An algebraic element α over K is separable if its minimal polynomial over K is separable.

An extension L/K is separable if every element of L is separable over K.

**Separable Degree**

For an extension L/K, the separable degree [L:K]s is the maximum degree of a separable subextension of L/K.

**Inseparable Degree**

The inseparable degree [L:K]i is defined as [L:K]i = [L:K]/[L:K]s.

Notes

**Normal Extensions**

An algebraic extension L/K is normal if every irreducible polynomial in K[x] that has one root in L has all its roots in L.

Equivalently, L/K is normal if L is the splitting field of a family of polynomials over K.

**Galois Extensions**

A field extension L/K is Galois if it is both normal and separable. For a Galois extension L/K:

1. The Galois group Gal(L/K) consists of all field automorphisms of L that fix K.
2. $|Gal(L/K)| = [L:K]$
3. There is a one-to-one correspondence between intermediate fields and subgroups of the Galois group.

**Examples of Finite Extensions**

**Example 1:** $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

- Degree: $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$
- Basis: $\{1, \sqrt{2}\}$
- Minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$: $x^2 - 2$
- This is a simple, separable, and normal extension.
- Galois group: $\mathbb{Z}_2$

**Example 2:** $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

- Degree: $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$
- Basis: $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$
- Minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$: $x^3 - 2$
- This is a simple extension but not normal.

**Example 3: $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$**



- Using the tower law: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$
- $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$
- $[\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$ (since $\sqrt{3}$ is not in $\mathbb{Q}(\sqrt{2})$)
- Therefore, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}] = 2 \times 2 = 4$
- Basis: $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$
- This is a Galois extension with Galois group isomorphic to Klein four-group.

### 3.3.4 Construction of Finite Fields

**Introduction to Finite Fields**

A finite field (or Galois field) is a field with a finite number of elements. The order of a finite field (the number of elements) must be a prime power $p^n$, where p is a prime and n is a positive integer.

For each prime power $p^n$, there exists exactly one finite field up to isomorphism, denoted as $GF(p^n)$ or $Fp^n$.

**Construction of Prime Fields**

The simplest finite fields are those of prime order, denoted GF(p) or Fp. These can be constructed as $\mathbb{Z}/p\mathbb{Z}$, the integers modulo p.

For example, $F_3 = \{0, 1, 2\}$ with addition and multiplication defined modulo 3.

**Construction of Extension Fields**

For constructing finite fields of order $p^n$ where $n > 1$, we need to construct field extensions of degree n over Fp.

**Method 1: Using Irreducible Polynomials**

To construct $GF(p^n)$:

Notes

1. Find an irreducible polynomial f(x) of degree n over Fp.
2. Form the quotient ring Fp[x]/(f(x)).
3. This quotient ring is a field with $p^n$ elements.

**Method 2: As Splitting Fields**

GF($p^n$) can also be constructed as the splitting field of the polynomial $xp^n$ - x over Fp.

**Properties of the Construction**

1. Every element of GF($p^n$) is a root of the polynomial $xp^n$ - x.
2. GF($p^n$) is the splitting field of $xp^n$ - x over Fp.
3. The multiplicative group GF($p^n$)* is cyclic of order $p^n$ - 1.

Examples of Finite Field Constructions

**Example 1: Construction of GF(4)**

To construct GF(4) = $F_2^2$:

1. Find an irreducible polynomial of degree 2 over $F_2$: $f(x) = x^2 + x + 1$
2. $F_2^2 = F_2[x]/(x^2 + x + 1)$
3. Elements: {0, 1, α, α+1} where α represents the coset $x + (x^2 + x + 1)$
4. Addition and multiplication tables can be derived using the condition $\alpha^2 + \alpha + 1 = 0$

**Example 2: Construction of GF(8)**

To construct GF(8) = $F_2^3$:

1. Find an irreducible polynomial of degree 3 over $F_2$: $f(x) = x^3 + x + 1$
2. $F_2^3 = F_2[x]/(x^3 + x + 1)$

3. Elements: {0, 1, α, $\alpha^2$, α+1, $\alpha^2$+1, $\alpha^2$+α, $\alpha^2$+α+1} where α represents the coset x + ($x^3$ + x + 1)
4. Operations defined via the condition $\alpha^3$ + α + 1 = 0

**Example 3: Construction of GF(9)**

To construct GF(9) = $F_3^2$:

1. Find an irreducible polynomial of degree 2 over $F_3$: f(x) = $x^2$ + 1
2. $F_3^2$ = $F_3$[x]/($x^2$ + 1)
3. Elements: {0, 1, 2, α, 2α, α+1, α+2, 2α+1, 2α+2} where α represents the coset x + ($x^2$ + 1)
4. Operations defined via the condition $\alpha^2$ = -1 = 2 (in $F_3$)

**Computational Techniques**

**Finding Irreducible Polynomials**

A polynomial of degree n over Fp is irreducible if and only if:

1. It divides $xp^n$ - x
2. It does not divide $xp^k$ - x for any k < n

Alternatively, we can check if the polynomial has no roots in Fp and is not divisible by any irreducible polynomial of lower degree.

**Primitive Polynomials**

A polynomial f(x) of degree n over Fp is primitive if its roots generate the multiplicative group of GF($p^n$).

Primitive polynomials are particularly useful in applications like linear feedback shift registers.

**3.3.5 Properties and Applications of Finite Fields**

**Structural Properties of Finite Fields**

Order and Characteristic

- A finite field $GF(p^n)$ has $p^n$ elements, where p is a prime (the characteristic of the field) and n is a positive integer.
- The additive group of $GF(p^n)$ is isomorphic to $(\mathbb{Z}p)^n$.
- The multiplicative group $GF(p^n)^*$ is cyclic of order $p^n - 1$.

**Primitive Elements**

A primitive element (or generator) of $GF(p^n)$ is an element whose powers generate all non-zero elements of the field.

Every finite field has at least one primitive element. In fact, the number of primitive elements in $GF(p^n)$ is $\varphi(p^n - 1)$, where $\varphi$ is Euler's totient function.

**Subfield Structure**

If $GF(p^m)$ is a subfield of $GF(p^n)$, then m divides n. Conversely, if m divides n, then $GF(p^m)$ is isomorphic to a subfield of $GF(p^n)$.

The subfields of $GF(p^n)$ form a lattice isomorphic to the lattice of divisors of n.

**Field Automorphisms**

**Frobenius Automorphism**

For any finite field $GF(p^n)$, the map $\sigma: x \mapsto x^p$ is an automorphism called the Frobenius automorphism.

The group of automorphisms of $GF(p^n)$ over Fp is cyclic of order n, generated by the Frobenius automorphism.

**Fixed Fields**

For any divisor m of n, the fixed field of $\sigma^m$ is $GF(p^m)$.

**Polynomial Factorization over Finite Fields**

**Factorization Patterns**

The polynomial $xp^n - x$ factors as the product of all monic irreducible polynomials over Fp whose degrees divide n.

**Counting Irreducible Polynomials**

The number of monic irreducible polynomials of degree d over Fp is given by:

$$N(p,d) = (1/d)\sum_i \mu(i)p^{(d/i)}$$

where the sum is over all divisors i of d, and μ is the Möbius function.

**Trace and Norm**

**Trace Function**

For an element α in $GF(p^n)$ over the subfield $GF(p^m)$, the trace is defined as:

$$Tr(\alpha) = \alpha + \alpha^{pm} + \alpha^{p2m} + ... + \alpha^{p(n/m-1)m}$$

The trace function is a linear transformation from $GF(p^n)$ to $GF(p^m)$.

**Norm Function**

Similarly, the norm of α is defined as:

$$N(\alpha) = \alpha \cdot \alpha^{pm} \cdot \alpha^{p2m} \cdot ... \cdot \alpha^{p(n/m-1)m}$$

The norm function is multiplicative and maps $GF(p^n)$ to $GF(p^m)$.

**Applications of Finite Fields**

**Coding Theory**

Finite fields are essential in the construction of error-correcting codes such as:

- Reed-Solomon codes
- BCH codes
- Algebraic geometric codes

These codes are used in digital communications, data storage, and satellite communications.

Notes

**Cryptography**

Finite fields play a crucial role in modern cryptography:

- In AES (Advanced Encryption Standard), operations are performed in GF($2^8$)
- Elliptic curve cryptography operates over finite fields
- Many public-key cryptosystems rely on the discrete logarithm problem in finite fields

**Computer Algebra**

Finite fields are used in:

- Polynomial factorization algorithms
- Solving systems of polynomial equations
- Computational number theory

**Combinatorial Designs**

Finite fields are used to construct various combinatorial designs:

- Finite projective planes
- Block designs
- Difference sets

Algebraic Geometry

Finite fields provide concrete examples for studying:

- Algebraic curves
- Zeta functions
- Discrete Fourier transform

**Solved Problems**

**Problem 1: Determine the degree of the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$.**

Notes

Solution: We can use the tower law to compute this degree: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}):\mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$

Step 1: $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ since the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.

Step 2: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$ since $\sqrt{3}$ is not in $\mathbb{Q}(\sqrt{2})$ and its minimal polynomial over $\mathbb{Q}(\sqrt{2})$ is $x^2 - 3$.

Step 3: We need to determine if $\sqrt{5}$ belongs to $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. If $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $\sqrt{5} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$ for some $a, b, c, d \in \mathbb{Q}$. Squaring both sides: $5 = (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3})^2 = a^2 + 2b^2 + 3c^2 + 6d^2 + 2ab\sqrt{2} + 2ac\sqrt{3} + 2ad\sqrt{2}\sqrt{3} + 2bc\sqrt{2}\sqrt{3} + 2bd\sqrt{6} + 2cd\sqrt{6}$

For this to equal 5, we need: $a^2 + 2b^2 + 3c^2 + 6d^2 = 5$ $ab = ac = ad = bc = bd = cd = 0$

These equations have no rational solutions except the trivial $a = b = c = d = 0$, which doesn't give $\sqrt{5}$. Therefore, $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}):\mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2$.

Thus, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}):\mathbb{Q}] = 2 \times 2 \times 2 = 8$.

**Problem 2: Construct the finite field GF(4) and provide its addition and multiplication tables.**

Solution: To construct GF(4), we need an irreducible polynomial of degree 2 over $F_2$. The polynomial $x^2 + x + 1$ is irreducible over $F_2$.

Therefore, $GF(4) = F_2[x]/(x^2 + x + 1)$.

Let $\alpha$ represent the coset $x + (x^2 + x + 1)$. Then $GF(4) = \{0, 1, \alpha, \alpha+1\}$.

From the relation $x^2 + x + 1 = 0$, we get $\alpha^2 + \alpha + 1 = 0$, which implies $\alpha^2 = \alpha + 1$.

Addition Table (using modulo 2 addition):

| + | 0 | 1 | α | α+1 |
|---|---|---|---|---|

0 | 0 1 α α+1

1 | 1 0 α+1 α

α | α α+1 0 1

α+1| α+1 α 1 0

Multiplication Table:

× | 0 1 α α+1

---

0 | 0 0 0 0

1 | 0 1 α α+1

α | 0 α α+1 1

α+1| 0 α+1 1 α

To verify these tables, let's compute some entries:

- $\alpha \times \alpha = \alpha^2 = \alpha + 1$ (from our relation)
- $\alpha \times (\alpha+1) = \alpha^2 + \alpha = (\alpha+1) + \alpha = 1$
- $(\alpha+1) \times (\alpha+1) = \alpha^2 + \alpha + \alpha + 1 = \alpha^2 + 1 = (\alpha+1) + 1 = \alpha$

**Problem 3: Prove that $x^p - x + a$ is irreducible over $F_p$ for any $a \neq 0$.**

Solution: We need to show that $f(x) = x^p - x + a$ has no roots in $F_p$ and is not divisible by any irreducible polynomial of degree less than p.

Step 1: Check if f(x) has roots in $F_p$. For any $b \in F_p$, we have $b^p = b$ (by Fermat's Little Theorem). So $f(b) = b^p - b + a = b - b + a = a$. Since $a \neq 0$, $f(b) \neq 0$ for all $b \in F_p$. Thus, f(x) has no roots in $F_p$.

Step 2: Show that f(x) is not divisible by any irreducible polynomial of degree d where $1 < d < p$.

Let's use the characteristic of the derivative. The derivative of f(x) is $f'(x) = px^{p-1} - 1 = -1$ (since $p = 0$ in $F_p$).

Since f'(x) = -1 ≠ 0, f(x) and f'(x) are coprime. This means f(x) has no repeated factors.

Now, if f(x) were divisible by an irreducible polynomial g(x) of degree d where 1 < d < p, then f(x) would have a root α in some extension field of $F_p$ with $[F_p(\alpha):F_p] = d$.

However, we can show that for any root α of f(x), the elements α, α+1, α+2, ..., α+(p-1) form a set of p distinct roots of f(x).

Since f(α) = 0, we have $\alpha^p = \alpha - a$. Now, for any $i \in F_p$, compute f(α+i): $f(\alpha+i) = (\alpha+i)^p - (\alpha+i) + a = \alpha^p + i^p - \alpha - i + a$ (since $(x+y)^p = x^p + y^p$ in $F_p$) $= \alpha^p + i - \alpha - i + a$ (since $i^p = i$ in $F_p$) $= \alpha^p - \alpha + a = 0$

So f(x) has at least p roots. But f(x) has degree p, so it can have at most p roots. Therefore, f(x) must have exactly p roots and must be irreducible over $F_p$.

**Problem 4: Find all subfields of GF(64).**

Solution: $GF(64) = GF(2^6)$

The subfields of $GF(2^6)$ are $GF(2^k)$ where k divides 6. The divisors of 6 are 1, 2, 3, and 6.

Therefore, the subfields of GF(64) are:

- $GF(2^1) = GF(2)$ (the prime field)
- $GF(2^2) = GF(4)$
- $GF(2^3) = GF(8)$
- $GF(2^6) = GF(64)$ (the field itself)

To verify this, we can check the subfield criterion: $GF(p^m)$ is a subfield of $GF(p^n)$ if and only if m divides n.

**Problem 5: Determine the number of irreducible polynomials of degree 4 over $F_3$.**

Notes

Solution: We can use the formula for counting monic irreducible polynomials:

$N(p,d) = (1/d)\sum_i \mu(i)p^{(d/i)}$

where the sum is over all divisors i of d, and μ is the Möbius function.

For p = 3 and d = 4, the divisors of 4 are 1, 2, 4. $\mu(1) = 1$ $\mu(2) = -1$ $\mu(4) = 0$

$N(3,4) = (1/4)[\mu(1)\cdot 3^4 + \mu(2)\cdot 3^2 + \mu(4)\cdot 3^1] = (1/4)[1\cdot 81 - 1\cdot 9 + 0\cdot 3] = (1/4)[81 - 9] = (1/4)[72] = 18$

Therefore, there are 18 irreducible polynomials of degree 4 over $F_3$.

To verify this another way, the polynomial $x^{34} - x$ splits completely over $F_3^4$ and factors as the product of all monic irreducible polynomials over $F_3$ whose degrees divide 4.

The total number of monic polynomials of degree dividing 4 is:

- Degree 1: 3 polynomials (x, x-1, x-2)
- Degree 2: 9 polynomials
- Degree 4: 81 polynomials

Of these, we know:

- 3 are irreducible of degree 1
- N(3,2) = 3 are irreducible of degree 2
- N(3,4) are irreducible of degree 4

So we have: $3\cdot 1 + 3\cdot 2 + N(3,4)\cdot 4 = 81$ This gives: $N(3,4) = (81 - 3 - 6)/4 = 18$

**Unsolved Problems**

Problem 1: Let α be a root of $x^4 + x + 1$ over $F_2$. Determine the minimal polynomial of $\alpha^2 + \alpha$ over $F_2$.

Problem 2: Prove that in a finite field of characteristic p, the map f(x) = $x^p$ is an automorphism.

Problem 3: Determine the number of primitive elements in GF($2^8$).

Problem 4: Find all elements α in GF(16) such that $\alpha^5 = 1$.

Problem 5: Let p be a prime and let F be a field with $p^2$ elements. If α is an element of F that is not in the prime subfield, show that F = Fp(α).

**Multiple Choice Questions (MCQs)**

1. **An extension field of a field F is:**
   a) A subset of F
   b) A field containing F as a subfield
   c) A group containing F
   d) None of the above

2. **An element is algebraic over a field F if:**
   a) It satisfies a polynomial equation with coefficients in F
   b) It is not a root of any polynomial in F[x]
   c) It is transcendental over F
   d) None of the above

3. **A simple extension of a field F is:**
   a) An extension generated by one element
   b) A transcendental extension
   c) An infinite extension
   d) None of the above

4. **Finite fields are also known as:**
   a) Prime fields
   b) Algebraic extensions
   c) Galois fields
   d) None of the above

5. **Every finite field has:**
   a) A prime number of elements

b) A power of a prime number of elements

c) An infinite number of elements

d) None of the above

6. **The characteristic of a finite field of order pn is:**

   a) 0

   b) p

   c) n

   d) None of the above

7. **The minimal polynomial of an algebraic element is:**

   a) The lowest-degree polynomial it satisfies

   b) A polynomial with no roots in any field

   c) The product of all polynomials it satisfies

   d) None of the above

8. **The multiplicative group of a finite field is:**

   a) Cyclic

   b) Abelian but not cyclic

   c) Non-abelian

   d) None of the above

**Short Answer Questions**

1. What is an extension field? Provide an example.
2. Differentiate between algebraic and transcendental elements.
3. Define an irreducible polynomial and give an example.
4. What is a simple extension of a field?
5. Explain the significance of algebraic extensions in field theory.
6. How do we construct finite fields?
7. What is the characteristic of a finite field?
8. Give an example of a finite field and explain its structure.

9. Define the degree of a field extension and provide an example.
10. Why is the multiplicative group of a finite field always cyclic?

**Long Answer Questions**

1. Explain in detail the concept of extension fields and their importance in algebra.
2. Differentiate between algebraic and transcendental numbers with examples.
3. Define irreducible polynomials and explain their role in constructing field extensions.
4. Discuss simple extensions and their applications in field theory.
5. How do we classify algebraic extensions? Give examples.
6. Explain the structure and properties of finite fields.
7. What is the significance of the minimal polynomial in field theory? Provide detailed examples.
8. Prove that the multiplicative group of a finite field is cyclic.
9. Discuss the applications of finite fields in cryptography and coding theory.
10. How do field extensions help in understanding the solutions of polynomial equations?

Answer Key MCQ :

1. b
2. a
3. a
4. c
5. b
6. b
7. a
8. a

# MODULE 4

## UNIT 4.1

## AUTOMORPHISMS OF FIELDS

**Objectives**

- Understand the concept of field automorphisms.
- Learn about conjugation isomorphisms and their significance.
- Explore the relationship between automorphisms and fixed fields.
- Study the Frobenius automorphism and its applications.
- Analyze the structure and importance of splitting fields.

### 4.1.1: Introduction to Field Automorphisms

Field automorphisms are fundamental structures in modern algebra that help us understand the internal symmetries and structures of fields. These mathematical objects serve as critical tools in various branches of mathematics, including Galois theory, algebraic geometry, and number theory. At the most basic level, a field automorphism is a structure-preserving mapping of a field to itself. Unlike general field homomorphisms that can map between different fields, automorphisms specifically deal with self-mappings. This restriction makes them particularly useful for studying the internal structure of a single field. The study of field automorphisms originated in the early 19th century, primarily through the work of Évariste Galois. His groundbreaking insights connected the automorphisms of a field with the solvability of polynomial equations, establishing what we now know as Galois theory. This connection revealed that the structure of automorphism groups directly relates to the structural properties of the field itself.

Field automorphisms preserve all the essential field operations — addition and multiplication — while maintaining the distinct identities

of the field. This preservation property ensures that the algebraic structure remains intact under the mapping. Additionally, automorphisms must be bijective, meaning they establish a one-to-one correspondence between elements. Consider a simple example: the field of real numbers. The identity mapping, which maps each real number to itself, is the only field automorphism of the reals. However, for more complex fields like the complex numbers, additional automorphisms exist, such as complex conjugation, which maps a complex number to its conjugate. The collection of all automorphisms of a field forms a group under composition, known as the automorphism group. This group structure provides deep insights into the field's properties. For instance, in Galois theory, the automorphism group of a field extension directly relates to the structure of polynomial equations that have roots in that extension. Field automorphisms also play crucial roles in understanding field extensions. When we extend a field by adjoining elements, the automorphisms that fix the original field help us analyze the structure of the extension. This connection proves invaluable in determining which polynomial equations are solvable by radicals and which are not. As we delve deeper into field automorphisms, we'll explore their formal definitions, examine concrete examples, study specific types like conjugation isomorphisms, and investigate the concept of fixed fields, which provides a powerful tool for analyzing field structures and extensions.

### 4.1.2: Definition and Examples of Field Automorphisms

**Definition of Field Automorphisms**

A field automorphism is a bijective mapping from a field to itself that preserves the field operations. Formally, if F is a field, then a function $\sigma: F \rightarrow F$ is a field automorphism if it satisfies the following conditions:

1. Bijective: $\sigma$ is both injective (one-to-one) and surjective (onto)
2. Preserves addition: For all $a, b \in F$, $\sigma(a + b) = \sigma(a) + \sigma(b)$

3. Preserves multiplication: For all a, b ∈ F, σ(a × b) = σ(a) × σ(b)

From these properties, several important consequences follow:

- σ(0) = 0 (preservation of additive identity)
- σ(1) = 1 (preservation of multiplicative identity)
- σ(-a) = -σ(a) (preservation of additive inverse)
- $\sigma(a^{-1}) = \sigma(a)^{-1}$ for a ≠ 0 (preservation of multiplicative inverse)

The set of all automorphisms of a field F forms a group under function composition, denoted by Aut(F). This group structure is central to understanding the algebraic properties of the field itself.

**Examples of Field Automorphisms**

**Example 1: The Identity Automorphism**

The simplest field automorphism is the identity automorphism, id: F → F, defined by id(a) = a for all a ∈ F. This automorphism exists for every field and serves as the identity element in the automorphism group.

**Example 2: Automorphisms of Q**

The field of rational numbers Q has only one automorphism: the identity automorphism. This can be proven by noting that any automorphism must fix the integers (since it preserves addition and the multiplicative identity), and by extension, it must fix all rational numbers.

Proof sketch: Let σ be an automorphism of Q. Then:

- σ(1) = 1 (preservation of multiplicative identity)
- σ(n) = σ(1 + 1 + ... + 1) = σ(1) + σ(1) + ... + σ(1) = n for any integer n
- For any rational number p/q, σ(p/q) = σ(p)/σ(q) = p/q

**Example 3: Automorphisms of R**

Notes

Similar to Q, the field of real numbers R also has only the identity automorphism. This result is less obvious and requires properties of ordered fields and continuity.

**Example 4: Automorphisms of C**

The complex field C has exactly two automorphisms:

1. The identity automorphism: id(a + bi) = a + bi
2. Complex conjugation: conj(a + bi) = a - bi

The fact that these are the only automorphisms of C can be proven using the fact that any automorphism must fix the reals (which can be shown using properties of ordered fields) and must either fix i or map it to -i.

**Example 5: Automorphisms of Finite Fields**

For a finite field with $p^n$ elements (where p is prime), there are exactly n automorphisms. For instance, consider the field $F_4 = \{0, 1, \alpha, \alpha+1\}$ where $\alpha^2 + \alpha + 1 = 0$. The automorphisms are:

1. The identity: id(x) = x for all $x \in F_4$
2. The Frobenius automorphism: $Frob(x) = x^2$ for all $x \in F_4$

Note that in $F_4$, $x^2 = x$ for all elements, so the Frobenius automorphism is also the identity in this specific case.

**Example 6: Automorphisms of Q(√2)**

The field $Q(\sqrt{2})$ consists of numbers of the form $a + b\sqrt{2}$ where $a, b \in Q$. This field has two automorphisms:

1. The identity: $id(a + b\sqrt{2}) = a + b\sqrt{2}$
2. The mapping σ defined by $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$

The second automorphism maps $\sqrt{2}$ to $-\sqrt{2}$ while fixing all rational numbers.

Notes

**Example 7: Frobenius Automorphism in Characteristic p Fields**

For a field F of characteristic $p > 0$, the Frobenius map $\varphi: F \to F$ defined by $\varphi(x) = x^p$ is always a field homomorphism. In finite fields of characteristic p, this map is also an automorphism.The collection of automorphisms forms a group structure that provides deep insights into the field's algebraic properties. This automorphism group, denoted Aut(F), is a central object of study in Galois theory.

### 4.1.3: Conjugation Isomorphisms

Conjugation isomorphisms are a special class of field automorphisms that play a crucial role in understanding field extensions and algebraic structures. They are particularly important in Galois theory and the study of splitting fields.

**Definition of Conjugation Isomorphisms**

Let F be a field and let E be an extension field of F. A conjugation isomorphism over F is an automorphism $\sigma$ of E that fixes every element of F. In other words, $\sigma(a) = a$ for all $a \in F$.

Formally, the set of all such automorphisms forms a group called the Galois group of E over F, denoted by Gal(E/F):

$Gal(E/F) = \{\sigma \in Aut(E) \mid \sigma(a) = a \text{ for all } a \in F\}$

Conjugation isomorphisms derive their name from their similarity to complex conjugation, which is the prototypical example of such an isomorphism.

**Properties of Conjugation Isomorphisms**

1. Fixed Field Preservation: Every element of the base field F is fixed by all conjugation isomorphisms in Gal(E/F).
2. Group Structure: The set of all conjugation isomorphisms forms a group under composition.
3. Finiteness in Algebraic Extensions: If E is a finite algebraic extension of F, then Gal(E/F) is a finite group.

4. Order Bound: If E is a finite extension of F with [E:F] = n (the degree of the extension), then $|Gal(E/F)| \leq n$, with equality holding when the extension is Galois.

5. Action on Roots: Conjugation isomorphisms permute the roots of irreducible polynomials. If $\alpha$ is a root of an irreducible polynomial f(x) over F, then $\sigma(\alpha)$ is also a root of f(x) for any $\sigma \in Gal(E/F)$.

**Examples of Conjugation Isomorphisms**

**Example 1: Complex Conjugation**

The classic example is complex conjugation on C viewed as an extension of R. The conjugation map $\sigma: C \rightarrow C$ defined by $\sigma(a + bi) = a - bi$ is an automorphism of C that fixes every real number. Thus, $Gal(C/R) = \{id, \sigma\}$, a group of order 2.

**Example 2: Conjugation in Q(√2)**

Consider the field extension $Q(\sqrt{2})/Q$. The conjugation map $\sigma: Q(\sqrt{2}) \rightarrow Q(\sqrt{2})$ defined by $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ for $a, b \in Q$ is an automorphism that fixes every rational number. Here, $Gal(Q(\sqrt{2})/Q) = \{id, \sigma\}$, also a group of order 2.

**Example 3: Cyclotomic Extensions**

For the cyclotomic extension $Q(\zeta_n)/Q$, where $\zeta_n$ is a primitive nth root of unity, the conjugation isomorphisms are given by $\sigma_k(\zeta_n) = \zeta_n^k$ for all k coprime to n. The Galois group $Gal(Q(\zeta_n)/Q)$ is isomorphic to the multiplicative group $(Z/nZ)^x$ of integers modulo n that are coprime to n.

**Example 4: Splitting Fields of Polynomials**

Let E be the splitting field of a separable polynomial f(x) over F. The conjugation isomorphisms in Gal(E/F) permute the roots of f(x). For instance, if $f(x) = x^3 - 2$ over Q, and E is its splitting field, then

Notes

Gal(E/Q) is isomorphic to $S_3$, the symmetric group on 3 letters, representing the permutations of the three cube roots of 2.

**Applications of Conjugation Isomorphisms**

1. Galois Theory: Conjugation isomorphisms are the foundation of Galois theory, which establishes a correspondence between subgroups of the Galois group and intermediate fields of the extension.

2. Solvability of Equations: The structure of the Galois group (composed of conjugation isomorphisms) determines whether a polynomial equation is solvable by radicals.

3. Field Invariants: Conjugation isomorphisms help identify elements that are invariant under certain field operations, leading to the concept of fixed fields.

4. Construction of Minimal Polynomials: For an element α in an extension field, the minimal polynomial of α over the base field can be constructed using the conjugation isomorphisms that act on α.

5. Normal Extensions: An extension E/F is normal if and only if it is the splitting field of a family of polynomials over F, which connects to the behavior of conjugation isomorphisms on the roots of these polynomials.

Conjugation isomorphisms provide a powerful tool for analyzing field extensions and understanding the algebraic structure of fields. They form the bridge between group theory and field theory, allowing us to apply group-theoretic methods to solve problems in field theory and vice versa.

### 4.2.1: Fixed Fields and Their Importance

The concept of fixed fields is central to understanding the relationship between field automorphisms and field extensions. It provides a powerful framework for analyzing the structure of fields and plays a key role in the fundamental theorem of Galois theory.

**Definition of Fixed Fields**

Given a field E and a group G of automorphisms of E, the fixed field of G, denoted $E^G$ or Fix(G), is the subfield of E consisting of all elements that are fixed (left unchanged) by every automorphism in G.

Formally: $E^G = \{a \in E \mid \sigma(a) = a \text{ for all } \sigma \in G\}$

The fixed field represents the elements of E that remain invariant under the action of the automorphism group G.

**Properties of Fixed Fields**

1. Subfield Structure: For any group G of automorphisms of E, the fixed field $E^G$ is indeed a subfield of E.
2. Galois Correspondence: If E/F is a Galois extension with Galois group G = Gal(E/F), then $F = E^G$. This is one of the fundamental relationships in Galois theory.
3. Monotonicity: If H is a subgroup of G, then $E^G \subseteq E^H$. In other words, smaller groups of automorphisms lead to larger fixed fields.
4. Fixed Field of Trivial Group: $E^{\wedge\{id\}} = E$, where {id} is the trivial group containing only the identity automorphism.
5. Fixed Field of Full Automorphism Group: If G = Aut(E), then E^G is the prime subfield of E (either Q or $F_p$ depending on the characteristic).

**Importance and Applications of Fixed Fields**

Notes

1. Galois Theory Correspondence: The fundamental theorem of Galois theory establishes a one-to-one correspondence between the subgroups of the Galois group Gal(E/F) and the intermediate fields between F and E. Specifically, for each subgroup H of Gal(E/F), $E^H$ is an intermediate field, and for each intermediate field K, Gal(E/K) is a subgroup of Gal(E/F).

2. Field Extension Analysis: Fixed fields help determine the degree of field extensions. If E/F is a Galois extension with Galois group G, then [E:F] = |G|.

3. Structural Understanding: The fixed field concept helps understand the internal structure of fields and their extensions, revealing how automorphism groups partition the elements of a field.

4. Constructive Field Theory: Fixed fields provide a constructive approach to generating subfields with specific properties, particularly useful in computational algebra.

5. Normal Extensions: An extension E/F is normal if and only if F is the fixed field of some group of automorphisms of E.

**Examples of Fixed Fields**

**Example 1: Fixed Field of Complex Conjugation**

Consider the field of complex numbers C and the group G = {id, conj} where conj is the complex conjugation. The fixed field $C^G$ consists of all complex numbers that remain unchanged under conjugation:

$C^G = \{a + bi \in C \mid a + bi = a - bi\} = \{a \in C \mid b = 0\} = R$

This confirms the well-known fact that the fixed field of the Galois group Gal(C/R) = {id, conj} is indeed R.

**Example 2: Cyclotomic Extensions**

Notes

Let E = $Q(\zeta_n)$ be the cyclotomic field obtained by adjoining a primitive nth root of unity $\zeta_n$ to Q. The Galois group Gal(E/Q) is isomorphic to $(Z/nZ)^x$, the group of units modulo n.

For a subgroup H of Gal(E/Q), the fixed field E^H represents an intermediate field between Q and $Q(\zeta_n)$. For instance, if n = p is a prime, and H is the subgroup of squares in $(Z/pZ)^x$, then $E^H$ =Q (√±p) where the sign depends on p mod 4.

**Example 3: Fixed Field of Frobenius Automorphism**

In a finite field $F_{pn}$, the Frobenius automorphism φ is defined by φ(x) = $x^p$ for all x ∈ $F_{pn}$. The fixed field of the group ⟨φ⟩ generated by φ is:

$F_{pn}^{\langle\varphi\rangle} = \{x \in F_{pn} \mid x^p = x\} = F_p$

This confirms that the prime subfield $F_p$ is the fixed field of the Frobenius automorphism.

**Example 4: Fixed Field in Q(√2, √3)**

Consider the field E = Q(√2, √3) and its Galois group G = Gal(E/Q), which has four elements:

- id: identity automorphism
- $\sigma_1$: maps √2 → -√2 and fixes √3
- $\sigma_2$: fixes √2 and maps √3 → -√3
- $\sigma_3$: maps √2 → -√2 and √3 → -√3

The fixed field $E^G$ is Q.

If we consider the subgroup H = {id, $\sigma_1$}, then $E^H$ = Q(√3). Similarly, for K = {id, $\sigma_2$}, $E^K$ = Q(√2). For L = {id, $\sigma_3$}, $E^L$ =Q (√6).

This illustrates the Galois correspondence between subgroups and intermediate fields.

**The Fundamental Theorem of Galois Theory**

The importance of fixed fields culminates in the Fundamental Theorem of Galois Theory, which can be stated as follows:

Let E/F be a Galois extension with Galois group G = Gal(E/F). Then:

1. There is a one-to-one correspondence between the subgroups H of G and the intermediate fields K (F ⊆ K ⊆ E), given by H ↦ $E^H$ and K ↦ Gal(E/K).
2. If H ↦ K under this correspondence, then:
    - [E:K] = |H| (the order of the subgroup)
    - [K:F] = [G:H] (the index of the subgroup)
    - H is a normal subgroup of G if and only if K/F is a normal extension
    - If H is normal in G, then Gal(K/F) ≅ G/H

This theorem encapsulates the deep connection between field theory and group theory, with fixed fields serving as the bridge between these two domains. It provides a powerful tool for analyzing field extensions and solving polynomial equations.

**Solved Problems on Field Automorphisms**

**Problem 1: Determining all Field Automorphisms of Q(√2)**

Problem: Find all field automorphisms of Q(√2) and determine the fixed field for each non-trivial automorphism.

**Solution:**

Step 1: Understand the structure of Q(√2). Q(√2) consists of all numbers of the form a + b√2 where a, b ∈ Q.

Step 2: Determine how automorphisms act on Q(√2). Any automorphism σ must fix the rational field Q. That is, σ(q) = q for all q ∈ Q. The only question is how σ acts on √2.

Since σ preserves multiplication: $\sigma(\sqrt{2})^2 = \sigma(\sqrt{2} \cdot \sqrt{2}) = \sigma(2) = 2$ Therefore, $\sigma(\sqrt{2}) = \pm\sqrt{2}$

This gives us two possibilities:

- $\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}$ (the identity automorphism)
- $\sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$ (sends $\sqrt{2}$ to $-\sqrt{2}$)

Step 3: Verify these are valid automorphisms. We need to check that $\sigma_2$ preserves addition and multiplication:

For addition: $\sigma_2((a + b\sqrt{2}) + (c + d\sqrt{2})) = \sigma_2((a + c) + (b + d)\sqrt{2}) = (a + c) - (b + d)\sqrt{2}$ And also: $\sigma_2(a + b\sqrt{2}) + \sigma_2(c + d\sqrt{2}) = (a - b\sqrt{2}) + (c - d\sqrt{2}) = (a + c) - (b + d)\sqrt{2}$

For multiplication: $\sigma_2((a + b\sqrt{2})(c + d\sqrt{2})) = \sigma_2(ac + ad\sqrt{2} + bc\sqrt{2} + 2bd) = ac + 2bd - (ad + bc)\sqrt{2}$ And also: $\sigma_2(a + b\sqrt{2})\sigma_2(c + d\sqrt{2}) = (a - b\sqrt{2})(c - d\sqrt{2}) = ac + 2bd - (ad + bc)\sqrt{2}$

Step 4: Determine the fixed field of $\sigma_2$. The fixed field consists of elements $a + b\sqrt{2}$ such that $\sigma_2(a + b\sqrt{2}) = a + b\sqrt{2}$. This means $a - b\sqrt{2} = a + b\sqrt{2}$, which implies $b = 0$. Therefore, the fixed field of $\sigma_2$ is Q.

Conclusion: The automorphism group of $Q(\sqrt{2})$ is $\{\sigma_1, \sigma_2\} \cong Z_2$, and the fixed field of the non-trivial automorphism $\sigma_2$ is Q.

**Problem 2: Automorphism Group of a Cyclotomic Field**

Problem: Determine the automorphism group of the cyclotomic field $Q(\zeta_5)$, where $\zeta_5$ is a primitive 5th root of unity, and identify the subgroups and their corresponding fixed fields.

**Solution:**

Step 1: Understand the structure of $Q(\zeta_5)$. Let $\zeta_5 = e^{(2\pi i/5)}$, a primitive 5th root of unity. Then $Q(\zeta_5)$ is the splitting field of the cyclotomic polynomial $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$.

Step 2: Determine the automorphisms of $Q(\zeta_5)$ over Q. Any automorphism σ of $Q(\zeta_5)$ must fix Q and send $\zeta_5$ to another primitive

5th root of unity. The primitive 5th roots of unity are $\zeta_5$, $\zeta_5^2$, $\zeta_5^3$, and $\zeta_5^4$.

This gives us four automorphisms:

- $\sigma_1(\zeta_5) = \zeta_5$ (identity)
- $\sigma_2(\zeta_5) = \zeta_5^2$
- $\sigma_3(\zeta_5) = \zeta_5^3$
- $\sigma_4(\zeta_5) = \zeta_5^4$

Step 3: Determine the group structure. We can compute the composition of these automorphisms:

- $\sigma_2 \circ \sigma_2(\zeta_5) = \sigma_2(\zeta_5^2) = (\zeta_5^2)^2 = \zeta_5^4 = \sigma_4(\zeta_5)$
- $\sigma_2 \circ \sigma_3(\zeta_5) = \sigma_2(\zeta_5^3) = (\zeta_5^3)^2 = \zeta_5^6 = \zeta_5 = \sigma_1(\zeta_5)$
- $\sigma_2 \circ \sigma_4(\zeta_5) = \sigma_2(\zeta_5^4) = (\zeta_5^4)^2 = \zeta_5^8 = \zeta_5^3 = \sigma_3(\zeta_5)$

Similar calculations for the other compositions show that the automorphism group is isomorphic to $(Z/5Z)^x \cong Z_4$, the cyclic group of order 4, with $\sigma_2$ as a generator.

Step 4: Identify subgroups and fixed fields. The subgroups of $Z_4$ are:

- $\{\sigma_1\}$ (the trivial subgroup)
- $\{\sigma_1, \sigma_3\}$ (the subgroup of order 2)
- $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ (the full group)

For the trivial subgroup $\{\sigma_1\}$, the fixed field is $Q(\zeta_5)$.

For $\{\sigma_1, \sigma_3\}$, we need to find elements fixed by both $\sigma_1$ and $\sigma_3$. An element $\alpha = a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3 + a_4\zeta_5^4$ is fixed by $\sigma_3$ if: $\sigma_3(\alpha) = a_0 + a_1\zeta_5^3 + a_2\zeta_5^6 + a_3\zeta_5^9 + a_4\zeta_5^{12} = a_0 + a_1\zeta_5^3 + a_2\zeta_5 + a_3\zeta_5^4 + a_4\zeta_5^2 = \alpha$

This gives us conditions: $a_1 = a_3$, $a_2 = a_4$ So the fixed field is $Q(\zeta_5 + \zeta_5^4, \zeta_5^2 + \zeta_5^3) = Q(\sqrt{5})$

For the full group, the fixed field is Q.

Conclusion: The automorphism group of $Q(\zeta_5)$ is cyclic of order 4, isomorphic to $(Z/5Z)^x$. The fixed fields are:

Notes

- For $\{\sigma_1\}$: $Q(\zeta_5)$
- For $\{\sigma_1, \sigma_3\}$: $Q(\sqrt{5})$
- For $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$: $Q$

**Problem 3: Frobenius Automorphism in Finite Fields**

Problem: Show that the Frobenius map $\varphi(x) = x^p$ on a finite field $F_{pn}$ is an automorphism, and determine its fixed field.

**Solution:**

Step 1: Verify that φ is a homomorphism. For addition: $\varphi(x + y) = (x + y)^p$ In a field of characteristic p, the binomial expansion gives: $(x+ y)^p = x^p + y^p$ (all other terms contain a factor of p and thusvanish) So $\varphi(x + y) = x^p + y^p = \varphi(x) + \varphi(y)$

For multiplication: $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$

Step 2: Show that φ is bijective (both injective and surjective). For injectivity, suppose $\varphi(x) = \varphi(y)$, then $x^p = y^p$. In a field, if $a^p = b^p$, then a = b (by taking the pth root). Therefore, x = y, proving φ is injective.For surjectivity, since $F_p{}^n$ is finite and φ is injective, it must also besurjective.

Step 3: Determine the fixed field of φ. The fixed field consists of elements x such that $\varphi(x) = x$, i.e., $x^p = x$. This equation is satisfied by all elements of the prime subfield $F_p$. To show this is the entire fixed field, note that the polynomial $x^p - x$ has at most p roots in any field, and we've identified p distinct roots (the elements of $F_p$). Therefore, the fixed field of φ is exactly $F_p$.

Step 4: Determine the order of φ in the automorphism group. Since $F_p{}^n$ contains $p^n$ elements, and φ raises elements to the power p,

Notes

the smallest positive integer k such that $\varphi^k$ is the identity is the smallest k with $p^k \equiv 1 \pmod{p^{n-1}}$. This gives k = n, so the order of φ in the automorphism group is n.

**Problem 4: Field Automorphisms of C and R**

Problem: Prove that the field of real numbers R has only the identity automorphism, and the field of complex numbers C has exactly two automorphisms.

**Solution:**

**Part 1: Automorphisms of R**

Step 1: Show that any automorphism σ of R must fix the rational numbers Q.

- σ(1) = 1 (preservation of multiplicative identity)
- For any integer n > 0, σ(n) = σ(1 + 1 + ... + 1) = σ(1) + σ(1) + ... + σ(1) = n
- For negative integers, σ(-n) = -σ(n) = -n
- For fractions, σ(p/q) = σ(p)/σ(q) = p/q Thus, σ(q) = q for all q ∈ Q.

Step 2: Show that σ preserves order. If a > b, then a - b > 0. Since σ preserves addition and positivity (as a field automorphism), σ(a) - σ(b) = σ(a - b) > 0. Therefore, σ(a) > σ(b), meaning σ preserves order.

Step 3: Show that σ is continuous. Using the order-preserving property, we can show that for any convergent sequence $(a_n)$ with limit a, the sequence $(\sigma(a_n))$ converges to σ(a).

Step 4: Use density of Q in R to conclude σ is the identity. For any x ∈ R and any ε > 0, there exist rationals p, q such that p < x < q and q - p < ε. Since σ fixes p and q and preserves order, p = σ(p) < σ(x) < σ(q) = q. This means |σ(x) - x| < ε for any ε > 0, which implies σ(x) = x.

Therefore, the only automorphism of R is the identity.

**Part 2: Automorphisms of C**

Notes

Step 1: Show that any automorphism σ of C must fix R. From Part 1, any automorphism of R is the identity. Since C is an extension of R, the restriction of σ to R must be the identity automorphism on R.

Step 2: Determine how σ acts on i. Since $i^2 = -1$, we have $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$. This means $\sigma(i) = \pm i$.

Step 3: Show that this gives exactly two automorphisms.

- If $\sigma(i) = i$, then $\sigma(a + bi) = a + bi$ for all $a, b \in R$ (the identity automorphism)
- If $\sigma(i) = -i$, then $\sigma(a + bi) = a - bi$ for all $a, b \in R$ (complex conjugation)

Both of these are clearly automorphisms of C. And since any automorphism must send i to either i or -i, these are the only two possibilities.

## UNIT 4.3

### 4.3.1: Frobenius Automorphism

The Frobenius automorphism is a fundamental concept in field theory and has significant applications in number theory, algebraic geometry, and cryptography. Named after Ferdinand Georg Frobenius, this automorphism applies to finite fields and provides a powerful tool for understanding their structure.

**Definition and Basic Properties**

Let F be a finite field of characteristic p (where p is a prime number). The Frobenius automorphism, typically denoted by Φ, is defined as:

$\Phi: F \rightarrow F \; \Phi(x) = x^p$

In other words, the Frobenius automorphism maps every element of the field to its p-th power.

Key Properties:

1. Homomorphism Property: For any elements a, b ∈ F:
   - $\Phi(a + b) = \Phi(a) + \Phi(b) = a^p + b^p$
   - $\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b) = a^p \cdot b^p$
2. Injectivity: The Frobenius automorphism is injective (one-to-one). Proof: If $\Phi(a) = \Phi(b)$, then $a^p = b^p$. In a field of characteristic p, this implies a = b.
3. Surjectivity: The Frobenius automorphism is surjective (onto). Since F is finite and Φ is injective, it follows that Φ is also surjective.
4. Fixed Field: The fixed field of the Frobenius automorphism is the prime subfield $F_p$. An element x is fixed by Φ if and onlyif $x^p = x$, which occurs precisely when $x \in F_p$.

**Frobenius Automorphism in Extension Fields**

Let $F_q$ be a finite field with $q = p^n$ elements, where p is prime and nis a positive integer. The Frobenius automorphism plays a crucial rolein understanding the structure of extension fields.

Notes

**Extension Field Properties:**

1. Iterated Application: The n-fold composition of the Frobenius automorphism, $\Phi^n$, is the identity map on $F_q$. This means that for any $x \in F_q$, we have $x^{pn} = x$.

2. Galois Group: For an extension $F_q/F_p$, the Galois group $Gal(F_q/F_p)$ is cyclic of order n, generated by the Frobenius automorphism.

3. Minimal Polynomials: The Frobenius automorphism helps determine the minimal polynomials of elements in extension fields.

**Applications of the Frobenius Automorphism**

1. Counting Solutions to Equations: The Frobenius automorphism helps count the number of solutions to polynomial equations over finite fields.

2. Cryptography: The computational difficulty of finding fixed points of the Frobenius automorphism in certain fields forms the basis for several cryptographic protocols.

3. Algebraic Geometry: In algebraic geometry, the Frobenius morphism provides a tool for studying varieties over finite fields.

**Examples of the Frobenius Automorphism**

**Example 1: Frobenius in $F_4$**

Consider the field $F_4 = \{0, 1, \alpha, \alpha+1\}$, where $\alpha$ is a root of the polynomial $x^2 + x + 1$ over $F_2$. The Frobenius automorphism $\Phi(x)= x^2$ acts as follows:

- $\Phi(0) = 0^2 = 0$
- $\Phi(1) = 1^2 = 1$
- $\Phi(\alpha) = \alpha^2 = \alpha+1$ (because $\alpha^2 + \alpha + 1 = 0$, so $\alpha^2 = \alpha+1$)
- $\Phi(\alpha+1) = (\alpha+1)^2 = \alpha^2 + 1 = \alpha+1+1 = \alpha$ (in characteristic 2)

Note that $\Phi^2$ is the identity map, confirming that the order of the Frobenius automorphism divides the extension degree.

**Example 2: Frobenius in $F_{27}$**

For the field $F_{27} = F_3[x]/(x^3 - 2)$, let $\beta$ be a root of $x^3 - 2$. The Frobenius automorphism $\Phi(x) = x^3$ acts as:

- $\Phi(\beta) = \beta^3 = 2$ (by definition)
- $\Phi(\beta^2) = (\beta^2)^3 = \beta^6 = (\beta^3)^2 = 2^2 = 4 = 1 \pmod 3$
- $\Phi(2\beta) = (2\beta)^3 = 2^3 \cdot \beta^3 = 8 \cdot 2 = 16 = 1 \pmod 3$

Here, $\Phi^3$ is the identity map, aligning with the extension degree of 3.

### 4.3.2: Splitting Fields: Definitions and Examples

**Definition of Splitting Fields**

A splitting field is a fundamental concept in field theory that provides the minimal extension of a field needed to factor a polynomial completely into linear factors.

**Formal Definition:**

Let F be a field and f(x) be a non-constant polynomial in F[x]. A field extension E of F is called a splitting field of f(x) over F if:

1. f(x) factors completely into linear factors in E[x]
2. $E = F(r_1, r_2, ..., r_n)$, where $r_1, r_2, ..., r_n$ are all the roots of f(x)

In other words, E is the smallest field extension of F that contains all the roots of f(x).

**Alternative Definition:**

Notes

A splitting field for a set of polynomials $\{f_1(x), f_2(x), ..., f_m(x)\}$ over a field F is the smallest field extension E of F such that each polynomial $f_i(x)$ splits completely into linear factors in E[x].

**Existence and Uniqueness of Splitting Fields**

**Existence:**

For any field F and non-constant polynomial f(x) in F[x], there exists a splitting field of f(x) over F.

Proof Sketch: We can construct a splitting field by iteratively adjoining roots of the polynomial. Starting with F, we adjoin one root at a time until all roots are included. The resulting field is the splitting field.

**Uniqueness:**

Splitting fields are unique up to isomorphism. That is, if $E_1$ and $E_2$ are two splitting fields of f(x) over F, then there exists an isomorphism $\varphi: E_1 \rightarrow E_2$ such that $\varphi(a) = a$ for all $a \in F$.

**Properties of Splitting Fields**

1. Degree Bound: If f(x) is a polynomial of degree n, then the degree of the splitting field extension [E:F] divides n!
2. Normality: A splitting field extension is always a normal extension.
3. Separability: If f(x) is separable (has no repeated roots in its splitting field), then the splitting field extension is a Galois extension.
4. Minimality: The splitting field is the smallest field extension that contains all the roots of the polynomial.

**Examples of Splitting Fields**

**Example 1: Splitting Field of $x^2 - 2$ over Q**

Notes

Consider the polynomial $f(x) = x^2 - 2$ over the rational numbers Q.

The roots of f(x) are $r_1 = \sqrt{2}$ and $r_2 = -\sqrt{2}$.

The splitting field of f(x) over Q is $E = Q(\sqrt{2})$, which is the field obtained by adjoining $\sqrt{2}$ to Q. Note that both roots are in this field since $-\sqrt{2}$ is also in $Q(\sqrt{2})$.

[E:Q] = 2, as the minimal polynomial of $\sqrt{2}$ over Q is $x^2 - 2$, which has degree 2.

**Example 2: Splitting Field of $x^3 - 2$ over Q**

Consider the polynomial $f(x) = x^3 - 2$ over Q.

The roots of f(x) are:

- $r_1 = \sqrt[3]{2}$ (the real cube root of 2)
- $r_2 = \omega \cdot \sqrt[3]{2}$, where $\omega$ is a primitive cube root of unity (e^(2πi/3))
- $r_3 = \omega^2 \cdot \sqrt[3]{2}$, where $\omega^2$ is the complex conjugate of $\omega$

The splitting field of f(x) over Q is $E = Q(\sqrt[3]{2}, \omega)$. This field contains all three roots of f(x).

[E:Q] = 6, as $[Q(\sqrt[3]{2}):Q] = 3$ and $[Q(\sqrt[3]{2}, \omega):Q(\sqrt[3]{2})] = 2$.

**Example 3: Splitting Field of $x^4 - 1$ over Q**

Consider the polynomial $f(x) = x^4 - 1$ over Q.

The roots of f(x) are:

- $r_1 = 1$
- $r_2 = -1$
- $r_3 = i$
- $r_4 = -i$

The splitting field of f(x) over Q is E = Q(i), which is the field of complex numbers with rational real and imaginary parts.

[E:Q] = 2, as the minimal polynomial of i over Q is $x^2 + 1$, which has degree 2.

**Example 4: Splitting Field of $x^p - 1$ over Q (p prime)**

For a prime number p, consider the polynomial $f(x) = x^p - 1$ over Q.

The roots of f(x) are:

- $r_1 = 1$
- $r_2 = \zeta$, where $\zeta$ is a primitive p-th root of unity ($e^{(2\pi i/p)}$)
- $r_3 = \zeta^2$
- ...
- $r_p = \zeta^{(p-1)}$

The splitting field of f(x) over Q is $E = Q(\zeta)$, which is the p-th cyclotomic field.

[E:Q] = p-1, as the minimal polynomial of $\zeta$ over Q is the p-th cyclotomic polynomial, which has degree p-1.

**Example 5: Splitting Field of $x^2 + 1$ over $F_3$**

Consider the polynomial $f(x) = x^2 + 1$ over the finite field $F_3$ (integers modulo 3).

We need to find the roots of $f(x) = x^2 + 1$ in some extension of $F_3$.

Let's check if there are any roots in $F_3$:

- $f(0) = 0^2 + 1 = 1 \neq 0$
- $f(1) = 1^2 + 1 = 2 \neq 0$
- $f(2) = 2^2 + 1 = 5 \equiv 2 \pmod 3 \neq 0$

So f(x) has no roots in $F_3$. We need to construct an extension field. Let $\alpha$ be a root of f(x), so $\alpha^2 = -1 \equiv 2 \pmod 3$.

Notes

The splitting field of f(x) over $F_3$ is $E = F_3(\alpha) = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$.

Actually, since $x^2 + 1$ is irreducible over $F_3$, we have $F_3(\alpha) \cong F_9$, the field with 9 elements.

The roots of f(x) in this extension are $\alpha$ and $2\alpha$ (since $(2\alpha)^2 = 4\alpha^2 = 4 \cdot 2 = 8 \equiv 2 \pmod 3$).

### 4.3.3: Properties of Splitting Fields

Splitting fields possess several important properties that make them central to field theory and Galois theory. In this section, we'll explore these properties in detail.

**Fundamental Properties of Splitting Fields**

**1. Minimality Property**

A splitting field E of a polynomial f(x) over a field F is the smallest field extension of F that contains all the roots of f(x).

Proof: Let E be a splitting field of f(x) over F, and let K be any field extension of F that contains all the roots of f(x). By definition, $E = F(r_1, r_2, ..., r_n)$, where $r_1, r_2, ..., r_n$ are all the roots of f(x). Since K contains all these roots, we have $E \subseteq K$.

**2. Uniqueness Property**

Splitting fields are unique up to isomorphism. If $E_1$ and $E_2$ are two splitting fields of a polynomial f(x) over F, then there exists an isomorphism $\varphi: E_1 \to E_2$ such that $\varphi(a) = a$ for all $a \in F$.

Proof Sketch: The proof uses the fact that if f(x) is irreducible over F and $\alpha_1$, $\alpha_2$ are roots of f(x) in extensions $E_1$ and $E_2$ respectively, then there exists an isomorphism from $F(\alpha_1)$ to $F(\alpha_2)$ that fixes F and maps $\alpha_1$ to $\alpha_2$. This can be extended to the full splitting fields by induction.

**3. Normality Property**

A field extension E/F is normal if and only if E is the splitting field of some polynomial (or set of polynomials) over F.

Definition: A field extension E/F is normal if every irreducible polynomial in F[x] that has one root in E has all its roots in E.

Proof: ($\Rightarrow$) If E/F is normal, then E is the splitting field of the set of minimal polynomials of all its elements. ($\Leftarrow$) If E is the splitting field of a polynomial f(x) over F, then by definition, all roots of f(x) are in E. For any irreducible factor g(x) of f(x), if one root of g(x) is in E, then all roots of g(x) are in E.

**4. Galois Extension Property**

If f(x) is a separable polynomial (has no repeated roots in its splitting field), then the splitting field E of f(x) over F is a Galois extension.

Definition: A field extension E/F is Galois if it is both normal and separable.

Proof: If f(x) is separable, then by definition, it has no repeated roots in its splitting field E. This means E/F is separable. Since E is a splitting field, it is also normal. Therefore, E/F is a Galois extension.

**Degree Properties of Splitting Fields**

**1. Degree Bound**

If f(x) is a polynomial of degree n over a field F, then the degree [E:F] of the splitting field E over F divides n!.

Proof Sketch: This follows from the fact that the Galois group of E/F, which has order [E:F], is a subgroup of the symmetric group $S_n$ on n letters (permuting the roots of f(x)). Since $|S_n| = n!$, we have [E:F] divides n!.

**2. Intermediate Extensions**

If E is the splitting field of f(x) over F, and K is an intermediate field ($F \subseteq K \subseteq E$), then E is also the splitting field of some polynomial over K.

Notes

Proof: Let $\{\alpha_1, \alpha_2, ..., \alpha_m\}$ be the elements of E that are not in K. Then $E = K(\alpha_1, \alpha_2, ..., \alpha_m)$. Let g(x) be the product of the minimal polynomials of each $\alpha_i$ over K. Then E is the splitting field of g(x) over K.

**Splitting Fields and Field Automorphisms**

**1. Automorphism Group**

If E is the splitting field of a polynomial f(x) over F, then the group of automorphisms of E that fix F (denoted Aut(E/F)) permutes the roots of f(x).

Proof: Let $\sigma \in$Aut(E/F) and let $\alpha$ be a root of f(x) in E. Then: $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$ So $\sigma(\alpha)$ is also a root of f(x).

**2. Fixed Field**

If E is the splitting field of a polynomial f(x) over F and G = Aut(E/F), then the fixed field of G in E is exactly F.

Definition: The fixed field of G is the set of all elements $e \in E$ such that $\sigma(e) = e$ for all $\sigma \in G$.

Proof: This is a consequence of the Fundamental Theorem of Galois Theory, which states that for a Galois extension, there is a one-to-one correspondence between subgroups of the Galois group and intermediate fields.

**Constructing Splitting Fields**

**1. Iterative Construction**

A splitting field can be constructed by iteratively adjoining roots of the polynomial.

**Procedure:**

1. Start with the base field F and the polynomial f(x).
2. Find an irreducible factor g(x) of f(x) over F.
3. Adjoin a root $\alpha$ of g(x) to create the field extension $F(\alpha)$.

4. Factor f(x) over F(α) and repeat the process until f(x) splits completely.

**2. Extension Degree Calculation**

The degree of the splitting field extension can be calculated from the degrees of the intermediate extensions.

Formula: If E is constructed as $F_0 = F$, $F_1 = F_0(\alpha_1)$, $F_2 = F_1(\alpha_2)$, ..., $F_n = E$, then: $[E:F] = [F_1:F_0] \cdot [F_2:F_1] \cdot ... \cdot [F_n:F_{n-1}]$

where each $[F_i:F_{i-1}]$ is the degree of the minimal polynomial of $\alpha_i$ over $F_{i-1}$.

**Applications of Splitting Fields**

**1. Solving Polynomial Equations**

Splitting fields provide the smallest field extension in which a polynomial equation can be solved completely.

**2. Galois Theory**

Splitting fields are central to Galois theory, which connects field theory with group theory and provides a framework for understanding polynomial equations.

**3. Finite Fields**

Every finite field is the splitting field of a polynomial of the form x^(p^n) - x over its prime subfield.

**4. Algebraic Closure**

The algebraic closure of a field F can be viewed as the splitting field of all polynomials in F[x].

**4.3.3: Applications of Field Automorphisms in Galois Theory**

Field automorphisms play a central role in Galois theory, providing the bridge between field extensions and group theory. This section explores the various applications of field automorphisms in Galois theory and their implications.

Notes

**The Fundamental Theorem of Galois Theory**

The Fundamental Theorem of Galois Theory establishes a correspondence between subgroups of the Galois group and intermediate fields of a Galois extension.

**Statement of the Theorem:**

Let E/F be a Galois extension with Galois group G = Gal(E/F). Then:

1. There is a one-to-one correspondence between the intermediate fields K ($F \subseteq K \subseteq E$) and the subgroups H of G.
    - For a subgroup $H \subseteq G$, the corresponding field is $K = E^H$ (the fixed field of H).
    - For an intermediate field K, the corresponding subgroup is H = Gal(E/K).
2. For any intermediate field K:
    - [E:K] = |Gal(E/K)|
    - [K:F] = [G:Gal(E/K)] = |G|/|Gal(E/K)|
3. K/F is a normal extension if and only if Gal(E/K) is a normal subgroup of G. In this case, $Gal(K/F) \cong G/Gal(E/K)$.

**Applications:**

1. Determining All Intermediate Fields: By finding all subgroups of the Galois group, we can identify all possible intermediate fields of a Galois extension.
2. Computing Extension Degrees: The order of a subgroup of the Galois group gives the degree of the extension E over the corresponding intermediate field.
3. Identifying Normal Extensions: An intermediate extension is normal if and only if the corresponding subgroup is normal in the Galois group.

### Cyclotomic Extensions

For the cyclotomic extension $Q(\zeta_n)/Q$, where $\zeta_n$ is a primitive n-th root of unity, the Galois group is isomorphic to $(Z/nZ)\times$, the multiplicative group of integers modulo n that are coprime to n.

Each automorphism $\sigma_k$ in $Gal(Q(\zeta_n)/Q)$ is determined by: $\sigma_k(\zeta_n) = \zeta_n^k$, where $gcd(k, n) = 1$

This allows us to understand the structure of cyclotomic extensions and solve problems related to cyclotomic polynomials.

### Quadratic Extensions

For a quadratic extension $Q(\sqrt{d})/Q$, where d is a square-free integer, the Galois group is isomorphic to Z/2Z (cyclic group of order 2).

The non-trivial automorphism $\sigma$ in $Gal(Q(\sqrt{d})/Q)$ is given by: $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$, for all $a, b \in Q$

This helps in understanding the structure of quadratic number fields and solving quadratic equations.

### Solvability by Radicals

One of the most celebrated applications of Galois theory is determining when a polynomial equation is solvable by radicals.

**Theorem (Abel-Ruffini):**

A polynomial equation is solvable by radicals if and only if its Galois group is solvable.

**Application:**

Field automorphisms allow us to determine the Galois group of a polynomial, which in turn tells us whether the polynomial is solvable by radicals.

For example:

- Polynomials of degree $\leq 4$ are always solvable by radicals because $S_4$ (the symmetric group on 4 letters) is solvable.
- The general polynomial of degree $\geq 5$ is not solvable by radicals because $S_5$ and higher symmetric groups are not solvable.

**Constructibility Problems in Geometry**

Field automorphisms help solve classical Greek constructibility problems.

**Theorem:**

A number is constructible with compass and straightedge if and only if it lies in a field extension of Q with degree a power of 2.

**Applications:**

1. Squaring the Circle: Impossible because $\pi$ is transcendental.
2. Doubling the Cube: Impossible because the cube root of 2 has minimal polynomial of degree 3.
3. Trisecting an Angle: Generally impossible because it leads to irreducible cubic equations.
4. Constructing Regular Polygons: A regular n-gon is constructible if and only if $n = 2^k p_1 p_2 ... p_m$, where $k \geq 0$ and each $p_i$ is a distinct Fermat prime (primes of the form $2^{2n} + 1$).

**Fixed Fields and the Invariant Theory**

Field automorphisms help identify elements that remain fixed under group actions.

**Theorem:**

If G is a finite group of automorphisms of a field E, then the fixed field $E^G$ has degree $[E:E^G] = |G|$.

**Applications:**

1. Symmetric Polynomials: The fixed field of $S_n$ acting on $Q(x_1, x_2, ..., x_n)$ is precisely $Q(e_1, e_2, ..., e_n)$, where $e_i$ are the elementary symmetric polynomials.

2. Invariant Theory: Field automorphisms help identify invariant elements under group actions, which has applications in representation theory and algebraic geometry.

**Finite Fields and the Frobenius Automorphism**

The Frobenius automorphism plays a special role in the theory of finite fields.

**Theorem:**

For a finite field $F_q$ with $q = p^n$ elements, the Galois group $Gal(F_q/F_p)$ is cyclic of order n, generated by the Frobenius automorphism $\Phi(x) = x^p$.

Applications:

1. Classification of Finite Fields: All finite fields of the same order are isomorphic, and for every prime power $q = p^n$, there exists a finite field with q elements.

2. Counting Solutions to Equations: Field automorphisms help count the number of solutions to equations over finite fields.

3. Error-Correcting Codes: Field automorphisms are used in the design and analysis of error-correcting codes based on finite fields.

**Kummer Theory and Cyclotomic Extensions**

Field automorphisms are central to Kummer theory, which studies abelian extensions.

**Kummer Theory:**

Notes

Let K be a field containing a primitive n-th root of unity, and let L/K be a Galois extension with $Gal(L/K) \cong (Z/nZ)^k$. Then $L = K(\alpha_1, \alpha_2, ..., \alpha_k)$, where $\alpha_i^n \in K$.

**Applications:**

1. Class Field Theory: Kummer theory is a key component of class field theory, which describes abelian extensions of number fields.
2. Reciprocity Laws: Field automorphisms help establish reciprocity laws in number theory, which describe when a number is an n-th power modulo another number.

**Solving Quintic Equations**

While the general quintic is not solvable by radicals, certain quintics are. Field automorphisms help identify such cases.

**Theorem:**

A quintic polynomial is solvable by radicals if and only if its Galois group is a solvable subgroup of $S_5$.

**Example:**

The polynomial $x^5 - x - 1$ has Galois group $S_5$, so it is not solvable by radicals. The polynomial $x^5 - 5x + 12$ has Galois group that is a solvable subgroup of $S_5$, so it is solvable by radicals.

**Solved Problems**

**Problem 1: Finding the Frobenius Automorphism in a Finite Field**

Problem: Consider the finite field $F_4 = F_2[x]/(x^2 + x + 1)$. Let $\alpha$ be a root of $x^2 + x + 1$ in $F_4$, so $F_4 = \{0, 1, \alpha, \alpha+1\}$. Find the action of the Frobenius automorphism $\Phi(x) = x^2$ on each element of $F_4$ and verify that $\Phi^2$ is the identity map.

**Solution:**

The Frobenius automorphism in a field of characteristic 2 maps x to $x^2$. Let's compute its action on each element of $F_4$:

1. $\Phi(0) = 0^2 = 0$
2. $\Phi(1) = 1^2 = 1$

To find $\Phi(\alpha)$, we use the fact that $\alpha$ satisfies $\alpha^2 + \alpha + 1 = 0$, which means $\alpha^2 = \alpha + 1$: 3. $\Phi(\alpha) = \alpha^2 = \alpha + 1$

To find $\Phi(\alpha + 1)$, we use the fact that in characteristic 2, $(a + b)^2 = a^2 + b^2$: 4. $\Phi(\alpha + 1) = (\alpha + 1)^2 = \alpha^2 + 1^2 = (\alpha + 1) + 1 = \alpha$

Now, let's verify that $\Phi^2$ is the identity map:

- $\Phi^2(0) = \Phi(\Phi(0)) = \Phi(0) = 0$
- $\Phi^2(1) = \Phi(\Phi(1)) = \Phi(1) = 1$
- $\Phi^2(\alpha) = \Phi(\Phi(\alpha)) = \Phi(\alpha + 1) = \alpha$
- $\Phi^2(\alpha + 1) = \Phi(\Phi(\alpha + 1)) = \Phi(\alpha) = \alpha + 1$

Indeed, $\Phi^2$ maps each element to itself, confirming that $\Phi^2$ is the identity automorphism. This aligns with the theory, as $[F_4:F_2] = 2$, so the Frobenius automorphism has order 2.

**Problem 2: Finding the Splitting Field of a Polynomial**

Problem: Find the splitting field of $f(x) = x^3 - 2$ over Q and determine its degree over Q.

**Solution:**

Step 1: Find the roots of $f(x) = x^3 - 2$. The roots are:

- $r_1 = \sqrt[3]{2}$ (the real cube root of 2)
- $r_2 = \omega \cdot \sqrt[3]{2}$, where $\omega = e^{(2\pi i/3)}$ is a primitive cube root of unity
- $r_3 = \omega^2 \cdot \sqrt[3]{2}$, where $\omega^2 = e^{(4\pi i/3)}$ is the complex conjugate of $\omega$

Notes

Step 2: Determine the splitting field. The splitting field E must contain all three roots, so E = $Q(\sqrt[3]{2}, \omega)$.

Step 3: Calculate the degree of the extension. First, let's determine $[Q(\sqrt[3]{2}):Q]$. The minimal polynomial of $\sqrt[3]{2}$ over Q is $x^3 - 2$, which has degree 3. Therefore, $[Q(\sqrt[3]{2}):Q] = 3$.

Next, let's determine $[Q(\sqrt[3]{2}, \omega):Q(\sqrt[3]{2})]$. The minimal polynomial of ω over Q is $x^2 + x + 1$, which remains irreducible over $Q(\sqrt[3]{2})$ (this can be proven, but we'll take it as given). Therefore, $[Q(\sqrt[3]{2}, \omega):Q(\sqrt[3]{2})] = 2$.

By the multiplicativity of extension degrees: $[E:Q] = [Q(\sqrt[3]{2}, \omega):Q] = [Q(\sqrt[3]{2}, \omega):Q(\sqrt[3]{2})] \times [Q(\sqrt[3]{2}):Q] = 2 \times 3 = 6$

Therefore, the splitting field of $x^3 - 2$ over Q is $Q(\sqrt[3]{2}, \omega)$, and it has degree 6 over Q.

**Problem 3: Determining Galois Groups Using Automorphisms**

Problem: Determine the Galois group of the splitting field of $f(x) = x^4 - 2$ over Q.

**Solution:**

Step 1: Find the roots of $f(x) = x^4 - 2$. The roots are:

- $r_1 = \sqrt[4]{2}$ (the real fourth root of 2)
- $r_2 = -\sqrt[4]{2}$
- $r_3 = i \cdot \sqrt[4]{2}$
- $r_4 = -i \cdot \sqrt[4]{2}$

Step 2: Identify the splitting field. The splitting field E must contain all four roots, so E = $Q(\sqrt[4]{2}, i)$.

Step 3: Calculate the degree of the extension. The minimal polynomial of $\sqrt[4]{2}$ over Q is $x^4 - 2$, which has degree 4, so $[Q(\sqrt[4]{2}):Q] = 4$.

The minimal polynomial of i over $Q(\sqrt[4]{2})$ is $x^2 + 1$, which remains irreducible over $Q(\sqrt[4]{2})$ (this can be proven, but we'll take it as given). Therefore, $[Q(\sqrt[4]{2}, i):Q(\sqrt[4]{2})] = 2$.

By the multiplicativity of extension degrees: $[E:Q] = [Q(\sqrt[4]{2}, i):Q] = [Q(\sqrt[4]{2}, i):Q(\sqrt[4]{2})] \times [Q(\sqrt[4]{2}):Q] = 2 \times 4 = 8$

Step 4: Determine the Galois group. Since $[E:Q] = 8$, the Galois group $G = Gal(E/Q)$ has order 8.

To identify which group of order 8 it is, we need to understand how the automorphisms act on the generators of E.

Any automorphism $\sigma \in G$ must map $\sqrt[4]{2}$ to another root of $x^4 - 2$, namely $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\cdot\sqrt[4]{2}$, or $-i\cdot\sqrt[4]{2}$. Similarly, $\sigma$ must map i to either i or -i.

Let's define the following automorphisms:

- $\sigma: \sqrt[4]{2} \mapsto i\cdot\sqrt[4]{2}$, $i \mapsto i$
- $\tau: \sqrt[4]{2} \mapsto \sqrt[4]{2}$, $i \mapsto -i$

We can verify that:

- $\sigma^4 = id$ (the identity automorphism)
- $\tau^2 = id$
- $\tau\sigma\tau = \sigma^{-1}$

This means that $G = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$

**Multiple Choice Questions (MCQs)**

1. **A field automorphism is:**
   a) A function that maps a field onto another field
   b) An isomorphism from a field to itself
   c) A mapping that preserves addition but not multiplication
   d) None of the above

Notes

2. **A conjugation isomorphism occurs when:**
   a) Two fields have the same number of elements
   b) One field is the fixed field of an automorphism
   c) Elements of one field are mapped to their conjugates in an extension
   d) None of the above

3. **The set of elements in a field that remain unchanged by all automorphisms forms:**
   a) A subgroup
   b) A fixed field
   c) An ideal
   d) None of the above

4. **The Frobenius automorphism is defined for:**
   a) All fields
   b) Only finite fields
   c) Only real fields
   d) None of the above

5. **A splitting field of a polynomial is:**
   a) The smallest field where the polynomial factors completely
   b) Any extension field containing the roots of the polynomial
   c) A finite field with a prime number of elements
   d) None of the above

6. **Which of the following statements about splitting fields is true?**
   a) Splitting fields are always unique up to isomorphism.
   b) Splitting fields exist only for irreducible polynomials.
   c) Every polynomial has a unique splitting field over any base field.
   d) None of the above.

7. **A field automorphism must preserve:**
   a) Only addition

b) Only multiplication

c) Both addition and multiplication

d) Neither addition nor multiplication

8. **The study of field automorphisms is crucial for:**

a) Ring theory

b) Group theory

c) Galois theory

d) None of the above

**Short Answer Questions**

1. Define a field automorphism and give an example.
2. What is a conjugation isomorphism? Provide an example.
3. Explain the concept of a fixed field and its significance.
4. State and explain the Frobenius automorphism.
5. How does the Frobenius automorphism act in finite fields?
6. Define a splitting field and explain its importance in field theory.
7. Why are splitting fields unique up to isomorphism?
8. How do automorphisms relate to Galois groups?
9. What is the significance of automorphisms in the classification of field extensions?
10. Give an example of a field extension where the automorphism group is nontrivial.

**Long Answer Questions**

1. Explain the concept of field automorphisms and their importance in algebra.
2. Discuss conjugation isomorphisms with detailed examples.

Notes

3. Define and explain the role of fixed fields in automorphism groups.
4. Prove that the Frobenius automorphism is a valid field automorphism in finite fields.
5. Explain the construction of splitting fields and their significance in field theory.
6. Discuss the relationship between field automorphisms and Galois theory.
7. How do splitting fields help in solving polynomial equations? Provide examples.
8. Discuss the role of automorphisms in the classification of field extensions.
9. What is the importance of field automorphisms in modern algebra and cryptography?

Answer Key MCQ :

1. b
2. c
3. b
4. b
5. a
6. a
7. c
8. c

**UNIT 5.1**

## SEPARABLE EXTENSIONS AND GALOIS THEORY

**Objectives**

- Understand the concept of separable extensions and their properties.
- Learn about normal extensions and their significance.
- Explore the main theorem of Galois theory and its implications.
- Study the relationship between field extensions and Galois groups.
- Analyze symmetric functions and their role in Galois theory.

### 5.1.1: Introduction to Separable Extensions

Separable extensions are a fundamental concept in field theory, representing an important class of field extensions with special properties. These extensions are characterized by certain behaviors of their minimal polynomials and have significant implications for the structure of field extensions.

**Basic Concepts and Definitions**

A field extension E/F is the situation where F is a subfield of E. We denote this as E/F, which is read as "E over F." The field E is called the extension field, and F is the base field.When considering field extensions, we often look at elements of E and examine how they relate to the base field F. An element $\alpha \in E$ is called algebraic over F if there exists a non-zero polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$. The monic polynomial of minimal degree that has $\alpha$ as a root is called the minimal polynomial of $\alpha$ over F, denoted by $\min F(\alpha)$.

**Separable Elements**

Notes

An algebraic element $\alpha \in E$ is called separable over F if its minimal polynomial minF(α) has no repeated roots in any extension field where it splits completely.Equivalently, an algebraic element α is separable over F if and only if the derivative of its minimal polynomial is not the zero polynomial. This can be expressed as:

α is separable over F if and only if minF(α)' ≠ 0

For fields of characteristic 0 (like $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$), this condition is always satisfied, so every algebraic element is separable. However, for fields of characteristic p > 0, there exist polynomials whose derivatives are zero, specifically those of the form f(x^p).

**Separable Extensions**

A field extension E/F is called separable if every element of E is separable over F. More precisely:

- A finite extension E/F is separable if every element of E is separable over F.
- An arbitrary extension E/F is separable if every finite subextension is separable.

If $E = F(\alpha)$ for some $\alpha \in E$, then E/F is separable if and only if α is separable over F.

**Properties of Separable Extensions**

1. Transitivity: If E/K and K/F are separable extensions, then E/F is also a separable extension.
2. Tower Property: If E/F is a field extension and K is an intermediate field ($F \subseteq K \subseteq E$), then E/F is separable if and only if both E/K and K/F are separable.
3. Compositum of Separable Extensions: If $E_1/F$ and $E_2/F$ are separable extensions, then their compositum $E_1E_2/F$ is also separable.

4. Relation to Perfect Fields: A field F is called perfect if every algebraic extension of F is separable. All fields of characteristic 0 are perfect, as are all finite fields.

### 5.1.2: Importance in Galois Theory

Separable extensions play a crucial role in Galois theory. The fundamental theorem of Galois theory establishes a correspondence between intermediate fields of a Galois extension and subgroups of its Galois group. For this correspondence to work, the extension must be separable (along with being normal and finite).A field extension E/F is Galois if and only if it is finite, separable, and normal. The separability condition ensures that the Galois group has the expected structure and that the correspondence between subgroups and intermediate fields is well-behaved.

**Examples of Separable and Non-Separable Extensions**

**Example 1: Separable Extension**

The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is separable because the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$, which has distinct roots $\pm\sqrt{2}$ in $\mathbb{C}$.

**Example 2: Non-Separable Extension**

Let F = Fp(t) be the field of rational functions over the finite field Fp, where p is a prime number. The polynomial f(x) = x^p - t has derivative f'(x) = px^(p-1) = 0 in characteristic p. This polynomial is irreducible over F, and thus it is the minimal polynomial of any of its roots. Since its derivative is zero, any extension generated by a root of this polynomial is non-separable.

### 5.1.3: Definition and Properties of Separable Polynomials

Separable polynomials form the backbone of separable field extensions. Their properties are integral to understanding how field extensions behave, especially in Galois theory.

**Definition of Separable Polynomials**

Notes

A polynomial $f(x) \in F[x]$ is called separable if it has no repeated roots in any extension field where it splits completely. Equivalently, a polynomial $f(x)$ is separable if and only if $f(x)$ and its formal derivative $f'(x)$ are relatively prime, i.e., $\gcd(f(x), f'(x)) = 1$.

For an irreducible polynomial, being separable means that when it factors into linear terms in some extension field, all its roots are distinct.

**Characterization in Terms of Derivative**

If F is a field and $f(x) \in F[x]$ is a polynomial, then:

1. If $\text{char}(F) = 0$, then $f(x)$ is separable if and only if $f(x)$ does not have repeated roots.
2. If $\text{char}(F) = p > 0$, then $f(x)$ is separable if and only if $f(x)$ is not of the form $g(x^p)$ for any polynomial $g(x) \in F[x]$.

The derivative test provides a practical way to check separability: compute $f'(x)$ and then find $\gcd(f(x), f'(x))$. If the gcd is 1, then $f(x)$ is separable.

Properties of Separable Polynomials

1. Product Rule: If $f(x)$ and $g(x)$ are separable polynomials in $F[x]$, then their product $f(x)g(x)$ is separable if and only if $f(x)$ and $g(x)$ are relatively prime.
2. Irreducible Case: If $f(x)$ is irreducible over F, then $f(x)$ is separable if and only if $f'(x) \neq 0$.
3. Field Extension: If $f(x) \in F[x]$ is separable and K/F is any field extension, then $f(x)$ remains separable when viewed as a polynomial in $K[x]$.
4. Characteristic Zero: In fields of characteristic 0, every irreducible polynomial is separable.

5. Finite Fields: In finite fields, a polynomial is separable if and only if it has no repeated roots.

**The Separable Degree**

For a finite extension E/F, the separable degree [E:F]s is defined as the maximum number of F-embeddings of E into an algebraic closure of F. For a separable extension, [E:F]s = [E:F], the ordinary degree of the extension.If E/F is not separable, then [E:F]s < [E:F], and the ratio [E:F]/[E:F]s is called the inseparable degree of the extension, denoted by [E:F]i.

**Separable Closure**

The separable closure Fs of a field F is the field obtained by adjoining to F all elements that are separable over F. It has the following properties:

1. Fs is algebraic over F.
2. Every element in Fs is separable over F.
3. If $\alpha$ is algebraic over F and separable, then $\alpha \in$ Fs.

The separable closure is important because it represents the largest separable extension of a field.

**5.1.4: Relation to Field Characteristics**

The behavior of separable polynomials is strongly influenced by the characteristic of the field:

1. Characteristic 0: All irreducible polynomials are separable, making all algebraic extensions separable.
2. Characteristic p > 0: A polynomial f(x) could have the form $g(x^p)$, making its derivative zero. Such polynomials are not separable.

**Discriminant of a Polynomial**

Notes

The discriminant of a polynomial provides another way to test for separability. For a monic polynomial $f(x) = \prod(x - \alpha i)$, the discriminant is defined as:

$\text{Disc}(f) = \prod(\alpha i - \alpha j)^2$

where the product is taken over all $i < j$.

A polynomial is separable if and only if its discriminant is non-zero.

**Examples of Separable and Non-Separable Polynomials**

**Example 1: Separable Polynomial**

In $\mathbb{Q}[x]$, the polynomial $f(x) = x^3 - 2$ is separable because its derivative $f'(x) = 3x^2$ is never zero for $x \neq 0$, and $\gcd(x^3 - 2, 3x^2) = 1$.

**Example 2: Non-Separable Polynomial**

In $F_2[x]$, the polynomial $f(x) = x^2 + 1 = (x + 1)^2$ has a repeated root ($1 + 1 = 0$ in $F_2$). Its derivative $f'(x) = 2x = 0$ in characteristic 2, confirming it's not separable.

**Example 3: Characteristic p > 0**

In $Fp(t)[x]$, the polynomial $f(x) = x^p - t$ is not separable because $f'(x) = px^{(p-1)} = 0$ in characteristic p.

### 5.2.1: Normal Extensions and Their Significance

Normal extensions, also called normal field extensions, are a critical concept in field theory and are especially important in Galois theory. They represent field extensions where all polynomials that have one root in the extension have all their roots in the extension.

**Definition of Normal Extensions**

A field extension E/F is called normal if every irreducible polynomial in F[x] that has at least one root in E completely splits in E (i.e., factors into linear terms in E[x]).

Equivalently, an extension E/F is normal if and only if E is the splitting field of some set of polynomials over F.

**Alternative Characterizations**

There are several equivalent ways to characterize normal extensions:

1. E/F is normal if and only if E is the splitting field of a family of polynomials in F[x].
2. E/F is normal if and only if the set of F-embeddings of E into an algebraic closure $\bar{F}$ that fix F pointwise is exactly the set of F-automorphisms of E.
3. For a finite extension E/F, E/F is normal if and only if E is fixed by every F-automorphism of its normal closure.
4. E/F is normal if and only if every F-embedding of E into an algebraic closure $\bar{F}$ that fixes F maps E onto itself.

Properties of Normal Extensions

1. Transitivity: If E/K and K/F are normal extensions, it does not necessarily follow that E/F is normal. However, if E/F is normal and K is an intermediate field, then E/K is normal.

2. Compositum of Normal Extensions: If $E_1/F$ and $E_2/F$ are normal extensions, then their compositum $E_1E_2/F$ is also normal.

3. Relation to Splitting Fields: A finite extension E/F is normal if and only if it is the splitting field of some polynomial in F[x].

4. Automorphism Group: If E/F is a normal extension, then the group of all F-automorphisms of E, denoted by Aut(E/F), has order dividing [E:F]. If E/F is also separable, then |Aut(E/F)| = [E:F].

### 5.2.2: Normal Closure

For any field extension E/F, there exists a field extension N/E such that N/F is normal and N is minimal with this property. This field N is called the normal closure of E over F.The normal closure can be constructed as the splitting field of the set of all minimal polynomials of elements in E over F.

### 5.2.3:Galois Extensions

A field extension E/F is called a Galois extension if it is both normal and separable. For Galois extensions, the Galois group Gal(E/F) = Aut(E/F) has special properties:

1. |Gal(E/F)| = [E:F], the degree of the extension.

2. There is a one-to-one correspondence between the intermediate fields of E/F and the subgroups of Gal(E/F).

3. If K is an intermediate field ($F \subseteq K \subseteq E$), then K corresponds to the subgroup Gal(E/K) of Gal(E/F), and [E:K] = |Gal(E/K)|.

### 5.2.4:Significance in Galois Theory

Normal extensions, especially when they are also separable (i.e., Galois extensions), are the cornerstone of Galois theory. The fundamental theorem of Galois theory establishes a correspondence between:

1. Intermediate fields of a Galois extension E/F.

2. Subgroups of the Galois group Gal(E/F).

This correspondence is order-reversing: if $K_1 \subseteq K_2$ are intermediate fields, then $Gal(E/K_1) \supseteq Gal(E/K_2)$.

Moreover, if K is an intermediate field and H = Gal(E/K) is the corresponding subgroup, then:

1. K is the fixed field of H: $K = E^H = \{a \in E \mid \sigma(a) = a \text{ for all } \sigma \in H\}$.
2. [K:F] = |Gal(E/F)|/|Gal(E/K)|.
3. K/F is normal if and only if H is a normal subgroup of Gal(E/F).

**Examples of Normal and Non-Normal Extensions**

**Example 1: Normal Extension**

The extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is normal because it is the splitting field of the polynomial $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$.

**Example 2: Non-Normal Extension**

The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$, which has roots $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$ (where $\omega$ is a primitive cube root of unity). Since $\omega\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$, the extension is not normal.

**Example 3: Normal Closure**

The normal closure of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega$ is a primitive cube root of unity. This field contains all roots of $x^3 - 2$.

**Solved Problems**

**Problem 1: Determine if the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is separable.**

Solution: To determine if $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is separable, we need to check if the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is separable.

Notes

Notes

The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $f(x) = x^2 - 2$.

The derivative of $f(x)$ is $f'(x) = 2x$.

Since $f'(x) \neq 0$ for $x \neq 0$, and $\sqrt{2} \neq 0$, we have $f'(\sqrt{2}) \neq 0$. This means that $f(x)$ and $f'(x)$ have no common roots, so $\gcd(f(x), f'(x)) = 1$.

Therefore, $f(x) = x^2 - 2$ is separable, which means that the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is separable.

Additionally, since $\mathbb{Q}$ has characteristic 0, all irreducible polynomials over $\mathbb{Q}$ are separable, providing another way to conclude that $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is separable.

**Problem 2: Show that the polynomial $f(x) = x^4 + x^2 + 1$ over $F_2$ is separable.**

Solution: To determine if $f(x) = x^4 + x^2 + 1$ is separable over $F_2$, we need to check if $f(x)$ and its derivative $f'(x)$ are relatively prime.

Computing the derivative: $f'(x) = 4x^3 + 2x = 0$ (in $F_2$)

Since the derivative is zero, we need a different approach.

In fields of characteristic $p > 0$, an irreducible polynomial is inseparable if and only if it is of the form g(x^p) for some polynomial g.

Let's check if $f(x)$ can be written as $g(x^2)$ for some polynomial g (since 2 is the characteristic of $F_2$): If $f(x) = g(x^2)$, then $g(y) = y^2 + y + 1$ where $y = x^2$.

Now we need to determine if $f(x)$ is irreducible over $F_2$. One way to check is to verify that $f(x)$ has no roots in $F_2$ and cannot be factored into two quadratics in $F_2[x]$.

The elements of $F_2$ are $\{0, 1\}$. $f(0) = 0^4 + 0^2 + 1 = 1 \neq 0$ $f(1) = 1^4 + 1^2 + 1 = 1 + 1 + 1 = 1$ (in $F_2$) $\neq 0$

So $f(x)$ has no roots in $F_2$.

Now we need to check if f(x) can be factored as a product of two quadratics. Any such factorization would be of the form: $f(x) = (x^2 + ax + b)(x^2 + cx + d)$

Expanding: $f(x) = x^4 + cx^3 + dx^2 + ax^3 + acx^2 + adx + bx^2 + bcx + bd = x^4 + (a+c)x^3 + (ac+b+d)x^2 + (ad+bc)x + bd$

For this to equal $x^4 + x^2 + 1$, we need: $a+c = 0$, which means $a = c$ in $F_2$ $ac+b+d = 1$ $ad+bc = 0$ $bd = 1$

From $a = c$, we get $ad+bc = ad+ba = a(d+b) = 0$, so $d = b$. From $bd = 1$, we get $b = d = 1$. But then $ac+b+d = a \cdot a+1+1 = a^2 + 0 = a^2 = 1$, which means $a = 1$.

However, if $a = c = 1$ and $b = d = 1$, then $a+c = 1+1 = 0$ in $F_2$, which satisfies our first equation. Let's verify: $(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + 1 = x^4 + 0 + 3x^2 + 2x + 1 = x^4 + x^2 + 0 + 1$ (in $F_2$) $= x^4 + x^2 + 1$

So $f(x) = (x^2 + x + 1)^2$, which means it's not irreducible and has repeated factors, making it inseparable over $F_2$.

Problem 3: Prove that if F is a field of characteristic 0, then every finite extension of F is separable.

Solution: Let F be a field of characteristic 0, and let E be a finite extension of F. We need to show that E/F is separable.

A field extension E/F is separable if and only if every element of E is separable over F. An element $\alpha \in E$ is separable over F if and only if its minimal polynomial $\text{min}_F(\alpha)$ has no repeated roots in its splitting field.

For any polynomial $f(x) \in F[x]$, the presence of repeated roots is equivalent to f(x) and its derivative f'(x) having a common factor, or equivalently, $\gcd(f(x), f'(x)) \neq 1$.

In a field of characteristic 0, the derivative of a non-constant polynomial is non-zero. Specifically, for an irreducible polynomial $p(x) \in F[x]$, its derivative p'(x) is non-zero.

Notes

Suppose p(x) has a repeated root α in some extension field. Then p(x) and p'(x) would have a common root α, which means that p(x) and p'(x) would have a common factor. But since p(x) is irreducible and p'(x) has lower degree than p(x), the only way they could have a common factor is if p'(x) is divisible by p(x), which is impossible due to degree considerations.

Therefore, in a field of characteristic 0, every irreducible polynomial is separable. Since E/F is a finite extension, E is generated by finitely many algebraic elements over F, each having an irreducible minimal polynomial over F. Since all these minimal polynomials are separable, every element of E is separable over F.

Hence, E/F is a separable extension.

Problem 4: Determine if the extension $F_2(t)(\alpha)/F_2(t)$ is normal, where α is a root of the polynomial $p(x) = x^2 - t$.

Solution: To determine if the extension $F_2(t)(\alpha)/F_2(t)$ is normal, we need to check if $p(x) = x^2 - t$ splits completely in $F_2(t)(\alpha)$.

The roots of $p(x) = x^2 - t$ are $\pm\sqrt{t}$. Let's denote $\alpha = \sqrt{t}$, so the roots are α and -α.

In $F_2$, we have $1 + 1 = 0$, which means $-1 = 1$. Therefore, $-\alpha = \alpha$ in characteristic 2.

So in $F_2(t)(\alpha)$, the polynomial $p(x) = x^2 - t = (x - \alpha)(x - (-\alpha)) = (x - \alpha)(x - \alpha) = (x - \alpha)^2$.

This means that p(x) has only one distinct root, α, with multiplicity 2. Since p(x) doesn't split into distinct linear factors in $F_2(t)(\alpha)$, the extension $F_2(t)(\alpha)/F_2(t)$ is not normal.

Alternatively, we can approach this from the definition: an extension E/F is normal if and only if it is the splitting field of some set of polynomials over F. In this case, $F_2(t)(\alpha)$ is not the splitting field of $x^2 - t$ over $F_2(t)$ (or any other set of polynomials), because it doesn't contain all the roots of $x^2 - t$ in an algebraic closure.

In characteristic 2, the splitting field of $x^2 - t$ would be $F_2(t)(\sqrt{t}) = F_2(t)(\alpha)$, which is the same as our extension. However, the issue is that $x^2 - t = (x - \alpha)^2$ in characteristic 2, so it doesn't split into distinct linear factors.

Therefore, $F_2(t)(\alpha)/F_2(t)$ is not a normal extension.

**Problem 5: Prove that if E/F is a Galois extension, then |Gal(E/F)| = [E:F].**

Solution: Let E/F be a Galois extension, which means E/F is both normal and separable.

First, let's recall that for any field extension E/F, the order of the automorphism group Aut(E/F) is at most [E:F]. This is because if $\alpha_1$, $\alpha_2$, ..., $\alpha_n$ is a basis for E over F, then any F-automorphism of E is uniquely determined by where it sends $\alpha_1$, $\alpha_2$, ..., $\alpha_n$.

For a Galois extension, we want to show that |Gal(E/F)| = [E:F], where Gal(E/F) = Aut(E/F) is the Galois group of E over F.

Since E/F is a finite, normal, and separable extension, it is the splitting field of a separable polynomial $f(x) \in F[x]$. Let's say f(x) has degree n and has distinct roots $\alpha_1$, $\alpha_2$, ..., $\alpha_n$ in E.

Any F-automorphism $\sigma$ of E must permute the roots of f(x), because if $f(\alpha_i) = 0$, then $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = \sigma(0) = 0$. Therefore, $\sigma(\alpha_i)$ is also a root of f(x).

Since E is generated over F by the roots of f(x), an F-automorphism of E is completely determined by how it permutes these roots. There are at most n! ways to permute n elements, but not all permutations of the roots give rise to automorphisms of E.

For a separable extension, the number of F-embeddings of E into an algebraic closure of F is exactly [E:F]. Since E/F is normal, any such embedding maps E to itself, so it's an automorphism in Gal(E/F).

Therefore, |Gal(E/F)| = [E:F].

Notes

Alternatively, we can use the Primitive Element Theorem, which states that since E/F is a finite separable extension, $E = F(\alpha)$ for some $\alpha \in E$. Let p(x) be the minimal polynomial of $\alpha$ over F. Since E/F is normal, p(x) splits completely in E.

Let the distinct roots of p(x) in E be $\alpha = \alpha_1, \alpha_2, ..., \alpha_n$, where $n = [E:F]$ is the degree of p(x). For each root $\alpha_i$, there is a unique F-isomorphism $\sigma_i : F(\alpha) \to F(\alpha_i)$ that fixes F and maps $\alpha$ to $\alpha_i$. Since E/F is normal, $F(\alpha_i) \subseteq E$, and since $[F(\alpha_i):F] = [F(\alpha):F] = [E:F]$, we must have $F(\alpha_i) = E$.

Thus, each $\sigma_i$ is an F-automorphism of E, and these are all the F-automorphisms of E. There are exactly $n = [E:F]$ of them, one for each root of p(x).

Therefore, $|Gal(E/F)| = [E:F]$.

**Unsolved Problems**

**Problem 1:**

Determine whether the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is separable. Justify your answer.

**Problem 2:**

Consider the polynomial $f(x) = x^4 + x^2 + x + 1 \in F_2[x]$. Determine whether f(x) is separable over $F_2$.

**Problem 3:**

Let F be a field of characteristic $p > 0$, and let $E = F(\alpha)$ where $\alpha$^p $\in F$ but $\alpha \notin F$. Prove that E/F is not a separable extension.

**Problem 4:**

Let E/F be a finite extension with $[E:F] = n$. Prove that E/F is a Galois extension if and only if $|Aut(E/F)| = n$.

**Problem 5:**

Let K = $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and F = $\mathbb{Q}$. Determine the Galois group Gal(K/F) and list all intermediate fields between F and K, establishing the Galois correspondence.

### 5.2.5: Introduction to Galois Theory

Galois theory stands as one of the most elegant achievements in mathematics, providing a deep connection between field theory, group theory, and the solvability of polynomial equations. Named after Évariste Galois, a brilliant French mathematician who died at the young age of 20 in 1832, this theory emerged from his groundbreaking work on determining which polynomial equations are solvable by radicals.

#### Historical Context

The journey toward Galois theory began with the quest to find formulas for solving polynomial equations. By the 16th century, mathematicians had discovered formulas for solving quadratic, cubic, and quartic equations using radicals (expressions involving addition, subtraction, multiplication, division, and root extraction). However, the general quintic equation (degree 5) resisted similar approaches.

In the early 19th century, mathematicians like Paolo Ruffini and Niels Henrik Abel proved that there is no general formula using radicals for solving polynomial equations of degree 5 or higher. Galois took this work further by developing a systematic approach to determine which specific equations are solvable by radicals and which are not.

#### Field Extensions

At the heart of Galois theory lies the concept of field extensions. Let's start with some fundamental definitions:

Definition (Field): A field is a set with two operations, addition and multiplication, that satisfy the usual arithmetic properties (associativity, commutativity, distributivity, existence of identity elements and inverses).

Definition (Field Extension): If F and K are fields and $F \subseteq K$, we say K is an extension field of F, denoted K/F.

The notation [K:F] represents the degree of the extension, which is the dimension of K as a vector space over F. If [K:F] is finite, we call K/F a finite extension.

Consider a polynomial p(x) with coefficients in a field F. We're often interested in finding a field extension K of F where p(x) splits completely into linear factors. This leads to the concept of splitting fields.

Definition (Splitting Field): A splitting field of a polynomial p(x) over F is the smallest field extension of F in which p(x) factors completely into linear factors.

Example: The splitting field of $p(x) = x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$, which is obtained by adjoining $\sqrt{2}$ to $\mathbb{Q}$.

### 5.2.6: Algebraic Elements and Extensions

Definition (Algebraic Element): An element $\alpha$ in a field extension K/F is algebraic over F if there exists a non-zero polynomial p(x) in F[x] such that $p(\alpha) = 0$.

Definition (Algebraic Extension): A field extension K/F is algebraic if every element of K is algebraic over F.

For any algebraic element $\alpha$ over F, there exists a unique monic irreducible polynomial in F[x] having $\alpha$ as a root. This polynomial is called the minimal polynomial of $\alpha$ over F.

### Field Automorphisms and Fixed Fields

Definition (Field Automorphism): A field automorphism of a field K is an isomorphism from K to itself. The set of all automorphisms of K forms a group under composition, denoted Aut(K).

Given a field extension K/F, we're particularly interested in automorphisms that fix F pointwise:

Definition (F-automorphism): An F-automorphism of K is a field automorphism σ of K such that σ(a) = a for all a in F. The set of all F-automorphisms of K forms a group, denoted Aut(K/F).

Definition (Fixed Field): Given a group G of automorphisms of a field K, the fixed field of G is the set of all elements in K that are fixed by every automorphism in G, denoted K^G = {a ∈ K | σ(a) = a for all σ ∈ G}.

These concepts form the foundation for the Galois correspondence, which we'll explore in the next section.

### 5.2.7: The Main Theorem of Galois Theory

The central achievement of Galois theory is establishing a correspondence between subgroups of the Galois group and intermediate fields of a field extension. Before stating the main theorem, we need to define Galois extensions.

#### Galois Extensions

Definition (Galois Extension): A field extension K/F is Galois if it is:

1. Algebraic
2. Normal: Every irreducible polynomial in F[x] that has one root in K splits completely in K
3. Separable: Every irreducible polynomial in F[x] with a root in K has distinct roots

For fields of characteristic 0 (like $\mathbb{Q}$), separability is automatic, so a Galois extension is simply a normal algebraic extension.

Definition (Galois Group): The Galois group of a Galois extension K/F, denoted Gal(K/F), is the group of all F-automorphisms of K.

#### The Fundamental Theorem of Galois Theory

Theorem (Fundamental Theorem of Galois Theory): Let K/F be a finite Galois extension with Galois group G = Gal(K/F). Then:

Notes

1. There is a one-to-one correspondence between the intermediate fields E ($F \subseteq E \subseteq K$) and the subgroups H of G given by:

- For each intermediate field E, the corresponding subgroup is $H = Gal(K/E)$
- For each subgroup H of G, the corresponding intermediate field is $E = K^H$ (the fixed field of H)

2. **Under this correspondence:**

- If $E_1 \subseteq E_2$, then $Gal(K/E_2) \subseteq Gal(K/E_1)$
- If $H_1 \subseteq H_2$, then $K^{H_2} \subseteq K^{H_1}$

3. **For each intermediate field E:**

- $[K:E] = |Gal(K/E)|$
- $[E:F] = [G:Gal(K/E)]$

4. **An intermediate field E is Galois over F if and only if Gal(K/E) is a normal subgroup of G. In this case, $Gal(E/F) \cong G/Gal(K/E)$.**

This theorem establishes a beautiful "upside-down" correspondence between intermediate fields and subgroups of the Galois group.

**Normal Subgroups and Solvability**

A key application of Galois theory is determining which polynomial equations are solvable by radicals.

Definition (Solvable Group): A group G is solvable if it has a subnormal series $G = G_0 \supset G_1 \supset ... \supset G_n = \{e\}$ such that each quotient group $G_i/G_{i+1}$ is abelian.

Theorem (Solvability by Radicals): A polynomial equation is solvable by radicals if and only if its Galois group is a solvable group.

This provides a powerful criterion for determining whether a polynomial equation can be solved using radicals, connecting abstract group theory to the classical problem of solving equations.

### 5.2.8: Galois Groups and Their Applications

The Galois group of a polynomial encodes crucial information about its roots and solvability. Let's explore how to compute Galois groups and apply this knowledge.

**Computing Galois Groups**

For a polynomial p(x) of degree n, the Galois group is a subgroup of the symmetric group $S_n$ (the group of permutations of n objects). Here are some approaches to determine the Galois group:

1. Factorization Method: Factor the polynomial over successive field extensions and track how the roots combine.
2. Discriminant Analysis: The discriminant of a polynomial provides information about the Galois group. For a quadratic $ax^2 + bx + c$, the discriminant is $b^2 - 4ac$. For higher degrees, the formula becomes more complex.
3. Resolvent Polynomials: Construct polynomials whose factorization pattern reveals information about the Galois group.

**Galois Groups of Cyclotomic Extensions**

Cyclotomic fields are among the most important examples in Galois theory.

Definition (Cyclotomic Field): The nth cyclotomic field is $\mathbb{Q}(\zeta_n)$, where $\zeta_n$ is a primitive nth root of unity (e.g., $e^{(2\pi i/n)}$).

Theorem: The Galois group $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$, the multiplicative group of integers modulo n that are coprime to n.

This isomorphism is given by $\sigma_k(\zeta_n) = \zeta_n^k$ where gcd(k,n) = 1.

Notes

### 5.2.9: Extension by Radicals

A key application of Galois theory is understanding extensions by radicals.

Definition (Radical Extension): A field extension K/F is a radical extension if there exists a tower of fields $F = F_0 \subset F_1 \subset ... \subset F_k = K$ where for each i, $F_i = F_{i-1}(\alpha_i)$ with $\alpha_i^{n_i} \in F_{i-1}$ for some integer $n_i > 0$.

Theorem: Let p(x) be an irreducible polynomial over a field F of characteristic 0. Then the roots of p(x) can be expressed using radicals if and only if the Galois group of p(x) is solvable.

This theorem provides the definitive answer to the ancient question of which polynomial equations can be solved by radicals.

**Insolvable Quintic Equations**

The general quintic equation is not solvable by radicals because the symmetric group $S_5$ is not solvable. However, not all quintic equations are unsolvable.

Example: The polynomial $x^5 - x - 1$ has Galois group $S_5$, making it unsolvable by radicals.

Example: The polynomial $x^5 - 5x + 12$ has a Galois group that is solvable, making it solvable by radicals.

**Field Extensions and Constructibility**

Galois theory also connects to classical geometric problems like constructibility with straightedge and compass.

Theorem: A number $\alpha$ is constructible with straightedge and compass if and only if there exists a tower of field extensions $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_k$ with $\alpha \in F_k$ and $[F_i:F_{i-1}] = 2$ for each i.

This provides a conclusive answer to ancient problems like doubling the cube, trisecting an angle, and squaring the circle.

### 5.2.10: Examples and Applications of Galois Theory

Let's explore concrete examples and applications of Galois theory to illustrate its power and elegance.

**Example 1: The Galois Group of $x^3 - 2$**

Consider the polynomial $p(x) = x^3 - 2$ over $\mathbb{Q}$.

The roots of this polynomial are $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega\sqrt[3]{2}$, and $\alpha_3 = \omega^2\sqrt[3]{2}$, where $\omega$ is a primitive cube root of unity.

The splitting field of $p(x)$ is $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. The elements of $Gal(K/\mathbb{Q})$ are determined by how they permute the roots of $p(x)$.

There are 6 possible automorphisms:

- $\sigma_1$: Identity mapping
- $\sigma_2$: Maps $\sqrt[3]{2} \to \omega\sqrt[3]{2}$, $\omega \to \omega$
- $\sigma_3$: Maps $\sqrt[3]{2} \to \omega^2\sqrt[3]{2}$, $\omega \to \omega$
- $\sigma_4$: Maps $\sqrt[3]{2} \to \sqrt[3]{2}$, $\omega \to \omega^2$
- $\sigma_5$: Maps $\sqrt[3]{2} \to \omega\sqrt[3]{2}$, $\omega \to \omega^2$
- $\sigma_6$: Maps $\sqrt[3]{2} \to \omega^2\sqrt[3]{2}$, $\omega \to \omega^2$

The Galois group is isomorphic to $S_3$, the symmetric group on 3 elements, which has order 6.

Since $S_3$ is solvable, the equation $x^3 - 2 = 0$ is solvable by radicals (which we already know since the solution is $\sqrt[3]{2}$).

**Example 2: Cyclotomic Extensions**

The cyclotomic polynomial $\Phi_n(x)$ is the monic polynomial whose roots are the primitive nth roots of unity. For instance:

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = x + 1$

Notes

- $\Phi_3(x) = x^2 + x + 1$
- $\Phi_4(x) = x^2 + 1$

For a prime p, $\Phi_p(x) = x^{(p-1)} + x^{(p-2)} + ... + x + 1$.

Let's consider $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$. The Galois group of this polynomial over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/5\mathbb{Z})^*$, which is a cyclic group of order 4, generated by the residue class of 2 or 3 modulo 5.

The intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_5)$ correspond to the subgroups of $(\mathbb{Z}/5\mathbb{Z})$. *Since $(\mathbb{Z}/5\mathbb{Z})$* has a unique subgroup of order 2, there is exactly one intermediate field, which is $\mathbb{Q}(\sqrt{5})$.

**Example 3: The Insolvability of the General Quintic**

To prove that the general quintic equation is not solvable by radicals, we need to show that the symmetric group $S_5$ is not solvable.A group is solvable if and only if its derived series terminates in the trivial subgroup. The derived subgroup of $S_5$ is $A_5$, the alternating group on 5 elements. The derived subgroup of $A_5$ is $A_5$ itself, which means $A_5$ is a perfect group. Therefore, $S_5$ is not solvable.This implies that there exist quintic equations that cannot be solved by radicals. One such example is $x^5 - x - 1 = 0$, whose Galois group over $\mathbb{Q}$ is $S_5$.

**Application: Impossibility of Certain Geometric Constructions**

Galois theory provides elegant proofs for the impossibility of certain classical geometric constructions:

1. Doubling the Cube: This requires constructing $\sqrt[3]{2}$. Since the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$, which has degree 3, and 3 is not a power of 2, $\sqrt[3]{2}$ is not constructible.
2. Trisecting an Arbitrary Angle: Trisecting a 60° angle leads to the equation $4x^3 - 3x = \cos(20°)$, which can be transformed into an irreducible cubic. Since the degree is 3, which is not a power of 2, this construction is impossible.

3. Squaring the Circle: This requires constructing $\pi$, which is transcendental (not algebraic). Since all constructible numbers are algebraic, this construction is impossible.

### 5.2.11: Application: Insolvability of the Quintic

The insolvability of the general quintic equation was a profound result that ended centuries of attempts to find a radical formula. Galois theory not only proved the impossibility but also provided criteria to determine which specific quintic equations are solvable.

For instance, if a quintic polynomial has exactly one real root and four complex roots, its Galois group must be either $S_5$ or $A_5$, making it potentially unsolvable by radicals.

**UNIT 5.3**

### 5.3.1: Symmetric Functions in Galois Theory

Symmetric functions of the roots of a polynomial play a crucial role in Galois theory, providing a bridge between the coefficients of the polynomial and its roots.

**Elementary Symmetric Polynomials**

Let $x_1, x_2, ..., x_n$ be variables. The elementary symmetric polynomials are defined as:

$e_1(x_1, ..., x_n) = x_1 + x_2 + ... + x_n$ $e_2(x_1, ..., x_n) = x_1x_2 + x_1x_3 + ... + x_{n-1}x_n$ $e_3(x_1, ..., x_n) = x_1x_2x_3 + x_1x_2x_4 + ... + x_{n-2}x_{n-1}x_n$ ... $e_n(x_1, ..., x_n) = x_1x_2...x_n$

For a monic polynomial $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ with roots $\alpha_1, \alpha_2, ..., \alpha_n$, the coefficients are related to the elementary symmetric polynomials by:

$a_0 = (-1)^n e_n(\alpha_1, ..., \alpha_n)$ $a_1 = (-1)^{n-1} e_{n-1}(\alpha_1, ..., \alpha_n)$ ... $a_{n-1} = -e_1(\alpha_1, ..., \alpha_n)$

**The Fundamental Theorem of Symmetric Polynomials**

Theorem (Fundamental Theorem of Symmetric Polynomials): Any symmetric polynomial in $x_1, x_2, ..., x_n$ can be expressed uniquely as a polynomial in the elementary symmetric polynomials $e_1, e_2, ..., e_n$.

This theorem is crucial in Galois theory because it tells us that if $f(x_1, ..., x_n)$ is a symmetric polynomial with coefficients in a field F, and if $\alpha_1, ..., \alpha_n$ are the roots of a polynomial in F[x], then $f(\alpha_1, ..., \alpha_n)$ is an element of F.

**Symmetric Functions and Resolvents**

Resolvent polynomials are constructed using symmetric functions to gather information about the Galois group of a polynomial.

For instance, if p(x) is a polynomial with roots $\alpha_1, ..., \alpha_n$, we can form the resolvent polynomial:

$r(x) = \prod(x - f(\sigma(\alpha_1), ..., \sigma(\alpha_n)))$ Notes

Where the product is taken over all σ in a particular coset of a subgroup of $S_n$, and f is a carefully chosen function.

The factorization pattern of r(x) can reveal information about the Galois group of p(x).

**Lagrange Resolvents**

A particular type of resolvent used in solving equations is the Lagrange resolvent.

For a polynomial of degree n, the Lagrange resolvent is defined as:

$\theta = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3 + ... + \zeta^{n-1}\alpha_n$

Where ζ is a primitive nth root of unity.

For the cubic equation $x^3 + px + q = 0$ with roots $\alpha_1$, $\alpha_2$, $\alpha_3$, the Lagrange resolvents are:

$\theta_1 = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$ $\theta_2 = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3$

Where ω is a primitive cube root of unity.

These resolvents satisfy a quadratic equation, which is the key to the classical solution of the cubic.

**5.3.2: Application of Galois Theory in Solving Polynomial Equations**

Galois theory provides a framework for understanding which polynomial equations are solvable by radicals and how to solve them when possible.

**Solving Quadratic Equations**

The quadratic formula $x = (-b \pm \sqrt{(b^2 - 4ac)})/2a$ for solving $ax^2 + bx + c = 0$ involves taking a square root. The Galois group of a general quadratic polynomial over $\mathbb{Q}$ is $S_2$, which is abelian and therefore solvable.

**Solving Cubic Equations**

Notes

For the general cubic equation $x^3 + px + q = 0$ (after removing the $x^2$ term), the classical solution method involves:

1. Setting $x = u + v$
2. Imposing the condition that $3uv + p = 0$
3. Solving the resulting system, which leads to $u^3$ and $v^3$ being the roots of the quadratic equation $z^2 + qz - (p/3)^3 = 0$
4. Finding u and v by taking cube roots
5. Computing $x = u + v$

The Galois group of a general cubic over $\mathbb{Q}$ is $S_3$, which is solvable but not abelian. The solution requires nested radicals.

**Solving Quartic Equations**

The general quartic equation $x^4 + px^3 + qx^2 + rx + s = 0$ can be solved by:

1. Removing the $x^3$ term by substitution
2. Factoring the resulting expression as a product of two quadratics
3. This factorization leads to a cubic equation (the "resolvent cubic")
4. Solving the resolvent cubic yields the coefficients of the quadratic factors
5. Solving the two quadratics

The Galois group of a general quartic is $S_4$, which is solvable.

**The Unsolvable Quintic**

The general quintic equation $x^5 + px^4 + qx^3 + rx^2 + sx + t = 0$ cannot be solved by radicals because its Galois group is $S_5$, which is not solvable.

However, some special quintic equations have Galois groups that are solvable subgroups of $S_5$, making them solvable by radicals.

**Solving Equations Using Galois Theory**

Here's a general approach to solving polynomial equations using Galois theory:

1. Determine the Galois group of the polynomial.
2. If the Galois group is not solvable, the equation cannot be solved by radicals.
3. If the Galois group is solvable, analyze its structure to construct a sequence of radical extensions.
4. Use this sequence to express the roots in terms of radicals.

This approach generalizes the classical solution methods for quadratics, cubics, and quartics, placing them within a unified theoretical framework.

**Solved Problems**

**Problem 1: Find the Galois group of $x^4 - 2$ over $\mathbb{Q}$.**

**Solution:**

The polynomial $p(x) = x^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with prime $p = 2$.

The roots of $p(x)$ are $\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = i\sqrt[4]{2}$, $\alpha_3 = -\sqrt[4]{2}$, and $\alpha_4 = -i\sqrt[4]{2}$.

The splitting field is $K = \mathbb{Q}(\sqrt[4]{2}, i)$. Let's determine the automorphisms of $K$ that fix $\mathbb{Q}$.

Any automorphism $\sigma$ in $Gal(K/\mathbb{Q})$ is determined by its action on $\sqrt[4]{2}$ and $i$:

- $\sigma(\sqrt[4]{2})$ must be a root of $x^4 - 2$, so $\sigma(\sqrt[4]{2}) \in \{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$
- $\sigma(i)$ must be a root of $x^2 + 1$, so $\sigma(i) \in \{i, -i\}$

Notes

This gives us 8 possible automorphisms:

1. $\sigma_1$: $\sigma_1(\sqrt[4]{2}) = \sqrt[4]{2}$, $\sigma_1(i) = i$ (identity)
2. $\sigma_2$: $\sigma_2(\sqrt[4]{2}) = i\sqrt[4]{2}$, $\sigma_2(i) = i$
3. $\sigma_3$: $\sigma_3(\sqrt[4]{2}) = -\sqrt[4]{2}$, $\sigma_3(i) = i$
4. $\sigma_4$: $\sigma_4(\sqrt[4]{2}) = -i\sqrt[4]{2}$, $\sigma_4(i) = i$
5. $\sigma_5$: $\sigma_5(\sqrt[4]{2}) = \sqrt[4]{2}$, $\sigma_5(i) = -i$
6. $\sigma_6$: $\sigma_6(\sqrt[4]{2}) = i\sqrt[4]{2}$, $\sigma_6(i) = -i$
7. $\sigma_7$: $\sigma_7(\sqrt[4]{2}) = -\sqrt[4]{2}$, $\sigma_7(i) = -i$
8. $\sigma_8$: $\sigma_8(\sqrt[4]{2}) = -i\sqrt[4]{2}$, $\sigma_8(i) = -i$

We can verify that these are all valid automorphisms and that they form a group under composition.

If we examine the structure, we can show that:

- $\sigma_2^4 = \sigma_1$ (identity)
- $\sigma_5^2 = \sigma_1$
- $\sigma_2\sigma_5 = \sigma_6$, $\sigma_5\sigma_2 = \sigma_6\sigma_3$
- This means $\sigma_2\sigma_5 \neq \sigma_5\sigma_2$

Analyzing the group structure reveals that Gal(K/$\mathbb{Q}$) is isomorphic to $D_4$, the dihedral group of order 8, which is the group of symmetries of a square.

Since $D_4$ is solvable, the equation $x^4 - 2 = 0$ is solvable by radicals (which we already know since the solution is $\sqrt[4]{2}$).

**Problem 2: Determine which of the following field extensions are Galois over $\mathbb{Q}$:**

(a) $\mathbb{Q}(\sqrt{2})$ (b) $\mathbb{Q}(\sqrt[3]{2})$ (c) $\mathbb{Q}(i, \sqrt{2})$

**Solution:**

Notes

(a) $\mathbb{Q}(\sqrt{2})$ The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $p(x) = x^2 - 2$. This polynomial has roots $\sqrt{2}$ and $-\sqrt{2}$, both of which are in $\mathbb{Q}(\sqrt{2})$. Therefore, $p(x)$ splits completely in $\mathbb{Q}(\sqrt{2})$. Since we're working in characteristic 0, separability is automatic. Thus, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a Galois extension.

The Galois group $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ consists of two automorphisms:

- The identity automorphism $\sigma_1(\sqrt{2}) = \sqrt{2}$
- The non-identity automorphism $\sigma_2(\sqrt{2}) = -\sqrt{2}$ This group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

(b) $\mathbb{Q}(\sqrt[3]{2})$ The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $p(x) = x^3 - 2$. This polynomial has roots $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$, where $\omega$ is a primitive cube root of unity. Only one of these roots, $\sqrt[3]{2}$, is in $\mathbb{Q}(\sqrt[3]{2})$. Since $p(x)$ doesn't split completely in $\mathbb{Q}(\sqrt[3]{2})$, this extension is not normal. Therefore, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a Galois extension.

(c) $\mathbb{Q}(i, \sqrt{2})$ Let's consider the minimal polynomials of $i$ and $\sqrt{2}$ over $\mathbb{Q}$:

- For $i$, the minimal polynomial is $x^2 + 1$, with roots $i$ and $-i$.
- For $\sqrt{2}$, the minimal polynomial is $x^2 - 2$, with roots $\sqrt{2}$ and $-\sqrt{2}$.

Both of these polynomials split completely in $\mathbb{Q}(i, \sqrt{2})$. Any irreducible polynomial over $\mathbb{Q}$ that has a root in $\mathbb{Q}(i, \sqrt{2})$ must be a factor of one of these minimal polynomials or a combination of them. Since we're working in characteristic 0, separability is automatic. Therefore, $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ is a Galois extension.

The Galois group $\text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$ has four automorphisms:

- $\sigma_1$: $\sigma_1(i) = i$, $\sigma_1(\sqrt{2}) = \sqrt{2}$ (identity)
- $\sigma_2$: $\sigma_2(i) = -i$, $\sigma_2(\sqrt{2}) = \sqrt{2}$
- $\sigma_3$: $\sigma_3(i) = i$, $\sigma_3(\sqrt{2}) = -\sqrt{2}$
- $\sigma_4$: $\sigma_4(i) = -i$, $\sigma_4(\sqrt{2}) = -\sqrt{2}$

Notes

This group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**Problem 3: Use Galois theory to prove that cos(2π/7) is not constructible with straightedge and compass.**

**Solution:**

A number is constructible with straightedge and compass if and only if it can be obtained from the rational numbers by a sequence of field extensions of degree 2.

Let's consider ζ = e^(2πi/7), a primitive 7th root of unity. We know that: cos(2π/7) = (ζ + ζ⁻¹)/2

So cos(2π/7) is constructible if and only if ζ + ζ⁻¹ is constructible.

The minimal polynomial of ζ over $\mathbb{Q}$ is the 7th cyclotomic polynomial: $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

The Galois group of $\Phi_7(x)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^*$, the multiplicative group of integers modulo 7 that are coprime to 7. This group has order 6 and is cyclic, generated by the residue class of 3 modulo 7.

The element ζ + ζ⁻¹ is fixed by the complex conjugation automorphism, which corresponds to the element of order 2 in $(\mathbb{Z}/7\mathbb{Z})^*$. This is the automorphism that maps ζ to ζ⁻¹.

The fixed field of this automorphism is $\mathbb{Q}(\zeta + \zeta^{-1})$. The degree of this extension over $\mathbb{Q}$ is: $[\mathbb{Q}(\zeta):\mathbb{Q}] / [\mathbb{Q}(\zeta):\mathbb{Q}(\zeta + \zeta^{-1})] = 6/2 = 3$

So $[\mathbb{Q}(\zeta + \zeta^{-1}):\mathbb{Q}] = 3$.

Since 3 is not a power of 2, the number cos(2π/7) is not constructible with straightedge and compass.

**Multiple Choice Questions (MCQs)**

1. **A field extension E/F is separable if:**
   a) Every element of E is a root of a separable polynomial over F.
   b) Every polynomial in F[x] has a multiple root.

c) EEE contains an algebraically closed subfield.

d) None of the above.

2. **A polynomial is separable if:**

   a) It has a repeated root.

   b) It has distinct roots in its splitting field.

   c) It is irreducible over its base field.

   d) None of the above.

3. **A field extension is normal if:**

   a) Every element of the larger field, splits completely within the field itself.
   b) Irreducible Polynomial
   c) Some element of the larger field, splits completely within the field itself

4. in the base field has all its roots in the extension.

   b) The extension field is algebraically closed.

   c)T he extension is transcendental.

   d) None of the above.

5. **The main theorem of Galois theory establishes a correspondence between:**

   a) Normal extensions and separable extensions.

   b) Subgroups of the Galois group and intermediate fields.

   c) Rings and groups.

   d) None of the above.

6. **The Galois group of a field extension E/F consists of:**

   a)A ll automorphisms of F.

   b) All automorphisms of EEE that fix F.

   c)A ll isomorphisms between EEE and F.

   d) None of the above.

7. **The order of a Galois group is equal to:**

   a)T he number of elements in the field extension.

   b) The degree of the field extension.

   c)T he number of distinct roots of the minimal polynomial.

   d) None of the above.

8. **The splitting field of a polynomial is:**
   a) The largest field containing at least one root of the polynomial.
   b) The smallest field where the polynomial factors completely into linear factors.
   c) Always infinite.
   d) None of the above.

9. **A polynomial equation is solvable by radicals if:**
   a) Its Galois group is abelian.
   b) It has at least one real root.
   c) It is reducible over its base field.
   d) None of the above.

10. **The symmetric group Sn appears in Galois theory as:**
    a) The Galois group of the general polynomial of degree n.
    b) A subgroup of the additive group of the field.
    c) The automorphism group of the field of rational functions.
    d) None of the above.

11. **Which of the following is true about Galois extensions?**
    a) Every finite field extension is a Galois extension.
    b) Every normal and separable extension is Galois.
    c) Every field extension is separable.
    d) None of the above.

**Short Answer Questions**

1. Define a separable polynomial and give an example.
2. What is a normal extension? Provide an example.
3. State the main theorem of Galois theory.
4. What is a Galois group, and how is it related to field extensions?
5. Define a splitting field and explain its significance.

6. How do symmetric functions relate to Galois theory?
7. Explain why a polynomial is solvable by radicals if its Galois group is abelian.
8. What is the significance of normal and separable extensions in Galois theory?
9. Define a cyclic extension and give an example.
10. Explain the relationship between subgroups of the Galois group and intermediate fields.

**Long Answer Questions**

1. Discuss in detail the concept of separable extensions with examples.
2. Explain normal extensions and their role in field theory.
3. Prove and explain the main theorem of Galois theory.
4. How does Galois theory help in solving polynomial equations? Give examples.
5. Explain the significance of the Galois group in the classification of field extensions.
6. How do splitting fields contribute to Galois theory? Provide a detailed explanation.
7. Discuss the connection between symmetric functions and Galois theory.
8. Describe the structure of the Galois group of a polynomial and its significance.
9. Prove that a polynomial is solvable by radicals if and only if its Galois group is solvable.

Notes

10. Explain how Galois theory is applied in modern algebra and number theory.

Answer Key MCQ :

1. a

2. b

3. a

4. b

5. b

6. b

7. b

8. b

9. a

10. a

11. a

## References:


**Module 1: Group Theory**

1. Dummit, D. S., & Foote, R. M. (2004). *Abstract Algebra* (3rd ed.). John Wiley & Sons.
2. Lang, S. (2002). *Algebra* (3rd ed.). Springer.
3. Rotman, J. J. (2015). *Advanced Modern Algebra* (3rd ed.). American Mathematical Society.
4. Artin, M. (2010). *Algebra* (2nd ed.). Pearson.
5. Robinson, D. J. S. (1996). *A Course in the Theory of Groups* (2nd ed.). Springer.

**Module 2: Applications of the Sylow Theory and Ring Theory**

1. Hungerford, T. W. (2012). *Abstract Algebra: An Introduction* (3rd ed.). Cengage Learning.
2. Fraleigh, J. B. (2002). *A First Course in Abstract Algebra* (7th ed.). Addison-Wesley.
3. Gallian, J. A. (2016). *Contemporary Abstract Algebra* (9th ed.). Cengage Learning.
4. Jacobson, N. (2009). *Basic Algebra I* (2nd ed.). Dover Publications.
5. Herstein, I. N. (1999). *Abstract Algebra* (3rd ed.). Wiley.

**Module 3: Field Theory**

1. Morandi, P. (1996). *Field and Galois Theory*. Springer.
2. Roman, S. (2005). *Field Theory* (2nd ed.). Springer.
3. Stewart, I. (2015). *Galois Theory* (4th ed.). Chapman and Hall/CRC.
4. Lidl, R., & Niederreiter, H. (1996). *Finite Fields* (2nd ed.).
5. Cox, D. A. (2012). *Galois Theory* (2nd ed.). Wiley.

**Module 4: Automorphisms of Fields**

1. Kaplansky, I. (2001). *Fields and Rings* (2nd ed.). University of Chicago Press.
2. Rotman, J. J. (2010). *Galois Theory* (2nd ed.). Springer.
3. Weintraub, S. H. (2008). *Galois Theory* (2nd ed.). Springer.
4. Lang, S. (2005). *Undergraduate Algebra* (3rd ed.). Springer.

5. Isaacs, I. M. (2009). *Algebra: A Graduate Course* (2nd ed.). American Mathematical Society.

**Module 5: Separable Extensions and Galois Theory**

1. Garling, D. J. H. (2021). *A Course in Galois Theory*. Cambridge University Press.
2. Escofier, J. P. (2001). *Galois Theory*. Springer.
3. Artin, E. (2007). *Galois Theory*. Dover Publications.
4. Stillwell, J. (2016). *Elements of Mathematics: From Euclid to Gödel*. Princeton University Press.
5. Edwards, H. M. (1984). *Galois Theory*. Springer.

# MATS UNIVERSITY

## MATS CENTRE FOR DISTANCE AND ONLINE EDUCATION


**UNIVERSITY CAMPUS:** Aarang Kharora Highway, Aarang, Raipur, CG, 493 441

**RAIPUR CAMPUS:** MATS Tower, Pandri, Raipur, CG, 492 002

**T :** 0771 4078994, 95, 96, 98 **Toll Free ODL MODE :** 81520 79999, 81520 29999

**Website:** www.matsodl.com