SURESH GYAN VIHAR UNIVERSITY
Accredited by NAAC with 'A+' Grade

MASTER OF SCIENCES

(M.Sc.)

MMT-101

ABSTRACT ALGEBRA

Semester-I

Author-Dr. Anil kumar pal

SURESH GYAN VIHAR UNIVERSITY

Centre for Distance and Online Education,

Mahal Road, Jagatpura, Jaipur-302017

EDITORIAL BOARD (CDOE, SGVU)

Published by:

S. B. Prakashan Pvt. Ltd.

WZ-6, Lajwanti Garden, New Delhi: 110046

Tel.: (011) 28520627 | Ph.: 9205476295

Email: info@sbprakashan.com | Web.: www.sbprakashan.com

Designed & Graphic by : S. B. Prakashan Pvt. Ltd.

Printed at :

Suresh Gyanvihar University

Department of Mathematics

School of Science,

M.Sc., Mathematics - Syllabus – I year – I Semester (Distance Mode)

COURSE TITLE : ABSTRACT ALGEBRA

COURSE CODE : MMT-101

COURSE CREDIT : 4

COURSE OBJECTIVES

While studying the **ABSTRACT ALGEBRA**, the Learner shall be able to:

CO 1: Discuss the class equation and Cauchy's theorem

CO 2: Study about the relationship between a finite ablelian group and its sylow subgroups

CO 3: Represent content of the polynomial and greatest common divisor

CO 4: Discuss the fundamental theorem of Galois theory.

CO 5: Describe the solvable groups and commutator subgroups

COURSE LEARNING OUTCOMES

After completion of the **ABSTRACT ALGEBRA**, the Learner will be able to:

CLO 1: To enrich the knowledge to find the number of Sylow subgroups.

CLO 2: Describe the non isomorphic abelian groups and able to find the number of such non isomorphic abelian groups.

CLO 3: Enable to find the roots of a polynomial and splitting field, Galois group of the given polynomial

CLO 4: Demonstrate an understanding about Galois group of the given polynomial

CLO 5: Demonstrate an understanding to check whether the given polynomial is solvable by radicals or not

BLOCK I: SYLOW'S THEOREM

Another Counting Principle – 1st, 2nd and 3rd parts of Sylow's Theorems – double coset – the normalizer of a group.

BLOCK II : FINITE ABELIAN GROUPS

External and Internal direct Products – structure theorem for finite abelian groups – non iso-morphic abelian groups - polynomial rings.

BLOCK III : SPLITTING FIELD

Polynomials over rational fields – the Eisenstein criterion - extension fields – roots of polynomials – splitting fields.

BLOCK IV : GALOIS THEORY

More about roots – simple extension – separable extension – fixed fields – symmetric rational functions – normal extension - Galois group – fundamental theorem of Galois theory.

BLOCK V : SOLVABILITY BY RADICALS

Solvable group – the commutator subgroup – Solvability by radicals - finite fields- Wedderburn Theorem.

REFERENCE BOOKS :

1.I.N. Herstein, Topics in Algebra, 2nd Edition, John Wiley and Sons, New York, 1975.

UNIT	Chapter(s)	Sections
I	2	2.11 & 2.12
II	2 & 3	2.13, 2.14, 3.9
III	3 & 5	3.10, 5.1, 5.3
IV	5	5.5 & 5.6
V	5 & 7	5.7, 7.1

2. S. Lang, "*Algebra*", 3rd Edition, Addison-Wesley, Mass, 1993.

3. John B. Fraleigh, "*A First Course in Abstract Algebra*", Addison Wesley, Mass, 1982.

4. M. Artin, "*Algebra*", Prentice-Hall of India, New Delhi, 1991.

5. V. K. Khanna and S.K. Bhambri, "*A Course in Abstract Algebra*", Vikas Publishing House Pvt Limited, 1993.

Contents

Block 1 - UNIT 1

Advanced Group Theory

Objectives

- To recall basic concepts of sets and groups
- We try to learn about the relation conjugacy
- To study about Class equation
- Try to learn about Cauchy's Theorem

1.1 Basic Notions

Set theory is a proper framework for abstract mathematical thinking. A set is a well-defined collection of objects; that is, it is defined in such a manner that we can determine for any given object x whether or not x belongs to the set. The objects that belong to a set are called its elements or members. We will denote sets by capital letters, such as A or X ; if a is an element of the set A, we write $a \in A$.

Some of the more important sets that we will consider are the following:

$\mathbb{N} = \{n : n$ is a natural number $\} = \{1, 2, 3, \ldots\}$;

$\mathbb{W} = \{n : n \text{ non-negative integers } \} = \{0, 1, 2, 3, \ldots\}$;
$\mathbb{Z} = \{n : n \text{ is an integer } \} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$;
$\mathbb{Q} = \{r : r \text{ is a rational number } \} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z} \text{ where } q \neq 0 \right\}$;
$\mathbb{R} = \{x : x \text{ is a real number } \}$;
$\mathbb{C} = \{z : z \text{ is a complex number } \}$:

We can find various relations between sets as well as perform operations on sets. A set A is a subset of B, written $A \subset B$ or $B \supset A$ if every element of A is also an element of B.

Notice that $\{4, 5, 8\} \subset \{2, 3, 4, 5, 6, 7, 8, 9\}$ and $\mathbb{N} \subset \mathbb{W} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Trivially, every set is a subset of itself. A set B is a proper subset of a set A if $B \subset A$ but $B \neq A$. If atleast one element of A is not in B, we say that A is not a subset of B. For example, if $A = \{4, 7, 9\}$ and $B = \{2, 4, 5, 8, 9\}$, then A is not a subset of B .

Two sets are equal, written $A = B$, if we can show that $A \subset B$ and $B \subset A$. It is convenient to have a set with no elements in it. This set is called the empty set and is denoted by $\emptyset$. Note that the empty set is a subset of every set. To construct new sets out of old sets, we can perform certain operations: the union $A \cup B$ of two sets A and B is defined as

$$A \cup B = \{x : x \in A \text{ or } x \in B\};$$

the intersection of A and B is defined by

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

If $A = \{1, 3, 5\}$ and $B = \{1, 2, 3, 9\}$, then

$$A \cup B = \{1, 2, 3, 5, 9\}$$

and $A \cap B = \{1, 3\}$. When two sets have no elements in common, they are said to be disjoint; for example, if E is the set of even

integers and O is the set of odd integers, then E and O are disjoint. Two sets A and B are disjoint exactly when $A \cap B = \emptyset$. Sometimes we will work within one fixed set U, called the universal set. For any set $A \subset U$, we define the complement of A, denoted by A', to be the set $A' = \{x : x \in U \text{ and } x \notin A\}$. We define the difference of two sets A and B to be $A \backslash B = A \cap B' = \{x : x \in A$ and $x \notin B\}$:

Example 1.1.1. *Let* $\mathbb{R}$ *be the set real numbers and suppose that* $A = \{x \in \mathbb{R} : 0 < x \leq 3\}$ *and* $B = \{x \in \mathbb{R} : 2 \leq x < 4\}$.
Then

$$A \cap B = \{x \in \mathbb{R} : 2 \leq x \leq 3\}$$

$$A \cup B = \{x \in \mathbb{R} : 0 < x < 4\}$$

$$A \backslash B = \{x \in \mathbb{R} : 0 < x < 2\}$$

$$A' = \{x \in \mathbb{R} : x \leq 0 \text{ or } x > 3.$$

Cartesian Products and Mappings

Given sets A and B, we can define a new set $A \times B$, called the Cartesian product of A and B, as a set of ordered pairs. That is, $A \times B = \{(a,b) : a \in A \text{ and } b \in B\}$.

Example 1.1.2. *If* $A = \{x,y\}, B = \{1,2,3\}$, *and* $C = \emptyset$, *then* $A \times B$ *is the set*
$\{(x,1),(x,2),(x,3),(y,1),(y,2),(y,3)\}$ *and* $A \times C = \emptyset$.

We define the Cartesian product of n sets to be
$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_i \in A_i, 1 \leq i \leq n\}$.
Subsets of $A \times B$ are called relations. We will define a mapping or function $f \subset A \times B$ from a set A to a set B to be the special type of relation where $(a,b) \in f$ if for every element $a \in A$ there exists

a unique element $b \in B$. Another way of saying this is that for every element in A, f assigns a unique element in B. We usually write $f : A \to B$.

Instead of writing down ordered pairs $(a,b) \in A \times B$, we write $f(a) = b$. The set A is called the domain of f and $f(A) = \{f(a) : a \in A\} \subset B$ is called the range or image of f. We can think of the elements in the function's domain as input values and the elements in the function's range as output values.

A relation is well-defined if each element in the domain is assigned to a unique element in the range. If $f : A \to B$ is a map and the image of f is B, i.e., $f(A) = B$, then f is said to be *onto* or *surjective*. In other words, if there exists an $a \in A$ for each $b \in B$ such that $f(a) = b$, then f is onto. A map is *one-to-one* or *injective* if $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$. Equivalently, a function is one-to-one if $f(a_1) = f(a_2)$ implies $a_1 = a_2$. A map that is both *one-to-one* and *onto* is called *bijective*.

An ordered pair, denoted (x,y), is a pair of elements x and y in which x is considered to be the first coordinate and y the second coordinate. A *relation* is a set of ordered pairs. The following are examples of relations:

(i) $S = \{(1,1),(1,2),(3,4),(5,6)\}$

(ii) $T = \{(-3,5),(4,12),(5,12),(7,-6)\}$

Every relation determines two sets:

1. The set of all the first coordinates of the ordered pairs is called the domain.

2. The set of all the second coordinates of the ordered pairs is called the range.

For the above examples:

(i) domain of $S = \{1,3,5\}$, range of $S = \{1,2,4,6\}$

(ii) domain of $T = \{-3,4,5,7\}$, range of $T = \{5,12,-6\}$.

Some relations may be defined by a rule relating the elements in the domain to their corresponding elements in the range. In order to define the relation fully, we need to specify both the rule and the domain. For example, the set $\{(x,y) : y = x+1, x \in \{1,2,3,4\}\}$ is the relation $\{(1,2),(2,3),(3,4),(4,5)\}$.

The domain is the set $X = \{1,2,3,4\}$ and the range is the set $Y = \{2,3,4,5\}$.

A function is a relation such that for each $x-$value there is only one corresponding $y-$value. This means that, if (a,b) and (a,c) are ordered pairs of a function, then $b = c$. In other words, a function cannot contain two different ordered pairs with the same first coordinate.

Relations on Sets

An equivalence relation on a set X is a relation $R \subset X \times X$ such that

- $(x,x) \in R$ for all $x \in X$ (reflexive property)
- $(x,y) \in R$ implies $(y,x) \in R$ for all $x,y \in X$ (symmetric property)
- (x,y) and $(y,z) \in R$ imply $(x,z) \in R$ for all $x,y,z \in X$ (transitive property)

Given an equivalence relation R on a set X, we usually write $x \sim y$ instead of $(x,y) \in R$. Equivalence relations are very special.

Definition 1.1.1. *Let $\sim$ be an equivalence relation on a set X and let $a \in X$. Then $[a] = \{y \in X : y \sim a\}$ is called the equivalence class of a.*

Why are equivalence classes so interesting? We need another definition.

Definition 1.1.2. *Let S be a set, and let $\mathscr{T}$ be a set of nonempty subsets of S. We say that $\mathscr{T}$ is a partition of S if every $a \in S$ lies in exactly one set in $\mathscr{T}$.*
Alternatively, a partition $\mathscr{P}$ of a set X is a collection of nonempty sets $\{X_1, X_2, \ldots,\}$ such that $X_i \cap X_j = \emptyset$, for $i \neq j$ and $\bigcup_t X_t = X$.

What is the connection between these concepts? We will see that an equivalence relation gives rise to a partition via equivalence classes.

Theorem 1.1.1. *Let S be a set, and $\sim$ an equivalence relation on S. Then the equivalence classes with respect to $\sim$ form a partition of S. In particular, if $a \in S$, then $a \in [a]$ and, furthermore, $a \in [b]$ if and only if $[a] = [b]$.*

Conversely, whenever a partition of a set exists, there is some natural underlying equivalence relation, as we state in the following result.
Result: *If $\mathscr{P} = \{X_a\}$ is a partition of a set X, then there is an equivalence relation on X with equivalence classes X_a.*

Definition 1.1.3. *Let $n \geq 2$ be an integer. The set of integers modulo n, denoted $\mathbb{Z}_n$, is the set of all equivalence classes of Z with respect to the equivalence relation $a = b(\mod n)$.We call these the congruence classes modulo n. Specifically, $Z_n = \{[0], [1], [2], \ldots, [n-1]\}$.*

Example 1.1.3. *The elements of Z_4 are $[0], [1], [2]$ and $[3]$, where*
$[0] = \{\ldots, -, 8, -4, 0, 4, 8, \ldots\}$
$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$
$[2] = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$
$[3] = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$.

Some Basic Results in Number Theory:

(Well Ordering Principle): Every non-empty set of natural numbers contains a smallest element.

The well ordering principle is an axiom that agrees with the common sense of most people familiar with the natural numbers. An empty set does not contain a smallest member because it contains no members at all. As soon as we have a set of natural numbers with some members then we can order those members in the usual fashion. Having ordered them, one will be smallest. This intuition agreeing with this latter claim depends strongly on the fact the integers are whole numbers spaced out in increments of one.

The concept of divisibility plays a fundamental role in the theory of numbers. We say a nonzero integer t is a divisor of an integer s if there is an integer u such that $s = tu$. In this case, we write $t|s$ (read t divides s). When t is not a divisor of s, we write $t \nmid s$. A prime is a positive integer greater than 1 whose only positive divisors are 1 and itself. We say an integer s is a multiple of an integer t if there is an integer u such that $s = tu$. As our first application of the Well Ordering Principle, we establish a fundamental property of integers that we will use often.

Theorem 1.1.2. *(Division Algorithm:)*

Let m and n be integers with $n \neq 0$. Then there exist unique integers q and r with the property that $m = nq + r$, where $0 \leq r < n$.

Definition 1.1.4. *(Least Common Multiple:)*

The least common multiple of two nonzero integers x and y is the smallest positive integer that is a multiple of both x and y. We will denote this integer by $lcm(x,y)$.

Definition 1.1.5. *: (Greatest Common Divisor)*

The greatest common divisor of two nonzero integers x and y is

the largest of all common divisors of x and y. We denote this integer by $gcd(x,y)$.

Definition 1.1.6. *(Relatively Prime Integers)*
Let $x,y \in \mathbb{Z}$. Then x and y are relatively prime if $(x,y) = 1$.

Theorem 1.1.3. *(GCD is a Linear Combination:)*
For any nonzero integers x and y, there exist integers s and t such that $gcd(x,y) = xs + yt$. Moreover, $gcd(x,y)$ is the smallest positive integer of the form $xs + yt$.

Thus, the last theorem says that if some linear combination of x and y equals 1, then x and y are relatively prime.

Corollary 1.1.1. *If x and y are relatively prime, there exist integers s and t such that $xs + yt = 1$*

Lemma 1.1.1. *(Euclid's Lemma:)*
If p is a prime that divides xy, then p divides x or p divides y.

Note that Euclid's Lemma may fail when p is not a prime, since $4|(6 \cdot 2)$ but $4 \nmid 6$ and $4 \nmid 2$.

Theorem 1.1.4. *(Fundamental Theorem of Arithmetic:)*
Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear. That is, if $x = p_1 p_2 \cdots p_m$ and $x = q_1 q_2 \cdots q_n$, where the $p's$ and $q's$ are primes, then $p's$ m=n $p's$ and, after renumbering the $q's$, we have $p_i = q_i, \forall i$.

Definition 1.1.7. *(First Principle of Mathematical Induction:)*
Let S be a set of integers containing x. Suppose S has the property that whenever some integer $n \geq x$ belongs to S, then the integer $n+1$ also belongs to S. Then, S contains every integer greater than or equal to x.

Theorem 1.1.5. *Mathematical Induction I: Suppose that $P(n)$ is a proposition that it either true or false for any given natural numbers n. If*
(i) $P(0)$ is true and,
(ii) when $P(n)$ is true so is $P(n+1)$
Then we may deduce that $P(n)$ is true for any natural number.

Definition 1.1.8. *(Second Principle of Mathematical Induction:)*
Let S be a set of integers containing x. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to x belongs to S. Then, S contains every integer greater than or equal to x.

A nice problem on which to demonstrate mathematical induction is counting how many subsets a finite set has.

Theorem 1.1.6. *(Subset counting):*
A set S with n elements has 2^n subsets.

1.2 Group Theory

The theory of groups is the proper place to begin the study of abstract algebra. Group Theory occupies a central position in mathematics. Modern group theory arose from an attempt to find the roots of a polynomial in terms of its coefficients. Groups now play a central role in such areas as coding theory, counting, and the study of symmetries; many areas of biology, chemistry, and physics have benefited from group theory. In this section we give basic definitions and theorems which are familiar to us in the under graduate level itself.

Definitions and examples

Definition 1.2.1. *A binary operation $*$ on a set G is a mapping from $G \times G$ into G. That is, $* : G \times G \longrightarrow G$.*

Definition 1.2.2. *A group $(G,*)$ is a non-empty set G together with a binary operation on G satisfying the following properties.*

Closure: *For all $a,b \in G$, the element $a * b$ is a uniquely defined element in G.*

Associativity: *For all $a,b,c \in G$, we have*

$$a * (b * c) = (a * b) * c$$

Existence of Identity: *There exists an identity element $e \in G$ such that*

$$e * a = a * e = a, \ \forall a \in G.$$

Existence of Inverse: *For each $a \in G$, there exists an inverse element $a^{-1} \in G$ such that*

$$a * a^{-1} = e \text{ and } a^{-1} * a = e.$$

Definition 1.2.3. *If a group G satisfies commutative property, that is, $a * b = b * a$ for all $a,b \in G$, then it is called commutative group or abeliean group.*

Definition 1.2.4. *If a set G satisfies closure property alone then it is called a Groupoid.*

Definition 1.2.5. *If a set G satisfies closure property and associative property then it is called a Semigroup.*

Definition 1.2.6. *If a set G satisfies closure property, associative property and identity property then it is called a Monoid.*

Example 1.2.1. *The set of Natural numbers* $\mathbb{N}$ *is a groupoid with respect to (i) addition, and to (ii) multiplication.*

Example 1.2.2. *The set of integers* $\mathbb{Z}$ *is a groupoid with respect to subtraction .*

Example 1.2.3. *The set of Natural numbers* $\mathbb{N}$ *is not a groupoid with respect to subtraction.*

Example 1.2.4. *The set of Natural numbers* $\mathbb{N}$ *is a semigroup with respect to (i) addition, and also to (ii) multiplication.*

Example 1.2.5. *The set of integers* $\mathbb{Z}$ *is a groupoid with respect to subtraction, but not a semigroup with respect to subtraction.*

Example 1.2.6. *The set of non-negative integers* $\mathbb{W}$ *is a monoid with respect to (i) addition and also to (ii) multiplication.*

Example 1.2.7. *The set of integers* $\mathbb{Z}$ *is a monoid but not a group with respect to multiplication.*

Example 1.2.8. *The set of integers* $\mathbb{Z}$ *is a group with respect to addition.*

Example 1.2.9. *The set of rational numbers* $\mathbb{Q}$ *is a group with respect to addition.*

Definition 1.2.7. *The number of elements in a group* G *is called order of the group and this is denoted as* $o(G)$ *or* $|G|$ *. If this order is finite then the group is called a finite group.*

1.3 Another Counting Principle

We have studied an equivalence relation on a finite set, which measures the size of the equivalence classes under this relation, and then equates the number of elements in the set to the sum of

the orders of these equivalence classes. In this unit, we study for the relation conjugacy.

Definition 1.3.1. *Let G be a group. Let* $a, b \in G$. *The element* b *is said to be conjugate to* a *if there exists an element* $c \in G$ *such that* $b = cac^{-1}$. *This relation is called conjugacy relation and it is denoted by* $\sim$.

Theorem 1.3.1. *Conjugacy is an equivalence relation*

Proof. (i) Reflexive Property :

Let $a \in G$. Then $a = eae^{-1}$. Thus $a \sim a$.

(ii) Symmetric property :

Let $a \sim b$.Then $b = cac^{-1}$ for some $c \in G$.

That is, $c^{-1}b = ac^{-1}$ (premultiply by c^{-1})

$c^{-1}bc = a$ (post multiply by c)

$a = c^{-1}b(c^{-1})^{-1}$. Thus $b \sim a$. Hence symmetric property is true.

(iii) Transitivity property:

Let $a \sim b$ and $b \sim c$.

Then

$$a = xbx^{-1} \text{ for some } x \in G \tag{1.3.1}$$

and

$$b = ycy^{-1} \text{ for some } y \in G \tag{1.3.2}$$

Substituting (1.3.2) in (1.3.1) , we get,

$a = x(ycy^{-1})x^{-1} = (xy)c(y^{-1}x^{-1}) = (xy)c(xy)^{-1}$.

That is $a \sim c$. Hence transitivity property is true. ■

Definition 1.3.2. *Let* G *be a group and let* $a \in G$. *Then,*

$C(a) = \{x \in G | x = cac^{-1}$ *for some* $c \in G\}$.

This $C(a)$ *is called conjugate class of* a. *Let* c_a *be the number of elements of* $C(a)$. *The union of all the conjugate classes of*

elements of G is equal to the whole group G. Thus,

$$\bigcup_{a \in G} C(a) = G.$$

Definition 1.3.3. *Let G be a group and let $a \in G$, then normalizer of a in G is defined as follows.*

$N(a) = \{y \in G \mid ay = ya\}$

Lemma 1.3.1. *$N(a)$ is a subgroup of G.*

Proof. Let $x, y \in N(a)$. Then,

$x \in N(a) \Rightarrow ax = xa.$

$y \in N(a) \Rightarrow ay = ya.$

Claim : $xy \in N(a)$.

$a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$.

Hence $x, y \in N(a) \Rightarrow xy \in N(a)$. Thus closure is verified.

Claim : $x^{-1} \in N(a)$.

Let $x \in N(a) \Rightarrow ax = xa$.

$x^{-1}a = x^{-1}ae = x^{-1}a(xx^{-1}) = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = (x^{-1}x)ax^{-1}$

That is, $x^{-1}a = ax^{-1}$. Hence $x^{-1} \in N(a)$.

Hence $N(a)$ is a subgroup of G. ■

Note : By Lagrange's theorem, $\frac{o(G)}{o(N(a))}$ is a constant

Lemma 1.3.2. *Let G be a finite group and let $a \in G$. Let $N(a)$ be the normalizer of a in G and $C(a)$ be the conjugate class of a in G. That is the number of distinct elements conjugate to a in G is the index of $N(a)$ in G.*

Proof. By definitions,

$$\begin{aligned} C(a) &= \{b \in G | \, b = xax^{-1} \quad \text{for some } x \in G\} \\ C(a) &= \{xax^{-1}, \text{ for some } \quad x \in G\} \\ N(a) &= \{x \in G | \, ax = xa\} \end{aligned}$$

Let us define

$M = \{N(a).x | \, x \in G\}$

(i.e) M = {Set of all distinct cosets of N(a) in G }

Claim : $o(M) = o(C(a))$

Define a map $f : M \to C(a)$, such that

$f(N(a)x) = x^{-1}ax, \forall x \in G$

We will prove that f is well defined.

Let $N(a).x = N(a).y,$ for some $x, y \in G$

$\Rightarrow N(a).xy^{-1} = N(a)$

$\Rightarrow xy^{-1} \in N(a)$

$\Rightarrow a(xy^{-1}) = (xy^{-1})a$

Premultiply by x^{-1} and post multiply by y, we have

$x^{-1}a(xy^{-1})y = x^{-1}(xy^{-1})ay$

$i.e,\ x^{-1}ax(y^{-1}y) = (x^{-1}x)y^{-1}ay$

$i.e,\ x^{-1}ax = y^{-1}ay$

$f(N(a).x) = f(N(a).y), \forall x, y \in G$

Thus f is well defined.

By retracing these steps, we can prove that f is one-one.

Now let us prove f is onto.

For given, $x^{-1}ax \in C(a), \exists N(a).x \in M$ such that $f(N(a)x) = x^{-1}ax$.

Thus f is onto. Therefore, $o(M) = o(C(a))$

$$\begin{aligned} But,\ M &= \text{Set of all distinct cosets of } N(a) \text{ in } G \\ i.e,\ o(M) &= \frac{o(G)}{o(N(a))} \end{aligned}$$

$$\begin{aligned} Thus, o(M) &= o(C(a)) \\ o(C(a)) &= \frac{o(G)}{o(N(a))} \\ c_a &= \frac{o(G)}{o(N(a))} \cdots (1) \end{aligned}$$

Hence the lemma. ■

Theorem 1.3.2. *If $N(a)$ be the normalizer of a in G, then $o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$.*

Proof. We know that $G = \bigcup_{a \in G} C(a)$. But the number of elements of $C(a)$ is c_a.

Therefore by Lemma 1.3.2, we have

$$\begin{aligned} o(G) &= \sum_{a \in G} c_a \\ &= \sum_{a \in G} \frac{o(G)}{o(N(a))} \\ &= \sum_{a \in Z(G)} \frac{o(G)}{o(N(a))} + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))} \\ &= o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))} \end{aligned}$$

$$Thus,\ o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

■

This equation is called the class equation of a group G.

1.4 Cauchy's Theorem

In this section we prove Cauchy's Theorem on groups.

Theorem 1.4.1. *Let G be a group. If $p \mid o(G)$, where p is prime, then there exist an element $a \neq e$ in G such that $a^p = e$.*
(OR)
If $p \mid o(G)$, where p is prime, then G has an element of order p.

Proof. Let us prove this theorem by method of induction on $o(G)$.
Basis for induction:
Suppose $o(G) = 1$, then the theorem is obviously true.
Induction Assumption:
Assume that this theorem is true for all subgroups W, such that $o(W) < o(G)$.
If $p \mid o(W)$, then by induction assumption, there exist an element $a \in W$ such that $a^p = e$. Therefore let us assume that p does not divide the order of any proper subgroup of G. We know that Cauchy's theorem is true for abelian groups. Therefore, Now we will prove that G is abelian. That is, we will prove that $G = Z(G)$.
But we know that $Z(G) \subseteq G \cdots (1)$
We have to prove that $G \subseteq Z(G)$.
Suppose $a \in G$ but $a \notin Z(G)$. Consider the class equation,

$$o(G) = o(Z(G)) + \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$$

Since $a \notin Z(G)$ we have $N(a) \neq G$. Therefore, $p \nmid o(N(a))$.
But $p \mid o(G)$ and $p \nmid o(N(a))$.
So,

$$p \mid \frac{o(G)}{o(N(a))}$$

Therefore,

$$p \mid \sum_{N(a)\neq G} \frac{o(G)}{o(N(a))}$$

That is, $p \mid o(G)$ and

$$p \mid \sum_{N(a)\neq G} \frac{o(G)}{o(N(a))}$$

Therefore,

$$p \mid \left(o(G) - \sum_{N(a)\neq G} \frac{o(G)}{o(N(a))} \right)$$

That is, $p \mid o(Z(G))$, which is a contradiction.

Hence, $a \in G \Rightarrow a \in Z(G)$.

That is $G \subseteq Z(G) \cdots$ (2)

From (1) and (2), we have $G = Z(G)$. Thus G is abelian. Hence Cauchy's theorem is true for all groups. ■

Theorem 1.4.2. *The number of conjugate classes in S_n is $P(n)$, the number of partitions of n.*

Proof. Here S_n is a permutation group acting on n elements. We know that every permutation can be expressed as product of disjoint cycles. Let $\sigma \in S_n$. We say that σ has a cycle decomposition $\{n_1, n_2, \cdots, n_r\}$ if it can be written as the product of disjoint cycles of lengths $\{n_1, n_2, \cdots, n_r\}, n_1 \leq n_2 \leq \cdots \leq n_r$ and $n = n_1 + n_2 + \cdots + n_r$.

Claim: Two permutations in S_n are conjugate if and only if they have same type of cycle decomposition.

Let $\theta, \sigma \in S_n$. To compute $\theta^{-1}\sigma\theta$, replace every symbol in σ by its image under θ.

Let $\sigma, \tau \in S_n$ having same cycle decomposition. Let

$\sigma = (a_1, a_2, \cdots, a_{n_1})(b_1, b_2, \cdots, b_{n_2}) \cdots (x_1, x_2, \cdots, x_{n_r})$

and $\tau = (\alpha_1, \alpha_2, \cdots, \alpha_{n_1})(\beta_1, \beta_2, \cdots, \beta_{n_2})$

$$\cdots(\chi_1, \chi_2, \cdots, \chi_{n_r})$$

Then by taking θ as,

$$\theta = \begin{pmatrix} a_1\, a_2\, \cdots\, a_{n_1}\, b_1\, b_2\, \cdots\, b_{n_2} \cdots x_1\, x_2 : \cdots\, x_{n_r} \\ \alpha_1\, \alpha_2\, \cdots\, \alpha_{n_1}\, \beta_1\, \beta_2\, \cdots\, \beta_{n_2} \cdots \chi_1\, \chi_2\, \cdots\, \chi_{n_r} \end{pmatrix}$$

We can show that $\tau = \theta^{-1}\sigma\theta$. Here θ is called conjugating permutation. Thus, τ and σ are conjugate. This proves our claim. From the above claim, we observe that, the set of permutations having same cycle decomposition (conjugates to each other) gives one partition for n. Thus for one conjugate class in S_n we have one partition for n. So, the number of partitions for n is same as the number of conjugate classes in S_n. Hence the number of conjugate classes in $S_n = P(n)$. Hence the theorem. ■

Example 1.4.1. *Let* $\theta, \sigma, \tau \in S_n$.

$\sigma = (1\ 2)\,(3\ 4\ 5)\,(6\ 7\ 8\ 9)$

and $\tau = (2\ 6)\,(1\ 4\ 7)\,(3\ 5\ 9\ 8)$

Then, $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 6 & 1 & 4 & 7 & 3 & 5 & 9 & 8 \end{pmatrix}$

Clearly, $\theta^{-1}\sigma\theta = \tau$. *Here* σ *and* τ *are conjugate with conjugacy permutation* θ.

Let $\eta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 2 & 5 & 4 & 7 & 8 & 9 & 6 \end{pmatrix}$

Then, $\eta^{-1}\tau\eta = (3\ \ 7)\ \ (1\ \ 5\ \ 8)(2\ \ 4\ \ 6\ \ 7)$

Let $\alpha = (1)(2\ \ 3)(4\ \ 5)(6\ \ 7\ \ 8\ \ 9)$ *and*

$\beta = (2)(6\ \ 1)(4\ \ 7)(3\ \ 5\ \ 9\ \ 8)$.

Then, $\theta^{-1}\alpha\theta = (2)(6\ \ 1)(4\ \ 7)(3\ \ 5\ \ 9\ \ 8)$

$\gamma = (1\ \ 3)(2\ \ 4)(9\ \ 5\ \ 7)(8\ \ 6\ \ 9)$

$\delta = (1\ \ 4)(3\ \ 2)(5\ \ 8)(7\ \ 9\ \ 6)$

$\mu = (4\ \ 5)(6\ \ 7)(9\ \ 1)(3\ \ 2\ \ 8)$

$\lambda = (1\ \ 5)(1\ \ 2\ \ 3)(4\ \ 9)(8\ \ 6\ \ 7)$

Then $\tau^{-1}\gamma\tau = \mu$ *and* $\alpha^{-1}\delta\alpha = \lambda$ *.*

Therefore

$[\sigma] = \{\sigma, \tau, \cdots\}, \{2+3+4=9\}$

$[\alpha] = \{\alpha, \beta, \cdots\}, \{1+2+2+4=9\}$

$[\mu] = \{\mu, \lambda, \gamma, \delta, ...\}, \{2+2+2+3=9\}$

Thus each conjugate class in S_9 *gives one partition for 9. Therefore number of conjugate classes in* S_9 *is equal to* $P(9)$ *.*

Summary of this unit.

In this unit we have studied the following:

- Let G be a group. Let $a, b \in G$. The element b is said to be conjugate to a if there exists an element $c \in G$ such that $b = cac^{-1}$. This relation is called conjugacy relation and it is denoted by $\sim$.
- Conjugacy is an equivalence relation
- Class equation:

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

- Cauchy's Theorem: Let G be a group. If $p \mid o(G)$, where p is prime, then there exist an element $a \neq e$ in G such that $a^p = e$.

  (OR)

  If $p \mid o(G)$, where p is prime, then G has an element of order p.
- The number of conjugate classes in S_n is $P(n)$, the number of partitions of n.

Multiple Choice Questions

1. Two elements $a, b \in G$ are conjugate if $g \in G$ such that
   a) $b = gag$
   b) $b = g^{-1}ga$
   c) $b = gag^{-1}$
   d) $b = g^{-1}ag^{-1}$

2. Two Conjugate elements in G have
   a) No order
   b) Different order
   c) Same order
   d) prime order

3. The number of elements in a conjugacy class C_a of an element a in G is equal to
   a) Index of its normalizer in G
   b) Order of its normalizer in G
   c) Index of its Centralizer in G
   d) Order of its centralizer in G

4. No two distinct elements are conjugate in
   a) Abelian group
   b) Non-abelian group
   c) symmetric group
   d) Dihedral group

5. Conjugacy classes of D_4 are
   a) 1 b) 3 c. 5 d) 7

6. Conjugacy classes of S_3 are
   a) 0 b) 1 c) 2 d) 3

7. Cauchy's theorems deal with
   a) Abelian group's
   b) Non-abelian group's

c) Both

d) None of these

8. If A is a finite abelian group and p a prime divisor of the order of A, then A contains an element of order p is statement of

a) Lagrange's theorem

b) Cayley's theorem

c) Sylow's theorem

d) Cauchy's theorem

9. If a prime p divides the order of a group G then G contains a/an

a) Subgroup of order p

b) Group of order p

c) Element of order p

d) Generator of order p

Answers:

1	2	3	4	5	6	7	8	9
c	c	a	a	c	d	c	d	c

Block 1 - UNIT 2

Sylow Theorems

Objectives

- We study First Sylow Theorem
- To Study about double cosets
- To study second Sylow theorem
- Learn about Third Sylow Theorem

2.1 First Sylow Theorem

In this section we prove first Sylow theorem.

Theorem 2.1.1. *(First Sylow Theorem)*
Let G *be a group and if* p *is a prime number such that* $p^\alpha \mid o(G)$ *, then* G *has a subgroup of order* p^α *.*

Proof. To prove this theorem, we need the following number-theoretic result.
Let $o(G) = p^\alpha m$, where p is a prime number.

If $p^r | o(G)$ but $p^{r+1} \nmid o(G)$, then,

$$p^r \mid \begin{pmatrix} p^\alpha m \\ p^\alpha \end{pmatrix} \text{ but } p^{r+1} \nmid \begin{pmatrix} p^\alpha m \\ p^\alpha \end{pmatrix} \quad \ldots(1)$$

More over $p^{\alpha+r} \mid p^\alpha m \quad \cdots(2)$

Proof of the Theorem: Let $\mathcal{M} = \{M \subset G \mid o(M) = p^\alpha\}$

Clearly $o(\mathcal{M}) = \begin{pmatrix} p^\alpha m \\ p^\alpha \end{pmatrix}$. Define a relation $\sim$ on $\mathcal{M}$ as follows.

For $M_1, M_2 \in \mathcal{M}$, define $M_1 \sim M_2$ if $\exists g \in G$ such that $M_1 = M_2 g$.

Claim 1: $\sim$ is an equivalence relation

(i) $\sim$ is reflexive

Since $M_1 = M_1 e$, where e is identity element of G, we have $M_1 \sim M_1$. Hence $\sim$ is reflexive.

(ii)) $\sim$ is symmetric

Let $M_1 \sim M_2$. Then $M_1 = M_2 g$ for some $g \in G$. Since G is a group, for $g \in G$ we have $g^{-1} \in G$. Therefore, $M_1 g^{-1} = M_2 g g^{-1} \Rightarrow M_1 g^{-1} = M_2$. That is,

$M_2 = M_1 g^{-1}$. This $\Rightarrow M_2 \sim M_1$. Thus, $\sim$ is symmetric

(iii) $\sim$ is transitive

Let $M_1 \sim M_2$ and let $M_2 \sim M_3$. Then

$M_1 = M_2 g_1$ for some $g_1 \in G \ \cdots(i)$

$M_2 = M_3 g_2$ for some $g_2 \in G \ \cdots(ii)$

Therefore, $M_1 = M_2 g_1 = (M_3 g_2) g_1 = M_3 (g_2 g_1) = M_3 g_3$,

where $g_3 = g_2 g_1 \in G$. Thus $M_1 \sim M_3$. So, $\sim$ is transitive .

Hence $\sim$ is an equivalence relation.

Therefore, this $\sim$ splits $\mathcal{M}$ in to distinct equivalence classes.

Let r be an integer such that $p^r \mid m$ but $p^{r+1} \nmid m \ \cdots(1)$

Claim 2 : There exists atleast one equivalence class whose size is

not divisible by p^{r+1}.

Suppose p^{r+1} divides the sizes of all equivalence classes of $\mathcal{M}$. Therefore it will divides their union. Therefore p^{r+1} is a divisor of the size of $\mathcal{M}$. That is,

$p^{r+1} \mid \begin{pmatrix} p^{\alpha}m \\ p^{\alpha} \end{pmatrix}$, which is a contradiction to (1). Therefore there exist atleast one equivalence class whose size is not divisible by p^{r+1}. Let this equivalence class be $\{M_1, M_2, \ldots, M_n\}$.

That is, $p^{r+1} \nmid n \quad \cdots(3)$

Clearly by definition, $\forall i = 1,2,\ldots,n$, $M_i = M_j g$ for some j, $1 \leq j \leq n$.

Let $H = \{g \in G \mid M_1 g = M_1\}$. Clearly H is a finite subset of G.

Claim 3: H is a subgroup of G.

Let $a, b \in G$. Then $M_1 a = M_1, M_1 b = M_1$.

Now $M_1 = M_1 b = (M_1 a)b = M_1(ab)$. Thus $ab \in H$. Therefore $a, b \in H \Rightarrow ab \in H$. Thus H is a closed subset of a finite group G. Hence H is a subgroup of G.

By Lagrange's theorem $o(H)$ is a divisor of $o(G)$.

Let $o(G) = n \,.\, o(H) \quad \cdots(4)$

From (2), we have, $p^{\alpha+r} \mid p^{\alpha}m$. That is, $p^{\alpha+r} \mid o(G)$.

That is, $p^{\alpha+r} \mid n \,.\, o(H)$ implies either $p^{\alpha+r} \mid n$ or $p^{\alpha+r} \mid o(H)$.

But $p^{r+1} \nmid n$ whence we get $p^{\alpha+r} \nmid n$. Therefore we must have, $p^{\alpha+r} \mid o(H)$.

That is, $p^{\alpha}p^{r} \mid o(H)$. This $\Rightarrow p^{\alpha} \mid o(H)$ and $p^{r} \mid o(H)$.

Therefore, $p^{\alpha} \mid o(H)$.

This shows that, $o(H) \geq p^{\alpha} \cdots(5)$

Let $m_1 \in M_1$ and $h \in H$. Therefore, $M_1 h = M_1$.

Now $m_1 h \in M_1 h = M_1 \Rightarrow m_1 h \in M_1$.

Since h is arbitrary, M_1 has atleast $o(H)$ elements.

Therefore, size of $M_1 \geq o(H)$.

That is, $p^{\alpha} \geq o(H) \cdots$.(6).

From (5) and (6), we have $o(H) = p^{\alpha}$.

Thus H is a subgroup of G having p^{α} elements.

Hence the theorem. ■

2.2 Second Sylow Theorem

In this section we define double cosets and prove second part of Sylow theorem.

Definition 2.2.1. *Let G be a group and let H and K are subgroups of G. Then the set $HaK = \{hak \mid h \in H, k \in K\}$ is called the double coset of H and K in G. If G is a finite group, clearly,*

$$G = \bigcup_{a \in G} HaK$$

and

$$o(G) = \sum_{a \in G} o(HaK)$$

Proposition 2.2.1. *Let H be a subgroup of G. Then for $x \in G$, the set xHx^{-1} is also a subgroup of G, such that $o(H) = o(xHx^{-1})$.*

Proof. The set xHx^{-1} is defined as follows.

$xHx^{-1} = \{xhx^{-1} \mid h \in H\}$.

Let $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1}$, where $h_1, h_2 \in H$.

Consider

$$\begin{aligned}(xh_1x^{-1})(xh_2x^{-1})^{-1} &= (xh_1x^{-1})(xh_2^{-1}x^{-1}) \\ &= xh_1(x^{-1}x)h_2^{-1}x^{-1} \\ &= x(h_1h_2^{-1})x^{-1} \in xHx^{-1}.\end{aligned}$$

Thus xHx^{-1} is a subgroup of G.

Now let us prove that $o(H) = o(xHx^{-1})$.

Indeed, let $f : H \longrightarrow xHx^{-1}$ such that $f(h) = xhx^{-1}$.

Initially let us prove f is 1-1:

Suppose let $f(h_1) = f(h_2) \Rightarrow xh_1x^{-1} = xh_2x^{-1}$.

By cancellation law, $h_1 = h_2$. Thus f is 1-1.

By definition, onto is obvious.

Hence $o(H) = o(xHx^{-1})$. ■

The number of elements in a double coset is obtained in following lemma.

Lemma 2.2.1. *Let A and B are finite subgroups of a group G, then,*

$$o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}$$

Proof. Define a map $T : AxB \to AxBx^{-1}$ such that $T(axb) = axbx^{-1}$.

We claim that this map is well defined.

Indeed let $a_1xb_1 = a_2xb_2$ for some $a_1, a_2 \in A$ and $b_1, b_2 \in B \cdots (1)$

Since $x \in G$, we have $x^{-1} \in G$.

Post multiply by x^{-1} on both sides, we have,

$a_1xb_1x^{-1} = a_2xb_2x^{-1}$.

That is, $T(a_1xb_1) = T(a_2xb_2)$.

Thus T is well defined.

By retracing these steps, we can prove that T is 1-1.

Secondly we claim that T is onto.

Note that for every $axbx^{-1} \in AxBx^{-1}, \exists axb \in AxB$ such that $T(axb) = axbx^{-1}$. Thus T is onto.

We know that $o(AxB) = o(AxBx^{-1}) \cdots$ (2)

$$o(AxB) = o(AxBx^{-1}) = \frac{o(A)o(xBx^{-1})}{o(A \cap xBx^{-1})}$$

But $o(B) = o(xBx^{-1})$. Therefore,

$$o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}$$

Hence the Lemma. ■

Second Sylow theorem:

Theorem 2.2.1. *If G is a finite group and if p is a prime number such that $p^n \mid o(G)$ and $p^{n+1} \nmid o(G)$, then any two subgroups of G of order p^n are conjugate.*
(OR) Any two $p - Sylow$ subgroups of G are conjugate.

Proof. Let A and B be any two $p - Sylow$ subgroups of G of order p^n. That is, $o(A) = o(B) = p^n$.
Claim : $A = xBx^{-1}$, for some $x \in G$.
Suppose $A \neq xBx^{-1}$, for every $x \in G$.
Consider the double cosets of A and B. Clearly,

$$G = \bigcup_{x \in G} AxB$$

and

$$o(G) = \sum_{x \in G} o(AxB)$$

$$i.e, \quad o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}$$

Since $A \neq xBx^{-1}, o(A \cap xBx^{-1}) < o(A)$.
Let $o(A \cap xBx^{-1}) = p^m$, where $m < n$.

$$\text{Therefore,} \quad o(AxB) = \frac{p^n p^n}{p^m} = p^{2n-m}.$$

But $2n - m \geq n + 1$. This implies,
$p^{n+1} \mid p^{2n-m} \Rightarrow p^{n+1} \mid o(AxB) \Rightarrow p^{n+1} \mid \sum o(AxB)$

This implies, $p^{n+1} \mid o(G)$, which is a contradiction. Therefore, $A = xBx^{-1}$ for some $x \in G$. Hence A and B are conjugate. Hence the theorem. ■

2.3 Third Sylow Theorem

In this section we prove third part of Sylow theorem.

Definition 2.3.1. *Let H be a $p-Sylow$ subgroup of G.Then normalizer of H in G is defined as follows.*
$N(H) = \{x \in G \mid xHx^{-1} = H\}$

Clearly, $N(H)$ is a subgroup of G.

Lemma 2.3.1. *Let H be a $p-Sylow$ subgroup of G. Then the number of $p-Sylow$ subgroups of G is equal to $\frac{o(G)}{o(N(H))}$*

Proof. We know that

$$\begin{aligned} o(Cl(H)) &= \frac{o(G)}{o(N(H))} \cdots (1) \\ Cl(H) &= \{A \subseteq G \mid A = gHg^{-1}, textfor g \in G\} \\ &= \text{Set of all p-Sylow subgroups of } G \\ &\quad \text{conjugate to } H \end{aligned}$$

That is, the total number of $p-Sylow$ subgroups of G is equal to $o(Cl(H)) \cdots (2)$
Substituting (2) in (1), we have
The total number of $p-Sylow$ subgroups of G is equal to $\frac{o(G)}{o(N(H))}$. ■

Third Sylow Theorem:

Theorem 2.3.1. *The total number of $p-Sylow$ subgroups of G is of the form $1+kp$, where p is a prime number and k is an integer.*

Proof. Let H be a $p-Sylow$ subgroup of G of order p^n. That is, $o(H)=p^n$.

Then, $p^n \mid o(G)$ but $p^{n+1} \nmid o(G)$. Decompose G in to double cosets of H as

$$G=\bigcup_{x\in G} HxH$$

$$i.e,\ G=\bigcup_{x\in G} HxH=\left(\bigcup_{x\in N(H)} HxH\right)\bigcup\left(\bigcup_{x\notin N(H)} HxH\right)$$

$$\text{Therefore, } o(G)=\sum_{x\in N(H)} o(HxH)+\sum_{x\notin N(H)} o(HxH)\cdots(1)$$

Here two cases arises.

Case(i): $x\in N(H)\Rightarrow Hx=xH$

$\Rightarrow HHx=HxH$

$\Rightarrow Hx=HxH$

That is, $HxH=Hx$.

Therefore,

$$\bigcup_{x\in N(H)} HxH=\bigcup_{x\in N(H)} Hx=N(H)$$

Therefore, $\sum_{x\in N(H)} o(HxH)=o(N(H))$.

Case(ii): $x\notin N(H)\Rightarrow Hx\neq xH$

$\Rightarrow xHx^{-1}\neq H$

Since $xHx^{-1}\neq H$, we have $o(H\cap xHx^{-1})<o(H)$

Let $o(H\cap xHx^{-1}=p^m$,where $m<n$.

$$i.e,\quad o(HxH)=\frac{o(H)o(H)}{o(H\cap xHx^{-1})}$$

$$= \frac{p^n p^n}{p^m} = p^{2n-m} \cdots (2)$$

Sub (2) in (1), we have

$$o(G) = o(N(H)) + \sum p^{2n-m} \cdots (3)$$

But $2n - m \geq n + 1$ for $m < n$. This implies,

$p^{n+1} \mid p^{2n-m} \Rightarrow p^{n+1} \mid \sum p^{2n-m}$

$\Rightarrow \sum p^{2n-m} = p^{n+1}.u$ where u is an integer $\cdots (4)$

Sub (4) in (3), $o(G) = o(N(H)) + p^{n+1}.u$

Dividing by $o(N(H))$, we have,

$\frac{o(G)}{o(N(H))} = 1 + \frac{p^{n+1}.u}{o(N(H))} \cdots (5)$

Since $\frac{o(G)}{o(N(H))}$ and 1 are integers , $\frac{o(G)}{o(N(H))} - 1$ is also an integer.

Therefore , $\frac{p^{n+1}.u}{o(N(H))}$ is an integer.

Let this integer be t (say).

Therefore , $\frac{p^{n+1}.u}{o(N(H))} = t$

That is, $p^{n+1}.u = t.o(N(H)) \cdots (6)$

Since $H \subseteq N(H)$ we have, $o(H) \mid o(N(H))$

$p^n \mid o(N(H))$

$\Rightarrow o(N(H)) = p^n.r \cdots (7)$

But from (6), $p^{n+1}.u = t.o(N(H)) = t.p^n.r$

That is, $p^{n+1}.u = t.p^n.r$

Dividing by p^n , we have, $p.u = t.r \cdots (8)$

Also, $\frac{t}{p} = \frac{u}{r} \cdots (9)$

This implies, $p \mid t.r$

If $p \mid r$, then $p.p^n \mid r.p^n$

i.e, $p^{n+1} \mid o(N(H)$ by (7)

i.e, $p^{n+1} \mid o(G)$ (since $o(N(H) \mid o(G)$), which is a contradiction.

Therefore, $p \nmid r$.

Hence we must have, $p \mid t \Rightarrow \frac{t}{p} = k\ (say)$, where k is a constant.

Therefore from (9), we have, $\frac{u}{r} = k \cdots (10)$

Now from (5), we have,

$$\begin{aligned}\frac{o(G)}{o(N(H))} &= 1+\frac{p^{n+1}.u}{o(N(H))}\\ &= 1+\frac{p^{n+1}.u}{p^n.r}\\ &= 1+\frac{p.u}{r}=1+kp\end{aligned}$$

Thus, $\frac{o(G)}{o(N(H))} = 1+kp$. But by Lemma 2.3.1, we have, The total number of $p-Sylow$ subgroups of G is equal to $\frac{o(G)}{o(N(H))}$. Hence, total number of $p-Sylow$ subgroups of G is of the form $1+kp$. ■

Lemma 2.3.2. *If G is a group and if p is a prime number and if G has only one $p-Sylow$ subgroup, then it must be normal.*

Proof. Let H be a $p-Sylow$ subgroup of G.

We claim that H is a normal subgroup of G.

Indeed, since H is a subgroup of G, xHx^{-1} is also a $p-Sylow$ subgroup of G. But it is given that G has only one subgroup of G. Therefore, $H = xHx^{-1}$. That is, $Hx = xH$. This implies, H is a normal subgroup. ■

Solved Problems

Problem 1. Prove that every group of order $11^2 \cdot 13^2$ is abelian.

Solution : It is given that $o(G) = 11^2 \cdot 13^2$. Here $11^2 \mid o(G)$ but $11^3 \nmid o(G)$.

There exist a $11-Sylow$ subgroup in G of order 11^2.

Similarly, $13^2 \mid o(G)$ but $13^3 \nmid o(G)$.

There exist a $13-Sylow$ subgroup in G of order 13^2. Let this group be B.

We know that the total number of $11-Sylow$ subgroups of G is of the form $1+11k$. We know that, $1+11k \mid o(G)$.

That is, $1+11k \mid 11^2.13^2$. But, $1+11k \nmid 11^2$. Therefore, $1+11k \mid 13^2$. This is possible only if, k=0. Therefore, the total number of $11-Sylow$ subgroups of G is only one. Let this group be A.

That is A is the only one $11-Sylow$ subgroup of G. Hence A is normal.

Again we know that the total number of $13-Sylow$ subgroups of G is of the form $1+13k$. We know that, $1+13k \mid o(G)$.

That is, $1+13k \mid 11^2.13^2$. But, $1+13k \nmid 13^2$. Therefore, $1+13k \mid 11^2$. This is possible only if, k=0. Therefore, the total number of $13-Sylow$ subgroups of G is only one. Let this group be B.

That is B is the only one $13-Sylow$ subgroup of G. Hence B is normal.

Therefore, $A \cap B = \{e\}$

Consider, $a \in A$ and $b \in B$. Therefore, $a^{-1} \in A$ and $b^{-1} \in B$

Consider $aba^{-1}b^{-1}$. Since $a \in A$ we have, $a \in G$.

Since B is normal, for $b \in B$ and $a \in G$, we get, $aba^{-1} \in B$.

That is $aba^{-1} \in B$. Also, $b^{-1} \in B$.

Therefore, $aba^{-1}b^{-1} \in B \cdots\cdots (1)$

Now, $b \in B \Rightarrow b \in G$. But, $a \in A \Rightarrow a^{-1} \in A$.

Now $a^{-1} \in A$, and $b \in G \Rightarrow ba^{-1}b^{-1} \in A$. (Since A is normal)

That is $ba^{-1}b^{-1} \in A$. Also, $a \in A$.

Therefore, $aba^{-1}b^{-1} \in A \cdots\cdots (2)$

That is, $aba^{-1}b^{-1} \in A$ and $aba^{-1}b^{-1} \in B$ and hence $aba^{-1}b^{-1} \in A \cap B$. But , $A \cap B = \{e\}$.

Therefore, $aba^{-1}b^{-1} = e$

Hence $ab = ba$. Therefore G is abelian.

Problem 2. Discuss the number and nature of 3-Sylow subgroups and 5-Sylow subgroups of a group of order $3^2 \cdot 5^2$

Solution: We know that the total number of $3-Sylow$ subgroups of G is of the form $1+3k$. We know that, $1+3k \mid o(G)$.

That is, $1+3k \mid 3^2.5^2$. But, $1+3k \nmid 3^2$. Therefore, $1+3k \mid 5^2$. This is possible for k=0 or k =8. Therefore G has either only one $3-Sylow$ subgroup or 25, $3-Sylow$ subgroups .

Also we know that the total number of $5-Sylow$ subgroups of G is of the form $1+5k$. We know that, $1+5k \mid o(G)$.

That is, $1+5k \mid 3^2.5^2$. But, $1+5k \nmid 5^2$. Therefore, $1+5k \mid 3^2$. This is possible for only k=0 . Therefore G has exactly one $5-Sylow$ subgroup.

We have that $o(G)=225$. But G has 25, $3-Sylow$ subgroups, each of order 9. Since the identity element is common to all these 25 subgroups, each subgroup has eight elements other than the identity element. Hence there are 200 elements other than identity elements and hence totally there are 201 elements in all these 25 subgroups. But G has exactly one $5-Sylow$ subgroup of order $5^2=25$ .Hence other than the identity it has 24 elements. Hence G has 200+24+1=225 elements which is equal to order of G. Thus we conclude that G has one $5-Sylow$ subgroup and 25, $3-Sylow$ subgroups.

Problem 3. If o(G)=30, show that either 3-Sylow sub group or 5-Sylow subgroup is normal in G.

Solution: $o(G)=30=2\cdot 3\cdot 5$

We know that the total number of $3-Sylow$ subgroups of G is of the form $1+3k$. We know that, $1+3k \mid o(G)$.

That is, $1+3k \mid 2\cdot 3\cdot 5$. But, $1+3k \nmid 3$. Therefore, $1+3k \mid 2\cdot 5$. This is possible for k=0 or k =3. Therefore G has either only one $3-Sylow$ subgroup or 10, $3-Sylow$ subgroups .

Also we know that the total number of $5-Sylow$ subgroups of G is of the form $1+5k$. We know that, $1+5k \mid o(G)$.

That is, $1+5k \mid 2\cdot 3\cdot 5$. But, $1+5k \nmid 5$. Therefore, $1+3k \mid 2\cdot 3$. This is possible for k=0 or k =1. Therefore G has either only one $5-Sylow$ subgroup or 6, $5-Sylow$ subgroups .

Suppose G has 10, $3-Sylow$ subgroups and 6, $5-Sylow$ subgroups.

The each of the ten 3-Sylow subgroups have 2 elements other than the identity. Therefore there are, 20+1=21 elements in 3-Sylow subgroups.

Each of the six 5-Sylow subgroups has 4 elements other than the identity. Therefore there are, 24+1=25 elements in 5-Sylow subgroups.

Thus all these subgroups has 46-1=45 elements where as the original group has one 30 elements which is not possible. Therefore we must have either there is only one 3-Sylow sub group or only one 5-Sylow subgroup and hence one must be normal. Hence G is not simple.

Problem 4. Prove that a group of order 56 is not simple.

Solution: $o(G)=56=2^3\cdot 7$

We know that the total number of $2-Sylow$ subgroups of G is of the form $1+2k$. We know that, $1+2k \mid o(G)$.

But, $1+2k \nmid 2^3$. But, Therefore, $1+2k \mid 7$. This is possible for k=0 or k =3. Therefore G has either only one $2-Sylow$ subgroup or 7, $2-Sylow$ subgroups .

Also we know that the total number of $7-Sylow$ subgroups of G is of the form $1+7k$. We know that, $1+7k \mid o(G)$.

But, $1+7k \nmid 7$. Therefore, $1+7k \mid 2^3$. This is possible for k=0 or k =1. Therefore G has either only one $7-Sylow$ subgroup or 8,

$7-Sylow$ subgroups .

Suppose G has 7, $2-Sylow$ subgroups and 8, $7-Sylow$ subgroups. Each of the seven 2-Sylow subgroups has 7 elements other than the identity. Therefore there are, 49+1=50 elements in 2-Sylow subgroups.

Each of the eight 7-Sylow subgroups has 6 elements other than the identity. Therefore there are, 48+1=49 elements in 7-Sylow subgroups.

Thus all these subgroups have 99-1=98 elements where as the original group has only 56 elements which is not possible. Therefore we must have either there is only one 2-Sylow sub group or only one 7-Sylow subgroup and hence one must be normal. Hence G is not simple.

Problem 5. Prove that a group of order 72 is not simple.

Solution: $o(G) = 56 = 2^3 \cdot 3^2$.

We know that the total number of $2-Sylow$ subgroups of G is of the form $1+2k$. We know that, $1+2k \mid o(G)$.

But , $1+2k \nmid 2^3$. Therefore, $1+2k \mid 9$. This is possible for k=0 or k =4. Therefore G has either only one $2-Sylow$ subgroup or 9, $2-Sylow$ subgroups .

Also we know that the total number of $3-Sylow$ subgroups of G is of the form $1+3k$. We know that, $1+3k \mid o(G)$.

But, $1+3k \nmid 9$. Therefore, $1+3k \mid 2^3$. This is possible for k=0 or k =1. Therefore G has either only one $3-Sylow$ subgroup or 4, $3-Sylow$ subgroups .

Suppose G has 9, $2-Sylow$ subgroups and 4, $3-Sylow$ subgroups. The each of the nine 2-Sylow subgroups has 7 elements other than the identity. Therefore there are, 63+1=64 elements in 2-Sylow subgroups.

Each of the 4, 3-Sylow subgroups has 8 elements other than the identity. Therefore there are, 32+1=33 elements in 3-Sylow subgroups.

Thus all these subgroups have 97-1=96 elements where as the original group has only 72 elements which is not possible. Therefore we must have either there is only one 2-Sylow sub group or only one 3-Sylow subgroup and hence one must be normal. Hence G is not simple.

Summary of this unit.

In this unit we have studied the following:

- First Sylow Theorem: Let G be a group and if p is a prime number such that $p^\alpha \mid o(G)$, then G has a subgroup of order p^α.
- Let G be a group and let H and K are subgroups of G. Then the set $HaK = \{hak \mid h \in H, k \in K\}$ is called the double coset of H and K in G.
- Let H be a subgroup of G. Then for $x \in G$, the set xHx^{-1} is also a subgroup of G, such that $o(H) = o(xHx^{-1})$.
- Let A and B are finite subgroups of a group G, then, $o(AxB) = \frac{o(A)o(B)}{o(A \cap xBx^{-1})}$
- Second Sylow Theorem: If G is a finite group and if p is a prime number such that $p^n \mid o(G)$ and $p^{n+1} \nmid o(G)$, then any two subgroups of G of order p^n are conjugate.
  (OR) Any two $p-Sylow$ subgroups of G are conjugate.
- Let H be a $p-Sylow$ subgroup of G.Then normalizer of H in G is defined as follows.
  $N(H) = \{x \in G \mid xHx^{-1} = H\}$

- Let H be a $p-Sylow$ subgroup of G. Then the number of $p-Sylow$ subgroups of G is equal to $\frac{o(G)}{o(N(H))}$
- Third Sylow Theorem: The total number of $p-Sylow$ subgroups of G is of the form $1+kp$, where p is a prime number and k is an integer.

Multiple Choice Questions

1. If $o(G)=30$, then
   a) either 3-Sylow sub group or 5-Sylow subgroup is normal in G.
   b) 3-Sylow sub group and 5-Sylow subgroup are normal in G.
   c) G is a simple group
   d) neither 3-Sylow sub group nor 5-Sylow subgroup is normal in G.

2. If $o(G)=72$, and if A and B are finite subgroups of a group G, of orders 8 and 9 respectively such that $o(A\cap B)=1$, then, for any $x\in G$, $o(AxB)=$
   a) 72 b) 8 c) 9 d) 36

3. Let G be a group of order 45. Let H be a 3-sylow subgroup of G and K be a 5- sylow subgroup of G. Then,
   a) Both H and K are normal in G
   b) H is normal in G but K is not normal in G
   c) H is not normal in G but K is normal in G
   d) Both H and K are not normal in G

4. If $o(G)=11^2.13^2$ and if A and B are respectively 11- Sylow and 13-Sylow subgroups of G then for any $t\in G$,
   a) $tA=At$ but $tB\neq Bt$
   b) $Bt=tB$ but $tA\neq At$
   c) $tA\neq At$ and $tB\neq Bt$
   d) $tA=At$ and $tB=Bt$.

5. If $o(G) = 225$, then G has

   a) one $5-Sylow$ subgroup and 25, $3-Sylow$ subgroups.

   b) one $3-Sylow$ subgroup and 25, $5-Sylow$ subgroups.

   c) either one $5-Sylow$ subgroup or 25, $3-Sylow$ subgroups .

   d) has only one $3-Sylow$ subgroup and exactly one $5-Sylow$ subgroup.

6. Any two conjugate subgroups of a group are

   a) Isomorphic

   b) Not isomorphic

   c) May or may not isomorphic

   d) All of these

7. Two conjugate subgroups of a group have the same

   a) Index b) Order c) Coset d) None of these

8. Let H,K be subgroups of a group G and x is an arbitrary element of G. Then the set HxK is

   a) Left Coset

   b) Right Coset

   c) Coset

   d) Double Coset

9. The order of a subgroup H of a finite group G is a power of p and the index of H is prime to p then H is

   a) Normalizer

   b) Centralizer

   c) Sylow p-subgroup

   d) None of these

10. A finite group whose order is divisible by a prime p contains a Sylow p-subgroup, is

    a) Sylow p-subgroup

b) Sylow's first theorem

c) Sylow's second theorem

d) Sylow's third theorem

11. A group of order 80 has how many Sylow 5-subgroup's?

a) 0 b) 1 c) 2 d) 3

12. A group of order 200 has how many Sylow 2-subgroup's ?

a) 3 b) 5 c) 7 d) 0

13. If $o(G) = 121$, then $o(Z(G))$ is

a)1 b) 11 c) 121 d) 112

14. Any two Sylow p-subgroups of a group G are

a) Normal to each other

b) Conjugate to each other

c) Centralizers

d) None of these

15. A finite group G has a unique Sylow p-subgroup H iff H is

a) Normal in G

b) Centralizer in G

c) Conjugate in G

d) Sylow p-subgroup

16. The number k of Sylow p-subgroup of a finite group is congruent to the

a) $p \mod 1$ b) $1 \mod p$

c) $1 \mod 2p$ d) $0 \mod p$

Answers:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a	a	a	d	a	a	b	d	c	b	b	b	c	b	a	b

Exercise

1. Prove that no group of order 96 is simple
2. Show that every group of order 160 has a normal subgroup.
3. Find the class equation for S_4.

Block 2 - UNIT 3

Finite abelian groups

Objectives

- We study internal direct product and external direct product
- Learn about 1-1 correspondence between internal direct product and external direct product
- Study about the relation between a finite abelian group and its Sylow subgroups
- Study about the relation between a finite abelian group and its cyclic subgroups
- To learn about Isomorphic abelian groups and its invariants
- To study about number of non-isomorphic abelian groups of order p^n.

In our under graduate level, in the investigation of cyclic groups we have found that every group of prime order is isomorphic to $\mathbb{Z}_p$, where p is a prime number. We also determined that $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, when $gcd(m,n) = 1$. In this chapter we define direct products on groups. In this unit, we first prove that every finite

abelian group is isomorphic to a direct product of cyclic groups of prime power order and then we prove the Fundamental Theorem of Finite abelian Groups.

3.1 Direct Products

In this section we construct a new group from some groups that we already have on hand.

Cartesian product of groups

Let A, B be any two groups. Consider the Cartesian product of A, B namely $A \times B$.

Let $G = A \times B$.

Then $G = \{(a_i, b_i) \mid a_i \in A \text{ and } b_i \in B\}$.

Define the multiplication in G as follows.

Let $(a_1, b_1), (a_2, b_2) \in G$. Then $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$.

Since $a_1, a_2 \in A$, we have $a_1a_2 \in A$ and $b_1, b_2 \in B$ we have $b_1b_2 \in B$, and therefore we have $(a_1a_2, b_1b_2) \in G$. With this definition a product defined in G, we prove G is a group as given in the following lemma.

Lemma 3.1.1. *If A and B are any two groups then their Cartesian product $G = A \times B$ is also a group with respect to multiplication.*

Proof. $G = \{(a, b) \mid a \in A \text{ and } b \in B\}$.

We prove all the four required axioms now.

Closure: Let $(a_1, b_1), (a_2, b_2) \in G$. Then $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2) \in G$ since $a_1a_2 \in A$ and $b_1b_2 \in B$.

Associativity: Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G$.

Then

$$\begin{aligned}[(a_1,b_1)(a_2,b_2)](a_3,b_3) &= (a_1a_2,b_1b_2)(a_3,b_3)\\ &= (a_1a_2a_3,b_1b_2b_3)\\ &= [a_1(a_2a_3),b_1(b_2b_3)]\\ &= (a_1,b_1)(a_2a_3,b_2b_3)\\ &= (a_1,b_1)[(a_2,b_2)(a_3,b_3)].\end{aligned}$$

That is, $[(a_1,b_1)(a_2,b_2)](a_3,b_3) = (a_1,b_1)[(a_2,b_2)(a_3,b_3)]$.

Existence of Identity: Let e, f be the identity elements of A and B respectively. Then $(e,f) \in G$.
Let $(a,b) \in G$. Then $(a,b)(e,f) = (ae,bf) = (a,b)$.
Similarly, $(e,f)(a,b) = (ea,fb) = (a,b)$.
Therefore, (e,f) is the identity element of G.

Existence of Inverse: Let $a \in A$. Then, $a^{-1} \in A$.
Let $b \in B$. Then, $b^{-1} \in B$.
Therefore, $(a,b) \in G \Rightarrow (a^{-1},b^{-1}) \in G$.
Consider $(a,b)(a^{-1},b^{-1}) = (aa^{-1},bb^{-1}) = (e,f)$.
Similarly, $(a^{-1},b^{-1})(a,b) = (a^{-1}a,b^{-1}b) = (e,f)$.
Therefore (a^{-1},b^{-1}) is the inverse of (a,b). Therefore G is a group which completes the proof of the Lemma. ■

Note: This cartesian product $A \times B$ is called the external direct product of A and B.

Corollary 3.1.1. *If A and B are any two groups then their external direct product $A \times B$ is also a group .*

Lemma 3.1.2. *If A and B are any two groups with identity*

elements e, f respectively. Then, $A \times \{f\}$ and $\{e\} \times B$ are the normal subgroups of G where $G = A \times B$.

Proof. Now we prove that $A \times \{f\}$ is a normal subgroup.

Let $(a_1, f), (a_2, f) \in A \times \{f\}$, where, $a_1, a_2 \in A, f \in \{f\}$.

Then, $(a_1, f)(a_2, f)^{-1}$

$= (a_1, f)(a_2^{-1}, f^{-1})$

$= (a_1, f)(a_2^{-1}, f)$

$= (a_1 a_2^{-1}, f) = (e, f) \in A \times \{f\}$.

Therefore , $A \times \{f\}$ is a subgroup of G.

Let $(a_1, b_1) \in G$, and let $(a, f) \in A \times \{f\}$. Then,

$(a_1, b_1)(a, f)(a_1, b_1)^{-1}$

$= (a_1, b_1)(a, f)(a_1^{-1}, b_1^{-1})$

$= (a_1 a a_1^{-1}, b_1 f b_1^{-1})$

$= (a_1 a a_1^{-1}, b_1 b_1^{-1})$

$= (a_1 a a_1^{-1}, f) \in A \times \{f\}$.

Thus $A \times \{f\}$ is a normal subgroup of G.

Similarly, $\{e\} \times B$ is also normal subgroup of G. Thus the Lemma is proved. ■

Lemma 3.1.3. *Let A and B be any two groups with identity elements e, f respectively and let $G = A \times B$. Then, $A \simeq A \times \{f\}$ and $B \simeq \{e\} \times B$.*

Proof. Define a map $\phi : A \to A \times \{f\}$ such that $\phi(a) = (a, f)$ for all $a \in A$.

We first claim that ϕ is 1-1 :

Indeed let, $\phi(a_1) = \phi(a_2)$, then $(a_1, f) = (a_2, f) \Rightarrow a_1 = a_2$.

Thus ϕ is 1-1.

Secondly, we show that ϕ is onto :

Note that $\forall\ (a, f) \in A \times \{f\}$, there exists $a \in A$ such that

$\phi(a) = (a, f)$.

Thus ϕ is onto.

Finally we prove that ϕ is a homomorphism:

Now, $\phi(ab) = (ab, f) = (a, f)(b, f) = \phi(a)\phi(b)$.

Thus ϕ is a homomorphism.

Similarly we can prove, $B \simeq \{e\} \times B$.

Hence $A \simeq A \times \{f\}$ and $B \simeq \{e\} \times B$. Hence the Lemma is proved. ■

3.2 Internal Direct product

Definition 3.2.1. *Define* $G = (A \times \{f\})(\{e\} \times B)$, *where* $G = A \times B$.

Thus if $(a, b) \in G$, *then* $(a, b) = (ae, fb) = (a, f)(e, b)$.

That is, $G = (A \times \{f\})(\{e\} \times B)$.

This $G = (A \times \{f\})(\{e\} \times B)$ *is called the internal direct product of* A *and* B *and this is denoted by* $G = AB$.

Now we generalize these concepts for a finite number of n groups. Let $G_1, G_2, \ldots, G_n$ be any groups and let $e_1, e_2, \ldots, e_n$ be the identity elements of $G_1, G_2, \ldots, G_n$ respectively. Then the cartesian product of $G_1, G_2, ..., G_n$ namely, $G = G_1 \times G_2 \times \cdots \times G_n$ is called the external direct product of $G_1, G_2, \cdots, G_n$.

The identity element of G is $(e_1, e_2, \cdots, e_n)$.

Consider the following sets.

$$\begin{aligned}
G_1 \times \{e_2\} \times \{e_3\} \times \{e_4\} \times \quad & \cdots \quad \times \{e_n\}) \\
\{e_1\} \times \{G_2\} \times \{e_3\} \times \{e_4\} \times \quad & \cdots \quad \times \{e_n\} \\
\{e_1\} \times \{e_2\} \times \{G_3\} \times \{e_4\} \times \quad & \cdots \quad \times \{e_n\} \\
\{e_1\} \times \{e_2\} \times \{e_3\} \times \{G_4\} \times \quad & \cdots \quad \times \{e_n\} \\
& \vdots \\
\{e_1\} \times \{e_2\} \times \{e_3\} \times \{e_4\} \times \quad & \cdots \quad \times \{G_n\}
\end{aligned}$$

Each of the above set is a normal subgroup of G,

where $G = G_1 \times G_2 \times \cdots . \times G_n$ and

$$\begin{aligned}
G_1 \times \{e_2\} \times \{e_3\} \times \{e_4\} \times \quad & \cdots \quad \times \{e_n\} \simeq G_1 \\
\{e_1\} \times \{G_2\} \times \{e_3\} \times \{e_4\} \times \quad & \cdots \quad \times \{e_n\} \simeq G_2 \\
\{e_1\} \times \{e_2\} \times \{G_3\} \times \{e_4\} \times \quad & \cdots \quad \times \{e_n\} \simeq G_3 \\
\{e_1\} \times \{e_2\} \times \{e_3\} \times \{G_4\} \times \quad & \cdots \quad \times \{e_n\} \simeq G_4 \\
& \vdots \\
\{e_1\} \times \{e_2\} \times \{e_3\} \times \{e_4\} \times \quad & \cdots \quad \times \{G_n\} \simeq G_n
\end{aligned}$$

Thus the product G is defined as

$$\begin{aligned}
G \;=\; & [G_1 \times \{e_2\} \times \cdots \times \{e_n\}] \\
& [\{e_1\} \times \{G_2\} \times \{e_3\} \times \cdots \times \{e_n\}] \\
& [\{e_1\} \times \{e_2\} \times \{G_3\} \times \{e_4\} \times \cdots \times \{e_n\}] \\
& \cdots [\{e_1\} \times \{e_2\} \times \{e_3\} \times \{e_4\} \times \cdots \times \{G_n\}].
\end{aligned}$$

This G is called the internal direct product of $G_1, G_2, \cdots, G_n$.

Let $G = \{(a,b) \mid a \in A, b \in B\}$, be a group with identity element (e,f).

Let $G_1 = \{(e,b) \mid e \in A, b \in B\}$

$G_2 = \{(a, f) \mid a \in A, f \in B\}$

Clearly $G_1 \subseteq G$ and $G_2 \subseteq G$.

We claim that G_1 is a normal subgroup of G.

Indeed, first we prove G_1 is a subgroup.

Let $(e, b_1), (e, b_2) \in G_1$. Therefore, $(e, b_1 b_2) \in G_1$. Thus closure is verified.

Since $b \in B$ we have $b^{-1} \in B$. Therefore $(e, b) \in G_1 \Rightarrow (e, b^{-1}) \in G_1$.

Consider $(e, b)(e, b^{-1}) \Rightarrow (e, bb^{-1}) \Rightarrow (e, f) \in G_1$.

Thus (e, b^{-1}) is the inverse element of (e, b).

Hence G_1 is a subgroup of G.

Now we prove G_1 is normal.

Consider $(e, b) \in G_1$ and $(x, y) \in G$.

Now $(x, y)(e, b)(x^{-1}, y^{-1}) \Rightarrow (xe, yb)(x^{-1}, y^{-1}) \Rightarrow (x, yb)(x^{-1}, y^{-1})$
$\Rightarrow (xx^{-1}, yby^{-1}) \Rightarrow (e, yy^{-1}b) \Rightarrow (e, b) \in G_1$.

Thus G_1 is a normal subgroup of G.

Similarly, G_2 is also normal subgroup of G.

Now we claim that $G = G_1 G_2$.

Let $g = g_1 g_2$ where $g_1 \in G_1$ and $g_2 \in G_2$. Then

$g = (a, b)$ where $a \in A$ and $b \in B$

$g_1 = (e, b)$ where $e \in A$ and $b \in B$

$g_2 = (a, f)$ where $a \in A$ and $f \in B$

$(a, b) = (e, b)(a, f) = (ea, bf) = (a, b)$.

Thus every element $g \in G$ can be expressed in a unique way as $g = g_1 g_2$ where $g_1 \in G_1$ and $g_2 \in G_2$.

This G is called the internal direct product of G_1 and G_2. More formally,

Definition 3.2.2. *Let $G_1, G_2, \cdots, G_n$ are normal subgroups of G. The group G is said to be the internal direct product of*

$G_1, G_2, \cdots, G_n$ *if*

(i). $G = G_1G_2 \cdots G_n$

(ii).Every element $g \in G$ *can be expressed in a unique way as* $g = g_1g_2g_3 \cdots g_n$ *where* $g_i \in G_i$.

Suppose that G is the internal direct product of the normal subgroups $N_1, \ldots, N_n$. For a little moment, we use these $N_1, \ldots, N_n$ as groups and construct their external direct product T as $T = N_1 \times N_2 \times \cdots \times N_n$. For every one, it is natural to ask about the relationship between G and T. Our aim is to show that this relation is up to an isomorphism. That is, we prove that G is isomorphic to T. We start with the following result.

Lemma 3.2.1. *Let* G *be the internal direct product of* $N_1, N_2, \cdots, N_n$. *Then,*

(i). $N_i \cap N_j = (e)$, *for* $i \neq j$. *More over*

(ii). if $a \in N_i$ *and* $b \in N_j$, *then* $ab = ba$.

Proof. Let $x \in N_i \cap N_j$. Then , $x \in N_i$ and $x \in N_j$.

$x = e_1e_2 \cdots e_{i-1}xe_{i+1} \cdots e_{j-1}e_je_{j+1} \cdots e_n$

where $e_t = e,\ t = 1,2,3,4,\cdots,n$ and $t \neq i$ as $x \in N_i$.

Again, $x = e_1e_2 \cdots e_{i-1}e_ie_{i+1} \cdots e_{j-1}xe_{j+1} \cdots e_n$

where $e_k = e,\ k = 1,2,3,4,\cdots,n$ and $k \neq j$ as $x \in N_j$.

But it is given that G is the internal direct product of $N_1, N_2, \cdots, N_n$.

Therefore every element in G has a unique expression.

As $x \in G$, the above two expressions for x must be equal.

Therefore, $x = e_i = e_j = e = x$. Thus $x = e$.

Hence $N_i \cap N_j = (e)$. This proves part (i).

To prove the second part of this Lemma, let $a \in N_i$ and $b \in N_j$.

$a \in N_i \Rightarrow a^{-1} \in N_i$

$b \in N_j \Rightarrow b^{-1} \in N_j$

Consider $aba^{-1}b^{-1}$

Since N_j is normal , we have, $aba^{-1} \in N_j$.

Also $b^{-1} \in N_j$. Therefore, $aba^{-1}b^{-1} \in N_j$.

Since N_i is normal , we have, $ba^{-1}b^{-1} \in N_i$.

Also $a \in N_i$. Therefore, $aba^{-1}b^{-1} \in N_i$.

Thus, $aba^{-1}b^{-1} \in N_i$ and $aba^{-1}b^{-1} \in N_j$ and therefore

$aba^{-1}b^{-1} \in N_i \cap N_j$. But $N_i \cap N_j = (e)$.

Therefore $aba^{-1}b^{-1} = e$. Hence $ab = ba$.

Hence the Lemma is proved. ■

Isomorphism between the external and internal direct products

We now prove the desired isomorphism between the external and internal direct products which we mentioned earlier.

Theorem 3.2.1. *Let G be a group and suppose that G is the internal direct product of $N_1, N_2, \cdots, N_n$. Let $T = N_1 \times N_2 \times \cdots \times N_n$. Then G and T are isomorphic.*

Proof. Define a map $\psi : T \to G$ by

$\psi(a_1, a_2, a_3, \cdots, a_n) = a_1a_2a_3 \cdots a_n$, where $a_i \in N_i$, for $i = 1, 2, 3, \cdots, n$.

To prove T and G are isomorphic, we have to prove the following.

(i) ψ is 1-1.

(ii) ψ is onto

(iii) ψ is a homomorphism

To prove ψ is 1-1.

Let $\psi(a_1, a_2, a_3, \cdots, a_n) = \psi(b_1, b_2, b_3, \cdots, b_n)$, where $a_i, b_i \in N_i$

$\Rightarrow a_1a_2a_3 \cdots a_n = b_1b_2b_3 \cdots b_n$

By uniqueness of elements in the internal direct product,

we have $a_i = b_i$ for all i . Thus ψ is 1-1.

To prove ψ is onto.

Since G is the internal direct product of $N_1, N_2, \cdots, N_n$,

every $x \in G$ is of the form $x = a_1a_2a_3 \cdots a_n$, for some $a_1 \in N_1, a_2 \in N_2, a_3 \in N_3, \cdots, a_n \in N_n$.

But by definition, $\psi(a_1, a_2, a_3, \cdots, a_n) = a_1a_2a_3 \cdots a_n = x$.

Hence ψ is onto.

To prove ψ is a homomorphism:

Let $X = (a_1, a_2, a_3, \cdots, a_n)$ and let $Y = (b_1, b_2, b_3, \cdots, b_n)$

be any two elements of T. Then,

$\psi(XY) = \psi[(a_1, a_2, a_3, \cdots, a_n)(b_1, b_2, b_3, \cdots, b_n)]$

$= \psi[(a_1b_1, a_2b_2, a_3b_3, \cdots, a_nb_n)]$

$= a_1b_1a_2b_2a_3b_3 \cdots a_nb_n$.

However by Lemma 3.2.1, we have, $a_ib_j = b_ja_i$, if $i \neq j$.

This says that,

$a_1b_1a_2b_2a_3b_3 \cdots a_nb_n = a_1a_2a_3 \cdots a_nb_1b_2b_3 \cdots b_n$

Thus, $\psi(XY) = a_1a_2a_3 \cdots a_nb_1b_2b_3 \cdots b_n$

But we can recognize

$a_1a_2a_3 \cdots a_n$ as $\psi(a_1, a_2, a_3, \cdots, a_n) = \psi(X)$ and

$b_1b_2b_3 \cdots b_n$ as $\psi(b_1, b_2, b_3, \cdots, b_n) = \psi(Y)$

That is, $\psi(XY) = \psi(X)\psi(Y)$.

Thus ψ is an isomorphism of T onto G. This proves the theorem. ■

Example 3.2.1. *Consider the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$, it contains the two subgroups $H = \{(h, 0), h \in \mathbb{Z}_2\}$ and $K = \{(0, k), k \in \mathbb{Z}_2\}$. We have that both H and K are normal, because the Klein group is commutative. We also have that $H \cap K = \{(0, 0)\}$, so the Klein group is indeed an internal direct product.*

Example 3.2.2. *Consider the subset D in the direct product given by $D = \{(g, g) \in G \times G | g \in G\} \subset G \times G$.*

We claim that D is a subgroup of $G \times G$.

Let, $(g, g), (h, h) \in G \times G$.

Now, $(g,g)(h,h) = (gh,gh) \in D$ *and*
$(g,g)^{-1} = (g^{-1},g^{-1}) \in D$.
That is for any $g,h \in G$, D *is closed under multiplications and inverses, and hence* D *is a subgroup of* $G \times G$.

3.3 Fundamental theorem on Finite abelian groups

Here we prove that every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order. That is, every finite abelian group is isomorphic to a group of the type $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \mathbb{Z}_{p^{n_k}}$. This is given as

Theorem 3.3.1. *Any finite abelian group is isomorphic to a direct product* $S_{p_1} \times \cdots \times S_{p_r}$ *where* $n = \prod_{i=1}^{r} p_i^{n_i}$ *is the prime decomposition of the order* $o(G) = n$ *and* S_{p_i} *is the unique Sylow* p_i*-subgroup in* G *of order* $p_i^{n_i}$*. This direct product decomposition is canonical: the subgroups* S_{p_i} *are uniquely determined, as are the primes* p_i *and their exponents* n_i.

Proof. Let us write S_i for the unique Sylow p_i-subgroup. Therefore, $o(S_i) = p_i^{n_i}$. For each index $1 \leq i \leq r$, define the product set $H_i = \prod_{j=1}^{i} S_j$. Since G is abelian, each H_i is a normal subgroup of G.
We now claim that, the order is $o(H_i) = \prod_{j=1}^{i} p_j^{n_j}$.
By definition, it is clear that, $o(H_1) = o(S_1) = p_1^{n_1}$.
When $i = 2$, the order of the subgroup $H_1 \cap S_2 = S_1 \cap S_2$ must divide both $p_1^{n_1}$ and $p_2^{n_2}$, and hence the intersection $H_1 \cap S_2$ is trivial. That is, $H_1 \cap S_2 = \{e\}$ and therefore, $o(H_1 \cap S_2) = 1$.
Using the result, $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)}$, we immediately have that for $H_2 = H_1S_2$,

$o(H_2) = o(H_1S_2) = \dfrac{o(H_1)o(S_2)}{o(H_1 \cap S_2)} = \dfrac{p_1^{n_1}p_2^{n_2}}{1} = p_1^{n_1}p_2^{n_2}$.

At the next stage we have $H_3 = H_2S_3$ and $H_2 \cap S_3$ is again trivial because these subgroups have different prime divisors; applying the same result, we get $o(H_3) = o(H_2)o(S_3) = p_1^{n_1}p_2^{n_2}p_3^{n_3}$. Continuing inductively we prove our claim.

This already implies that G is a direct product. In fact, since $o(G) = o(H_r)$ we see that G is equal to the product set $S_1S_2 \cdots S_r$. It remains only to check that if $a_1a_2 \cdots a_r = e$ with $a_i \in S_i$, then each $a_i = e$. Let q be the smallest index such that a non-trivial decomposition of the identity occurs. Certainly $q > 1$ and $a_q \neq e$, and then $a_q^{-1} = a_1 \cdots a_{q-1}$. But on the left we have an element of S_q and on the right an element of the subgroup H_{q-1}. These subgroups have trivial intersection, which is impossible if $a_q \neq e$. Thus every element in G has a unique decomposition of the form $a_1a_2 \cdots a_r$, and G is the direct product of its Sylow subgroups. ■

Theorem 3.3.2. *(Fundamental Theorem of Finite Abelian Groups) Every finite abelian group is the direct product of its cyclic subgroups.*

Proof. We know that every finite abelian group is isomorphic to the direct product of Sylow subgroups. To prove our theorem it is enough to prove that every Sylow subgroup is the direct product of its cyclic subgroups. Hence without loss of generality, let us assume that the given group G is of order p^n, where p is a prime.

Let $a_1 \in G$ such that $o(a_1) = p^{n_1}, n_1 \leq n$ and such that this a_1 has the highest possible order. Let A_1 be the cyclic group generated by a_1.

That is, $A_1 = (a_1)$.

Let $\overline{G} = \dfrac{G}{A_1}$.

Choose b_2 in G such that $o(\overline{b_2})$ is maximal in $\frac{G}{A_1}$, say p^{n_2} such that

$$b_2^{p^{n_2}} = e. \tag{3.3.1}$$

Therefore $p^{n_2}|o(b_2)$. This shows $n_2 \leq n_1$.

Let p^{n_2} be the least positive integer such that $b_2^{p^{n_2}} \in A_1$.

Since A_1 is the cyclic group generated by a_1 and

$$b_2^{p^{n_2}} \in A_1, \text{we have } b_2^{p^{n_2}} = a_1^i, \text{for some } i. \tag{3.3.2}$$

We claim that there exists a cyclic group, say A_2, of order p^{n_2}.

To prove this claim, let us find an element a_2 in G, with help of b_2, such that $A_2 = (a_2)$.

Consider

$$\begin{aligned} a_1^{ip^{n_1-n_2}} &= (a_1^i)^{p^{n_1-n_2}} \\ &= (b_2^{p^{n_2}})^{p^{n_1-n_2}} \\ &= b_2^{p^{n_2}p^{n_1-n_2}} \\ &= b_2^{p^{n_2}p^{n_1}p^{-n_2}} \\ &= b_2^{p^{n_1}} = e \quad (by (3.3.1)). \end{aligned}$$

That is, $a_1^{ip^{n_1-n_2}} = e$.

But $o(a_1) = p^{n_1} \Rightarrow p^{n_1}|ip^{n_1-n_2} \Rightarrow p^{n_1}p^{n_2}|ip^{n_1}$

$\Rightarrow p^{n_2}|i \Rightarrow i = p^{n_2}.j,$ for some j.

Therefore

$$b_2^{p^{n_2}} = a_1^i = a_1^{p^{n_2}.j}. \tag{3.3.3}$$

Let $a_2 = a_1^{-j}b_2$.

Therefore,

$$\begin{aligned} a_2^{p^{n_2}} &= (a_1^{-j}b_2)^{p^{n_2}} \\ &= a_1^{-jp^{n_2}}b_2^{p^{n_2}} \\ &= a_1^{-jp^{n_2}}a_1^{p^{n_2}.j} \\ &= e \quad (using(3.3.3)). \end{aligned}$$

That is,

$$a_2^{p^{n_2}} = e. \tag{3.3.4}$$

Thus we have found a_2 with help of b_2, such that $o(a_2) = p^{n_2}$.

This proves our Claim .

Now we show that $A_1 \cap A_2 = \{e\}$.

Let $a_2^t \in A_1 \cap A_2$. This implies, $a_2^t \in A_1$ and $a_2^t \in A_2$.

Let us prove that $a_2^t = e$.

Since $a_2 = a_1^{-j}b_2$, we have $a_2^t = \left(a_1^{-j}b_2\right)^t \in A_1$

$\Rightarrow a_1^{-jt}b_2^t \in A_1 \Rightarrow b_2^t \in A_1 \quad (\text{since} \quad a_1^{-jt} \in A_1)$.

But p^{n_2} is the least positive integer such that $b_2^{p^{n_2}} \in A_1$.

Therefore $p^{n_2}/t \Rightarrow t = p^{n_2}k_1$, for some k_1.

But $a_2^t = a_2^{p^{n_2}k_1} = \left(a_2^{p^{n_2}}\right)^{k_1} = e^{k_1} = e$. (using (3.3.4)).

Thus we have shown that $a_2^t = e$.

Let us consider the quotient group $\frac{G}{A_1A_2}$. Choose b_3 in G such that the image of b_3 in $\frac{G}{A_1A_2}$ has maximal order in $\frac{G}{A_1A_2}$, say p^{n_3} such that, $(\overline{b_3})^{p^{n_3}} = e$, $b_3^{p^{n_2}} \in A_1$ and p^{n_3} is the least positive integer such that $b_3^{p^{n_3}} \in A_1A_2$. Therefore $n_3 \leq n_2$.

We can prove that there exist an element a_3, which can be defined with the help of b_3. Let A_3 be the cyclic group generated by a_3 such that $o(A_3) = p^{n_3}$ and $A_3 \cap (A_1A_2) = e$.

Continuing in this way, we get cyclic groups,

$A_1 = (a_1), A_2 = (a_2), \cdots, A_k = (a_k)$ of orders, $p^{n_1}, p^{n_2}, \cdots, p^{n_k}$ respectively, with $n_1 \geq n_2 \geq n_3 \geq \cdots \geq n_k$ such that $G = A_1 A_2 \cdots A_k$ and such that for all i, $A_i \cap (A_1 A_2 \cdots A_{i-1}) = (e)$.
This says that every $x \in G$ has a unique representation as
$x = a_1' a_2' a_3' \cdots a_k'$ where each $a_i' \in A_i$, for $i = 1, 2, 3, \cdots, k$.
Thus G is the direct product of cyclic groups, $A_1, A_2, \cdots, A_k$ of G.
Hence the Theorem is proved. ■

Definition 3.3.1. *The integers $n_1, n_2, \cdots, n_k$ are called invariants of G.*

Definition 3.3.2. *If G is an abelian group and s is any integer, then $G(s) = \{x \in G | x^s = e\}$*

Because G is abelian it is evident that $G(s)$ is a subgroup of G. We now show this in the following lemma.

Lemma 3.3.1. *The set $G(s) = \{x \in G | x^s = e\}$ is a subgroup of an abelian group G.*

Proof. We know that, for an abelian group G,
$(ab)^n = a^n b^n, \forall a, b \in G$ and $n \in \mathbb{N}$.
Let $x, y \in G(s)$. Then, $x^s = e$, and $y^s = e$.
Consider $(xy)^s = x^s y^s = e.e = e$. That is, $x, y \in G(s)$ implies $xy \in G(s)$. Hence, $G(s)$ has closure property.
Now, $(x^{-1})^s = (x^s)^{-1} = e^{-1} = e$. That is, $x \in G(s)$ implies $x^{-1} \in G(s)$. Hence, $G(s)$ is a subgroup of G. This proves the lemma. ■

We now prove a result on isomorphic images of abelian groups.

Lemma 3.3.2. *If G and G' are isomorphic abelian groups, then for every integer $s, G(s)$, and $G'(s)$ are isomorphic.*

Proof. Let ϕ be an isomorphism of G onto G'. We claim that ϕ maps $G(s)$ isomorphically onto $G'(s)$. First we show that $\phi(G(s)) \subset G'(s)$. For, if $x \in G(s)$ then $x^s = e$. Hence $\phi(x^s) = \phi(e) = e'$. But $\phi(x^s) = (\phi(x))^s$. Hence $\phi(x)^s = e'$ and so $\phi(x)$ is in $G'(s)$. Thus $\phi(G(s)) \subset G'(s)$. On the other hand, if $u' \in G'(s)$ then $(u')^s = e'$. But, since ϕ is onto, $u' = \phi(y)$ for some $y \in G$. Therefore $e' = (u')^s = \phi(y)^s = \phi(y^s)$. Because ϕ is one-to-one, we have $y^s = e$ and so $y \in G(s)$. Thus ϕ maps $G(s)$ onto $G'(s)$. Therefore since ϕ is one-to-one, onto, and a homomorphism from $G(s)$ to $G'(s)$, we conclude that $G(s)$ and $G'(s)$ are isomorphic. ■

Lemma 3.3.3. *Let G be an abelian group of order p^n, p a prime. Suppose that $G = A_1 \times A_2 \times \cdots \times A_k$, where each $A_i = (a_i)$ is cyclic of order p^{n_i} and $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. If m is an integer such that $n_1 > n_t > m \geq n_{t+1}$ then $G(p^m) = B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k$ where B_i is cyclic of order p^m, generated by $a_i^{p^{n_i - m}}$, for $i \leq t$. The order of $G(p^m)$ is p^u, where*

$$u = mt + \sum_{i=t+1}^{k} n_i \tag{3.3.5}$$

Proof. It is given that $G = A_1 \times A_2 \times \cdots \times A_k$, and $o(A_i) = p^{n_i}$, $A_i = (a_i)$, $\forall n_1 \geq n_2 \geq \cdots n_k > 0$.

Since $A_i = (a_i)$ and $o(A_i) = p^{n_i}$, we have,

$$o(a_i) = p^{n_i} \Rightarrow a_i^{p^{n_i}} = e \tag{3.3.6}$$

$G(p^m) = \{x \in G | x^{p^m} = e\}$, , where $n_t > m \geq n_{t+1}$

CLAIM 1. $A_i \subseteq G(p^m)$, $\forall i = t+1, t+2, \cdots k$.

It is given that $n_1 \geq n_2 \geq \cdots n_t > m \geq n_{t+1} \geq \cdots \geq n_k > 0$.

Since $m \geq n_{t+1} \geq \cdots \geq n_k > 0$, for every $j \geq t+1$, we have,

$$a_j^{p^m} = (a_j^{p^{n_j}})^{p^{m-n_j}} = e^{p^{m-n_j}} = e. \tag{3.3.7}$$

That is, $a_j^{p^m} = e$, for $j \geq t+1$.

Therefore, $(a_j^{p^m}) \subseteq G(p^m)$

That is, $A_i \subseteq G(p^m)$, $\forall i = t+1, t+2, \cdots, k$.

CLAIM 2. $B_i \subseteq G(p^m)$, for $1 \leq i \leq t$

Clearly, $n_t > m$, when $i \leq k$.

It is given that $B_i = (a_i^{p^{n_i-m}})$.

Now consider,

$$(a_i^{p^{n_i-m}})^{p^m} = (a_i^{p^{n_i}}) = e. \tag{3.3.8}$$

Therefore, $a_i^{p^{n_i-m}} \subseteq G(p^m)$

That is, $B \subseteq G(p^m)$.

Thus, $B_1, B_2, \cdots, B_t, A_{t+1}, \cdots, A_k \subseteq G(p^m)$.

Since, $B_1, B_2, \cdots, B_t, A_{t+1}, \cdots A_k$ are all in $G(p^m)$, their product is also in $G(p^m)$.

That is, $B_1 \times B_2 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k \subseteq G(p^m)$.

CLAIM 3: $G(p^m) \subseteq B_1 \times B_2 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k$.

Let $x \in G(p^m)$. Therefore, $x = a_1^{\lambda_1} a_2^{\lambda_2} a_3^{\lambda_3} \cdots a_k^{\lambda_k}$.

Since, $x \in G(p^m)$, we have, $x^{p^m} = e$.

Therefore, $x^{p^m} = (a_1^{\lambda_1} a_2^{\lambda_2} a_3^{\lambda_3} \cdots a_k^{\lambda_k})^{p^m} = e$

That is, $a_1^{\lambda_1 p^m} a_2^{\lambda_2 p^m} a_3^{\lambda_3 p^m} \cdots a_k^{\lambda_k p^m} = e$

Since the product $G = A_1 \times A_2 \times \cdots A_k$ is direct, we have, $a_i^{\lambda_i p^m} = e$, for $i = 1, 2, \cdots k$.

Since $m \geq t+1 \geq t+2 \geq \cdots \geq n_k$, for $i \geq t+1$, we have $p^{n_i} | p^m$.

As $o(a_i) = p^{n_i}$ and $a_i^{\lambda_i p^m} = e$, we have $p^{n_i} | \lambda_i p^m$.

That is, $p^{n_i-m} | \lambda_i$, for $i \leq t$.

Therefore, $\lambda_i = p^{n_i-m} v_i$, for $i \leq k$.

Now, $x = a_1^{v_1 p^{n_1-m}} a_2^{v_2 p^{n_2-m}} \cdots a_t^{v_t p^{n_t-m}} a_{t+1}^{\lambda_{t+1}} \cdots a_k^{\lambda_k}$

$\Rightarrow x \in B_1 \times B_2 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k$.

$\therefore G(p^m) \subseteq B_1 \times B_2 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k$.

Hence we have

$G(p^m) = B_1 \times \cdots \times B_t \times A_{t+1} \times \cdots \times A_k$. Now,

$o(G(p^m)) = o(B_1) \cdots o(B_t) o(A_{t+1}) o(A_{t+2}) \cdots o(A_k)$.

But $o(B_i) = p^m$, and $o(A_i) = p^{n_i}$,, we have,

$o(G(p^m)) = \underbrace{p^m p^m \cdots p^m}_{t-times} p^{n_{t+1}} \cdots p^{n_k}$. Thus, if order of $G(p^m)$ is p^u, then,

$$u = mt + \sum_{i=t+1}^{k} n_i \tag{3.3.9}$$

and the Theorem is proved. ■

Corollary 3.3.1. *If G is as in Lemma 3.3.3, then $o(G(p)) = p^k$.*

Proof. For the case $m = 1$ in above lemma, we have $t = k$. Therefore, $u = 1k = k$. Hence $o(G) = p^k$. ■

Theorem 3.3.3. *Two abelian groups of order p^n are isomorphic if and only if they have the same invariants.*
In other words, if G and G' are abelian groups of order p^n and $G = A_1 \times \cdots \times A_k$, where each A_i is a cyclic group of order $p^{n_i}, n_1 \geq \cdots \geq n_k > 0$, and $G' = B_1' \times \cdots \times B_s'$, where each B_i' is a cyclic group of order $p^{h_i}, h_1 \geq \cdots \geq h_s > 0$, then G and G' are isomorphic if and only if $k = s$ and for each $i, n_i = h_i$.

Proof. One way is very easy, namely, if G and G' have the same invariants then they are isomorphic. For then $G = A_1 \times \cdots \times A_k$ where $A_i = (a_i)$ is cyclic of order p^{n_i}, and $G' = B_1' \times \cdots \times B_s'$, where $B_i' = (b_i')$ is cyclic of order p^{n_i}.
Define a map ϕ from G onto G' such that $\phi(a_1^{\alpha_1} \cdots a_k^{\alpha_k}) = (b_1')^{\alpha_1} \cdots (b_k')^{\alpha_k}$. We leave it to the reader to verify that this defines an isomorphism of G onto G'.

Now for the other direction. Suppose that $G = A_1 \times \cdots \times A_k$, and $G' = B'_1 \times \cdots \times B'_s$, A_i, B'_i as described above, cyclic of orders p^{n_i}, p^{h_i}, respectively, where $n_1 \geq \cdots \geq n_k > 0$ and $h_1 \geq \cdots \geq h_s > 0$. We want to show that if G and G' are isomorphic then $k = s$ and each $n_i = h_i$.

If G and G' are isomorphic then, by Lemma 3.3.2, $G(p^m)$ and $G'(p^m)$ must be isomorphic for any integer $m \geq 0$, hence must have the same order.

Suppose let $m = 1$. Then by Corollary 3.3.1, $o(G(p)) = p^k$ and $o(G'(p)) = p^s$. Hence $p^k = p^s$ and so $k = s$. Thus we observed that the number of invariants for G and G' is the same.

If $n_i \neq h_i$ for some i, let t be the first i such that $n_t \neq h_t$; we may suppose that $n_t > h_t$. Let $m = h_t$. Consider the subgroups, $H = \{x^{p^m} | x \in G\}$ and $H' = \{(x')^{p^m} | x' \in G'\}$, of G and G', respectively. Since G and G' are isomorphic, it follows easily that H and H' are isomorphic.

We now find the invariants of H and H'.

Because $G = A_1 \times \cdots \times A_k$, where $A_i = (a_i)$ is of order p^{n_i} , we get that $H = C_1 \times \cdots \times C_t \times \cdots \times C_r$, where $C_i = (a_i^{p^m})$ is of order $p^{n_i - m}$, and where r is such that $n_r > m = h_t \geq n_{r-1}$. Thus the invariants of H are $n_1 - m, n_2 - m, \cdots, n_r - m$ and the number of invariants of H is $r \geq t$.

Because $G' = B'_1 \times \cdots \times B'_k$, where $B_i = (b'_i)$ is cyclic of order p^{h_i} , we get that $H' = D'_1 \times \cdots \times D'_{t-1}$, where $D'_i = ((b'_i)^{p^m})$ is cyclic of order $p^{h_i - m.}$ Thus the invariants of H' are $h_1 - m, \cdots, h_{t-1} - m$ and so the number of invariants of H' is $t - 1$. But H and H' are isomorphic. This shows that they have the same number of invariants. Consequently, each $n_i = h_i$, and the theorem is proved. ■

3.4 Non-isomorphic abelian groups

Theorem 3.4.1. *The number of non-isomorphic abelian groups of order p^n, where p is a prime, equals the number of partitions of n.*

Proof. If $n_1 \geq n_2 \geq \cdots \geq n_k > 0$, where $n = n_1 + n_2 + \cdots + n_k$, is any partition of n, then we can easily construct an abelian group of order p^n whose invariants are $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. To do this, let A_i be a cyclic group of order p^{n_i} and let $G = A_1 \times A_2 \times \cdots \times A_k$ be the external direct product of $A_1, A_2, \ldots, A_k$. Then, by the very definition, the invariants of G are $n_1 \geq n_2 \geq \cdots \geq n_k > 0$. Finally, two different partitions of n give rise to nonisomorphic abelian groups of order p^n. Hence the Theorem is proved. ■

Example 3.4.1. *The possible isomorphism types of abelian groups of order 16 are:* $\mathbb{Z}_{16}; \mathbb{Z}_8 \times \mathbb{Z}_2; \mathbb{Z}_4 \times \mathbb{Z}_4; \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2; \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 3.4.2. *The possible isomorphism types of abelian groups of order 100 are*

$\mathbb{Z}_{100}; \mathbb{Z}_{50} \times \mathbb{Z}_2; \mathbb{Z}_{25} \times \mathbb{Z}_4; \mathbb{Z}_{10} \times \mathbb{Z}_{10} : \mathbb{Z}_{20} \times \mathbb{Z}_5$.

Example 3.4.3. *Obviously, all finite groups are finitely generated. For example, the group S_3 is generated by the permutations (12) and (123).*

The group $\mathbb{Z} \times \mathbb{Z}_n$ is an infinite group but is finitely generated by $\{(1,0),(0,1)\}$.

Example 3.4.4. *Find all distinct finite Abelian groups of order $16 = 2^4$.*

Solution: We first list all partitions of 4.

$$4$$
$$3+1$$
$$2+2$$
$$2+1+1$$
$$1+1+1+1$$

This then yields distinct groups:

$$\begin{aligned}
\mathbb{Z}_{2^4} &= \mathbb{Z}_{16} \\
\mathbb{Z}_{2^3} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_8 \times \mathbb{Z}_2 \\
\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} &= \mathbb{Z}_4 \times \mathbb{Z}_4 \\
\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
\mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2
\end{aligned}$$

Example 3.4.5. *Find all distinct finite Abelian groups of order* $72 = 2^3 3^2$

Solution: We first list all partitions for 3 using partitions $3 = 3 = 2+1 = 1+1$:

This then yields distinct groups:

$\mathbb{Z}_8$

$\mathbb{Z}_4 \times \mathbb{Z}_2$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

The partitions for 2 is: $2 = 2 = 1+1$:

This partition yields following distinct groups:

$\mathbb{Z}_9$

$\mathbb{Z}_3 \times \mathbb{Z}_3$

Then we create all possible combinations as

$\mathbb{Z}_8 \times \mathbb{Z}_9$

$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9$

$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

Example 3.4.6. *Suppose that we wish to classify all abelian groups of order* $540 = 2^2.3^3.5$ *. The Fundamental Theorem of Finite Abelian Groups tells us that we have the following six possibilities.*

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$;
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$;
- $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;
- $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$;
- $\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$.

Summary of this unit.

In this lesson we have studied the following:

- If A and B are any two groups then their Cartesian product $G = A \times B$ is also a group with respect to multiplication.
- Let $G_1, G_2, \cdots, G_n$ are normal subgroups of G. The group G is said to be the internal direct product of $G_1, G_2, \cdots, G_n$ if
  (i). $G = G_1 G_2 \cdots G_n$
  (ii).Every element $g \in G$ can be expressed in a unique way as $g = g_1 g_2 g_3 \cdots g_n$ where $g_i \in G_i$.

- Let G be the internal direct product of $N_1, N_2, \cdots, N_n$. Then,
  (i). $N_i \cap N_j = (e)$, for $i \neq j$. More over
  (ii). if $a \in N_i$ and $b \in N_j$, then $ab = ba$.

- Let G be a group and suppose that G is the internal direct product of $N_1, N_2, \cdots, N_n$. Let $T = N_1 \times N_2 \times \cdots N_n$. Then G and T are isomorphic.

- Any finite abelian group is isomorphic to a direct product of its Sylow subgroups.

- Every finite abelian group is the direct product of its cyclic subgroups.

- The set $G(s) = \{x \in G | x^s = e\}$ is a subgroup of an abelian group G.

- If G and G' are isomorphic abelian groups, then for every integer $s, G(s)$, and $G'(s)$ are isomorphic.

- Two abelian groups of order p^n are isomorphic if and only if they have the same invariants.

- The number of non-isomorphic abelian groups of order p^n, where p is a prime, equals the number of partitions of n.

Multiple Choice Questions

1. If G is an abelian group then the set of all elements in G of same order is a
   a) subgroup of G
   b) normal subgroup of G
   c) not a subgroup of G
   d) subgroup but not a normal subgroup of G.

2. The possible isomorphism types of abelian groups of order 16 are:
   a) $Z_{16}$and Z_8
   b) $Z_8 \times Z_2$and $Z_4 \times Z_2$
   c) $Z_4 \times Z_4$and $Z_8 \times Z_2$
   d) $Z_2 \times Z_2 \times Z_2$and $Z_8 \times Z_4$.

3. Let $G = Z_{200} \times Z_8 \times Z_6$. Then G is isomorphic to
   a) $Z_{10} \times Z_8 \times Z_{120}$
   b) $Z_{150} \times Z_4 \times Z_{10}$
   c) $Z_{120} \times Z_6 \times Z_{20}$
   d) $Z_{110} \times Z_4 \times Z_{12}$

4. The abelian groups of order 720 upto isomorphism are
   a) $Z_{16} \times Z_9 \times Z_5$and $Z_4 \times Z_5 \times Z_9 \times Z_5$
   b) $Z_4 \times Z_4 \times Z_9 \times Z_5$and $Z_2 \times Z_8 \times Z_9 \times Z_5$
   c) both (a) and (b)
   d) neither (a) nor (b)

5. The abelian groups upto isomorphism of order 1800 are
   a) $Z_8 \times Z_9 \times Z_{25}$and $Z_4 \times Z_2 \times Z_3 \times Z_3 \times Z_{25}$
   b) $Z_8 \times Z_3 \times Z_3 \times Z_3 \times Z_5$and $Z_8 \times Z_9 \times Z_5 \times Z_5$
   c) both (a) and (b)
   d) (a) is true but (b) is not true.

6. The number of nonisomorphic abelian groups of order 625 is
   a) 5 b) 25 c) 125 d) 625

7. Find generator of Z_{11}
   a) 2 b) 4 c) 5 d) 3

8. Suppose that the order of a finite abelian group G is divisible by 10. Then
   a) G has a cyclic subgroup of order 10.

b) G has a cyclic subgroup of order 12.

c) G has a cyclic subgroup of order 14.

d) G has a cyclic subgroup of order 16.

9. Suppose that G is a finite abelian group that has exactly one subgroup for each divisor of $o(G)$. Then G is

   a) cyclic

   b) not cyclic

   c) simple

   d)not simple

10. A finite Abelian group of prime-power order is an internal direct product of

    a) cyclic groups

    b) noncyclic groups

    c) 2- Sylow subgroups

    d) 3- Sylow subgroups

11. If A and B are cyclic groups of order m and n respectively, then $A \times B$ is cyclic if the possible values of m and n respectively,

    a) 4,6 b) 7,35 c) 5,20 d) 6,7

Answers:

1	2	3	4	5	6	7	8	9	10	11
b	c	a	b	c	a	a	a	a	a	d

Exercise:

1. If A and B are groups, prove that $A \times B$ is isomorphic to $B \times A$.

2. Let A, B be cyclic groups of order m and n, respectively. Prove that $A \times B$ is cyclic if and only if m and n are relatively

prime.

3. Let G be a group. Show that $D = \{(g,g) \in G \times G | g \in G\}$ is isomorphic to G.

4. If G is a group and if $D = \{(g,g) \in G \times G | g \in G\}$, prove that D is normal in $G \times G$ if and only if G is abelian.

5. Find all of the abelian groups of order less than or equal to 40 up to isomorphism.

6. Find all of the abelian groups of order 200 up to isomorphism.

7. Prove that if a finite abelian group has subgroups of orders m and n, then it has a subgroup whose order is the least common multiple of m and n.

8. Describe all finite abelian groups of order 2^6

9. Describe all finite abelian groups of order 11^6

10. Describe all finite abelian groups of order 7^5

11. Describe all finite abelian groups of order $2^4.3^4$

12. Show how to get all abelian groups of order $2^3.3^4.5$

13. Find the number of nonisomorphic abelian groups of order 2^4.

14. Find all abelian groups (up to isomorphism) of order 720.

15. Find up to isomorphism all abelian groups of order 1800.

Block 2 - UNIT 4

Ring Theory

Objectives

- We try to learn about the polynomials
- To study about degree of polynomials
- Try to learn about Division Algorithm
- We study about irreducible polynomial

In this unit, we study about rings and polynomials.

4.1 Ring of Polynomials

If R is a ring, the ring of polynomials in x with coefficients in R is denoted $R[x]$. It consists of all formal sums

$$\sum_{i=0}^{\infty} a_i x^i.$$

Here $a_i = 0$ for all but finitely many values of i. We can replace a formal sum with the infinite vector whose components are the

coefficients of the sum:

$$\sum_{i=0}^{\infty} a_i x^i = (a_0, a_1, a_2, \ldots).$$

All of the operations which we will define using formal sums can be defined using vectors. But it's traditional to represent polynomials as formal sums, so this is what we will do.

4.2 Arithmetic in Polynomials

Definition 4.2.1. *A nonzero polynomial* $f(x) = \sum_{i=0}^{\infty} a_i x^i$ *has degree* n *if* $n \geq 0$ *and* $a_n \neq 0$ *, and* n *is the largest integer with this property. Write* $\deg f(x)$ *to denote the degree of* $f(x)$ *.*

Definition 4.2.2. *If all the coefficients in a polynomial is zero, then it is called a zero polynomial.*

The zero polynomial is defined by convention to have degree $-\infty$. (This is necessary in order to make the degree formulas work out.) Alternatively, we can say that the degree of the zero polynomial is undefined; in that case, we will need to make minor changes to some of the results below.

Polynomials are added component wise, and multiplied using the convolution formula:

Theorem 4.2.1. *If* $f(x) = \sum_{i=0}^{\infty} a_i x^i$ *and* $g(x) = \sum_{i=0}^{\infty} b_i x^i$ *, then,*

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) \cdot \left(\sum_{j=0}^{\infty} b_j x^j\right) = \sum_{k=0}^{\infty} c_k x^k, \quad \text{where} \quad c_k = \sum_{i+j=k} a_i b_j$$

These formulas will help us to compute sums and products as usual.

Example 4.2.1. *(Polynomial arithmetic)*

(a) Compute

$(i).(x^2+2x+2)+(x^2+3)$ *and*

(ii). $(x^2+2x+2)\cdot(x^2+3)$ *in* $\mathbb{Z}[x]$.

(b) Compute

$(i).(2x^2+1)+(4x^2+5)$ *and*

$(ii).\quad (3x+2)\cdot(2x+3)$ *in* $\mathbb{Z}[x]$.

Solution:

(a) (i). $(x^2+2x+2)+(x^2+3)=2x^2+2x.$

(ii). $(x^2+2x+2)\cdot(x^2+3)=x^4+2x^3+x+1.$

(b) (i). $(2x^2+1)+(4x^2+5)=0.$

(ii). $(3x+2)\cdot(2x+3)=6x^2+13x+6=x.$

Lemma 4.2.1. *Let* $p(x)$ *and* $q(x)$ *be polynomials in* $R[x]$*, where* R *is an integral domain. Then* $\deg p(x)+\deg q(x)=\deg\left(p(x)q(x)\right)$. *Furthermore,* $R[x]$ *is an integral domain.*

Proof. Suppose that we have two nonzero polynomials $p(x)=a_mx^m+\cdots+a_1x+a_0$ and $q(x)=b_nx^n+\cdots+b_1x+b_0$ with $a_m\neq 0$ and $b_n\neq 0$. The degrees of $p(x)$ and $q(x)$ are m and n, respectively. The leading term of $p(x)q(x)$ is $a_mb_nx^{m+n}$, which cannot be zero since R is an integral domain; hence, the degree of $p(x)q(x)$ is $m+n$, and $p(x)q(x)\neq 0$. Since $p(x)\neq 0$ and $q(x)\neq 0$ imply that $p(x)q(x)\neq 0$, we know that $R[x]$ must also be an integral domain. ■

The verifications amount to writing out the formal sums, with a little attention paid to the case of the zero polynomial. These formulas do work if either $f(x)$ or $g(x)$ is equal to the zero polynomial, provided that $-\infty$ is understood to behave in the obvious ways (e.g. $-\infty+c=-\infty$ for any $c\in\mathbb{Z}$).

Example 4.2.2. *(Degrees of polynomials)*

(a) Give examples of polynomials $f(x), g(x) \in R[x]$ *such that* $deg(f(x)+g(x)) < \max(deg(f(x)), deg(g(x)))$.

(b) Give examples of polynomials $f(x), g(x) \in \mathbb{Z}_4[x]$ *such that* $deg(f(x)\cdot g(x)) \neq deg(f(x)) + deg(g(x))$.

Solution:

(a) $deg\left[(x^2+2)+(-x^2+5)\right] = deg\, 7 = 0$, whereas $\max\left[deg(x^2+2), deg(-x^2+5)\right] = 2$.

This shows that equality might not hold in $deg(f(x)+g(x)) \leq \max(deg f(x), deg\, g(x))$.

(b) $deg([(2x)\cdot(2x+1)]) = deg(2x) = 1$, but $deg(2x) + deg(2x+1) = 1+1 = 2$.

Lemma 4.2.2. *Let* F *be a field, and let* $F[x]$ *be the polynomial ring in one variable over* F*. The units in* $F[x]$ *are exactly the nonzero elements of* F*.*

Proof. It is clear that the nonzero elements of F are invertible in $F[x]$, since they are already invertible in F.

Conversely, suppose that $f(x) \in F[x]$ is invertible, so $f(x)g(x) = 1$ for some $g(x) \in F[x]$.

Then $deg\, f(x) + deg\, g(x) = deg\, 1 = 0$, which is impossible unless f(x) and g(x) both have degree 0.

In particular, $f(x)$ is a nonzero constant, that is an element of F. ■

Theorem 4.2.2. *(Division Algorithm):*

Let F *be a field, and let* $f(x), g(x) \in F[x]$. *Suppose that* $g(x) \neq 0$. *There are unique polynomials* $q(x), r(x) \in F[x]$ *such that* $f(x) = g(x)q(x) + r(x)$, *and* $deg\, r(x) < deg\, g(x)$.

Proof. The idea is to imitate the proof of the Division Algorithm for

$\mathbb{Z}$.

Let $S = \{f(x) - g(x)q(x) \mid q(x) \in F[x]\}$.

The set $\{deg(s(x)) \mid s(x) \in S\}$ is a subset of the nonnegative integers, and therefore must contain a smallest element by well-ordering.

Let $r(x) \in S$ be an element in S of smallest degree, and write $r(x) = f(x) - g(x)q(x)$, where $q(x) \in F[x]$.

We need to show that $deg\, r(x) < deg\, g(x)$. If $r(x) = 0$, then since $g(x) \neq 0$, we have $deg\, g(x) \geq 0 > -\infty = deg\, r(x)$.

Suppose then that $r(x) \neq 0$. Assume toward a contradiction that $deg\, r(x) \geq deg\, g(x)$.

Write $r(x) = r_n x^n + \cdots + r_1 x + r_0$,

$g(x) = g_m x^m + \cdots + g_1 x + g_0$.

Assume $r_n, g_m \neq 0$, and $n \geq m$.

Consider the polynomial

$r(x) - \frac{r_n}{g_m} x^{n-m} g(x) =$

$(r_n x^n + \cdots + r_1 x + r_0) - \left(r_n x^n + \frac{r_n}{g_m} x^{n-1} + \cdots \right)$.

Its degree is less than n, since the n-th degree terms cancel out.

However,

$$r(x) - \frac{r_n}{g_m} x^{n-m} g(x) = f(x) - g(x)q(x) - \frac{r_n}{g_m} x^{n-m} g(x)$$

$$= f(x) - g(x) \left(q(x) + \frac{r_n}{g_m} x^{n-m} \right).$$

The latter is an element of S.

We have found an element of S of smaller degree than $r(x)$, which is a contradiction.

It follows that $deg\, r(x) < deg\, g(x)$.

Finally, to prove uniqueness, suppose

$f(x) = g(x)q(x) + r(x) = g(x)q'(x) + r'(x)$, and
$deg\, r(x), deg\, r'(x) < deg\, g(x)$. Rearranging the equation, we get
$g(x)(q(x) - q'(x)) = r'(x) - r(x)$.
Then
$deg\,(r'(x) - r(x)) = deg[g(x)(q(x) - q'(x))] = deg\, g(x) + deg(q(x) - q'(x))$.
But $deg(r'(x) - r(x)) < deg\, g(x)$.
The equation can only hold if
$r'(x) - r(x) = 0$ and $q(x) - q'(x) = 0$.
Hence, $r(x) = r'(x)$ and $q(x) = q'(x)$. ■

4.3 Irreducible Polynomials

In this section we prove some results on irreducible polynomials.

Definition 4.3.1. *A polynomial $p(x) \in F[x]$ is irreducible over F if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$, then either $a(x)$ or $b(x)$ has degree zero. That is $a(x)$ or $b(x)$ is a constant.*

Proposition 4.3.1. *A nonzero nonconstant polynomial $f(x) \in F[x]$ is irreducible if and only if $f(x) = g(x)h(x)$ implies that either $g(x)$ or $h(x)$ is a constant.*

Proof. Suppose $f(x)$ is irreducible and $f(x) = g(x)h(x)$. Then one of $g(x)$, $h(x)$ is a unit. But we have shown earlier that the units in $F[x]$ are the constant polynomials.
Suppose that $f(x)$ is a nonzero nonconstant polynomial, and $f(x) = g(x)h(x)$ implies that either $g(x)$ or $h(x)$ is a constant polynomial.
Since $f(x)$ is nonconstant, it is not a unit. Note that if
$f(x) = g(x) = h(x)$, then $g(x), h(x) \neq 0$ since $f(x) \neq 0$.
Therefore, the condition that $f(x) = g(x)h(x)$ implies that either

$g(x)$ or $h(x)$ is a constant polynomial means that $f(x) = g(x)h(x)$ implies that either $g(x)$ or $h(x)$ is a unit.
Again, the nonzero constant polynomials are the units in $F[x]$. This is what it means for $f(x)$ to be irreducible. ■

Example 4.3.1. *Show that* $x^2 + 1$ *is irreducible in* $\mathbb{R}[x]$ *but not in* $\mathbb{C}[x]$.

$x^2 + 1$ has no real roots, so by the Root Theorem it has no linear factors. Hence, it is irreducibile in $\mathbb{R}[x]$.
However, $x^2 + 1 = (x + i)(x - i)$ in $\mathbb{C}[x]$.

Corollary 4.3.1. *Let* F *be a field. A polynomial of degree* 2 *or* 3 *in* $F[x]$ *is irreducible if and only if it has no roots in* F.

Proof. Suppose $f(x) \in F[x]$ has degree 2 or 3.
If $f(x)$ is not irreducible, then $f(x) = g(x)h(x)$, where neither $g(x)$ nor $h(x)$ is a constant polynomial.
Now $deg\, g(x) \geq 1$ and $deg\, h(x) \geq 1$, and

$$deg\, g(x) + deg\, h(x) = deg\, f(x) = 2 \quad \text{or} \quad 3.$$

This is only possible if at least one of $g(x)$ or $h(x)$ has degree 1. This means that at least one of $g(x)$ or $h(x)$ is a linear factor $ax + b$, and must therefore have a root in F. Since $f(x) = g(x)h(x)$, it follows that $f(x)$ has a root in F as well.
Conversely, if $f(x)$ has a root c in F, then $x - c$ is a factor of $f(x)$ by the Root Theorem. Since $f(x)$ has degree 2 or 3, $x - c$ is a proper factor, and $f(x)$ is not irreducible. ■

Remark: The result is false for polynomials of degree 4 or higher. For example, $(x^2 + 1)^2$ has no roots in $\mathbb{R}$, but it is not irreducible over $\mathbb{R}$.

Definition 4.3.2. *Let F be a field, let $F[x]$ be the ring of polynomials with coefficients in F, and let $f(x), g(x) \in F[x]$, where $f(x)$ and $g(x)$ are not both zero. The greatest common divisor of $f(x)$ and $g(x)$ is the monic polynomial which is a greatest common divisor of $f(x)$ and $g(x)$ (in the integral domain sense).*

Let F be a field, and suppose $p(x) \in F[x]$. $\langle p(x) \rangle$ is the set of all multiples (by polynomials) of $p(x)$, the (principal) ideal generated by $p(x)$. When we form the quotient ring $\frac{F[x]}{\langle p(x) \rangle}$, it is as if we have to set multiples of $p(x)$ equal to 0.

If $a(x) \in F[x]$, then $a(x) + \langle p(x) \rangle$ is the coset of $\langle p(x) \rangle$ represented by $a(x)$.

Define $a(x) \equiv b(x) \mod p(x)$.

That is, $a(x)$ is congruent to $b(x)$ mod $p(x)$ to mean that

$$p(x) \mid a(x) - b(x).$$

In words, this means that $a(x)$ and $b(x)$ are congruent mod $p(x)$ if they differ by a multiple of $p(x)$. In equation form, this says $a(x) - b(x) = k(x) \cdot p(x)$ for some $k(x) \in F[x]$, or $a(x) = b(x) + k(x) \cdot p(x)$ for some $k(x) \in F[x]$.

Lemma 4.3.1. *Let R be a commutative ring, and suppose $a(x), b(x), p(x) \in R[x]$. Then $a(x) \equiv b(x) \mod p(x)$ if and only if $a(x) + \langle p(x) \rangle = b(x) + \langle p(x) \rangle$.*

Proof. Suppose $a(x) \equiv b(x) \mod p(x)$. Then $a(x) = b(x) + k(x) \cdot p(x)$ for some $k(x) \in R[x]$. Hence,

$$a(x) + \langle p(x) \rangle = (b(x) + k(x) \cdot p(x)) + \langle p(x) \rangle = b(x) + \langle p(x) \rangle.$$

Conversely, suppose $a(x) + \langle p(x)\rangle = b(x) + \langle p(x)\rangle$. Then

$$a(x) \in a(x) + \langle p(x)\rangle = b(x) + \langle p(x)\rangle.$$

Hence,

$$a(x) = b(x) + k(x) \cdot p(x) \quad \text{for some} \quad k(x) \in R[x].$$

This means that $a(x) \equiv b(x) \mod p(x)$.
Depending on the situation, we may write $a(x) \equiv b(x) \mod p(x)$ or $a(x) + \langle p(x)\rangle = b(x) + \langle p(x)\rangle$. ■

Example 4.3.2. *(A quotient ring of the rational polynomial ring) Take* $p(x) = x - 2$ *in* $\mathbb{Q}[x]$. *Then two polynomials are congruent mod* $(x-2)$ *if they differ by a multiple of* $x - 2$.
(a) Show that $2x^2 + 3x + 5 \equiv x^2 + 4x + 7 \mod (x-2)$.
(b) Find a rational number r such that $x^3 - 4x^2 + x + 11 \equiv r \mod (x-2)$.
(c) Prove that $\dfrac{\mathbb{Q}[x]}{\langle x-2\rangle} \simeq \mathbb{Q}$.

Solution:

(a) $(2x^2 + 3x + 5) - (x^2 + 4x + 7) = x^2 - x - 2 = (x+1)(x-2)$.
So, $2x^2 + 3x + 5 = x^2 + 4x + 7 \mod (x-2)$.
(b) By the Remainder Theorem, when $f(x) = x^3 - 4x^2 + x + 11$ is divided by $x - 2$, the remainder is
$f(2) = 2^3 - 4 \cdot 2^2 + 2 + 11 = 5$.
Thus, $x^3 - 4x^2 + x + 11 = (x-2)q(x) + 5$.
That is, $x^3 - 4x^2 + x + 11 \equiv 5 \mod (x-2)$
(c) We will use the First Isomorphism Theorem. Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}$ by $\phi(f(x)) = f(2)$.

That is, ϕ evaluates a polynomial at $x = 2$. Note that

$$\phi(f(x) + g(x)) = f(2) + g(2) = \phi(f(x)) + \phi(g(x))$$

$$\text{and} \quad \phi(f(x)g(x)) = f(2)g(2) = \phi(f(x))\,\phi(g(x)),$$

It follows that ϕ is a ring homomorphism. We claim that $Ker\,\phi = \langle x-2\rangle$.

Now $f(x) \in Ker\,\phi$ if and only if $f(2) = \phi(f(x)) = 0$.

That is, $f(x) \in Ker\phi$ if and only if 2 is a root of $f(x)$. By the Root Theorem, this is equivalent to $x - 2 \mid f(x)$, which is equivalent to $f(x) \in \langle x-2\rangle$.

That is, $Ker\,\phi =< x-2 >$.

Next, we will show that ϕ is surjective. Let $q \in \mathbb{Q}$. We can think of q as a constant polynomial, and doing so, $\phi(q) = q$, Therefore, ϕ is surjective.

Using these results, $\dfrac{\mathbb{Q}[x]}{\langle x-2\rangle} \simeq \mathbb{Q}$.

In the last example, $\dfrac{F[x]}{\langle p(x)\rangle}$ was a field. The next result says that this is the case exactly when $p(x)$ is irreducible.

Theorem 4.3.1. *$\dfrac{F[x]}{\langle p(x)\rangle}$ is a field if and only if $p(x)$ is irreducible.*

Proof. Since $F[x]$ is a commutative ring with identity, so is $\dfrac{F[x]}{\langle p(x)\rangle}$.

Suppose $p(x)$ is irreducible. We need to show that $\dfrac{F[x]}{\langle p(x)\rangle}$ is a field. That is we have to show that nonzero elements are invertible.

Take a nonzero element of $\dfrac{F[x]}{\langle p(x)\rangle}$ (say) $a(x) + \langle p(x)\rangle$, for $a(x) \in F[x]$.

What does it mean for $a(x) + \langle p(x)\rangle$ to be nonzero?

It means that $a(x) \notin \langle p(x)\rangle$, so $p(x) \nmid a(x)$.

Now what is the greatest common divisor of $a(x)$ and $p(x)$?

Well, $(a(x), p(x)) \mid p(x)$, but $p(x)$ is irreducible, so, its only factors

are units and unit multiples of $p(x)$.

Suppose $(a(x), p(x)) = k \cdot p(x)$, where $k \in F$ and $k \neq 0$. Then $k \cdot p(x) \mid a(x)$, that is, $k \cdot p(x)b(x) = a(x)$ for some $b(x)$.

But then $p(x)[k \cdot b(x)] = a(x)$ shows that $p(x) \mid a(x)$, contrary to assumption.

The only other possibility is that $(a(x), p(x)) = k$, where $k \in F$ and $k \neq 0$.

So we can find polynomials $m(x)$, $n(x)$, such that $a(x)m(x) + p(x)n(x) = k$.

Then, $a(x) \cdot \left(\frac{1}{k}m(x)\right) + p(x) \cdot \left(\frac{1}{k}n(x)\right) = 1$.

Hence,

$$\begin{aligned} 1+ < p(x) > &= \left[a(x)\left(\frac{1}{k}m(x)\right) + p(x)\left(\frac{1}{k}n(x)\right)\right] + \langle p(x)\rangle \\ 1 + \langle p(x)\rangle &= a(x)\left(\frac{1}{k}m(x)\right) + \langle p(x)\rangle \\ 1 + \langle p(x)\rangle &= (a(x) + \langle p(x)\rangle)\left(\frac{1}{k}m(x) + \langle p(x)\rangle\right) \end{aligned}$$

This shows that $\frac{1}{k}m(x) + \langle p(x)\rangle$ is the multiplicative inverse of $a(x) + \langle p(x)\rangle$. Therefore, $a(x) + \langle p(x)\rangle$ is invertible, and $\frac{F[x]}{\langle p(x)\rangle}$ is a field, which proves one part of the theorem.

Going the other way, suppose that $p(x)$ is not irreducible. Then we can find polynomials $c(x)$, $d(x)$ such that $p(x) = c(x)d(x)$, where $c(x)$ and $d(x)$ both have smaller degree than $p(x)$.

Because $c(x)$ and $d(x)$ have smaller degree than $p(x)$, they are not divisible by $p(x)$.

In particular, $c(x) + \langle p(x)\rangle \neq 0$ and $d(x) + \langle p(x)\rangle \neq 0$.

But $p(x) = c(x)d(x)$ gives

$p(x) + \langle p(x)\rangle = c(x)d(x) + \langle p(x)\rangle$

$\Rightarrow\ 0 = (c(x) + \langle p(x)\rangle)(d(x) + \langle p(x)\rangle)$

This shows that $\frac{F[x]}{\langle p(x)\rangle}$ has zero divisors. Therefore, it is not an

integral domain and since fields are integral domains, it can not be a field, either. ■

Example 4.3.3. *(A quotient ring which is not an integral domain) Prove that* $\frac{\mathbb{Q}[x]}{\langle x^2-1\rangle}$ *is not an integral domain by exhibiting a pair of zero divisors.*

$(x-1)+\langle x^2-1\rangle$ *and* $(x+1)+\langle x^2-1\rangle$ *are zero divisors, because* $(x-1)(x+1) = x^2-1 \equiv 0 \mod x^2-1$.

Solved Problems

Problem 1 Find the greatest common divisor of the following polynomials over $\mathbb{Q}$, the field of rational numbers: x^2+1 and x^6+x^3+x+1.

Solution: Using long division method, we have

$x^6+x^3+x+1 = (x^2+1)(x^4-x^2+x+1)$.

So we have $gcd(x^6+x^3+x+1, x^2+1) = gcd(x^2+1, 0) = x^2+1$.

So we have $gcd(x^6+x^3+x+1, x^2+1) = x^2+1$

Problem 2 Prove that x^2+x+1 is irreducible over $\mathbb{Z}_2$, the field of integers $\mod 2$.

Solution: We have

$$x^2+x+1\,|_{x=0} = 1 \mod 2$$
$$x^2+x+1\,|_{x=1} = 1 \mod 2$$

So $x^2+x+1 \neq 0, \forall\, x \in \mathbb{Z}_2$, implying x^2+x+1 is irreducible in $\mathbb{Z}_2[x]$.

Problem 3 Prove that x^2+1 is irreducible over $\mathbb{Z}_7$, the integers $\mod 7$.

Solution: We have

$$\begin{aligned} x^2+1\,|_{x=0} &= 1 \mod 7 \\ x^2+1\,|_{x=1} &= 2 \mod 7 \\ x^2+1\,|_{x=2} &= 5 \mod 7 \\ x^2+1\,|_{x=3} &= 3 \mod 7 \\ x^2+1\,|_{x=4} &= 3 \mod 7 \\ x^2+1\,|_{x=5} &= 5 \mod 7 \\ x^2+1\,|_{x=6} &= 2 \mod 7 \end{aligned}$$

So $x^2+1 \neq 0, \forall\, x \in \mathbb{Z}_7$. So x^2+1 is irreducible in $\mathbb{Z}_7[x]$

Problem 3 Let F, K be two fields $F \subset K$ and suppose $f(x), g(x) \in F[x]$ are relatively prime in $F[x]$. Prove that they are relatively prime in $K[x]$.

Solution: First we can easily see that if 1 is the multiplicative identity of F, then it is also the multiplicative identity of K too. Now since $f(x), g(x)$ are relatively prime in $F[x]$, so $1 = \lambda(x)f(x) + \mu(x)g(x)$, for some $\lambda(x), \mu(x) \in F[x]$. But since $F \subset K$, therefore $1, \lambda(x), \mu(x), f(x), g(x)$ are also elements of $K[x]$. So the relation $1 = \lambda(x)f(x) + \mu(x)g(x)$ is equally valid in $K[x]$. But that would mean $f(x), g(x)$ as elements of $K[x]$ are relatively prime in $K[x]$. Hence the result.

Problem 4 Prove that x^2+1 is irreducible over the field $\mathbb{Z}_{11}$ of integers $\mod 11$, is a field having 121 elements.

Solution: We have

$$\begin{aligned}
x^2+1\,|_{x=0} &= 1 \mod 11\\
x^2+1\,|_{x=1} &= 2 \mod 11\\
x^2+1\,|_{x=2} &= 5 \mod 11\\
x^2+1\,|_{x=3} &= 10 \mod 11\\
x^2+1\,|_{x=4} &= 6 \mod 11\\
x^2+1\,|_{x=5} &= 4 \mod 11\\
x^2+1\,|_{x=6} &= 4 \mod 11\\
x^2+1\,|_{x=7} &= 6 \mod 11\\
x^2+1\,|_{x=8} &= 10 \mod 11\\
x^2+1\,|_{x=9} &= 5 \mod 11\\
x^2+1\,|_{x=10} &= 2 \mod 11
\end{aligned}$$

So $x^2+1 \neq 0$, $\forall\, x \in \mathbb{Z}_{11}$. So x^2+1 is irreducible over $\mathbb{Z}_{11}[x]$.
Now consider $\dfrac{\mathbb{Z}_{11}[x]}{\langle x^2+1\rangle}$.
Since $\langle x^2+1\rangle$ is an ideal of $\mathbb{Z}_{11}[x]$, so $\dfrac{\mathbb{Z}_{11}[x]}{\langle x^2+1\rangle}$ is a ring.
Also $\dfrac{\mathbb{Z}_{11}[x]}{\langle x^2+1\rangle} = \{\langle x^2+1\rangle + ax + b \mid a, b \in \mathbb{Z}_{11}\}$.
Since $\mathbb{Z}_{11}$ has 11 elements, so $\dfrac{\mathbb{Z}_{11}[x]}{\langle x^2+1\rangle}$ has $11 \times 11 = 121$ elements.

Summary of this unit.

In this unit we have studied the following:

- Let $p(x)$ and $q(x)$ be polynomials in $R[x]$, where R is an integral domain. Then $\deg p(x) + \deg q(x) = \deg\,(p(x)q(x))$. Furthermore, $R[x]$ is an integral domain.
- (Division Algorithm): Let F be a field, and let $f(x), g(x) \in F[x]$. Suppose that $g(x) \neq 0$. There are unique polynomials

$q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$, and $deg\, r(x) < deg\, g(x)$.

- A polynomial $p(x) \in F[x]$ is irreducible over F if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$, then either $a(x)$ or $b(x)$ has degree zero. That is $a(x)$ or $b(x)$ is a constant.
- A nonzero nonconstant polynomial $f(x) \in F[x]$ is irreducible if and only if $f(x) = g(x)h(x)$ implies that either $g(x)$ or $h(x)$ is a constant.

Multiple Choice Questions

1. The polynomial $x^2 + 1$ is reducible over
   a) R b) Q c) Z d) Z_2
2. The polynomial $x^2 + 1$ is irreducible over
   a) C b) Q(i) c) Z[i] d) R
3. Highest Degree of irreducible polynomial over Real numbers is
   a) 1 b) 2 c) 3 d) 4
4. Highest Degree of irreducible polynomial over Complex numbers is
   a) 1 b) 2 c) 3 d) 4
5. Find the polynomial which is irreducible over Q
   a) $x^2 + 3$
   b) $x^2 + 5x + 4$
   c) x^4
   d) $x^2 - 1$
6. Find the polynomial which is reducible over Q
   a) $x^2 + 3$
   b) $x^2 + 5x$

c) $x^4 - 2$

d) $x^2 + 1$

7. Find the number of Quadratic polynomials which is irreducible over Z_2

a) 3 b) 1 c) 4 d) 8

8. $\frac{Z_2[x]}{<x^3+x^2+1>}$ is

a) a field having 8 elements

b) a field having 9 elements

c) an infinite field

d) not a field.

9. The set $\frac{Q[x]}{< x^2-1 >}$ is a

a) quotient ring

b) Integral domain

c) quotient ring but not an integral domain

d) both (a) and (b) are true

10. The gcd of $x^2 + 1$ and $x^6 + x^3 + x + 1$ over Q is

a) $x^2 + 1$ b) $x + 1$ c) $x - 1$ d) $x^2 - 1$

11. The set $\frac{Z_{11}[x]}{< x^2+1 >}$ is a

a) ring

b) ring but not a field

c) field with 11 elements

d) field with 121 elements

Answers:

1	2	3	4	5	6	7	8	9	10	11
d	d	b	a	a	b	b	a	c	a	d

Exercise

1. Prove that $\dfrac{\mathbb{Z}_2[x]}{\langle x^2+x+1\rangle}$ is a field.
2. Prove that x^3-9 is irreducible over $\mathbb{Z}_{31}$ the integers $\mod 31$.
3. Prove that x^3-9 is reducible over $\mathbb{Z}_{11}$ the integers $\mod 11$.
4. Find $ax+b\in\mathbb{Z}_2[x]$ so that

$$(x^4+x^3+1)+\langle x^2+x+1\rangle=(ax+b)+\langle x^2+x+1\rangle.$$

5. Construct addition and multiplication tables for $\dfrac{\mathbb{Z}_2[x]}{\langle x^2+x+1\rangle}$.
6. How many elements are in the quotient ring $\dfrac{\mathbb{Z}_3[x]}{\langle 2x^2+x+2\rangle}$?
7. Reduce the following product in $\dfrac{\mathbb{Z}_3[x]}{\langle 2x^2+x+2\rangle}$ to the form $(ax+b)+\langle 2x^2+x+2\rangle$:

$$(2x+1+\langle 2x^2+x+2\rangle)\cdot(x+1+\langle 2x^2+x+2\rangle).$$

8. Find $[x+2+\langle 2x^2+x+2\rangle]^{-1}$ in $\dfrac{\mathbb{Z}_3[x]}{\langle 2x^2+x+2\rangle}$.
9. Show that $\dfrac{\mathbb{Z}_3[x]}{\langle x^3+2x+1\rangle}$ is a field.
10. How many elements are there in $\dfrac{\mathbb{Z}_3[x]}{\langle x^3+2x+1\rangle}$?
11. Compute:
    $\left[(x^2+x+2)+\langle x^3+2x+1\rangle\right]\left[(2x^2+1)+\langle x^3+2x+1\rangle\right]$.
    Express your answer in the form $(ax^2+bx+c)+\langle x^3+2x+1\rangle$, where $a,b,c\in\mathbb{Z}_3$.
12. Find $\left[(x^2+1)+\langle x^3+2x+1\rangle\right]^{-1}$.
13. Prove directly that $\dfrac{\mathbb{Z}_{11}[x]}{\langle x^2+1\rangle}$ is a field having 121 elements.
14. Prove directly that $\dfrac{\mathbb{Z}_{11}[x]}{\langle x^2+x+4\rangle}$ is a field having 121 elements.

Block 3 - UNIT 5

Polynomial over the Rational Field

Objectives

- We try to learn about Primitive polynomials
- To study about the Content of the polynomial
- Learn about greatest common divisor
- Try to learn about Gauss' Lemma
- We study monic polynomials
- To Study about Eisenstein Criterion

In this unit, we study polynomials over the field of rational numbers.

5.1 Primitive Polynomials

Definition 5.1.1. ***(The pigeonhole principle):***

If n objects are distributed over m places, and if $n > m$, then some

place receives atleast two objects.

Definition 5.1.2. ***(The Content of the polynomial):***
Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x + \cdots + \alpha_m x^m$, *where the* $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_m$, *are integers. The content of* $f(x)$ *is defined as the* gcd *of* $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_m$.

Clearly, given any polynomial $f(x)$ with integer coefficients it can be written as $f(x) = c \cdot g(x)$ where c is the content of $f(x)$ and where $g(x)$ is a primitive polynomial.

Definition 5.1.3. ***(Primitive polynomial):***
The polynomial $f(x) = a_0 + a_1 x + a_2 x + \cdots + a_n x_n$, *where the* $a_0, a_1, a_2, \ldots, a_n$, *are integers is said to be primitive if the* gcd *of* $a_0, a_1, \ldots, a_n$ *is* 1. *That is, the content is* 1.

Lemma 5.1.1. *If* $f(x)$ *and* $g(x)$ *are primitive polynomials, then* $f(x)g(x)$ *is a primitive polynomial.*

Proof. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n, a_n \neq 0$ and
$g(x) = b_0 + b_1 x + \cdots + b_m x^m, b_m \neq 0.$
Let $f(x)g(x) = h(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{m+n} x^{m+n}, c_{m+n} \neq 0.$
Let us prove this theorem by method of contradiction.
Suppose that $h(x)$ is not primitive, then there exists some prime number p such that it divides all the coefficients of $h(x)$.
Since $f(x)$ is primitive, p can not divide all the coefficients of $f(x)$.
That is, there exist some coefficients of $f(x)$ which are not divisible by p.
Let a_j be the first coefficient of $f(x)$ which p does not divide. That is, $p \mid a_{j-1}, a_{j-2}, \cdots, a_1, a_0$.
But, $p \nmid a_j, a_{j+1}, \cdots, p \nmid a_n$.
Similarly let b_k be the first coefficient of $g(x)$ which p does not divide. That is, $p \mid b_{k-1}, b_{k-2}, \cdots, b_1, b_0$.

But, $p \nmid b_k, b_{k+1}, \cdots, p \nmid b_m$.

In $p(x)$, the coefficient c_{j+k} of x^{j+k} is of the form

$c_{j+k} = a_j b_k + (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0) + (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0 b_{j+k}) \cdots (1)$

Since, $p \mid b_{k-1}, b_{k-2}, \cdots, b_1, b_0$, we get

$p|(a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0)$.

Again since, $p \mid a_{j-1}, a_{j-2}, \cdots, a_1, a_0$, we get

$p \mid (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + \cdots + a_0 b_{j+k})$.

But by assumption, we have, p divides all the coefficients of $h(x)$ and whence $p \mid c_{j+k}$.

Thus by equation (1) , we get, $p \mid a_j b_k$, which is a contradiction since $p \nmid a_j$ and $p \nmid b_k$. This proves the lemma. ■

Lemma 5.1.2. *(Gauss' Lemma)*

If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.

Proof. Suppose that $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ have rational coefficients.

By clearing of fractions and taking out common factors, we can then write $f(x) = \frac{\alpha}{\beta} \cdot a(x) \cdot b(x)$ where α and β are integers and where both $a(x)$ and $b(x)$ have integer coefficients and are primitive.

Thus $\beta f(x) = \alpha a(x) \cdot b(x)$. The content of the left-hand side is β , since $f(x)$ is primitive; since both $a(x)$ and $b(x)$ are primitive, by Lemma 5.1.1 , their product $a(x) \cdot b(x)$ is also primitive, so that the content of the right-hand side is α. Therefore $\alpha = \beta$, whence, $\frac{\alpha}{\beta} = 1$, and therefore, $f(x) = a(x) \cdot b(x)$, where, both $a(x)$ and $b(x)$ have integer coefficients, which proves the theorem. ■

Definition 5.1.4. *A monic polynomial is a polynomial whose leading coefficient is 1.*

Example 5.1.1. *For example, here are some monic polynomials over* $\mathbb{Q}$ *:*

$$x^3 - 3x + 5, \quad x^{100} - \frac{2}{3}x^{17}, \quad x + 42.$$

Definition 5.1.5. *(Integer Monic)*
A polynomial is said to be integer monic if all its coefficients are integers and its highest coefficient is 1.

Thus an integer monic polynomial is merely one of the form $x^m + \alpha_1 x^{m-1} + \alpha_2 x^{m-2} + \cdots + \alpha_m$ where the $\alpha's$ are integers. Clearly an integer monic polynomial is primitive.

Corollary 5.1.1. *If an integer monic polynomial factors as the product of two nonconstant polynomials having rational coefficients then it factors as the product of two integer monic polynomials.*

Definition 5.1.6. *Let* F *be a field, let* $F[x]$ *be the ring of polynomials with coefficients in* F*, and let* $f(x), g(x) \in F[x]$ *, where* $f(x)$ *and* $g(x)$ *are not both zero. The greatest common divisor of* $f(x)$ *and* $g(x)$ *is the monic polynomial which is a greatest common divisor of* $f(x)$ *and* $g(x)$ *(in the integral domain sense).*

Example 5.1.2. *(Polynomial greatest common divisors)*
Find the greatest common divisor of $x^2 - 4$ *and* $x^2 - x - 2$ *in* $\mathbb{Q}[x]$.
$x - 2$ *is a greatest common divisor of* $x^2 - 4$ *and* $x^2 - x - 2$:

$$x^2 - 4 = 1 \cdot (x^2 - x - 2) + (x - 2)$$

$$x^2 - x - 2 = (x + 1)(x - 2) + 0$$

Notice that any nonzero constant multiple of $x - 2$ is also a greatest common divisor of $x^2 - 4$ and $x^2 - x - 2$ (in the integral domain sense):
For example, $\frac{1}{100}(x - 2)$ works.

This makes sense, because the units in $\mathbb{Q}[x]$ are the nonzero elements of $\mathbb{Q}$.

But by convention, will refer to $x-2$, the monic greatest common divisor as the greatest common divisor of x^2-4 and x^2-x-2.

5.2 The Eisenstein Criterion

Here we give a criteria which declare that a given polynomial is irreducible or not.

Lemma 5.2.1. *(THE EISENSTEIN CRITERION):*
Let $f(x)=a_0+a_1x+a_2x+\cdots+a_nx^n$ be a polynomial with integer coefficients. Suppose that for some prime number p ,
(i) $p \mid a_0, a_1, a_2, \ldots, a_{n-1}$
(ii) $p \nmid a_n$
(iii) $p^2 \nmid a_0$. Then $f(x)$ is irreducible over the rationals.

Proof. It is given that $f(x)=a_0+a_1x+a_2x+\cdots+a_nx^n \cdots(1)$ is a polynomial with integer coefficients. Let us prove this theorem by method of contradiction.

Without loss of generality we may assume that $f(x)$ is primitive and reducible over rationals.

Since $f(x)$ is reducible, we can factor this as a product of two polynomials over rationals and hence by Gauss's lemma, over integers. That is, we can write $f(x)$ as

$f(x)=(b_0+b_1x+\cdots+b_rx^r)(c_0+c_1x+\cdots+c_sx^s) \cdots(2)$

where the b's and c's are integers and where $r>0$ and $s>0$.

Comparing the coefficients of (1) and (2), we first get $a_0=b_0c_0$.

Since $p \mid a_0$, p must divide either b_0 or c_0.

Since $p^2 \nmid a_0$, p cannot divide both b_0 and c_0.

Let us assume that $p \mid b_0, p \nmid c_0$. Since $p \nmid a_n$, we get, not all the

coefficients $b_0, b_1, \cdots, b_r$ can be divisible by p. Let b_k be the first coefficient, not divisible by p, $k \leq r < n$.

Thus $p \mid b_{k-1}, b_{k-2}, \cdots, b_1, b_0$.

But $a_k = b_k c_0 + b_{k-1} c_1 + b_{k-2} c_2 + \cdots + b_0 c_k \cdots (3)$

Now, $p \mid a_k$ and $p \mid b_{k-1}, b_{k-2}, \cdots, b_1, b_0$, whence from (3), we get, $p \mid b_k c_0 \cdots (4)$

However, we have, $p \nmid c_0$ and $p \nmid b_k$, which is a contradiction to (4). This contradiction proves that we could not have factored $f(x)$ and so $f(x)$ is irreducible, whence the lemma. ■

Summary of this unit.

In this unit we have studied the following:

- The polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, where the $a_0, a_1, a_2, \ldots, a_n$, are integers is said to be primitive if the gcd of $a_0, a_1, \ldots, a_n$ is 1.
- If $f(x)$ and $g(x)$ are primitive polynomials, then $f(x)g(x)$ is a primitive polynomial.
- Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x + \cdots + \alpha_m x^m$, where the $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_m$, are integers. The content of $f(x)$ is defined as the gcd of $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_m$.
- Gauss' Lemma : If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficients, it can be factored as the product of two polynomials having integer coefficients.
- A monic polynomial is a polynomial whose leading coefficient is 1.
- A polynomial is said to be integer monic if all its coefficients are integers and its highest coefficient is 1.

- If an integer monic polynomial factors as the product of two nonconstant polynomials having rational coefficients then it factors as the product of two integer monic polynomials.

- Let F be a field, let $F[x]$ be the ring of polynomials with coefficients in F, and let $f(x), g(x) \in F[x]$, where $f(x)$ and $g(x)$ are not both zero. The greatest common divisor of $f(x)$ and $g(x)$ is the monic polynomial which is a greatest common divisor of $f(x)$ and $g(x)$.

- THE EISENSTEIN CRITERION : Let $f(x) = a_0 + a_1x + a_2x + \cdots + a_nx^n$ be a polynomial with integer coefficients. Suppose that for some prime number p,
  (i) $p \mid a_0, a_1, a_2, \ldots, a_{n-1}$
  (ii) $p \nmid a_n$
  (iii) $p^2 \nmid a_0$. Then $f(x)$ is irreducible over the rationals.

Multiple Choice Questions

1. The content of the polynomial $f(x) = 4 + 10x + 16x^2 + 32x^3$ is
   a) 2 b) 4 c) 6 d) 8

2. The polynomial $f(x) = 1 + 2x + 3x^2 + 4x^3$ is
   a) primitive
   b) has all roots in Z
   c) has atleast two roots in Z
   d) has all the roots in Q

3. If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficients, then
   a) it can be factored as the product of two polynomials having integer coefficients.
   b) it can be factored as the product of two polynomials having real coefficients.

c) it can be factored as the product of two polynomials having non-real coefficients.

d) it can be factored as the product of two polynomials having irrational coefficients.

4. The polynomial $f(x) = 1 + 11x - 13x^2 + 6x^3$ is

   a) primitive and monic

   b) primitive but not monic

   c) Not primitive but monic

   d) Not primitive and not monic

5. The polynomial $x^8 - 7 \in Q[x]$ is

   a) irreducible in Z but reducible in Q

   b) reducible in Q but irreducible in R

   c) irreducible in Q

   d)None of the above

6. The polynomial $1 + x + x^2 + \cdots + x^{16}$ is

   a) reducible in Z

   b) reducible in Q

   c) irreducible in Q

   d)None of the above

7. which of the following are monic polynomials?

   a) $2x^3 + 5x^2 + 6x + 1$ and $\frac{2}{5}x^3 + x^2 + \frac{6}{5}x + \frac{1}{5}$

   b) $4x^3 + 2x^2 + x + 1$ and $x^3 + \frac{1}{2}x^2 + \frac{1}{4}x + 1$

   c) $x^3 + 2x^2 + 5x + 10$ and $x^{301} + \frac{1}{2}x^2 + 16x + 11$

   d) $x^2 + 1$ and $2x^3 + 5x + 1$

8. The integer monic polynomials are

   a) $4x^3 + 5x^2 + 1$ and $x^5 + 6$

   b) $4x^3 + 2x^2 + x + 1$ and $x^3 + \frac{3}{5}x^2 + \frac{1}{9}x + 1$

c) $x^3 + 51x^2 + 91$ and $x^{15} + 116$

d) $x^3 + \frac{3}{51}x^2 + 11$ and $x^3 + 2x^2 + x + 1$

Answers:

1	2	3	4	5	6	7	8
b	a	a	a	c	c	c	c

Block 3 - UNIT 6

Extension Fields

Objectives

- We try to learn finite extensions
- To study about algebraic elements
- Learn about algebraic extension
- Try to learn about finite extension of a finite extension
- We study algebraic extension of an algebraic extension
- To Study about algebraic number

In this unit, we shall be concerned with the relation of one field to another. A field K is an extension field of a field F if F is a sub field of K. The field F is called the base field . We write $F \subset K$. Throughout this unit, F will denote a given field and K an extension of F.

6.1 Introduction

The concept of field extensions can soon lead to very interesting and peculiar results. The following examples will illustrate this: Initially, take the field Q. Now, clearly, we have the polynomial $p(x) = x^2 - 2 \in Q[x]$; however, it should be evident that its roots, $\pm\sqrt{2} \notin Q$. This polynomial is then said to be irreducible over Q. Thus, by considering the quotient ring $\frac{Q[x]}{(x^2-2)}$, we find that we obtain another field, denoted $Q(\sqrt{2})$ or $Q(-\sqrt{2})$
Secondly take the field R. Again, we may easily find a polynomial, which is irreducible over our field. Choosing $p(x) = x^2 + 1 \in R[x]$, it is obvious that the roots, $\pm i \notin R$. Thus, if we consider the quotient ring, $\frac{R[x]}{(x^2+1)}$, we obtain the field $R(i)(\simeq C!)$.

Example 6.1.1. *For example, let $F = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ and let $E = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ be the smallest field containing both $\mathbb{Q}$ and $\sqrt{2} + \sqrt{3}$. Both E and F are extension fields of the rational numbers. We claim that E is an extension field of F. To see this, we need only show that $\sqrt{2}$ is in E. Since $\sqrt{2} + \sqrt{3}$ is in E, $\frac{1}{(\sqrt{2}+\sqrt{3})} = \sqrt{3} - \sqrt{2}$ must also be in E. Taking linear combinations of $\sqrt{2} + \sqrt{3}$ and $\sqrt{3} - \sqrt{2}$, we find that $\sqrt{2}$ and $\sqrt{3}$ must both be in E.*

6.2 Finite Extensions

Let K be a finite extension of a field F. If we regard K as a vector space over F, then we can bring the machinery of linear algebra to bear on the problems that we will encounter in our study of fields. The elements in the field K are vectors; the elements in the field

F are scalars. We can think of addition in K as adding vectors. When we multiply an element in K by an element of F, we are multiplying a vector by a scalar. This view of field extensions is especially fruitful if a field extension K of F is a finite dimensional vector space over F. Thus if we prove that K is a vector space over F, then K has a basis over F. We know that the dimension of K over F is denoted by, $dim_F K$. The degree of K over F is denoted by $[K : F] = dim_F K$. If $[K : F]$ is finite then we say that K is a finite extension of F. The next theorem is a counting theorem, similar to Lagrange's Theorem in group theory.

Theorem 6.2.1. *Let K be a finite extension of F and let L be an extension of K then L is a finite extension of F. More over* $[L : K][K : F] = [L : F]$
(OR) Every finite extension of a finite extension is finite.

Proof. It is given that K is a finite extension of F.
Therefore $[K : F]$ is finite.
Let $[K : F] = n$. That is, $dim_F K = n$.
Then K has a basis consisting of n elements over F.
Let $v_1, v_2, \cdots, v_n$ be a basis for K over F.
It is also given that L is a finite extension of K.
Therefore $[L : K]$ is finite.
Let $[L : K] = m$. That is, $dim_K L = m$.
Then L has a basis consisting of m elements over K.
Let $w_1, w_2, \cdots, w_m$ be a basis for L over K.
Consider the subset
$S = \{v_1w_1, v_2w_1, v_3w_1, \cdots v_nw_1, v_1w_2, v_2w_2, v_3w_2, \cdots$
$v_nw_2, \cdots\cdots v_1w_m, v_2w_m, v_3w_m, \cdots, v_nw_m\}$.

Clearly the set S has mn elements.
Since m and n are finite we have mn is also finite.

We claim that S is a basis for L over F.

Indeed, first we prove that S is linearly independent.

Consider the linear combination

$f_{11}v_1w_1 + f_{21}v_2w_1 + f_{31}v_3w_1 + \cdots + f_{n1}v_nw_1 +$

$f_{12}v_1w_2 + f_{22}v_2w_2 + f_{32}v_3w_2 + \cdots + f_{n2}v_nw_2 +$

$f_{13}v_1w_3 + f_{23}v_2w_3 + f_{33}v_3w_3 + \cdots + f_{n3}v_nw_3 +$

. . . . . .

$f_{1i}v_1w_i + f_{2i}v_2w_i + f_{3i}v_3w_i + \cdots + f_{ni}v_nw_i +$

. . . . . .

$f_{1m}v_1w_m + f_{2m}v_2w_m + f_{3m}v_3w_m + \cdots + f_{nm}v_nw_m = 0 \cdots\cdots (1)$

That is,

$(f_{11}v_1 + f_{21}v_2 + f_{31}v_3 + \cdots + f_{n1}v_n)w_1 +$

$(f_{12}v_1 + f_{22}v_2 + f_{32}v_3 + \cdots + f_{n2}v_n)w_2 +$

$(f_{13}v_1 + f_{23}v_2 + f_{33}v_3 + \cdots + f_{n3}v_n)w_3 +$

. . . . . .

$(f_{1i}v_1 + f_{2i}v_2 + f_{3i}v_3 + \cdots + f_{ni}v_n)w_i +$

. . . . . .

$(f_{1m}v_1 + f_{2m}v_2 + f_{3m}v_3 + \cdots + f_{nm}v_n)w_m = 0$

$k_1w_1 + k_2w_2 + k_3w_3 + \cdots + k_mw_m = 0 \cdots\cdots (2)$ where

$k_1 = f_{11}v_1 + f_{21}v_2 + f_{31}v_3 + \cdots + f_{n1}v_n$

$k_2 = f_{12}v_1 + f_{22}v_2 + f_{32}v_3 + \cdots + f_{n2}v_n$

$k_3 = f_{13}v_1 + f_{23}v_2 + f_{33}v_3 + \cdots + f_{n3}v_n$

. . . . . .

$k_i = f_{1i}v_1 + f_{2i}v_2 + f_{3i}v_3 + \cdots + f_{ni}v_n$

. . . . . .

$k_m = f_{1m}v_1 + f_{2m}v_2 + f_{3m}v_3 + \cdots + f_{nm}v_n$

Clearly $k_1, k_2, k_3, \cdots, k_m \in K$.

Since $\{w_1, w_2, \cdots, w_m\}$ is a basis for L over K, they are linearly independent over K.

Therefore, $k_1w_1 + k_2w_2 + k_3w_3 + \cdots + k_mw_m = 0$

$\Rightarrow k_1 = 0, k_2 = 0, k_3 = 0, \cdots, k_m = 0$

Now $k_1 = 0 \Rightarrow f_{11}v_1 + f_{21}v_2 + f_{31}v_3 + \cdots + f_{n1}v_n = 0;$

$k_2 = 0 \Rightarrow f_{12}v_1 + f_{22}v_2 + f_{32}v_3 + \cdots + f_{n2}v_n = 0;$

$k_3 = 0 \Rightarrow f_{13}v_1 + f_{23}v_2 + f_{33}v_3 + \cdots + f_{n3}v_n = 0;$

. . . . . .

$k_i = 0 \Rightarrow f_{1i}v_1 + f_{2i}v_2 + f_{3i}v_3 + \cdots + f_{ni}v_n = 0;$

. . . . . .

$k_m = 0 \Rightarrow f_{1m}v_1 + f_{2m}v_2 + f_{3m}v_3 + \cdots + f_{nm}v_n = 0;$

But $\{v_1, v_2, \cdots, v_n\}$ is a basis for K over F.

Therefore, they are linearly independent over F.

$f_{11}v_1 + f_{21}v_2 + f_{31}v_3 + \cdots + f_{n1}v_n = 0$

$\Rightarrow f_{11} = 0, f_{21} = 0, f_{31} = 0, \cdots f_{n1} = 0$.

Similarly, $f_{12} = 0, f_{22} = 0, f_{32} = 0, \cdots, f_{n2} = 0 \cdots, f_{1m} = 0, f_{2m} = 0, f_{3m} = 0, \cdots, f_{nm} = 0$.

Thus all f'_{ij}s are separately zero.

Thus S is linearly independent.

Next we will prove S span L over F.

Let $t \in L$. Since $\{w_1, w_2, \cdots, w_m\}$ is a basis for L over K, we have,

$t = k_1w_1 + k_2w_2 + k_3w_3 + \cdots + k_mw_m$.

Since $\{v_1, v_2, \cdots, v_n\}$ is a basis for K over F, we have,

$k_1 = f_{11}v_1 + f_{21}v_2 + f_{31}v_3 + \cdots + f_{n1}v_n$

$k_2 = f_{12}v_1 + f_{22}v_2 + f_{32}v_3 + \cdots + f_{n2}v_n$

$k_3 = f_{13}v_1 + f_{23}v_2 + f_{33}v_3 + \cdots + f_{n3}v_n$

. . . . . .

$k_i = f_{1i}v_1 + f_{2i}v_2 + f_{3i}v_3 + \cdots + f_{ni}v_n$

. . . . . .

$k_m = f_{1m}v_1 + f_{2m}v_2 + f_{3m}v_3 + \cdots + f_{nm}v_n$, where all $f_{ij} \in F$.

Thus, $t = (f_{11}v_1 + f_{21}v_2 + f_{31}v_3 + \cdots + f_{n1}v_n)w_1 +$

$(f_{12}v_1 + f_{22}v_2 + f_{32}v_3 + \cdots + f_{n2}v_n)w_2 +$

$(f_{13}v_1 + f_{23}v_2 + f_{33}v_3 + \cdots + f_{n3}v_n)w_3 +$

. . . . . .

$(f_{1i}v_1 + f_{2i}v_2 + f_{3i}v_3 + \cdots + f_{ni}v_n)w_i +$

. . . . . .

$(f_{1m}v_1 + f_{2m}v_2 + f_{3m}v_3 + \cdots + f_{nm}v_n)w_m$.

That is,

$t = f_{11}v_1w_1 + f_{21}v_2w_1 + f_{31}v_3w_1 + \cdots + f_{n1}v_nw_1 +$

$f_{12}v_1w_2 + f_{22}v_2w_2 + f_{32}v_3w_2 + \cdots + f_{n2}v_nw_2 +$

$f_{13}v_1w_3 + f_{23}v_2w_3 + f_{33}v_3w_3 + \cdots + f_{n3}v_nw_3 +$

. . . . . .

$f_{1i}v_1w_i + f_{2i}v_2w_i + f_{3i}v_3w_i + \cdots + f_{ni}v_nw_i +$

. . . . . .

$f_{1m}v_1w_m + f_{2m}v_2w_m + f_{3m}v_3w_m + \cdots + f_{nm}v_nw_m$.

Thus every element in L can be expressed as a linear combination of elements of S over F.

Hence S span L over F.

Therefore S is a basis for L over F.

Since S has mn elements, dimension of L over F is mn.

That is $[L : F] = mn = nm = [L : K][K : F]$. Hence the theorem. ■

Corollary 6.2.1. *If K is a finite extension of F and L is a finite extension of K then $[L : K]|[L : F]$ or $[K : F]|[L : F]$.*

It is important to note that if $[L : F]$ is a prime number, then there can be no fields properly between F and L.

If the polynomial $q(x) \in F[x]$, the ring of polynomials in x over F, and $q(x) = \beta_0x^m + \beta_1x^{m-1} + \cdots + \beta_m$, then for any element $b \in K$, by $q(b)$ we shall mean the element $\beta_0b^m + \beta_1b^{m-1} + \cdots + \beta_m$, in K. In the expression commonly used, $q(b)$ is the value of the polynomial $q(x)$ obtained by substituting b for x. The element

b is said to satisfy $q(x)$ if $q(b) = 0$.

Definition 6.2.1. *An element a is said to be a root of a polynomial $f(x)$ if $f(a) = 0$, where $f(x)$ is a nonzero polynomial.*

6.3 Algebraic elements

Definition 6.3.1. *An element $a \in K$ is said to be algebraic over F if it satisfies a nonzero polynomial over F.*

Example 6.3.1. *The number $\sqrt{2}$ is algebraic over the field Q. The extension $Q(\sqrt{2})$ of Q is algebraic. Since every element $\alpha \in Q(\sqrt{2},$ can be expressed as $\alpha = a + b\sqrt{2}$ for $a, b \in Q$, it can very easily be seen that α is the root of some polynomial in $Q[x]$ (Simply take the polynomial $p(x) = x^2 - 2ax + a^2 + b^2$. Its roots are $a + b\sqrt{2}$ and $a - b\sqrt{2}$. On the other hand, the extension R of Q is not algebraic (because of the existence of transcendental numbers such as e and π which are not the roots of any polynomials in $Q[x]$).*

Example 6.3.2. *Both $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$ since they are roots of the polynomials $x^2 - 2$ and $x^2 + 1$, respectively. Clearly π and e are algebraic over the real numbers; however, it is a nontrivial fact that they are transcendental over $\mathbb{Q}$. Numbers in $\mathbb{R}$ that are algebraic over $\mathbb{Q}$ are in fact quite rare. Almost all real numbers are transcendental over $\mathbb{Q}$. (In many cases we do not know whether or not a particular number is transcendental; for example, it is not known whether $\pi + e$ is transcendental or algebraic.)*

Example 6.3.3. *We will show that $\sqrt{2 + \sqrt{3}}$ is algebraic over $\mathbb{Q}$. If $\beta = \sqrt{2 + \sqrt{3}}$ then $\beta^2 = 2 + \sqrt{3}$. Hence, $\beta^2 - 2 = \sqrt{3}$ and $(\beta^2 - 2)^2 = 3$.*

Since $\beta^4 - 4\beta^2 + 1 = 0$*, it must be true that* β *is a root of the polynomial* $x^4 - 4x^2 + 1 \in \mathbb{Q}[x]$.

Definition 6.3.2. *An element* $a \in K$ *is said to be algebraic of degree* n *over* F *if it satisfies a nonzero polynomial over* F *of degree* n *but no polynomial of degree less than* n*.*

Let K be an extension of F and let a be in K.
Let $\mathcal{M}$ be the collection of all subfields of K which contain both F and a.
$\mathcal{M}$ is not empty, for K itself is an element of $\mathcal{M}$.
Now, as is easily proved, the intersection of any number of subfields of K is again a subfield of K.
Thus the intersection of all those subfields of K which are members of $\mathcal{M}$ is a subfield of K.
We denote this subfield by $F(a)$.
Certainly it contains both F and a, since this is true for every subfield of K which is a member of $\mathcal{M}$.
Moreover, by the very definition of intersection, every subfield of K in $\mathcal{M}$ contains $F(a)$, yet $F(a)$ itself is in $\mathcal{M}$.
Thus $F(a)$ is the smallest subfield of K containing both F and a.
We call $F(a)$ the subfield obtained by adjoining a to F.
The description of $F(a)$, so far, has been purely an external one. We now give an alternative and more constructive description of $F(a)$.
Consider all these elements in K which can be expressed in the form $\beta_0 + \beta_1 a + \cdots + \beta_r a^r$. Here the β' can range freely over F and r can be any non negative integer. As elements in K, one such element can be divided by another, provided the latter is not 0. Let U be the set of all such quotients. clearly U is a subfield of K.

On one hand, U certainly contains F and a, whence $U \supset F(a)$. On the other hand, any subfield of K which contains both F and a, by virtue of closure under addition and multiplication, must contain all the elements $\beta_0 + \beta_1 a + \cdots + \beta_r a^r$, where each $\beta_i \in F$. Thus $F(a)$ must contain all these elements; being a subfield of K, $F(a)$ must also contain all quotients of such elements. Therefore, $F(a) \supset U$. The two relations $U \subset F(a)$, $U \supset F(a)$ imply that $U = F(a)$. In this way we have obtained an internal construction of $F(a)$, namely as U.

We now intertwine the property that $a \in K$ is algebraic over F with macroscopic properties of the field $F(a)$ itself. This is

Theorem 6.3.1. *An element $a \in K$ is algebraic over F if and only if $F(a)$ is a finite extension of F*

Proof. (**If part**): Let $F(a)$ is a finite extension of F.

We claim that a is algebraic over F.

Clearly, $a \in F(a)$.

$\therefore a^2, a^3, \cdots, a^n \in F(a)$.

That is, $1, a, a^2, a^3, \cdots, a^n \in F(a)$.

But $F(a)$ is a vector space of dimension n.

Hence these $(n+1)$ elements are linearly dependent over F.

Therefore there exist scalars $\alpha_0, \alpha_1, \cdots \alpha_n$ not all zero such that

$\alpha_0 1 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_n a^n = 0$

That is, a satisfies a nonzero polynomial $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$ over F.

Hence a is algebraic over F.

(**Only if part**): Let $a \in K$ is algebraic over F

we prove that $F(a)$ is a finite extension of F.

Suppose $a \in K$ is algebraic over F. We will prove that $F(a)$ is a finite extension of F.

Consider the ring of polynomials $F[x]$ over F.

Since $a \in K$ is algebraic over F , a satisfies a nonzero polynomial over F.

Let $p(x)$ be the minimal polynomial for a.

Clearly $p(a) = 0$, and $p(x) \in F[x]$.

Now we show that $p(x)$ is irreducible over F.

Suppose $p(x)$ is reducible over F.

Then it can be written as $p(x) = f(x)g(x)$, for some, $f(x), g(x) \in F[x]$.

Clearly, $deg(f(x)) \leq deg(p(x))$ and $deg(g(x)) \leq deg(p(x))$.

Since $p(x) = f(x)g(x)$, we have, $p(a) = f(a)g(a)$.

That is, $0 = f(a)g(a)$. This implies that $f(a) = 0$ or $g(a) = 0$.

This implies that a satisfies either $f(x)$ or $g(x)$, which is a contradiction.

$\therefore p(x)$ is irreducible over F.

Let $deg(p(x)) = n$. Consider the ideal generated by $p(x)$.

$< p(x) >= V = \{t(x) \in F[x] | p(x)$ divides $t(x)$ or $t(x)$ is a multiple of $p(x)\}$.

Since $p(x)$ is irreducible, we have V is maximal.

Therefore $\frac{F[x]}{V}$ is a field.

Since $F \subseteq F[x]$, $\frac{F[x]}{V}$ is an extension of F.

Moreover $dim_F(\frac{F[x]}{V}) = deg(p(x))$, which is a finite quantity .

Therefore $\frac{F[x]}{V}$ is a finite extension of F.

Further we claim that $F(a) \simeq \frac{F[x]}{V}$

Define $\psi : F[x] \to F[a]$ such that $\psi(f(x)) = f(a)$.

Now let us prove that ψ is a ring homomorphism.

$\psi(f(x) + g(x)) = f(a) + g(a) = \psi(f(x)) + \psi(g(x))$

$\psi(f(x).g(x)) = f(a).g(a) = \psi(f(x)).\psi(g(x))$

Therefore ψ is a ring homomorphism.

$$\begin{aligned} Ker\psi &= \{f(x) \in F[x] | \psi(f(x)) = 0\} \\ Ker\psi &= \{f(x) \in F[x] | f(a) = 0\} \\ &= \{set\ of\ all\ polynomials\ satisfied\ by\ a\} \\ &= \{set\ of\ all\ polynomials\ divisible\ by\ p(x)\} \\ &= \{set\ of\ all\ polynomials\ which\ are\ multiples\ of\ p(x)\} \\ &= V,\ the\ ideal\ generated\ by\ p(x). \end{aligned}$$

That is $Ker\psi = V$

Therefore by fundamental homomorphism theorem on rings, we have,

$\frac{F[x]}{V} \simeq \psi(F[x])$.

But for every $\alpha \in F, \psi(\alpha) = \alpha$.

$\therefore F \subseteq \psi(F[x])$.

Moreover $a \in \psi(F[x])$.

Thus, $\psi(F[x])$ is a field which contains both F and a.

But $F(a)$ is the smallest field containing both F and a.

Hence $\psi(F[x]) = F(a)$.

$\therefore F(a) \simeq \frac{F[x]}{V}$

Since $\frac{F[x]}{V}$ is a finite extension of F and $F(a) \simeq \frac{F[x]}{V}$, we have $F(a)$ is a finite extension of F. Hence the theorem. ■

Theorem 6.3.2. *If $a \in K$ is algebraic of degree n over F, then $[F(a) : F] = n$.*

Definition 6.3.3. *Let K be a finite extension of F. Let $a, b \in K$ are algebraic over F, then $F(a, b)$ is a field obtained by adjoining a to F and then adjoining b to $F(a)$. Clearly $F(a, b) = F(b, a)$.*

Definition 6.3.4. *Let $a_1, a_2, \cdots, a_n \in K$ are algebraic over F. Then $F(a_1, a_2, \cdots, a_n)$ is a field obtained by adjoining $a_1, a_2, \cdots, a_n$ to F.*

6.4 Algebraic Closure

Given a field F, the question arises as to whether or not we can find a field K such that every polynomial $p(x)$ has a root in K. This leads us to the following theorem.

Theorem 6.4.1. *Let K be a finite extension of F. If $a, b \in K$ are algebraic over F, then, $a \pm b, ab, \frac{a}{b}, (b \neq 0)$ are also algebraic over F. (OR) If K is a finite extension of F, then the set of all algebraic elements of a field F forms a sub field of F.*

Proof. It is given that a is algebraic over F.
Therefore $F(a)$ is a finite extension of F.
Let $F(a) = T$. That is, $[T : F]$ is finite. Clearly, $F \subseteq T$. It is also given that b is algebraic over F.
Since $F \subseteq T, b$ is algebraic over F implies, b is algebraic over T.
Therefore $T(b)$ is a finite extension of T.
Let $T(b) = W$. That is, $[W : T]$ is finite.
Clearly, W is a subfield of K.
Since $a, b \in W$, and W is a field, we have, $a \pm b, ab, \frac{a}{b}, (b \neq 0)$ are also in W.
Therefore, $a \pm b, ab, \frac{a}{b}, (b \neq 0)$ are algebraic over F. Hence the theorem.

■

Here, too, we have proved somewhat more. Since $[W : F] \leq mn$, every element in W satisfies a polynomial of degree at most mn over F, whence the

Corollary 6.4.1. *If a and b in K are algebraic over F of degrees m and n, respectively, then $a \pm b, ab,$ and $\frac{a}{b}$ (if $b \neq 0$) are algebraic over F of degree at most mn.*

Definition 6.4.1. *Let K be a finite extension of F. If every element in K is algebraic over F, then K is called an algebraic extension of F.*

Theorem 6.4.2. *If K is algebraic extension of F and L is algebraic extension of K then, L is algebraic extension of F. (OR) Algebraic extension of an algebraic extension is algebraic.*

Proof. It is given that K is algebraic extension of F and L is algebraic extension of K.
Our aim is to show that L is algebraic extension of F.
Let $a \in L$, be arbitrary. We will show that a satisfies a nonzero polynomial over F.
Since L is algebraic extension of K, a satisfies a nonzero polynomial over K.
Let this polynomial be $h(x) = k_0 + k_1x + k_2x^2 + \cdots + k_nx^n$, where, $k_0, k_1, k_2, \cdots, k_n \in K$.
Since K is algebraic extension of F, we have
$F(k_0, k_1, k_2, \cdots, k_n)$ is a finite extension of F.
Let $M = F(k_0, k_1, k_2, \cdots, k_n)$. Now $h(x)$ is a polynomial over M. Hence a is algebraic over M. Therefore $M(a)$ is a finite extension of M.
Now, M is a finite extension of F and $M(a)$ is a finite extension of M and therefore, $M(a)$ is a finite extension of F.
That is, $[M(a) : F] =$ finite. Therefore, a is algebraic over F.
Since a is arbitrary, all the elements of L are algebraic over F.
Hence, L is algebraic extension of F. Hence the theorem. ■

The preceding results are of special interest in the particular case in which F is the field of rational numbers and K the field of complex numbers.

Definition 6.4.2. *A complex number is said to be an algebraic number if it is algebraic over the field of rational numbers.*

The set of all algebraic numbers form a field.

Definition 6.4.3. *An algebraic number a is said to be an algebraic integer if it satisfies an equation of the form $a^m + \alpha_1 a^{m-l} + \cdots + \alpha_m = 0$, where $\alpha_1, \alpha_2, \alpha_3, \cdots \alpha_m$ are integers.*

Definition 6.4.4. *A number which is not algebraic is called transcendental.*

Solved Problems

Problem 1. Prove that the mapping $\psi : F[x] \to F(a)$ defined by $\psi(h(x)) = h(a)$ is a homomorphism.

Solution: Let $f(x), g(x)$ be two elements in $F[x]$. Then $\psi(f(x) + g(x)) = \psi(f+g)(x) = (f+g)(a) = f(a) + g(a) = \psi(f(x)) + \psi(g(x))$.

Moreover $\psi(f(x)g(x)) = f(a)g(a) = \psi(f(x))\psi(h(x))$. Hence is a homomorphism.

Problem 2. Let F be a field and let $F[x]$ be the ring of polynomials in x over F. Let $g(x)$ of degree n, be in $F[x]$ and let $V =< g(x) >$ be the ideal generated by $g(x)$ in $F[x]$. Prove that $\frac{F[x]}{V}$ is an n-dimensional vector space over F.

Solution: $\frac{F[x]}{V} = \{f(x) + V \mid f(x) \in F[x]\}$. V is the ideal generated by the polynomial $g(x)$ of degree n. Since $F[x]$ is a Euclidean ring there exists $h(x)$ and $r(x) \in F[x]$ such that $f(x) = g(x)h(x) + r(x)$ where either $r(x) = 0$ or $degr(x) < degg(x)$. Group structure of $\frac{F[x]}{V}$ is already known. For any $\lambda \in F$, and $f(x) + V \in \frac{F[x]}{V}$ define $\lambda(f(x) + V) = \lambda f(x) + V$, with this addition and multiplication by an element of F, the set $\frac{F[x]}{V}$ forms a vector space over the field F. Every element of $\frac{F[x]}{V}$

can be written uniquely as a linear combination of the elements $1+V, x+V, \cdots, x^{n-1}+V$. Indeed let $f(x)+V = a_0+a_1x+\cdots+a_{n-1}x^{n-1}+V = b_0+b_1x+\cdots+b_{n-1}x^{n-1}+V$ Then $(a_0-b_0)+(a_1-b_1)x+\cdots+(a_{n-1}-b_{n-1})x^{n-1} \in V$. But every non-zero element in V has degree $\lambda \geq n$. Hence $(a_0-b_0)+(a_1-b_1)x+\cdots+(a_{n-1}-b_{n-1})x^{n-1}=0$. Then $a_i = b_i$ for all $i = 0, \cdots, n-1$. Therefore the set $\{1+V, x+V, \cdots, x^{n-1}+V\}$ forms a basis for the vector space $\frac{F[x]}{V}$ of dimension n. On the other hand, it is clear that every element in $\frac{F[x]}{V}$ can be written as a linear combination of the above elements.

Problem 3. (a) Let $\mathbb{R}$ be the field of real numbers and $\mathbb{Q}$ the field of rational numbers. In $\mathbb{R}$, $\sqrt{2}$ and $\sqrt{3}$ are both algebraic over $\mathbb{Q}$. Exhibit a polynomial of degree 4 over $\mathbb{Q}$ satisfied by $\sqrt{2}+\sqrt{3}$.
(b) What is the degree of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$? Prove your answer.
(c) What is the degree of $\sqrt{2}\sqrt{3}$ over $\mathbb{Q}$?
Solution: Let $x = \sqrt{2}+\sqrt{3}$ then $x^2 = 2+3+2\sqrt{6}$ and $x^2-5 = 2\sqrt{6}$
$(x^2-5)^2 = 4\times 6$
$x^4-10x^2+25 = 24$
$x^4-10x^2+1 = 0$
$f(x) = x^4-10x^2+1 \in \mathbb{Q}[x]$ has $\sqrt{2}+\sqrt{3}$ as a root.
(b) $f(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$. Firstly $f(x)$ does not have any root in $\mathbb{Q}$ because the only possible roots in $\mathbb{Q}$ are ± 1 but $f(\pm 1) \neq 0$. On the other hand $f(x)$ cannot be factored as a product of polynomials of degree 2. One can see this by substituting $t = x^2$ in the above equation. Hence $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$.
(c) Let $x = \sqrt{2}\sqrt{3}$ then $x^2 = 2\times 3$. Hence $f(x) = x^2-6$ is satisfied by $\sqrt{2}\sqrt{3}$ and by Eisenstein criterion $f(x)$ is irreducible. Hence $[\mathbb{Q}(\sqrt{2}\sqrt{3}) : \mathbb{Q}] = 2$.

Problem 4. With the same notation as in problem 3 , show that $\sqrt{2}+\sqrt[3]{5}$ is algebraic over $\mathbb{Q}$ of degree 6.

Solution: Let $a = \sqrt{2}+\sqrt[3]{5}$. Then $(a-\sqrt{2})^3 = 5$. We get $a^3 - 3a^2\sqrt{2} + 6a - 2\sqrt{2} = 5a^3 + 6a - 5 = (3a^2+2)\sqrt{2}$.

Hence $(a^3+6a-5)^2 = 2(3a^2+2)^2$.

So $a^6 - 6a^4 - 10a^3 + 12a^2 - 60a + 17 = 0$.

Now if one goes backwards finds that the polynomial $p(x) = x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17$ is satisfied by a.

Now we need to show that $[\mathbb{Q}(a) : \mathbb{Q}] = 6$. We will show that the possibilities $[\mathbb{Q}(a) : \mathbb{Q}) = 3$ or $[\mathbb{Q}(a) : \mathbb{Q}] = 2$ cannot occur. Then we conclude that $[\mathbb{Q}(a) : \mathbb{Q}] = 6$.

Let $F = \mathbb{Q}(\sqrt[3]{5}, \sqrt{2})$. Then, $[\mathbb{Q}(a, \sqrt{2}), \mathbb{Q}] = [\mathbb{Q}(a, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}), \mathbb{Q}] = 6$.

If $[\mathbb{Q}(a) : \mathbb{Q}] = 3$, then,

$\underbrace{[\mathbb{Q}(a, \sqrt[3]{5}) : \mathbb{Q}(a)]}_{2}\underbrace{[\mathbb{Q}(a) : \mathbb{Q}]}_{3} = 6$. There exists $p(x) \in \mathbb{Q}(a)[x]$ such that $p(\sqrt[3]{5}) = 0$.

The polynomial $p(x)$ is irreducible and of degree 2. But $p(x)$ must divide $x^3 - 5$, since $x^3 - 5$ satisfies $\sqrt[3]{5}$. This implies the polynomial $x^3 - 5$ must have a root in $\mathbb{Q}(a) \subseteq R$, but $x^3 - 5$ has only one real root in R, namely $\sqrt[3]{5}$.

This implies $\sqrt[3]{5} \in \mathbb{Q}(a)$; this is impossible as $\mathbb{Q}(a, \sqrt[3]{5}) = F$ and $[F : \mathbb{Q}] = 6$. Hence the possibility $[\mathbb{Q}(a) : \mathbb{Q}] = 3$ cannot occur.

If $[\mathbb{Q}(a) : \mathbb{Q}] = 2$, then $[\mathbb{Q}(a, \sqrt{2}) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] \leq 4$. $x^2 - 2 \in \mathbb{Q}(a)[x]$ and satisfies $\sqrt{2}$. Then either $\sqrt{2} \in \mathbb{Q}(a)$ or $[\mathbb{Q}(a, \sqrt{2}) : \mathbb{Q}(a)] = 2$ certainly $\sqrt{2} \notin \mathbb{Q}(a)$. Otherwise $\sqrt[3]{5} \in \mathbb{Q}(a)$ and hence $\mathbb{Q}(a) = \mathbb{Q}(\sqrt[3]{5}, \sqrt{2}) = F$ and this is impossible as $[F : \mathbb{Q}] = 6$.

Hence $[\mathbb{Q}(a, \sqrt{2}) : \mathbb{Q}] = 4$ which is impossible.

Hence $[\mathbb{Q}(a) : \mathbb{Q}] = 6$ and $\mathbb{Q}(a) = F$.

Summary of this unit.

In this unit we have studied the following:

- Let K be a finite extension of F and let L be an extension of K then L is a finite extension of F. More over $[L:K][K:F] = [L:F]$
  (OR) Every finite extension of a finite extension is finite.
- An element a is said to be a root of a polynomial $f(x)$ if $f(a) = 0$, where $f(x)$ is a nonzero polynomial.
- An element $a \in K$ is said to be algebraic over F if it satisfies a nonzero polynomial over F.
- An element $a \in K$ is said to be algebraic of degree n over F if it satisfies a nonzero polynomial over F of degree n but no polynomial of degree less than n.
- An element $a \in K$ is algebraic over F if and only if $F(a)$ is a finite extension of F
- If $a \in K$ is algebraic of degree n over F, then $[F(a):F] = n$.
- Let K be a finite extension of F. Let $a, b \in K$ are algebraic over F, then $F(a,b)$ is a field obtained by adjoining a to F and then adjoining b to $F(a)$. Clearly $F(a,b) = F(b,a)$.
- Let K be a finite extension of F. If $a, b \in K$ are algebraic over F, then, $a \pm b, ab, \frac{a}{b}, (b \neq 0)$ are also algebraic over F.
  (OR) If K is a finite extension of F, then the set of all algebraic elements of a field F forms a sub field of F.
- Let K be a finite extension of F. If every element in K is algebraic over F, then K is called an algebraic extension of F.

- If K is algebraic extension of F and L is algebraic extension of K then, L is algebraic extension of F. (OR) Algebraic extension of an algebraic extension is algebraic.
- A complex number is said to be an algebraic number if it is algebraic over the field of rational numbers.
- A number which is not algebraic is called transcendental.

Multiple Choice Questions

1. If L is a finite extension of F and K is a subfield of L which contains F, then
   a) $[L:F]|[K:F]$ b) $[K:F]|[L:F]$
   c) $[K:F]|[F:L]$ d) $[F:K]|[L:F]$
2. Find algebraic element over Q
   a) $\sqrt{2}$ b) π c) e d) $\pi+1$
3. Find dimension of $Q(\sqrt{2})$ over Q is
   a) 2 b) 3 c) 5 d) 1
4. Find dimension of $Q(i)$ over Q is
   a) 1 b) 3 c) 5 d) 2
5. Find dimension of R over Q is
   a) 1 b) 3 c) ∞ d) 2
6. The dimension of $Q(\sqrt{2}+\sqrt{3})$ over Q is
   a) 2 b) 3 c) 4 d) 6 .
7. Find dimension of $Q(\sqrt{2},\sqrt{3})$ over Q is
   a) 1 b) 4 c) ∞ d) 2
8. Select the number which is not an element of $Q(\sqrt{2})$
   a) 1 b) 4 c) $\sqrt[3]{2}$ d) 2

9. The field $Q(\sqrt{3}+\sqrt{7})$ is isomorphic to

   a) Q b) R c) $Q(\sqrt{3},\sqrt{7})$ d) C

10. Which of the following number is conjugate to $\sqrt{3}$

    a) 1 b) 2 c) 3 d) $-\sqrt{3}$

11. Let E is $Q(\sqrt{3},\sqrt{7})$ Then number of automorphisms of E which leaves Q fixed is

    a) 1 b) 2 c) 3 d. 4

12. Number of automorphisms from $Q(\sqrt{2})$ to $Q(\sqrt{3})$ is

    a) 1 b) 2 c) 3 d) 0

13. Find the fixed field of $Q(\sqrt{2})$ of the mapping $\sqrt{2}$ goes to $-\sqrt{2}$

    a) Q b) R c) C d) Z

14. Let E is $Q(\sqrt{3},\sqrt{7})$ and F is Q. Then index of E over F is

    a) 2 b) 3 c) 4 d) 1

Answers:

1	2	3	4	5	6	7	8	9	10	11	12	13	14
b	a	a	d	c	c	b	c	c	d	d	d	a	c

Exercise:

1. If V is a finite-dimensional vector space over the field K, and if F is a subfield of K such that $[K:F]$ is finite, show that V is a finite-dimensional vector space over F and that moreover $dim_F(V) = (dim_K(V))([K:F])$.

2. Prove that $F(a,b) = F(b,a)$.

3. If $a,b \in K$ are algebraic over F of degrees m and n, respectively, and if m and n are relatively prime, prove that $F(a,b)$ is of degree mn over F.

4. If a is any algebraic number, prove that there is a positive integer n such that na is an algebraic integer.

5. Prove that the sum of two algebraic integers is an algebraic integer.

6. Prove that the product of two algebraic integers is an algebraic integer.

Block 3 - UNIT 7

Roots of polynomials

Objectives

- We try to learn about Remainder theorem
- To study about multiple root of a polynomial
- To Study about minimal polynomial of an element
- Try to learn about Fundamental Theorem on Algebra
- We study splitting field of the polynomial

In earlier units we discussed elements in a given extension K of F which were algebraic over F, that is, elements which satisfied polynomials in $F[x]$. We now turn the problem around; given a polynomial $p(x)$ in $F[x]$ we wish to find a field K which is an extension of F in which $p(x)$ has a root. No longer is the field K available to us; in fact it is our prime objective to construct it. Once it is constructed, we shall examine it more closely and see what consequences we can derive.

7.1 Fundamental Theorem on Algebra

Definition 7.1.1. *If $p(x) \in F[x]$, then an element $a \in K$, where K is some extension of F is called a root of $p(x)$ if $p(a) = 0$.*

Let us begin with the familiar result known as the Remainder Theorem.

Theorem 7.1.1. *(Remainder theorem) : Let K be a finite extension of F and let $p(x)$ be a polynomial over F . Let $a \in K$. Then there exists a polynomial $q(x) \in K[x]$ such that $p(x) = (x-a)q(x) + p(a)$, where $degq(x) = degp(x) - 1$.*

Proof. Since $p(x) \in F[x]$ and $F \subseteq K$, we have $p(x) \in K[x]$.
Since $a \in K$, $x - a \in K$.
Divide $p(x)$ by $(x-a)$. Let the quotient be $q(x)$ and the remainder be $r(x)$.
Clearly, $deg(q(x)) = deg(p(x)) - 1$.
$\therefore p(x) = (x-a)q(x) + r(x) \cdots (1)$.
Here either $r(x) = 0$ or $degr(x) < deg(x-a)$.
Since $(x-a)$ is of degree $1, r(x)$ must be a constant polynomial.
Therefore let us take $r(x) = r$.
From equation (1), we have,
$p(x) = (x-a)q(x) + r \cdots (2)$
Put $x = a$ in (2). Then we have, $p(a) = (a-a)q(a) + r$.
That is, $p(a) = r. \cdots (3)$
Sub (3) in (2), we have,
$p(x) = (x-a)q(x) + p(a)$ where $degq(x) = degp(x) - 1$.
Hence the theorem. ■

Definition 7.1.2. *An element $a \in K$ is a multiple root of a polynomial $p(x)$ with multiplicity m if $(x-a)^m | p(x)$, whereas $(x-a)^{m+1} \nmid p(x)$.*

One can have a reasonable question to ask, how many roots can a polynomial have in a given field? Before answering we must decide how to count a root of multiplicity m. We shall always count it as m roots. Even with this convention we can prove

Theorem 7.1.2. *(Fundamental Theorem on Algebra) A polynomial of degree n over a field can have at most n roots in any extension field.*

Proof. Let us prove this theorem by method of induction on degree of the polynomial $p(x)$ (say).

Basis for induction: Let $deg(p(x)) = 1$.

Then $p(x)$ is of the form $p(x) = \alpha x + \beta$, where, $\alpha \neq 0, \alpha, \beta \in F$.

Let $p(x) = 0$.

Therefore, $\alpha x + \beta = 0 \Rightarrow x = -\beta/\alpha$.

Therefore $-\frac{\beta}{\alpha}$ is the only root of $p(x)$.

Thus $p(x)$ has at most one root.

Induction hypothesis: Let us assume that this theorem is true for all polynomials of degree less than n.

Let $deg(p(x)) = n$. Let K be any extension of F.

Let $\alpha \in K$ be a multiple root of $p(x)$ with multiplicity m.

Therefore, $(x-\alpha)^m | p(x)$ but $(x-\alpha)^{m+1} \nmid p(x)$.

Therefore, $p(x) = (x-\alpha)^m.q(x)$, for some $q(x)$ where, $deg(q(x)) = n - m < n$.

Clearly α is not a root of $q(x)$.

Let $\beta \neq \alpha$ be a root of $p(x)$. That is , $p(\beta) = 0$.

But, $p(x) = (x-\alpha)^m.q(x)$.

Therefore, $p(\beta) = (\beta-\alpha)^m.q(\beta)$.

Since, $\beta \neq \alpha$, we have, $q(\beta) = 0$.

That is, β is a root of $q(x)$.

Thus, any root of $p(x)$ other than α is also a root of $q(x)$.

By Induction hypothesis we have, $q(x)$ can have at most $(n-m)$ roots.

Therefore $p(x)$ can have at most $m+(n-m)$ roots.

That is, $p(x)$ can have at most n roots in K. Hence theorem. ■

The previous results are having only of subsidiary interest. We now set ourselves to our prime task, that of providing ourselves with suitable extensions of F in which a given polynomial has roots. Once this is done, we shall be able to analyze such extensions to a reasonable enough degree of accuracy to get results. The most important step in the construction is accomplished for us in the next theorem.

Theorem 7.1.3. *Let $p(x) \in F[x]$ is of degree $n \geq 1$ and irreducible over F. Then there exists a finite extension E of F, such that $[E:F] = n$, in which $p(x)$ has a root.*

Proof. It is given that $p(x)$ is an irreducible polynomial over F.

Let V be a ideal generated by $p(x)$.

That is, $V =< p(x) >$.

Therefore V is a maximal ideal.

Hence $\frac{F[x]}{V}$ is a field. Let us denote, $E = \frac{F[x]}{V}$.

Claim 1: E is the required field.

First let us show that E is an extension field of F.

Let us define a map $\psi : F \to \frac{F[x]}{V}$ such that $\psi(\alpha) = \alpha + V$.

(i) First let us prove ψ is a homomorphism.

$\psi(\alpha+\beta) = (\alpha+\beta)+V = (\alpha+V)+(\beta+V) = \psi(\alpha)+\psi(\beta)$.

That is, $\psi(\alpha+\beta) = \psi(\alpha)+\psi(\beta)$.

Now, $\psi(\alpha.\beta) = (\alpha.\beta)+V = (\alpha+V).(\beta+V) = \psi(\alpha).\psi(\beta)$.

That is, $\psi(\alpha.\beta) = \psi(\alpha).\psi(\beta)$.

That is, ψ is a homomorphism.

(ii) ψ is 1-1.

Let , $\psi(\alpha) = \psi(\beta) \Rightarrow (\alpha + V) = (\beta + V) \Rightarrow (\alpha - \beta) + V = V \Rightarrow (\alpha - \beta) \in V \Rightarrow (\alpha - \beta) = p(x)q(x)$, where $q(x) \in F[x]$.

This is possible only if $q(x) = 0$.

That is, $(\alpha - \beta) = p(x)q(x) = p(x).0 = 0$;

That is, $(\alpha - \beta) = 0; \Rightarrow \alpha = \beta$.

This implies, $\psi(\alpha) = \psi(\beta) \Rightarrow \alpha = \beta$.

Hence ψ is $1 - 1$.

$\therefore \psi$ is an isomorphism from F to E .

Let $\overline{F}$ be the image of F under ψ .

But ψ is an isomorphism from F on to E .

Thus, $F \simeq \overline{F}$.

Since $\overline{F}$ is a sub field of E , we can say that E is an extension of $\overline{F}$.

Since $F \simeq \overline{F}$, we can say that E is an extension of F .

Claim 2: E is a finite extension of F . That is, $[E : F] = n$.

Let us consider the set, $S = \{1 + V, x + V, x^2 + V, \cdots, x^{n-1} + V\}$ of elements of E .

(i) Now let us prove that, S is linearly independent.

Consider the linear combination

$\alpha_0(1 + V) + \alpha_1(x + V) + \alpha_2(x^2 + V) + \alpha_3(x^3 + V) + \cdots + \alpha_{n-1}(x^{n-1} + V) = 0 + V. \cdots (1).$

= $\alpha_0 + V + \alpha_1 x + V + \alpha_2 x^2 + V + \alpha_3 x^3 + V + \cdots + \alpha_{n-1} x^{n-1} + V = 0 + V$

= $[\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + V + \cdots + \alpha_{n-1} x^{n-1}] + V = 0 + V$

$\Rightarrow [\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + V + \cdots + \alpha_{n-1} x^{n-1}] \in V.$

Let $m(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + V + \cdots + \alpha_{n-1} x^{n-1}$

That is, $m(x) \in V.$

This $\Rightarrow m(x) = p(x)f(x)$, where $f(x) \in E[x].$

Here LHS is of degree $n - 1$ where as RHS is of degree n .

This is possible only if $f(x) = 0.$

That is, $m(x) = p(x)f(x) = p(x).0 = 0$;

That is , $m(x)$ is a zero polynomial.

That is, $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + V + \cdots + \alpha_{n-1}x^{n-1}$ is a zero polynomial.

This shows $\alpha_0 = 0, \alpha_1 = 0, \alpha_2 = 0, \alpha_3 = 0, \cdots, \alpha_{n-1} = 0$

Thus, S is linearly independent.

(ii) Next we prove that S span E.

Let $f(x) + V \in \frac{F[x]}{V} = E$.

By division algorithm there exist $q(x), r(x)$ such that $f(x) = p(x)q(x) + r(x)$, where, either $r(x) = 0$ or $deg\, r(x) < deg p(x)$.

So, $f(x) + V = (p(x)q(x) + r(x)) + V = (p(x)q(x)) + V + (r(x) + V) = r(x) + V$ ($\because p(x)$ generates V).

Take, $r(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \cdots + \alpha_{n-1}x^{n-1}$.

$f(x) + V = [\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \cdots + \alpha_{n-1}x^{n-1}] + V$

$f(x) + V = \alpha_0 + V + \alpha_1 x + V + \alpha_2 x^2 + V + \alpha_3 x^3 + V + \cdots + \alpha_{n-1}x^{n-1} + V$

That is, $f(x) + V = \alpha_0(1 + V) + \alpha_1(x + V) + \alpha_2(x^2 + V) + \alpha_3(x^3 + V) + \cdots + \alpha_{n-1}(x^{n-1} + V) \cdots (2)$.

Thus every element in E can be expressed as a linear combination of elements of S over F.

Thus S is a basis for E over F.

Hence E is a finite extension of F.

It remains to prove that $p(x)$ has a root in E.

Let $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \cdots + \alpha_{n-1}x^{n-1} + \alpha_n x^n \in F[x]$.

Replacing , α_0 by $\alpha_0 + V, \alpha_1$ by $\alpha_1 + V, \alpha_2$ by $\alpha_2 + V, \cdots, \alpha_n$ by $\alpha_n + V$, we have,

$p(x) = (\alpha_0 + V) + (\alpha_1 + V)x + (\alpha_2 + V)x^2 + (\alpha_3 + V)x^3 + \cdots + (\alpha_{n-1} + V)x^{n-1} + (\alpha_n + V)x^n \in E[x]$.

Consider $p(x + V) = (\alpha_0 + V) + (\alpha_1 + V)(x + V) + (\alpha_2 + V)(x + V)^2 + \cdots + (\alpha_{n-1} + V)(x + V)^{n-1} + (\alpha_n + V)(x + V)^n \cdots (3)$

But $(x+V)^2 = (x+V)(x+V) = x^2+V$

Similarly, $(x+V)^3 = x^3+V, (x+V)^4 = x^4+V, \cdots, (x+V)^n = x^n+V$.

Substituting these values in (3), we get,

$p(x+V) = (\alpha_0+V)+(\alpha_1+V)(x+V)+(\alpha_2+V)(x^2+V)+\cdots+(\alpha_{n-1}+V)(x^{n-1}+V)+(\alpha_n+V)(x^n+V)$

$= (\alpha_0+V)+(\alpha_1 x+V)+(\alpha_2 x^2+V)+\cdots+(\alpha_{n-1}x^{n-1}+V)+(\alpha_n x^n+V)$

$= \alpha_0+\alpha_1 x+\alpha_2 x^2+\cdots+\alpha_{n-1}x^{n-1}+\alpha_n x^n+V$

$= p(x)+V = V,$ which is the zero element of E.

Thus, $(x+V)$ is a root of $p(x)$ which is in E. Hence the theorem. ■

An immediate consequence of this theorem is the

Corollary 7.1.1. *If $f(x) \in F[x]$ then there exists a finite extension E of F, in which $f(x)$ has a root and $[E:F] \leq$ degree of $f(x)$.*

Proof. Let $f(x)$ is irreducible. Then corollary follows from theorem.

Therefore let $f(x)$ is not irreducible over F.

Then there exists an irreducible factor $p(x)$ for $f(x)$.

More over $deg(p(x)) \leq deg(f(x))$.

Now $p(x)$ is an irreducible polynomial in $F[x]$.

Therefore by above theorem there exists a finite extension E for F in which $p(x)$ has a root.

Let this root be a. Hence a is also a root of $f(x)$.

Thus, $f(x)$ has a root in E. Now $[E:F] =$ degree of $p(x) \leq deg(f(x))$.

That is, $[E:F] \leq deg(f(x))$. ■

Theorem 7.1.4. *Let $f(x) \in F[x]$ is of degree $n \geq 1$ then there exists a finite extension E of F in which $f(x)$ has all the roots.*

More over , such that $[E : F] \leq n!$.

Proof. It is given that $f(x) \in F[x]$ is of degree $n \geq 1$.
Therefore by above corollary, there exists a finite extension E_1 of F, in which $f(x)$ has a root and $[E_1 : F] \leq n$.
Let this root be α .
Divide $f(x)$ by $(x - \alpha)$. Let the quotient be $q(x)$.
Obviously, $q(x) \in F[x]$.
But F is a subset of E_1. That is $F \subseteq E_1$.
Therefore $q(x) \in E_1[x]$.
Again from above corollary, there exists a finite extension E_2 of E_1 in which $q(x)$ has a root and $[E_2 : E_1] \leq (n - 1)$.
But, $[E_2 : F] = [E_2 : E_1][E_1 : F] \leq n(n - 1)$.
Let this root be β .
Divide $q(x)$ by $(x - \beta)$. Let the quotient be $q_1(x)$, and degree of $q_1(x) = n - 2$ and $q_1(x) \in F[x]$.
Again $F \subseteq E_2[x]$.
Using the corollary continuously, we will get an extension E for F which has all the roots of $f(x)$.
$[E : F] \leq n(n - 1).(n - 2).(n - 3).\cdots 2.1 = n!$.
That is, $[E : F] \leq n!$. Hence the theorem. ■

7.2 Splitting fields

The above theorem asserts the existence of a finite extension E in which the given polynomial $f(x)$, of degree n, over F has n roots. If $f(x) = a_0x^n + a_1x^{n-l} + \cdots + a_m, a_0 \neq 0$ and if the n roots in E are $\alpha_1, \alpha_2, \cdots, \alpha_n$, then by a known result, we can say $f(x)$ can be factored over E as $f(x) = a_0(x - 1)(x - \alpha_2)\cdots(x - \alpha_n)$. Thus $f(x)$ splits up completely over E as a product of linear (first degree)

factors. Since a finite extension of F exists with this property, a finite extension of F of minimal degree exists which also enjoys this property of decomposing $f(x)$ as a product of linear factors. For such a minimal extension, no proper subfield has the property that $f(x)$ factors over it into the product of linear factors. This yields the

Definition 7.2.1. *Splitting field : Let $f(x)$ be a polynomial over a field F. Then the smallest field having all the roots of the polynomial $f(x)$ is called the splitting field of the polynomial. (OR)*
Let $f(x)$ be a polynomial over a field F. A field E is said to be a splitting field of $f(x)$ if E has all the roots of $f(x)$ and no proper subfield of E has all the roots of $f(x)$.

Example 7.2.1. *Let $p(x) = x^4 + 2x^2 - 8$ be in $\mathbb{Q}[x]$. Then $p(x)$ has irreducible factors $x^2 - 2$ and $x^2 + 4$. Therefore, the field $\mathbb{Q}(\sqrt{2}, i)$ is a splitting field for $p(x)$.*

Example 7.2.2. *Let $p(x) = x^3 - 3$ be in $\mathbb{Q}[x]$. Then $p(x)$ has a root in the field $\mathbb{Q}(\sqrt[3]{3})$. However, this field is not a splitting field for $p(x)$ since the complex cube roots of 3, $\frac{-\sqrt[3]{3} \pm (\sqrt[6]{3})^5 i}{2}$ are not in $\mathbb{Q}(\sqrt[3]{3})$.*

An immediate question arises: given two splitting fields E_1 and E_2 of the same polynomial $f(x)$ in $F[x]$, what is their relation to each other? We will answer this question in following theorems. Let F and F' be two fields and let τ be an isomorphism of F onto F'. For convenience let us denote the image of any $\alpha \in F$ under τ by α'; that is, $\alpha\tau = \alpha'$. We shall maintain this notation for the next few pages.

We can make use of τ to set up an isomorphism between $F[x]$ and $F'[t]$, the respective polynomial rings over F and F'. For an arbitrary polynomial $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n \in F[x]$ we

define τ^* by $f(x)\tau^* = (\alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n)\tau^* = (\alpha_0' t^n + \alpha_1' t^{n-1} + \cdots + \alpha_n')$

Lemma 7.2.1. *τ^* defines an isomorphism of $F[x]$ onto $F'[t]$ with the property that $\alpha\tau^* = \alpha'$ for every $\alpha \in F$.*

The proof is easy and straight forward matter, which we leave to the reader, to verify.

Lemma 7.2.2. *There is an isomorphism τ^{**} of $\frac{F[x]}{(f(x))}$ onto $\frac{F'[t]}{(f'(t))}$ with the property that for every $\alpha \in F, \alpha\tau^{**} = \alpha', (x + (f(x)))\tau^{**} = t + (f'(t))$.*

Proof. Before starting with the proof proper, we should make clear what is meant by the last part of the statement of the lemma. As we have already done several times, we can consider F as imbedded in $\frac{F[x]}{(f(x))}$ by identifying the element $\alpha \in F$ with the coset $\alpha + (f(x))$ in $\frac{F[x]}{(f(x))}$.
Similarly, we can consider F' to be contained in $\frac{F'[t]}{(f'(t))}$.
The isomorphism τ^{**} is then supposed to satisfy $(\alpha + (f(x)))\tau^{**} = \alpha' + (f'(t))$.
We seek an isomorphism τ^{**} of $\frac{F[x]}{(f(x))}$ onto $\frac{F'[t]}{(f'(t))}$.
What could be simpler or more natural than to try the τ^{**} defined by
$[g(x) + (f(x))]\tau^{**} = g'(t) + (f'(t))$ for every $g(x) \in F[x]$.
Clearly τ^{**} is an isomorphism from $\frac{F[x]}{(f(x))}$ onto $\frac{F'[t]}{(f'(t))}$. ■

Theorem 7.2.1. *If $p(x)$ is irreducible in $F[x]$ and if v is a root of $p(x)$, then $F(v)$ is isomorphic to $F'(w)$ where w is a root of $p'(t)$; moreover, this isomorphism σ can so be chosen that*

1. $v\sigma = w$.
2. $\alpha\sigma = \alpha'$ *for every* $a \in F$.

Proof. Let v be a root of the irreducible polynomial $p(x)$ lying in some extension K of F.

Let $M = \{f(x) \in F[x] | f(v) = 0\}$.

Trivially M is an ideal of $F[x]$, and $M \neq F[x]$.

Since $p(x) \in M$ and is an irreducible polynomial, we have that $M = (p(x))$.

As given in earlier proofs, map $F[x]$ into $F(v) \subseteq K$ by the mapping ψ defined by

$q(x)\psi = q(v)$ for every $q(x) \in F[x]$.

We saw earlier that ψ maps $F[x]$ onto $F(v)$.

The kernel of ψ is precisely M, so must be $(p(x))$.

By the fundamental homomorphism theorem for rings there is an isomorphism

ψ^* of $\frac{F[x]}{(p(x))}$ onto $F(v)$.

Note further that $\alpha\psi^* = \alpha$ for every $\alpha \in F$.

Thus, ψ^* is an isomorphism of $\frac{F[x]}{(p(x))}$ onto $F(v)$ leaving every element of F fixed and with the property that $v = (x + (p(x))\psi^*$.

Since $p(x)$ is irreducible in $F[x]$, $p'(t)$ is irreducible in $F'[t]$.

Therefore by a known Lemma, there is an isomorphism θ^* of $\frac{F'[t]}{(p'(t))}$ onto $F'(w)$

where w is a root of $p'(t)$ such that θ^* leaves every element of F' fixed and such that $[t + (p'(t))]\theta^* = w$.

Therefore, there is an isomorphism τ^{**} of $\frac{F[x]}{(p(x))}$ onto $\frac{F'[t]}{(p'(t))}$ which coincides with τ on F and which takes $x + (p(x))$ onto $t + (p'(t))$.

Motivated by $F(v) \xrightarrow{(\psi^*)^{-1}} \frac{F[x]}{(p(x))} \xrightarrow{\tau^{**}} \frac{F'[t]}{(p'(t))} \xrightarrow{\theta^*} F'w$,

Consider the mapping $\sigma = (\psi^*)^{-1}\tau^{**}\theta^*$ of $F(v)$ onto $F'(w)$.

It is an isomorphism of $F(v)$ onto $F'(w)$ since all the mapping ψ^*, τ^{**}, and θ^* are isomorphisms and onto.

Moreover, since $v = [x + (p(x))]\psi^*$, we have,

$v\sigma = (v(\psi^*)^{-1})\tau^{**}\theta^*$

$= ([x + (p(x)]\tau^{**})\theta^*$

$= [t + (p'(t))]\theta^* = w$.

Also, for $\alpha \in F$,

$\alpha\sigma = ((\alpha(\psi^*)^{-1})\tau^{**}\theta^*$

$= (\alpha\tau^{**})\theta^*$

$= \alpha'\theta^*$

$= \alpha'$.

We have shown that σ is an isomorphism satisfying all the requirements of the isomorphism in the statement of the theorem. Thus the Theorem is proved. ■

A special case, but itself of interest, is the

Corollary 7.2.1. *If $p(x) \in F[x]$ is irreducible and if a, b are two roots of $p(x)$, then $F(a)$ is isomorphic to $F(b)$ by an isomorphism which takes a on to b and which leaves every element of F fixed.*

We now come to the theorem which is, as we indicated earlier, the foundation stone on which the whole Galois theory rests. For us it is the focal point of this whole chapter.

Theorem 7.2.2. *If $f(x) \in F[x]$ and $f'(t) \in F'[t]$ are two polynomials and if E and E' are the splitting fields of $f(x)$ and f' respectively then there is an isomorphism ϕ from E to E' with the property that $\alpha\phi = \alpha', \forall \alpha \in F$*

Proof. Let us prove this theorem by method of Induction on $[E : F]$.

Basis for induction:

Let $[E : F] = 1$. Therefore, $E = F$.

Since E is the splitting field of $f(x)$, we have F is the splitting field of $f(x)$.

Similarly, F' is the splitting field of $f'(t)$, we have $E' = F'$.

Therefore by a known theorem, there is an isomorphism

$\tau : F \to F'$ such that $\alpha\tau = \alpha', \forall \alpha \in F$

Take $\tau = \phi$. Hence, $\phi : E \to E'$ is an isomorphism such that $\alpha\phi = \alpha', \forall \alpha \in F$

($\because E = F$ and $E' = F'$) .

Induction hypothesis:

Assume that this theorem is true for all splitting fields of degree less than n .

That is, if F_0 and F_0' are any two fields and $f(x) \in F_0[x]$ and if E_0 is the splitting field of $f(x)$ such that $[E_0 : F_0] < n$, then E_0 is isomorphic to E_0' where E_0' is the splitting field of $f'(t) \in F_0'[t]$.

Let $[E : F] = n > 1$, where E is the splitting field of $f(x)$.

Since $n > 1$, $f(x)$ has an irreducible factor $p(x)$ of degree $r > 1$.

Let $p'(t)$ be the corresponding irreducible factor of $f'(t)$.

Since E is splitting field of $f(x)$, all the roots of $f(x)$ are in E .

Let v be any root of $p(x)$. Therefore $p(v) = 0$.

Since $deg(p(x)) = r$, we have $[F(v) : F] = r$.

Similarly there is a w in E' such that w is a root of $p'(t)$. That is, $p'(w) = 0$.

By a known theorem, there is an isomorphism

σ from $F(v)$ to $F'(w)$ with the property that $\alpha\sigma = \alpha', \forall \alpha \in F$

Now, $[E : F] = n$ and $[F(v) : F] = r$.

Since $F \subset F(v) \subset E$, we have $[E : F] = [E : F(v)][F(v) : F]$.

That is, $n = [E : F(v)].r$

That is, $[E : F(v)] = \dfrac{n}{r} < n.$

Since $F \subseteq F(v)$ and since $f(x) \in F[x]$ we have $f(x)$ is a polynomial over $F(v)$ and $[E : F(v)] < n.$

Similarly, $f'(t)$ is a polynomial over $F'(w)$ and E' is the splitting field of $f'(t)$ and $[E' : F(w)] < n.$

Therefore by induction hypothesis, there exists an isomorphism

$\phi : E \to E'$ such that $\alpha\phi = \alpha', \forall \alpha \in F$.

Hence for every $\alpha \in F, \alpha\phi = \alpha', \forall \alpha \in F$. Hence the theorem. ■

Theorem 7.2.3. *Any two splitting fields of the same polynomial over a given field F are isomorphic by an isomorphism leaving every element of F fixed.*

Proof. Take $F = F'$.

Let τ be the identity map.

That is $\alpha\tau = \alpha, \forall \alpha \in F$.

Let E_1 and E_2 be two splitting fields of $f(x)$.

Clearly $F \subseteq E$ and $F \subseteq E'$.

Take $E_1 = E$ and $E_2 = E'$. Then by above theorem, E_1 and E_2 are isomorphic with the property that $\alpha\tau = \alpha, \forall \alpha \in F$. Hence the theorem. ■

Example 7.2.3. *Let $f(x) = x^2 - 2$ and $g(x) = x^4 - 4x^2 + 1$. These polynomials are the minimal polynomials of $\sqrt{2}$ and $\sqrt{2+\sqrt{3}}$, respectively.*

Proposition 7.2.1. *Let E be a field extension of F and $\alpha \in E$ be algebraic over F. Then $F(\alpha) \simeq \frac{F[x]}{< p(x) >}$, where $p(x)$ is the minimal polynomial of α over F.*

Proof. Let $\phi : F[x] \to E$ be the evaluation homomorphism. The kernel of this map is $< p(x) >$, where $p(x)$ is the minimal polynomial of α. By the First Isomorphism Theorem for rings, the image of ϕ in E is isomorphic to $F(\alpha)$ since it contains both F and α. ■

Example 7.2.4. *Let $p(x) = x^5 + x^4 + 1 \in Z_2[x]$. Then $p(x)$ has irreducible factors $x^2 + x + 1$ and $x^3 + x + 1$. For a field extension E of $\mathbb{Z}_2$ such that $p(x)$ has a root in E, we can let E be either*

$\frac{\mathbb{Z}_2[x]}{< x^2+x+1 >}$ *or* $\frac{\mathbb{Z}_2[x]}{< x^3+x+1 >}$. *We will leave it as an exercise to show that* $\frac{\mathbb{Z}_2[x]}{< x^3+x+1 >}$ *is a field with* $2^3 = 8$ *elements.*

Solved Problems

Problem: 1 Determine an extension field of $\mathbb{Q}$ containing $\sqrt{3}+\sqrt{5}$.

Solution: It is easy to determine that the minimal polynomial of $\sqrt{3}+\sqrt{5}$ is x^4-16x^2+4. It follows that $[\mathbb{Q}(\sqrt{3}+\sqrt{5}):\mathbb{Q}] = 4$.

We know that $\{1,\sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$. Hence, $\sqrt{3}+\sqrt{5}$ cannot be in $\mathbb{Q}(\sqrt{3})$. It follows that $\sqrt{5}$ cannot be in $\mathbb{Q}(\sqrt{3})$ either. Therefore, $\{1,\sqrt{5}\}$ is a basis for $\mathbb{Q}(\sqrt{3},\sqrt{5}) = (\mathbb{Q}(\sqrt{3}))(\sqrt{5})$ over $\mathbb{Q}(\sqrt{3})$ and $\{1,\sqrt{3},\sqrt{5},\sqrt{3}\sqrt{5} = \sqrt{15}\}$ is a basis for $\mathbb{Q}(\sqrt{3},\sqrt{5}) = \mathbb{Q}(\sqrt{3}+\sqrt{5})$ over $\mathbb{Q}$. This example shows that it is possible that some extension $F(a_1,\cdots,a_n)$ is actually a simple extension of F even though $n > 1$.

Problem 2: Determine the irreducible polynomial for $\alpha = i+\sqrt{2}$ over $\mathbb{Q}$.

Solution: There were several ways to do this problem. The basic idea is to find a linear combination of powers of α that equals zero. Then one needs to explain why the associated polynomial is irreducible. $\alpha^2 = -1+2\sqrt{-2}+2 = 1+2\sqrt{-2}$.

Thus $(\alpha^2-1)^2 = -8$ hence α satisfies $(x^2-1)^2+8 = x^4-2x^2+9 = f(x)$. It is easy to prove that this is irreducible by the theory of field extensions .

Let K be the splitting field for $f(x)$. Clearly, $\mathbb{Q}(\sqrt{2},i)$ contains K. But, $\mathbb{Q}(\sqrt{2})$ has degree 2 over $\mathbb{Q}$ and since $i \notin \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i,\sqrt{2})$ has degree 2 over $\mathbb{Q}(\sqrt{2})$.

Consequently, $K = \mathbb{Q}(\sqrt{2},i), [K:\mathbb{Q}] = 4$ and $f(x)$ is irreducible.

Problem 3: Determine the degree of the splitting field of the polynomial $f(x) = x^3+x+1$ over $\mathbb{Q}$.

Solution: It has no rational roots, so it is irreducible. Since $f'(x) = 3x^2 + 1 > 0, f(x)$ is increasing on the real line and has exactly one real root α. By the Fundamental Theorem of Algebra, it has two complex roots β and $\overline{\beta}$. Consider the extension $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, there we have $f(x) = (x-\alpha)g(x)$. Since both roots of $g(x)$ are not real, they do not belong to $\mathbb{Q}(\alpha)$, so $g(x)$ is irreducible over $\mathbb{Q}(\alpha)$. Then we can consider the field $K = \mathbb{Q}(\alpha, \beta)$ where $f(x)$ factors completely. We have $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 3 = 6$.

Problem 4: Find the splitting field of the polynomial $x^p - 1 = 0$ where p is a prime number. Also find its degree.

Solution: The given polynomial is $x^p - 1 = 0$ where p is a prime number.

Let $f(x) = x^p - 1$. That is, $f(x) = (x-1)(x^{p-1} + x^{p-2} + x^{p-3} + \cdots + x + 1) = 0$.

That is $f(x) = (x-1)q(x)$, where, $q(x) = x^{p-1} + x^{p-2} + x^{p-3} + \cdots + x + 1$.

It is clear that the degree of $q(x) = p - 1$.

Clearly 1 is a root of $f(x)$ which is in F.

Then the remaining roots of $f(x)$ are exactly the roots of $q(x)$.

Let ω be any root of $q(x)$. Now consider the field $F(\omega)$.

Then, $\omega, \omega^2, \omega^3, \cdots, \omega^{n-1} \in F(\omega)$.

Thus, $F(\omega)$ has all the roots of $f(x)$ and no proper subfield of $F(\omega)$ has all the roots of $f(x)$.

Hence $F(\omega)$ is the splitting field of $f(x)$.

Since ω is a root of $q(x)$ and degree of $q(x)$ is $p-1$, we can say that ω is algebraic of degree $p-1$.

Therefore $[F(\omega) : F] = p - 1$.

Problem 5: Find the degree of the splitting field of the polynomial $x^{17} - 1 = 0$. Here 17 is a prime.

Solution: The given polynomial is $x^p - 1 = 0$.

We know that if, $x^p - 1 = 0$ where p is a prime number, then the degree of the splitting field of $x^p - 1 = 0$ is $p - 1$.

Therefore the degree of the splitting field of the polynomial $x^{17} - 1 = 0$ is $17 - 1 = 16$.

Problem 6: Let F be the field of rational numbers and let $f(x) = x^4 + x^2 + 1$ is a polynomial over F. Find the splitting field of the polynomial $f(x)$ and determine its degree.

Solution: $f(x) = x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1) = g(x)h(x)$, where, $g(x) = (x^2 + x + 1), h(x) = (x^2 - x + 1)$.

But $g(-x) = h(x)$. Therefore the roots of $g(x)$ is also the roots of $h(x)$ with negative sign.

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

The roots of $g(x)$ are:

$-1 \pm \frac{\sqrt{(1^2 - 4.1.1)}}{2.1} = (-1 \pm \frac{\sqrt{-3}}{2})$.

Let $\omega = (-1 + \frac{i\sqrt{3}}{2})$, $\omega^2 = (-1 - \frac{i\sqrt{3}}{2})$

But, $h(x) = (x^2 - x + 1)$.

Clearly, $-\omega = (-1 - \frac{i\sqrt{3}}{2})$, $-\omega^2 = (-1 + \frac{i\sqrt{3}}{2})$ are the roots of $h(x)$.

Thus, $\omega, \omega^2, -\omega, -\omega^2$ are all the four roots of $f(x)$.

These roots are in $F(\omega)$. But no proper subfield of $F(\omega)$ has all the roots.

Hence, $F(\omega)$ is the splitting field of the polynomial $f(x)$.

Since ω satisfies $g(x)$ and degree of $g(x)$ is 2, we have, $[F(\omega) : F] = 2$.

Therefore the degree of the splitting field of the polynomial $f(x)$ is 2.

Summary of this unit.

In this unit we have studied the following:

- If $p(x) \in F[x]$, then an element $a \in K$, where K is some extension of F is called a root of $p(x)$ if $p(a) = 0$.
- **Remainder theorem** : Let K be a finite extension of F and let $p(x)$ be a polynomial over F . Let $a \in K$. Then there exists a polynomial $q(x) \in K[x]$ such that $p(x) = (x-a)q(x) + p(a)$, where $degq(x) = degp(x) - 1$.
- An element $a \in K$ is a multiple root of a polynomial $p(x)$ with multiplicity m if $(x-a)^m | p(x)$, whereas $(x-a)^{m+1} \nmid p(x)$.
- **Fundamental Theorem on Algebra** : A polynomial of degree n over a field can have at most n roots in any extension field.
- Let $p(x) \in F[x]$ is of degree $n \geq 1$ and irreducible over F. Then there exists a finite extension E of F, such that $[E : F] = n$, in which $p(x)$ has a root.
- If $f(x) \in F[x]$ then there exists a finite extension E of F, in which $f(x)$ has a root and $[E : F] \leq$ degree of $f(x)$.
- Let $f(x) \in F[x]$ is of degree $n \geq 1$ then there exists a finite extension E of F in which $f(x)$ has all the roots. More over , such that $[E : F] \leq n!$.
- **Splitting field** : Let $f(x)$ be a polynomial over a field F. Then the smallest field having all the roots of the polynomial $f(x)$ is called the splitting field of the polynomial. (OR)
  Let $f(x)$ be a polynomial over a field F. A field E is said to be a splitting field of $f(x)$ if E has all the roots of $f(x)$ and no proper subfield of E has all the roots of $f(x)$.
- Any two splitting fields of the same polynomial over a given field F are isomorphic by an isomorphism leaving every

element of F fixed.

- Let E be a field extension of F and $\alpha \in E$ be algebraic over F. Then $F(\alpha) \simeq \frac{F[x]}{< p(x) >}$, where $p(x)$ is the minimal polynomial of α over F.

Multiple Choice Questions

1. Find splitting field of $x^2 - 2, x^2 - 3$ over Q
   a) $Q(\sqrt{3}, \sqrt{2})$
   b) $Q(\sqrt{3})$
   c) $Q(\sqrt{2})$
   d) R

2. Find the inverse of 3 in Z_5
   a) 4 b) 1 c) 3 d. 2

3. Find the splitting field of $x^3 - 2$ over Q
   a) $Q(i\sqrt{3}, \sqrt[3]{2})$
   b) $Q(\sqrt{3})$
   c) $Q(\sqrt{2})$
   d) R

4. Find a zero of $x^3 - 2$ in Z_5
   a) 0 b) 1 c) 3 d) 2

5. Find splitting of $x^3 - 1$ over Q
   a) $Q(i\sqrt{3}, \sqrt[3]{2})$
   b) $Q(\zeta)$
   c) $Q(\sqrt{2})$
   d) R

6. The degree of the splitting field of $x^3 + x + 1$ over Q is
   a) 3 b)4 c) 5 d) 6

7. The degree of the splitting field of $x^2 + ax + p \in Q[x]$ is

   a) 2 b) 3 c) 4 d) 5

8. The degree of the splitting field of $x^3 - 2 \in Q[x]$ is

   a) 6 b) 5 c) 4 d) 3

9. The number of automorphisms on $Q\sqrt[3]{2}$ is

   a) 24 b) 6 c) 2 d) 1

10. The number of automorphisms other than the identity automorphism on $Q\sqrt[3]{2}$ is

    a) 0 b) 2 c) 6 d) 1

Answers:

1	2	3	4	5	6	7	8	9	10
a	d	a	c	b	d	a	a	d	a

Exercise:

Let F be the field of rational numbers. Determine the degrees of the splitting fields of the following polynomials over F.

1. $x^4 + 1$
2. $x^6 + 1$
3. $x^4 - 2$
4. $x^5 - 1$
5. $x^6 + x^3 + 1$
6. If F is the field of rational numbers, find necessary and sufficient conditions on a and b so that the splitting field of $x^3 + ax + b$ has degree exactly 3 over F

Block 4 - UNIT 8

More about Roots

Objectives

- We try to learn about the derivative of polynomials
- To study the relation between characteristic of F and polynomials over F
- Try to learn about simple extension of a field F
- We study separable extension a field F
- To Study about perfect extensions

In this unit, we show that all finite extensions are simple extensions. Let F be any field and, as usual, let $F[x]$ be the ring of polynomials in x over F.

8.1 Derivative of Polynomials

Definition 8.1.1. *If* $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \cdots + \alpha_i x^{n-i} + \cdots + \alpha_{n-1} x + \alpha_n$ *in* $F[x]$*, then the derivative of* $f(x)$ *is denoted as*

$f'(x)$ *and is defined as*
$f'(x) = n\alpha_0 x^{n-1} + (n-1)\alpha_1 x^{n-2} + \cdots + (n-i)\alpha_i x^{n-i-1} + \cdots + \alpha_{n-1}$ *in* $F[x]$.

Earlier , we defined what is meant by the characteristic of a field. Let us recall it now. A field F is said to be of characteristic 0 if $ma \neq 0$ for $a \neq 0$ in F and $m > 0$, an integer. If $ma = 0$ for some $m > 0$ and some $a \neq 0 \in F$, then F is said to be of finite characteristic. In this second case, the characteristic of F is defined to be the smallest positive integer p such that $pa = 0$ for all $a \in F$. It turned out that if F is of finite characteristic then its characteristic p is a prime number.

We return to the question of the derivative. Let F be a field of characteristic $p \neq 0$. In this case, the derivative of the polynomial x^p is $px^{p-1} = 0$. Thus the usual result from the calculus that a polynomial whose derivative is 0 must be a constant no longer need hold true. We now prove the analogs of the formal rules of differentiation that we know so well.

Lemma 8.1.1. *For any* $f(x), g(x) \in F[x]$ *and any* $\alpha \in F$,

1. $(f(x)+g(x))' = f'(x)+g'(x)$.
2. $(\alpha f(x))' = \alpha f'(x)$
3. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Proof. First let us prove (iii): Let $f(x) = x^i$ and $g(x) = x^j$.
Then $f(x)g(x) = x^i x^j = x^{i+j}$.
So, $(f(x)g(x))' = (x^{i+j})' = (i+j)x^{i+j-1} \cdots (1)$
But $f'(x) = ix^{i-1}$ and $g'(x) = jx^{j-1}$.
Therefore $f'(x)g(x) = ix^{i-1}x^j = ix^{i+j-1} \cdots (2)$
$f(x)g'(x) = x^i jx^{j-1} = jx^{i+j-1} \cdots (3)$
Now, (2) + (3) gives,
$f'(x)g(x) + f(x)g'(x) = (i+j)x^{i+j-1} \cdots (4)$

Hence, from equations (1) and (4), we have,
$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$. Hence the Theorem. ■

It should be note that in elementary calculus the equivalence is shown between the existence of a multiple root of a function and the simultaneous vanishing of the function and its derivative at a given point. Even in our setting, where F is an arbitrary field, such an interrelation exists.

Remark: If $f(x)$ and $g(x)$ in $F[x]$ have a nontrivial common factor in $K[x]$, for K an extension of F, then they have a nontrivial common factor in $F[x]$. For, were they relatively prime as elements in $F[x]$, then we would be able to find two polynomials $a(x)$ and $b(x)$ in $F[x]$ such that $a(x)f(x) + b(x)g(x) = 1$. Since this relation also holds for those elements viewed as elements of $K[x]$, in $K[x]$ they would have to be relatively prime.

Lemma 8.1.2. *The polynomial $f(x) \in F[x]$ has a multiple root if and only if $f(x)$ and $f'(x)$ have a nontrivial (that is, of positive degree) common factor.*

Proof. Without loss of generality let us assume that F has all the roots of $f(x)$. If $f(x)$ has a multiple root α , then $f(x) = (x-\alpha)^m q(x)$, where $m > 1$.
However, note that, $((x-\alpha)^m)' = m(x-\alpha)^{m-1}$.
Hence, by Lemma 8.1.1,
$f'(x) = (x-\alpha)^m q'(x) + m(x-\alpha)^{m-1}q(x) = (x-\alpha)r(x)$, since $m > 1$.
But this says that $f(x)$ and $f'(x)$ have the common factor $(x-\alpha)$, thus the lemma is true.
On the other hand, if $f(x)$ has no multiple root then
$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ where each α_i are all distinct

(we are supposing $f(x)$ to be monic).

But then $f'(x) = \sum_{i=1}^{n} (x-\alpha_1)\cdots\widehat{(x-\alpha_i)}\cdots(x-\alpha_n)$ where the $\widehat{\ }$ denotes the term is omitted.

We claim no root of $f(x)$ is a root of $f'(x)$. Indeed, $f'(\alpha_i) = \prod_{i\neq j}(\alpha_i - \alpha_j) \neq 0$, since the roots are all distinct.

However, if $f(x)$ and $f'(x)$ have a nontrivial common factor, they have a common root, namely, any root of this common factor.

Thus, $f(x)$ and $f'(x)$ have no nontrivial common factor, and so the lemma has been proved in the other direction. ■

Corollary 8.1.1. *If $f(x) \in F[x]$ is irreducible, then*

i) If the characteristic of F is 0, then $f(x)$ has no multiple roots.

ii) If the characteristic of F is $p \neq 0$, then $f(x)$ has a multiple root only if it is of the form $f(x) = g(x^p)$.

iii) If the characteristic of the field F is $p \neq 0$, then the polynomial $x^{p^m} - x \in F[x]$ for $n \geq 1$, has distinct roots.

Proof. Since $f(x)$ is irreducible, its only factors in $F[x]$ are 1 and $f(x)$ itself.

If $f(x)$ has a multiple root, then by Lemma 8.1.2, $f(x)$ and $f'(x)$ have a nontrivial common factor.

Hence $f(x) \mid f'(x)$.

However, since the degree of $f'(x)$ is less than that of $f(x)$, we get, $f'(x)$ must be a zero polynomial.

In characteristic 0 this implies that $f(x)$ is a constant, which has no roots; in characteristic $p \neq 0$, this forces $f(x) = g(x^p)$. ■

Corollary 8.1.2. *If F is a field of characteristic $p \neq 0$, then the polynomial $x^{p^n} - x \in F[x]$, for $n \geq 1$, has distinct roots.*

Proof. The derivative of $x^{p^n} - x$ is $p^n x^{p^n-1} - 1$.

Since F is of characteristic p, we have $pa = 0$.

Therefore, $p^n x^{p^n-1} - 1 = -1$.

Therefore $x^{p^n} - x$ and its derivative are certainly relatively prime, which, by the lemma, implies that $x^{p^n} - x$ has no multiple roots. ■

The Corollary 8.1.1, does not rule out the possibility that in characteristic $p \neq 0$ an irreducible polynomial might have multiple roots. The presence of irreducible polyno-
mials with multiple roots leads to many interesting cases. Here after we make the assumption that all fields occurring in the text material are fields of characteristic 0.

8.2 Simple extension

Definition 8.2.1. *The extension K of F is a simple extension of F if $K = F(\alpha)$ for some $\alpha \in K$.*

Theorem 8.2.1. *If the characteristic of F is 0 and a, b are algebraic over F, then there exists an element $c \in F(a,b)$ such that $F(a,b) = F(c)$.*

Proof. Let $f(x)$ and $g(x)$, are irreducible polynomials over F of degrees m and n, satisfied by a and b, respectively.
Let K be the splitting field of both $f(x)$ and $g(x)$.
Since the characteristic of F is 0, all the roots of $f(x)$ and $g(x)$ are distinct.
Let the roots of $f(x)$ be $a = a_1, a_2, \cdots, a_m$ and those of $g(x), b = b_1, b_2, \cdots, b_n$.
If $j \neq 1$, then $b_i \neq b_1 = b$, hence the equation $a_i + \lambda b_j = a_1 + \lambda b_1 = a + \lambda b$ has only one solution λ in K, namely, $\lambda = \dfrac{a_i - a}{b - b_j}$.
Since F is of characteristic 0 it has an infinite number of elements,

so we can find an element $\gamma \in F$ such that $a_i + \gamma b_j = a + \gamma b$ for all i and for $j \neq 1$.

Let $c = a + \gamma b$. We claim that $F(c) = F(a, b)$.

Since $c \in F(a, b)$, we have, $F(c) \subset F(a, b) \cdots (1)$

We will now show that both a and b are in $F(c)$ from which it will follow that $F(a, b) \subset F(c)$.

Now b satisfies the polynomial $g(x)$ over F, hence satisfies $g(x)$ considered as a polynomial over $K = F(c)$.

Moreover, if $h(x) = f(c - \gamma x)$ then $h(x) \in K[x]$ and $h(b) = f(c - \gamma b) = f(a) = 0$, since $a = c - \gamma b$.

Thus in some extension of K, $h(x)$ and $g(x)$ have $x - b$ as a common factor. We show that $x - b$ is their greatest common divisor.

For, if $b_j \neq b$, is another root of $g(x)$, then $h(b_j) = f(c - \gamma b_j) \neq 0$, since by our choice of y, $c - \gamma b_j$ for $j \neq 1$ avoids all roots a_i of $f(x)$.

Also, since $(x - b)^2$ does not divide $g(x)$, $(x - b)^2$ cannot divide the greatest common divisor of $h(x)$ and $g(x)$.

Thus $(x - b)$ is the greatest common divisor of $h(x)$ and $g(x)$ over some extension of K.

But then they have a nontrivial greatest common divisor over K, which must be a divisor of $x - b$.

Since the degree of $x - b$ is 1, we see that the greatest common divisor of $g(x)$ and $h(x)$ in $K[x]$ is exactly $x - b$.

Thus $x - b \in K[x]$, whence $b \in K$; remembering that $K = F(c)$, we obtain that $b \in F(c)$.

Since $a = c - \gamma b$, and since $b, c \in F(c), y \in F \subset F(c)$, we get that $a \in F(c)$, whence $F(a, b) \subseteq F(c) \cdots (2)$

Equations (1) and (2) together yields $F(a, b) = F(c)$. Hence the theorem. ■

We can expand the result from 2 elements to any finite number. That is, if $\alpha_1, \alpha_2, \cdots, \alpha_n$ are algebraic over F, then there is an element $c \in F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ such that $F(c) = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$. Thus the

Corollary 8.2.1. *Any finite extension of characteristic 0 is a simple extension.*

Definition 8.2.2. *An element $a \in K$ where K is some extension of F is called separable over F if it satisfies a polynomial over F having no multiple roots.*

Definition 8.2.3. *An extension K of F is called separable extension if all its elements are separable.*

Definition 8.2.4. *A field F is called perfect if all finite extensions are separable.*

Example 8.2.1. *The polynomial $x^2 - 2$ is separable over $\mathbb{Q}$ since it factors as $(x - \sqrt{2})(x + \sqrt{2})$. In fact, $\mathbb{Q}(\sqrt{2})$ is a separable extension of $\mathbb{Q}$.*
Let $\alpha = a + b\sqrt{2}$ be any element in $\mathbb{Q}(\sqrt{2})$. If $b = 0$, then α is a root of $x - a$. If $b \neq 0$, then α is the root of the separable polynomial $x^2 - 2ax + a^2 - 2b^2 = (x - (a + b\sqrt{2}))(x - (a - b\sqrt{2}))$.

Summary of this unit.

In this unit we have studied the following:

- If $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \cdots + \alpha_i x^{n-i} + \cdots + \alpha_{n-1} x + \alpha_n$ in $F[x]$, then the derivative of $f(x)$ is denoted as $f'(x)$ and is defined as
  $f'(x) = n\alpha_0 x^{n-1} + (n-1)\alpha_1 x^{n-2} + \cdots + (n-i)\alpha_i x^{n-i-1} + \cdots + \alpha_{n-1}$ in $F[x]$.
- For any $f(x), g(x) \in F[x]$ and any $\alpha \in F$,
  1. $(f(x) + g(x))' = f'(x) + g'(x)$.

2. $(\alpha f(x))' = \alpha f'(x)$
3. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

- The polynomial $f(x) \in F[x]$ has a multiple root if and only if $f(x)$ and $f'(x)$ have a nontrivial (that is, of positive degree) common factor.

- If $f(x) \in F[x]$ is irreducible, then
  i) If the characteristic of F is 0, then $f(x)$ has no multiple roots.
  ii) If the characteristic of F is $p \neq 0$, then $f(x)$ has a multiple root only if it is of the form $f(x) = g(x^p)$.
  iii) If the characteristic of the field F is $p \neq 0$, then the polynomial $x^{p^m} - x \in F[x]$ for $n \geq 1$, has distinct roots.

- If F is a field of characteristic $p \neq 0$, then the polynomial $x^{p^n} - x \in F[x]$, for $n \geq 1$, has distinct roots.

- The extension K of F is a simple extension of F if $K = F(\alpha)$ for some $\alpha \in K$.

- If the characteristic of F is 0 and a, b are algebraic over F, then there exists an element $c \in F(a, b)$ such that $F(a, b) = F(c)$.

- Any finite extension of characteristic 0 is a simple extension.

- An element $a \in K$ where K is some extension of F is called separable over F if it satisfies a polynomial over F having no multiple roots.

- An extension K of F is called separable extension if all its elements are separable.

- A field F is called perfect if all finite extensions are separable.

Multiple Choice Questions

1. The polynomial $f(x) \in F[x]$ has a multiple root if
   a) $f(x)$ and $f'(x)$ have a trivial common factor.
   b) $f(x)$ and $f'(x)$ have a nontrivial common factor.
   c) $f(x)$ and $f'(x)$ have a no common factor.
   d) None of the above

2. If f(x) is an irreducible polynomial of degree 5 over a perfect field F, then f(x) has
   a) 2 multiple root and 3 distinct roots
   b) 4 multiple root and 1 distinct root
   c) All are distinct roots
   d) All are multiple roots

3. If F is of characteristic 0 and if $f(x) \in F[x]$ is irreducible of degree 8, then
   a) $f(x)$ has 6 multiple roots and two distinct roots
   b) $f(x)$ has 4 multiple roots and four distinct roots
   c) $f(x)$ has only multiple roots
   d) $f(x)$ has only distinct roots

4. If F is of characteristic 0 and if $f(x) \in F[x]$ is irreducible of degree 21, then
   a) $f(x)$ has 6 multiple roots and 15 distinct roots
   b) $f(x)$ has 4 multiple roots and 17 distinct roots
   c) $f(x)$ has only multiple roots
   d) $f(x)$ has only distinct roots

5. If F is of characteristic 2 then the polynomial $x^{32} - x \in F[x]$ has
   a) has 6 multiple roots and 26 distinct roots

b) has 16 multiple roots and 16 distinct roots

c) has only distinct roots

d) has only multiple roots

6. If F is of characteristic 3 then the polynomial $x^{81} - x \in F[x]$ has

a) has 56 multiple roots and 25 distinct roots

b) has only distinct roots

c) has only multiple roots

d) has 70 multiple roots and 11 distinct roots

7. If F is of characteristic 5 then the polynomial $x^{125} - x \in F[x]$ has

a) has 100 multiple roots and 25 distinct roots

b) has 70 multiple roots and 55 distinct roots

c) has only multiple roots

d) has only distinct roots

8. If F is of characteristic 7 then the polynomial $x^{35} - x^7 \in F[x]$ is

a) $35x^{34}$

b) $-7x^6$

c) 0

d) $35x^{34} - 7x^6$

9. Any finite extension of characteristic 0 is

a) simple extension

b) perfect extension

c) separable extension

d) algebraic extension

Answers:

1	2	3	4	5	6	7	8	9
a	c	d	d	c	b	d	c	a

Exercise:

1. If F is of characteristic 0 and $f(x) \in F[x]$ is such that $f'(x) = 0$, prove that $f(x) = \alpha \in F$.
2. If F is of characteristic $p \neq 0$ and if $f(x) \in F[x]$ is such that $f'(x) = 0$, prove that $f(x) = g(x^p)$ for some polynomial $g(x) \in F[x]$.
3. Show that any field F is of characteristic 0 is perfect.
4. Show that any finite field is perfect
5. Prove that the set of all separable elements of K over F form a subfield of K.
6. If any one of a, b is separable then show that $F(a, b)$ is simple extension.
7. Prove that a finite, separable extension is simple.

Block 4 - UNIT 9

Galois Theory

Objectives

- We try to learn about automorphism on a field F
- To study fixed field of a group G.
- Try to learn about normal extension of a field F
- We study elementary symmetric functions of given variables
- To Study about symmetric rational functions of given variables
- We study about fundamental theorem of the Galois theory

In this unit will discuss what is nowadays called Galois theory (it was originally called theory of equations), the interrelation between field extensions and certain groups associated to them, called Galois groups. Given a polynomial $p(x)$ in $F[x]$, the polynomial ring in x over F, we shall associate with the Galois group of $p(x)$. There is a very close relationship between the roots of a polynomial and its Galois group; In fact, the Galois group will turn out to be a certain permutation group of the roots of the polynomial. Through the splitting field of $p(x)$ over F, the Galois group of $p(x)$ is

defined as a certain group of automorphisms of this splitting field. A beautiful duality, expressed in the fundamental theorem of the Galois theory exists between the subgroups of the Galois group and the sub fields of the splitting field. This theory will enable us to prove Galois's theorem describing precisely when the quadratic formula can be generalized to polynomials of higher degree.

9.1 Automorphisms on a field

In this section we define automorphisms on fields and study the linearly independence of $\sigma_1(u), \sigma_2(u),$
$\sigma_3(u), \cdots, \sigma_n(u)$ where , $\sigma_1, \sigma_2, \sigma_3, \cdots, \sigma_n$ are automorphisms on K acting on the elements $u \in K$.

Definition 9.1.1. *Let K be a field. A mapping $\sigma : K \to K$ is said to be an automorphism on K if*

1. σ is 1 - 1

2. $\sigma(x+y) = \sigma(x) + \sigma(y)$

3. $\sigma(xy) = \sigma(x)\sigma(y), \forall x, y \in K.$

Definition 9.1.2. *Two automorphisms σ and τ on K are said to be equal if $\sigma(x) = \tau(x), \forall x, \in K$.*
Two automorphisms σ and τ on K are said to be distinct if $\sigma(x) \neq \tau(x)$, for some x in K.

Theorem 9.1.1. *Let K be a field. Let $\sigma_1, \sigma_2, \cdots, \sigma_n$, be distinct automorphisms on K, then it is impossible to find elements $a_1, a_2, \cdots a_n$ in K, not all zero such that*
$a_1\sigma_1(u) + a_2\sigma_2(u) + a_3\sigma_3(u) + \cdots + a_n\sigma_n(u) = 0, \forall u \in K.$

Proof. Let us prove this theorem by method of contradiction.
Suppose there exists a finite set of elements $a_1, a_2, \cdots a_n$ in K, not

all zero such that

$a_1\sigma_1(u) + a_2\sigma_2(u) + a_3\sigma_3(u) + \cdots + a_n\sigma_n(u) = 0, \forall u \in K$ is true.

Let the minimal relation among those is

$a_1\sigma_1(u) + a_2\sigma_2(u) + a_3\sigma_3(u) + \cdots + a_m\sigma_m(u) = 0,\ \forall u,\ m < n,\ a_i \neq 0 \cdots (1)$

Suppose $m = 1$. Then $a_1\sigma_1(u) = 0, \forall u \in K$. Here $a_1 \neq 0$.

Therefore $\sigma_1(u) = 0$. This implies σ_1 is a zero mapping, which is a contradiction.

Therefore let $m > 1$.

Let $c, u \in K$. Therefore $cu \in K$.

Since equation (1) is true for all $u \in K$, it must be true for each cu.

Therefore $a_1\sigma_1(cu) + a_2\sigma_2(cu) + a_3\sigma_3(cu) + \cdots + a_m\sigma_m(cu) = 0$, for $a_i \neq 0$.

That is,

$a_1\sigma_1(c)\sigma_1(u) + a_2\sigma_2(c)\sigma_2(u) + a_3\sigma_3(c)\sigma_3(u) + \cdots + a_m\sigma_m(c)\sigma_m(u) = 0 \cdots (2)$

Multiply (1) by $\sigma_1(c)$, we get,

$a_1\sigma_1(u)\sigma_1(c) + a_2\sigma_2(u)\sigma_1(c) + a_3\sigma_3(u)\sigma_1(c) + \cdots + a_m\sigma_m(u)\sigma_1(c) = 0 \cdots (3).$

(2) $-$ (3) gives,

$a_2\sigma_2(u)(\sigma_2(c) - \sigma_1(c)) + a_3\sigma_3(u)(\sigma_3(c) - \sigma_1(c)) + \cdots +$

$a_m\sigma_m(u)(\sigma_m(c) - \sigma_1(c)) = 0$, where $a_2, a_3, \cdots, a_m \neq 0$.

This expression has $(m-1)$ elements and we have a contradiction for the minimal expression has m elements. Hence the theorem is true. ■

Fixed fields

We now define the fixed field of a group and study its properties.

Definition 9.1.3. *Let G be a group of all automorphisms on K.*

Then the fixed field of G *is denoted by* K_G *and is defined as follows.*

$K_G = \{x \in K | \sigma(x) = x, \forall \sigma \in G\}$

Theorem 9.1.2. *The fixed field of* G *is a subfield of* K.

Proof. : Let $a, b \in K_G$. Then $\sigma(a) = a, \sigma(b) = b, \forall \sigma \in G$.

Now, $\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a \pm b, \forall \sigma \in G$.

Thus the fixed field is an additive abelian group.

Similarly, $\sigma(ab) = \sigma(a)\sigma(b) = ab, \forall \sigma \in G$.

Let $b \neq 0$. Then $\sigma(b^{-1}) = (\sigma(b))^{-1} = (b)^{-1}$.

That is $\sigma(b^{-1}) = (b)^{-1} \forall \sigma \in G$. Thus $b^{-1} \in K_G$.

Hence the fixed field of G is a subfield of K. ■

Definition 9.1.4. *Let* K *be a field and let* F *be the subfield of* K. *The set of all automorphisms on* K *leaving every element of* F *is fixed is called the group of all automorphisms on* K *relative to* F. *This is denoted by* $G(K, F)$. *That is, the automorphism* σ *of* K *is in* $G(K, F)$ *iff* $\sigma(\alpha) = \alpha, \forall \alpha \in F$.

Theorem 9.1.3. *If* K *is a finite extension of* F, *then* $G(K, F)$ *is a finite group and its order* $o(G(K, F))$ *satisfies the condition* $o(G(K, F)) \leq [K : F]$.

Proof. It is given that K is a finite extension of F.

Therefore $[K : F]$ is finite.

Let $[K : F] = n$. That is, $dim_F K = n$.

Then K has a basis consisting of n elements over F.

Let $u_1, u_2, \cdots, u_n$ be a basis for K over F.

Suppose

that there are $(n + 1)$ distinct automorphisms $\sigma_1, \sigma_2, \cdots, \sigma_{n+1}$ in $G(K, F)$.

Consider the system of homogenous equations with the unknowns $x_1, x_2, \cdots, x_{n+1}$.

$\sigma_1(u_1)x_1 + \sigma_2(u_1)x_2 + \sigma_3(u_1)x_3 + \cdots + \sigma_{n+1}(u_1)x_{n+1} = 0$

$\sigma_1(u_2)x_1 + \sigma_2(u_2)x_2 + \sigma_3(u_2)x_3 + \cdots + \sigma_{n+1}(u_2)x_{n+1} = 0$

$\sigma_1(u_3)x_1 + \sigma_2(u_3)x_2 + \sigma_3(u_3)x_3 + \cdots + \sigma_{n+1}(u_3)x_{n+1} = 0$

. . . . . .

. . . . . .

$\sigma_1(u_n)x_1 + \sigma_2(u_n)x_2 + \sigma_3(u_n)x_3 + \cdots + \sigma_{n+1}(u_n)x_{n+1} = 0$

Now we have a system of n homogenous equations with $(n+1)$ unknowns.

Therefore there exists a nontrivial solution for this system.

Let $x_1 = a_1, x_2 = a_2, \cdots, x_{n+1} = a_{n+1}$ be a non trivial solution set for the above system of equations.

That is, not all a_i is zero. Therefore

$\sigma_1(u_1)a_1 + \sigma_2(u_1)a_2 + \sigma_3(u_1)a_3 + \cdots + \sigma_{n+1}(u_1)a_{n+1} = 0$

$\sigma_1(u_2)a_1 + \sigma_2(u_2)a_2 + \sigma_3(u_2)a_3 + \cdots + \sigma_{n+1}(u_2)a_{n+1} = 0$

$\sigma_1(u_3)a_1 + \sigma_2(u_3)a_2 + \sigma_3(u_3)a_3 + \cdots + \sigma_{n+1}(u_3)a_{n+1} = 0$

. . . . . .

. . . . . .

$\sigma_1(u_n)a_1 + \sigma_2(u_n)a_2 + \sigma_3(u_n)a_3 + \cdots + \sigma_{n+1}(u_n)a_{n+1} = 0$

Let $t \in K$ be arbitrary.

Then $t = \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 + \cdots + \alpha_n u_n$, where each σ is in F.

Then, $\sigma_1(t) = \sigma_1(\alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 + \cdots + \alpha_n u_n)$

i.e, $\sigma_1(t) = \sigma_1(\alpha_1 u_1) + \sigma_1(\alpha_2 u_2) + \sigma_1(\alpha_3 u_3) + \cdots + \sigma_1(\alpha_n u_n)$

i.e, $\sigma_1(t) = \sigma_1(\alpha_1)\sigma_1(u_1) + \sigma_1(\alpha_2)\sigma_1(u_2) + \sigma_1(\alpha_3)\sigma_1(u_3) + \cdots + \sigma_1(\alpha_n)\sigma_1(u_n)$

i.e, $\sigma_1(t) = \alpha_1\sigma_1(u_1) + \alpha_2\sigma_1(u_2) + \cdots + \alpha_n\sigma_1(u_n)$

Multiply by a_1 , we have,

$a_1\sigma_1(t) = a_1\alpha_1\sigma_1(u_1) + a_1\alpha_2\sigma_1(u_2) + \cdots + a_1\alpha_n\sigma_1(u_n)$

Similarly,

$a_2\sigma_2(t) = a_2\alpha_1\sigma_2(u_1) + a_2\alpha_2\sigma_2(u_2) + \cdots + a_2\alpha_n\sigma_2(u_n)$

. . . . . .

. . . . . .

$a_n\sigma_n(t) = a_n\alpha_1\sigma_n(u_1) + a_n\alpha_2\sigma_n(u_2) + \cdots + a_n\alpha_n\sigma_n(u_n)$

$a_{n+1}\sigma_{n+1}(t) \quad =$

$a_{n+1}\alpha_1\sigma_{n+1}(u_1) + a_{n+1}\alpha_2\sigma_{n+1}(u_2) + \cdots + a_{n+1}\alpha_n\sigma_{n+1}(u_n)$

Adding we get

$a_1\sigma_1(t) + a_2\sigma_2(t) + \cdots a_{n+1}\sigma_{n+1}(t) \quad = \quad \alpha_1[a_1\sigma_1(u_1) + a_2\sigma_2(u_1) +$

$a_{n+1}\sigma_{n+1}(u_1)] + \cdots + \alpha_n[a_1\sigma_1(u_n) + a_2\sigma_2(u_n) + a_{n+1}\sigma_{n+1}(u_n)]$

$\Rightarrow \alpha_1.0 + \alpha_2.0 + \alpha_3.0 + \cdots + \alpha_n.0 = 0.$

Thus, $a_1\sigma_1(t) + a_2\sigma_2(t) + \cdots a_{n+1}\sigma_{n+1}(t) = 0,$ where not all a's are zero. This is contradiction to a well known theorem.

Hence $o(G(K,G)) \leq n.$

Therefore $o(G(K,F)) \leq [K:F].$ ■

Example 9.1.1. *Let us look at the splitting field and Galois group of* $f(x) = x^3 - 5$ *over* Q*. Clearly* $Q(\sqrt[3]{5})$ *contains a root of* $f(x)$ *but is not a splitting field for* $f(x)$ *since* $Q(\sqrt[3]{5})$ *only contains one root of* $f(x)$*. Then,in* $Q(\sqrt[3]{5})[x]$ *we have* $f(x) = (x - \sqrt[3]{5})(x^2 + \sqrt[3]{5}x + \sqrt[3]{25})$ *and the quadratic factor is irreducible over* $Q(\sqrt[3]{5})$*. So let* $\zeta = (-1 + i\sqrt{3})\sqrt[3]{5}/2$*. Then* ζ *is a root of* $f(x)$ *over* Q*, hence is a root of* $x^2 + \sqrt[3]{5}x + \sqrt[3]{25}$ *over* $Q(\sqrt[3]{5})$*. Then it becomes clear that* $F = Q(\sqrt[3]{5}, \zeta)$ *is a splitting field of* $x^3 - 5$ *over* Q*. Furthermore,* $[F:Q] = [Q(\sqrt[3]{5}, \zeta) : Q(\sqrt[3]{5})][Q(\sqrt[3]{5}) : Q] = 2 \times 3 = 3!$*.*

To compute the Galois group, any element of the Galois group must permute the roots $\sqrt[3]{5}, \zeta, \overline{\zeta}$ *where* $\overline{\zeta}$ *denotes the complex conjugate of* ζ*. So let* $\sigma, \tau \in G(F,Q)$ *be defined by letting* τ *correspond to complex conjugation and let* σ *correspond to a cyclic permutation of the roots.*

So $\sigma(\sqrt[3]{5}) = \zeta, \sigma(\zeta) = \overline{\zeta}, \sigma(\overline{\zeta}) = \sqrt[3]{5}$ *and* $\sigma(q) = q$ *for all* $q \in Q$*. We leave it as an exercise to show that* σ *is an automorphism. Clearly* σ *has order* 3 *and* τ *has order* 2*. Furthermore,* $\sigma\tau(\zeta) = \sqrt[3]{5}$ *while* $\tau\sigma(\zeta) = \zeta$*, so* $G(F,K)$ *is noncommutative. Finally, we*

have $o(G(F,Q)) = 6$, *hence* $G(F,Q) \simeq S_3$.

9.2 Field of Rational Functions

Let R be a ring. Then $R[x_1]$ is also a ring. We know that $R[x_1]$ is the set of all polynomials in x_1 with coefficient from R. Let $R_1 = R[x_1]$. The set of all polynomials in x_2 with coefficient from R_1 is denoted by $R_1[x_2]$. Let $R_2 = R_1[x_2]$. The set of all polynomials in x_3 with coefficient from R_2 is denoted $R_2[x_3]$. Let $R_3 = R_2[x_3]$. Continuing this way we get $R_n = R_{n-1}[x_n]$. Clearly $R_n = R_1[x_1, x_2, \cdots, x_n]$. If the ring R is an integral domain, then $R[x_1, x_2, \cdots, x_n]$ is an integral domain. If the ring R becomes field F, then $F[x_1, x_2, \cdots, x_n]$ is an integral domain. The field of quotients, $F(x_1, x_2, \cdots, x_n)$, is also field. This field is called the field of rational functions in $x_1, x_2, \cdots, x_n$ over F.

The elements of $F(x_1, x_2, \cdots, x_n)$ are denoted as

$r(x_1, x_2, \cdots, x_n)$.

Thus, $r(x_1, x_2, \cdots, x_n) \in F(x_1, x_2, \cdots, x_n)$ is called a rational function in $x_1, x_2, \cdots, x_n$.

Elementary symmetric functions

Here we define elementary symmetric functions in n variables and its relation to rational functions.

Let $A = \{x_1, x_2, \cdots, x_n\}$ be a finite set.

Let $a_1 = \sum_{i=1}^{n} x_i$

$a_2 = \sum_{i<j} x_i x_j$

$a_3 = \sum_{i<j<k} x_i x_j x_k$

. . . . . .

. . . . . .

$a_{n-1} = \sum_{i<j<\cdots<(n-1)} x_i x_j x_k \cdots x_{n-1}$

$a_n = \prod_{i=1}^{n} x_i$

These $a_1, a_2, \cdots, a_n$ are called elementary symmetric functions in $x_1, x_2, \cdots, x_n$.

For $n = 2, a_1 = x_1 + x_2$ and $a_2 = x_1 x_2$.

For $n = 3, a_1 = x_1 + x_2 + x_3, a_2 = x_1 x_2 + x_1 x_3 + x_2 x_3$ and $a_3 = x_1 x_2 x_3$.

When $n = 2, x_1, x_2$ are the roots of the equation

$t^2 - a_1 t + a_2 = 0$

When $n = 3, x_1, x_2, x_3$ are the roots of the equation

$t^2 - a_1 t^2 + a_2 t - a_3 = 0$

. . . . . .

. . . . . .

When $n = 10, x_1, x_2, x_3, x_4, \cdots, x_9, x_{10}$ are the roots of the equation

$t^{10} - a_1 t^9 + a_2 t^8 - \cdots - a_9 t + a_{10} = 0$

Theorem 9.2.1. *Let F be a field and let $F(x_1, x_2, \cdots, x_n)$ be the field of rational functions in $x_1, x_2, \cdots, x_n$ over F. Suppose S is the field of symmetric rational functions in $x_1, x_2, \cdots, x_n$ over F. Then*

1. $[F(x_1, x_2, \cdots, x_n) : S] = n!$
2. $G(F(x_1, x_2, \cdots, x_n), S) = S_n$, *where S_n is a symmetric group of degree n.*
3. *If $a_1, a_2, \cdots, a_n$ are called elementary symmetric functions in $x_1, x_2, \cdots, x_n$, then $S = F(a_1, a_2, \cdots a_n)$*
4. $F(x_1, x_2, \cdots, x_n)$ *is the spitting field of the polynomial* $t^n - a_1 t^{n-1} + a_2 t^{n-2} + \cdots + (-1)^n a_n$ *over* $F(a_1, a_2, \cdots a_n) = S$.

Proof. Define a map

$\sigma : F(x_1, x_2, \cdots, x_n) \to F(x_1, x_2, \cdots, x_n)$

such that $\sigma(r(x_1, x_2, \cdots, x_n) = r(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)})$.

This σ is a automorphism on $F(x_1, x_2, \cdots, x_n)$.

The fixed field of S_n is defined as follows.

$$\begin{aligned} S &= \{r(x_1, x_2, \cdots, x_n) \in F(x_1, x_2, \cdots, x_n) | \\ &\qquad \sigma(r(x_1, x_2, \cdots x_n)) = r(x_1, x_2, \cdots x_n) \forall \sigma \in S_n\}. \end{aligned}$$

That is,

$r(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)}) = r(x_1, x_2, \cdots x_n), \forall \sigma \in S_n\}$.

Clearly, $S_n \subseteq G(F(x_1, x_2, \cdots, x_n), S)$

$\Rightarrow o(S_n) \leq o(G(F(x_1, x_2, \cdots, x_n), S))$

$\Rightarrow n! \leq o(G(F(x_1, x_2, \cdots, x_n), S))$

But it is clear that

$o(G(F(x_1, x_2, \cdots, x_n), S)) \leq [F(x_1, x_2, \cdots x_n) : S]$

Therefore, $n! \leq [F(x_1, x_2, \cdots x_n) : S] \quad \cdots (1)$

Consider the polynomial $p(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} + \cdots + (-1)^n a_n$, where $a_1, a_2, \cdots, a_n \in F(a_1, a_2, \cdots, a_n)$ are the elementary symmetric functions in $x_1, x_2, \cdots, x_n$.

Therefore, $x_1, x_2, \cdots, x_n$ are the roots of the polynomial $p(t)$.

That is $p(t)$ can be written as

$p(t) = (t - x_1)(t - x_2) \cdots (t - x_n)$ where $x_1, x_2, \cdots, x_n \in F(x_1, x_2, \cdots, x_n)$.

Thus $F(x_1, x_2, \cdots, x_n)$ has all the roots of the polynomial $p(t)$ namely $x_1, x_2, \cdots, x_n$.

But no proper subfield of $F(x_1, x_2, \cdots, x_n)$ has all the roots of the polynomial $p(t)$.

Therefore $F(x_1, x_2, \cdots, x_n)$ is the splitting field of the polynomial $p(t)$.

As the degree of $p(t)$ is n, we have

$[F(x_1, x_2, \cdots, x_n) : F(a_1, a_2, \cdots a_n)] \leq n!$.

But $F(a_1, a_2, \cdots a_n) \subseteq S \subseteq F(x_1, x_2, \cdots x_n)$. Therefore,

$[F(x_1, x_2, \cdots, x_n) : F(a_1, a_2, \cdots a_n)] = [F(x_1, x_2, \cdots x_n) : S][S : F(a_1, a_2, \cdots a_n)]$.

That is, $n! \geq [F(x_1, x_2, \cdots x_n) : S][S : F(a_1, a_2, \cdots a_n)]$.

That is, $n! \geq n![S : F(a_1, a_2, \cdots a_n)]$.

That is, $[S : F(a_1, a_2, \cdots a_n)] = 1$

Therefore $[F(x_1, x_2, \cdots x_n) : S] = 1 \Rightarrow S = F(a_1, a_2, \cdots a_n)$.

Thus we have proved first, third and fourth parts of the theorem.

From (1), we have

$o(S_n) = n! \leq o(G(F(x_1, x_2, \cdots x_n), S) \leq [F(x_1, x_2, \cdots x_n) : S] = n!$.

$(i.e), o(S_n) = o(G(F(x_1, x_2, \cdots, x_n), S))$

$\Rightarrow S_n = G(F(x_1, x_2, \cdots x_n), S)$.

Hence the theorem. ■

9.3 Normal extensions

In this section we define normal extension of a field F and study the relationship with the splitting fields of polynomials.

Definition 9.3.1. *Let K be a field and let F be the subfield of K. Let $G(K, F)$ be the group of all automorphisms on K relative to F. If the fixed field of $G(K, F)$ is F then the extension K is called the normal extension of F.*

Theorem 9.3.1. *Suppose K is a finite extension of F. Let H be a subgroup of $G(K, F)$.*
Let $K_H = \{x \in K | \sigma(x) = x, \forall \sigma \in H\}$ be the fixed field of H. Then,

1. $[K : K_H] = o(H)$
2. $G(K, K_H) = H$

In particular, when $G(K, F) = H$, then $[K : F] = o(G(K, F))$.

Proof. It is given that H is a subgroup of $G(K,F)$ where

$G(K,F) = \{\sigma \in \mathcal{A}(K) | \sigma(x) = x, \forall x \in F\} \cdots (1)$

(i.e), $H \subseteq G(K,F) \quad \cdots (2)$

The fixed field of H is given as

$K_H = \{x \in K | \sigma(x) = x, \forall \sigma \in H\} \quad \cdots (3)$

It also given that K is a finite extension of F.

Clearly, $F \subseteq K_H \subseteq K$.

Hence by Theorem 6.2.1, $[K:F] = [K:K_H][K_H:F]$.

Since $[K:F]$ is finite, we must have $[K:K_H]$ is finite.

Also we know that, $o(G(K,K_H)) \leq [K:K_H] \quad \cdots (4)$

Thus $G(K,K_H)$ is a finite group.

But $G(K,K_H) = \{\sigma \in \mathcal{A}(K) | \sigma(x) = x, \forall x \in K_H\} \cdots (5)$.

We claim that $H \subseteq G(K,K_H)$.

Let $y \in K_H$ and let $\sigma \in H \quad \cdots (A)$.

Then $\sigma(y) = y$. This is true for all $y \in K_H$.

This implies $\sigma \in G(K,K_H) \cdots (B)$.

From (A) and (B) we have $\sigma \in H \Rightarrow \sigma \in G(K,K_H)$.

Therefore, $H \subseteq G(K,K_H)$.

$\Rightarrow o(H) \leq o(G(K,K_H))$.

$\Rightarrow o(H) \leq [K,K_H]$, [By eqn (4)] $\cdots\cdots (6)$.

Now we prove that $H \supseteq G(K,K_H)$.

That is $o(H) \geq o(G(K,K_H))$. That is we have to prove $o(H) \geq [K : K_H]$.

Let $o(H) = n$ and let $[K:K_H] = m \quad \cdots (7)$

We will prove that $n \geq m$.

Let $H = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$, where σ_1 is the identity element of H.

Therefore $\sigma_1(x) = x, \forall x$.

Since K_H is of characteristic 0, we have K is a finite extension.

Therefore there exists an element $a \in K$ such that $K_H(a) = K$.

Therefore $[K_H(a) : K_H] = m$.

That is a is algebraic over K_H of degree m.

That is a satisfies a nonzero polynomial over K_H of degree m.

Let $\sigma_1(a) = x_1, \sigma_2(a) = x_2, \cdots, \sigma_n(a) = x_n$.

Then $x_1, x_2, \cdots, x_n$ are in K.

Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ are the elementary symmetric functions

in the variables $x_1, x_2, \cdots, x_n$.

Then, define

$$\alpha_1 = \sum_{i=1}^{n} \sigma_i(a)$$
$$\alpha_2 = \sum_{i<j} \sigma_i(a)\sigma_j(a)$$
$$\alpha_3 = \sum_{i<j<k} \sigma_i(a)\sigma_j(a)\sigma_k(a)$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$\alpha_{n-1} = \sum_{i<j<\cdots<(n-1)} \sigma_i(a)\sigma_j(a)\cdots\sigma_{n-1}(a)$$
$$\alpha_n = \prod_{i=1}^{n} \sigma_i(a)$$

Clearly, each α_i is invariant under σ_j, for all $\sigma_j \in H$.

(i.e), $\alpha_1, \alpha_2, \cdots, \alpha_n \in K_H$.

Consider the polynomial,

$p(t) = (t - x_1)(t - x_2)\cdots(t - x_n)$

(i.e), $p(t) = t^n - \alpha_1 t^{n-1} + \alpha_2 t^{n-2} + \cdots + (-1)^n \alpha_n$, where

$\alpha_1, \alpha_2, \cdots, \alpha_n \in K_H$.

Clearly, $p(t)$ is a polynomial over K_H.

Now $p(a) = (a - x_1)(a - x_2)\cdots(a - x_n)$

(i.e), $p(a) = (a - \sigma_1(a))(a - \sigma_2(a))\cdots(a - \sigma_n(a))$

(i.e), $p(a) = (a - a)(a - x_2)\cdots(a - x_n)$ $[\because \sigma_1(a) = a]$.

(i.e), $p(a) = 0$.

Thus a is a root of $p(t)$.

But degree of $p(t)$ is n and a is algebraic of degree m.

Hence $n \geq m$. Therefore $o(H) \geq [K : K_H] \quad \cdots(8)$.

From (6) and (8), we have $o(H) = [K : K_H] \quad \cdots(9)$.

But we have, $H \subseteq G(K, K_H)$ and $H \supseteq G(K, K_H)$.

Therefore, $H = G(K, K_H) \quad \cdots (10)$

But it is given that, $H = G(K, F) \quad \cdots (11)$.

Therefore, From (10) and (11), we conclude that, $F = K_H$.

Now $H = G(K, F) \Rightarrow o(H) = o(G(K, F)) \quad \cdots (12)$

Since $F = K_H, o(H) = [K : K_H]$

$\Rightarrow o(H) = [K : F] \quad \cdots (13)$ [By eqn (9)].

Thus from (12) and (13) we have $o(G(K, F)) = [K : F]$. Hence the theorem. ■

We state following two results to prove next Lemma.

Result: 1. If an extension is normal extension, then it is a finite extension

Result: 2. If the field F is of characteristic zero, then all finite extension are simple extensions.

Lemma 9.3.1. *If K is a normal extension of F, then K is a splitting field of some polynomial over F.*

Proof. It is given that K is a normal extension of F.

Therefore by above results, it is a finite extension of F.

Therefore $K = F(a)$ for some $a \in K$.

Let $G(K, F) = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$.

Consider the polynomial

$p(x) = (x - \sigma_1(a))(x - \sigma_2(a)) \cdots (x - \sigma_n(a))$ over F.

Let $\alpha_1, \alpha_2, \cdots \alpha_n$ are elementary symmetric functions in $\sigma_1(a), \sigma_2(a), \cdots, \sigma_n(a)$.

Therefore $p(x) = x^n - \alpha_1 x^{n-1} + \alpha_2 x^{n-2} + \cdots + (-1)^n \alpha_n$, where $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$.

But each α_j is invariant under $\sigma, \forall \sigma \in G(K, F)$.

Now $p(x)$ is a polynomial over F. Thus K splits $p(x)$ as a product of linear factors in F.

But a is a root of $p(x)$. Therefore all the roots of $p(x)$ are in K.
Thus K is a splitting field of some polynomial over F. ■

We now provide following results to prove next lemma.
Result 1: If $p(x) \in F[x]$ is irreducible and if a and b are the roots of $p(x)$, then $F(a) \simeq F(b)$, by an isomorphism which takes a onto b.
Result 2. Any two splitting field of the same polynomial over F are isomorphic by an isomorphism leaving every element of F fixed.

Lemma 9.3.2. *Suppose $f(x)$ is a polynomial in $F[x]$, and let K be the splitting field of $f(x)$, and let $p(x)$ is an irreducible factor of $f(x)$. If $\alpha_1, \alpha_2, \cdots \alpha_r$ are the roots of $p(x)$ then for each i, there exists an automorphism σ_i in $G(K, F)$ such that $\sigma_i(\alpha_1) = \alpha_i$.*

Proof. It is given that K be the splitting field of $f(x)$.
It is also given that $p(x)$ is an irreducible factor of $f(x)$.
Let all the roots of $p(x)$ are $\alpha_1, \alpha_2, \cdots, \alpha_r$.
Therefore, $\alpha_1, \alpha_2, \cdots, \alpha_r$ are the roots of $f(x)$.
Therefore, $\alpha_1, \alpha_2, \cdots \alpha_r$ are in K.
Let α_1, α_i be any two roots of $p(x)$. Then by result 1 given above, there exists an isomorphism τ such that $\tau(\alpha_1) = \alpha_i$,
and leaving every element of F fixed.
Let $F(\alpha_1) = F_1$ and $F(\alpha_j) = F_1'$.
Now $f(x) \in F[x] \Rightarrow f(x) \in F_1[x]$.
Similarly, $f(x) \in F[x] \Rightarrow f(x) \in F_1'[x]$.
Let K be the splitting field of $f(x)$, where $f(x) \in F_1[x]$ and let K be the splitting field of $f(x)$, where $f(x) \in F_1'[x]$.
Then there exists an isomorphism,
$\sigma_i : K \to K$, leaving every element of F fixed.

That is, $\sigma_i(x) = x, \forall x \in F$.

That is $\sigma = \tau$ on F_1. Thus, $\sigma_i(\alpha_1) = \tau(\alpha_1) = \alpha_i$. ■

Lemma 9.3.3. *If K is a splitting field of some polynomial over F, then K is a normal extension of F.*

Proof. We will prove this lemma by method of induction on $[K : F]$.

Basis for induction :

If $[K : F] = 1$, then we have $K = F$.

Thus F is a normal extension of F. Hence the lemma is obviously true.

Induction Hypothesis:

Assume that this Lemma is true for all extension K of F such that $[K : F] < n$.

Let $[K : F] = n$ and let $f(x) \in F[x]$.

Since K is a splitting field of $f(x)$, there exists an irreducible factor $p(x)$ of $f(x) \in F[x]$.

Let degree of $p(x) = r, r > 1$. Let $\alpha_1, \alpha_2, \cdots \alpha_r$ are the roots of $p(x)$ and they are in K.

Since α_1 is algebraic of degree r, we have, $[F(\alpha_1) : F] = r$.

But, $[K : F] = [K : F(\alpha_1)][F(\alpha_1) : F] \Rightarrow n = [K : F(\alpha_1)].r$

$\Rightarrow [K : F(\alpha_1) = \frac{n}{r} < n$.

Since $[K : F(\alpha_1)] < n$, by induction hypothesis, we have K is the normal extension of $F(\alpha_1)$.

Let $\theta \in K$ be fixed by every automorphism $\sigma \in G(K, F(\alpha_1))$.

We claim that $\theta \in F$. This will imply fixed field of $G(K, F(\alpha_1))$ is F.

That is, K will be normal over F.

By induction hypothesis, we have proved that K is the normal extension of $F(\alpha_1)$. So , $[K, F((\alpha_1)]$ is finite and the fixed field of $G(K, F(\alpha_1))$ is $F(\alpha_1)$.

Since $\theta \in F(\alpha_1)$ and every element of $F(\alpha_1)$ is of the form

$\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\alpha^3 + \cdots + \lambda_{r-1}\alpha^{r-1}$, where, $\lambda_0, \lambda_1, \cdots, \lambda_{r-1} \in F$.

$\Rightarrow \theta = \lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\alpha^3 + \cdots + \lambda_{r-1}\alpha^{r-1} \cdots (A)$

where, $\lambda_0, \lambda_1, \cdots, \lambda_{r-1} \in F$. Hence by above Lemma, $\forall i$, there exists $\sigma_i(\alpha_1) = \alpha_i$.

Since θ is fixed by every automorphism $\sigma_i \in G(K, F)$, we have $\sigma_i(\theta) = \theta$.

Operating σ_i on both sides of (A)

$\sigma_i(\theta) = \sigma_i(\lambda_0 + \lambda_1\alpha_1 + \lambda_2\alpha_1^2 + \lambda_3\alpha_1^3 + \cdots + \lambda_{r-1}\alpha_1^{r-1})$

$\sigma_i(\theta) =$

$\sigma_i(\lambda_0) + \sigma_i(\lambda_1\alpha_1) + \sigma_i(\lambda_2\alpha_1^2) + \sigma_i(\lambda_3\alpha_1^3) + \cdots + \sigma_i(\lambda_{r-1}\alpha_1^{r-1})$

$\theta = \lambda_0 + \lambda_1\alpha_i + \lambda_2\alpha_i^2 + \lambda_3\alpha_i^3 + \cdots + \lambda_{r-1}\alpha_i^{r-1}$

$0 = (\lambda_0 - \theta) + \lambda_1\alpha_i + \lambda_2\alpha_i^2 + \lambda_3\alpha_i^3 + \cdots + \lambda_{r-1}\alpha_i^{r-1}$, for $i = 1, 2, 3 \cdots r$.

Let $q(x) = (\lambda_0 - \theta) + \lambda_1 x + \lambda_2 x^2 + \lambda_3 x^3 + \cdots + \lambda_{r-1}x^{r-1}$

Thus $q(x)$ has r distinct roots, namely, $\alpha_1, \alpha_2, \cdots \alpha_r$. But degree of $q(x) = r - 1$.

Thus we have a polynomial of degree $r - 1$ with r roots. This is possible only if $q(x)$ is a zero polynomial.

This implies, $(\theta - \lambda_0) = 0, \lambda_1 = 0, \lambda_2 = 0, \cdots \lambda_{r-1} = 0$

i.e $\theta - \lambda_0 = 0 \Rightarrow \theta = \lambda_0$.

Since $\lambda_0 \in F$, we have, $\theta \in F$. Hence the lemma. ■

Theorem 9.3.2. *A field K is a normal extension of F if and only if it is a splitting field of some polynomial over F.*

Proof. Write the proofs of above three theorems. ■

9.4 Fundamental Theorem on Galois Theory

Galois theory analyzes the connection between algebraic extensions K of a field F and the corresponding Galois groups $G(K,F)$. This connection will enable us to prove the converse of Galois's theorem: If F is a field of characteristic 0, and if $f(x) \in F[x]$ has a solvable Galois group, then $f(x)$ is solvable by radicals. The fundamental theorem of algebra is also a consequence of this analysis. We have already seen several theorems about Galois groups whose hypothesis involves an extension being a splitting field of some polynomial. Let us begin by asking whether there is some intrinsic property of an extension K of F that characterizes its being a splitting field, without referring to any particular polynomial in $F[x]$. It turns out that the way to understand splitting fields K over F is to examine them in the context of both separability and the action of the Galois group $G(K,F)$ on K. Let K be a field and let $\mathcal{A}(K)$ be the group of all (field) automorphisms of K. If F is any subfield of K, then $G(K,F)$ is a subgroup of $\mathcal{A}(K)$, and so it acts on K. Whenever a group acts on a set, we are interested in its orbits and stabilizers, but we now ask for those elements of K stabilized by every σ in some subset H of $\mathcal{A}(K)$.

Correspondence between sub fields and subgroups

Now we state fundamental theorem on Galois Theory as

Theorem 9.4.1. *Let $f(x) \in F[x]$ and let K be the splitting field of $f(x)$. Let $G(K,F)$ be the Galois group of $f(x)$. For any subfield T of K which contains F, ($F \subseteq T \subseteq K$), let*
$G(K,T) = \{\sigma \in G(K,F) | \sigma(t) = t, \forall t \in T\}$.
For any subgroup H of $G(K,F)$, let $K_H = \{x \in K | \sigma(x) = x, , \forall \sigma \in H\}$.
Then the association of T with $G(K,T)$, is a one to one

correspondence between the set of all subfield of K *which contains* F *on to the set of all subgroups of* $G(K,F)$ *such that*

1. $K_{G(K,T)} = T$
2. $G(K, K_H) = H$
3. $[K : T] = o(G(K,T)$,
   $[T : F] =$ *index of* $G(K,T)$ *in* $G(K,F)$
4. T *is the normal extension of* F *iff* $G(K,T)$ *is a normal subgroup of* $G(K,F)$ *.*
5. *If* T *is the normal extension of* F *then*
   $G(T,F) \simeq \dfrac{G(K,F)}{G(K,T)}$

Proof. Let $f(x) \in F[x]$ and let T be the extension of F such that $F \subseteq T \subseteq K$.

Then for any polynomial $f(x) \in F[x]$, we have $f(x) \in T[x]$.

It is given that K is the splitting field of $f(x)$ over F .

That is K is the splitting field of $f(x)$ over T .

$\Rightarrow K$ is the normal extension of T .

$\Rightarrow$ Fixed field of $G(K,T)$ is T . That is, $K_{G(K,T)} = T$. This proves (1).

Since K is the normal extension of F , for any subgroup H of $G(K,F)$, by a known result, we have $G(K, K_H) = H$.

Let T be a subfield of K such that $F \subseteq T$.

Let $\sigma \in G(K,T)$. This means, σ is an automorphism on K such that $\sigma(t) = t, \forall t \in T$.

This means, σ is an automorphism on K such that $\sigma(x) = x, \forall x \in F \Rightarrow \sigma \in G(K,F)$.

Thus we have obtained a subgroup $G(K,T)$ of $G(K,F)$.

Let $A = \{T | F \subseteq T \subseteq K\}$ and define

$B = \{G(K,T_i),$ where, $F \subseteq T_1 \subseteq \cdots \subseteq T_n \subseteq K | G(K,T_n) \subseteq$

$G(K, T_{n-1}) \subseteq \cdots \subseteq G(K, F)\}$.

Let us define a map $\phi : A \to B$ such that $\phi(T) = G(K, T)$.

Clearly ϕ is onto.

Now let us prove ϕ is 1-1.

Let $\phi(T_1) = \phi(T_2)$. This implies,

$G(K, T_1) = G(K, T_2) \Rightarrow T_1 = T_2$.

Thus ϕ is $1-1$ map from $A \to B$.

Thus we have established a $1-1$ correspondence between A and B.

Let T be the extension of F such that $F \subseteq T \subseteq K$.

Then K is the normal extension of $T \Rightarrow [K : T] = o(G(K, T))$

Then K is the normal extension of $F \Rightarrow [K : F] = o(G(K, F))$

But $[K : F] = [K : T][T : F]$. Therefore

$[T : F] = \dfrac{[K : F]}{[K : T]} = \dfrac{o(G(K : F))}{o(G(K : T))}$

That is, index of $G(K : T)$ in $G(K : F)$. This proves part 3.

Lemma 9.4.1. *T is normal extension of F such that $F \subseteq T \subseteq K$ if and only if $\forall \sigma \in G(K, F), \sigma(T) \subset T$.*

Proof. Let $\sigma(T) \subset T$. This implies, $\sigma(t) \in T$, $\forall t \in T$.

But we know that, $T = F(a)$ for some $a \in T$. If $a \in T$, then $\sigma(a) \in T$ for all $\sigma \in G(K, F)$.

This implies T has all the roots of the polynomial

$p(x) = \prod(x - \sigma(a)), \forall \sigma \in G(K, F)$.

$\Rightarrow T$ is the splitting field of the polynomial $p(x)$ over F.

$\Rightarrow T$ is normal extension of F.

Conversely, assume that T is a normal extension of F

Then T is finite extension of F. Let $T = F(a)$, for some $a \in T$. Let the minimal polynomial for a be

$p(x) = \prod(x - \sigma(a))$.

But T has all the roots of $p(x)$.

Therefore if a is a root for $p(x)$, then $\sigma(a)$ is also a root of $p(x), \forall \sigma \in G(K,F)$

Thus $a \in T \Rightarrow \sigma(a) \in T, \forall \sigma \in G(K,F)$

$\sigma(T) \subset T, \forall \sigma \in G(K,F)$. Hence the lemma. ■

Now let us prove 4: Let T is the normal extension of F

$\sigma(T) \subset T, \forall \sigma \in G(K,F)$

$\sigma(t) \subset T, \forall \sigma \in G(K,F)$

Let $\tau \in G(K,T)$ and $t \in T$

$\tau(\sigma(t)) = \sigma(t); \forall \tau \in G(K,T), t \in T, \forall \sigma \in G(K,F)$

$(\sigma^{-1}\tau\sigma)(t) = \sigma^{-1}\tau(\sigma t) = t \in T.$

$(\sigma^{-1}\tau\sigma) \in G(K,T)$

Finally, if T is normal over F, given $\sigma \in G(K,F)$, since $\sigma(T) \subset T$, σ induces an automorphism σ_* of T defined by $\sigma_*(t) = \sigma(t)$ for every $t \in T$. Because σ_* leaves every element of F fixed, σ_* must be in $G(T,F)$.

Also, as is evident, for any $\sigma, \psi \in G(K,F), (\sigma\psi)_* = \sigma_*\psi_*$ whence the mapping of $G(K,F)$ into $G(T,F)$ defined by $\sigma \to \sigma_*$ is a homomorphism of $G(K,F)$ into $G(T,F)$. Now let us find the kernel of this homomorphism. It consists of all elements σ in $G(K,F)$ such that σ_* is the identity map on T. That is, the kernel is the set of all $\sigma \in G(K,F)$ such that $t = \sigma_*(t) = \sigma(t)$; by the very definition, we get that the kernel is exactly $G(K,T)$.

The image of $G(K,F)$ in $G(T,F)$, by fundamental homomorphism Theorem on groups, it is isomorphic to $\frac{G(K,F)}{G(K,T)}$, whose order is $\frac{o(G(K,F))}{o(G(K,T))} = [T:F] = o(G(T,F))$. Thus the image of $G(K,F)$ in $G(T,F)$ is all of $G(T,F)$ and so we have $G(T,F)$ isomorphic to $\frac{G(K,F)}{G(K,T)}$. Hence the theorem. ■

Example 9.4.1. *Let K be the field of complex numbers and let F*

be the field of real numbers.

We compute $G(K,F)$. *If* (σ *is any automorphism of* K, *since* $i^2 = -1, \sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$, *hence* $\sigma(i) = \pm i$.

If, in addition, σ *leaves every real number fixed, then for any* $a + bi$ *where* a *and* b *are real,* $\sigma(a + bi) = \sigma(a) + \sigma(b)\,\sigma(i) = a \pm bi$.

Each of these possibilities, namely the mapping $\sigma_1(a + bi) = a + bi$ *and* $\sigma_2(a + bi) = a - bi$ *defines an automorphism of* K, σ_1 *being the identity automorphism and* σ_2 *complex-conjugation.*

Thus $G(K,F)$ *is a group of order 2. Now let us find the fixed field of* $G(K,F)$.

It certainly must contain F. *Now let us check does the fixed field of* $G(K,F)$ *some more elements or not.*

If $a + bi$ *is in the fixed field of* $G(K,F)$ *then* $a + bi = \sigma_2(a + bi) = a - bi$, *whence* $b = 0$ *and* $a = a + bi \in F$.

Thus, in this case we see that the fixed field of $G(K,F)$ *is precisely* F *itself.*

Solved Problems

Problem 1. Let $\sigma : \mathbb{Q}(\sqrt{3}, \sqrt{5}) \to \mathbb{Q}(\sqrt{3}, \sqrt{5})$ be the automorphism that maps $\sqrt{3}$ to $-\sqrt{3}$. Then $\mathbb{Q}(\sqrt{5})$ is the subfield of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ left fixed by σ.

Problem 2. Show that the complex conjugation, defined by $\sigma : a + bi \mapsto a - bi$, is an automorphism of the complex numbers.

Solution: Since $\sigma(a) = \sigma(a + 0i) = a - 0i = a$. The automorphism defined by complex conjugation must be in $G(\mathbb{C}, \mathbb{R})$.

Problem 3. Find the Galois group of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$.

Solution: Consider the fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Then for $a, b \in \mathbb{Q}(\sqrt{5})$, $\sigma(a + b\sqrt{3}) = a - b\sqrt{3}$ is an automorphism of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ leaving $\mathbb{Q}(\sqrt{5})$ fixed. Similarly, $\tau(a + b\sqrt{5}) = a - b\sqrt{5}$ is an automorphism of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ leaving $\mathbb{Q}(\sqrt{3})$ fixed. The automorphism $\mu = \sigma\tau$ moves both $\sqrt{3}$ and $\sqrt{5}$. It will soon be

clear that $\{I, \sigma, \tau, \mu\}$ is the Galois group of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$. The following table shows that this group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

	I	σ	τ	μ
I	I	σ	τ	μ
σ	σ	I	μ	τ
τ	τ	μ	I	σ
μ	μ	τ	σ	I

We may also regard the field $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ as a vector space over $\mathbb{Q}$ that has basis $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$. It is no coincidence that $o(G(\mathbb{Q}(\sqrt{3}, \sqrt{5}), \mathbb{Q})) = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$.

We can now confirm that the Galois group of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$ in Problem 3 given above is indeed isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Certainly the group $H = \{I, \sigma, \tau, \mu\}$ is a subgroup of $G(\mathbb{Q}(\sqrt{3}, \sqrt{5}), \mathbb{Q})$, however, H must be all of $G(\mathbb{Q}(\sqrt{3}, \sqrt{5}), \mathbb{Q})$, since $o(H) = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = o(G(\mathbb{Q}(\sqrt{3}, \sqrt{5}), \mathbb{Q})) = 4$.

Problem 4: Compute the Galois group of $f(x) = x^4 + x^3 + x^2 + x + 1$ over $\mathbb{Q}$.

Solution: We know that $f(x)$ is irreducible.

Furthermore, since $(x-1)f(x) = x^5 - 1$, we can use DeMoivre's Theorem to determine that the roots of $f(x)$ are ω^i, where $i = 1, 2, 3, 4$ and $\omega = cos\left(\frac{2\pi}{5}\right) + i\, sin\left(\frac{2\pi}{5}\right)$. Hence, the splitting field of $f(x)$ must be $\mathbb{Q}(\omega)$. We can define automorphisms σ_i of $\mathbb{Q}(\omega)$ by $\sigma_i(\omega) = \omega^i$ for $i = 1, 2, 3, 4$. It is easy to check that these are indeed distinct automorphisms in $G(\mathbb{Q}(\omega), \mathbb{Q})$. Since $[\mathbb{Q}(\omega) : \mathbb{Q}] = o(G(\mathbb{Q}(\omega), \mathbb{Q})) = 4$, the σ_i's must be all of $G(\mathbb{Q}(\omega), \mathbb{Q})$. Therefore, $G(\mathbb{Q}(\omega), \mathbb{Q}) \simeq \mathbb{Z}_4$ since ω is a generator for the Galois group.

Problem 5: Let F be the field of rational numbers and let $f(x) = x^3 - 2$. Find the Galois group of $f(x)$.

Solution: In the field of complex numbers the three roots of $f(x)$ are $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$, where $\omega = (-1+\sqrt{3}i)/2$ and where $\sqrt[3]{2}$ is a real cube root of 2. Now $F(\sqrt[3]{2})$ cannot split x^3-2, for, as a subfield of the real field, it cannot contain the complex, but not real, number $\omega\sqrt[3]{2}$. Without explicitly determining it, what can we say about K, the splitting field of x^3-2 over F? By a known theorem $[K : F] \leq 3! = 6$. Since x^3-2 is irreducible over F and since $[F(\sqrt[3]{2}) : F] = 3$, we have, $3 = [F(\sqrt[3]{2}) : F] \mid [K : F]$. Finally, $[K : F] > [F(\sqrt[3]{2}) : F] = 3$.

The only way out is $[K : F] = 6$.

Therefore, $o(G(K : F)) = [K : F] = 6$.

Let us find the 6 elements $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ of $G(K, F)$.

$$\sigma_1 = \begin{pmatrix} \sqrt[3]{2} & \omega\sqrt[3]{2} & \omega^2\sqrt[3]{2} \\ \sqrt[3]{2} & \omega\sqrt[3]{2} & \omega^2\sqrt[3]{2} \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} \sqrt[3]{2} & \omega\sqrt[3]{2} & \omega^2\sqrt[3]{2} \\ \omega\sqrt[3]{2} & \sqrt[3]{2} & \omega^2\sqrt[3]{2} \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} \sqrt[3]{2} & \omega\sqrt[3]{2} & \omega^2\sqrt[3]{2} \\ \omega^2\sqrt[3]{2} & \omega\sqrt[3]{2} & \sqrt[3]{2} \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} \sqrt[3]{2} & \omega\sqrt[3]{2} & \omega^2\sqrt[3]{2} \\ \sqrt[3]{2} & \omega^2\sqrt[3]{2} & \omega\sqrt[3]{2} \end{pmatrix}$$

$$\sigma_5 = \begin{pmatrix} \sqrt[3]{2} & \omega\sqrt[3]{2} & \omega^2\sqrt[3]{2} \\ \omega\sqrt[3]{2} & \omega^2\sqrt[3]{2} & \sqrt[3]{2} \end{pmatrix}$$

and

$$\sigma_6 = \begin{pmatrix} \sqrt[3]{2} & \omega\sqrt[3]{2} & \omega^2\sqrt[3]{2} \\ \omega^2\sqrt[3]{2} & \sqrt[3]{2} & \omega\sqrt[3]{2} \end{pmatrix}$$

Let $\beta = \sqrt[3]{2}$. We know that

$K = \{a_0 + a_1\beta + a_2\beta^2 + a_3\omega + a_4\beta\omega + a_5\beta^2\omega | a_i \in \mathbb{Q},\ i = 0, \cdots, 5\}$.

Moreover, $\sigma_i(\beta) = \beta$ or $\omega\beta$ or $\omega^2\beta$, and $\sigma_i(\omega) = \omega$ or ω^2. The image of any element of K under σ_i can be elementarily determined. Therefore, the only six elements are: $G(K, F) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$

Problem: 6 Let F be the field of rational numbers and let $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$. Find the Galois group of $f(x)$.

Solution: The polynomial $f(x) = x^4 - 5x^2 + 6 \in \mathbb{Q}[x]$ factors as $x^4 + 5x^2 + 6 = (x^2 + 2)(x^2 + 3)$.

$f(x)$ splits in $\mathbb{Q}(i\sqrt{2}, i\sqrt{3})$ as $f(x) = (x + i\sqrt{2})(x - i\sqrt{2})(x + i\sqrt{3})(x - i\sqrt{3})$.

Let the splitting field be $K = \mathbb{Q}(i\sqrt{2}, i\sqrt{3})$. Let

$K = \{a_0 + a_1(i\sqrt{2}) + a_2(i\sqrt{3}) + a_3(i\sqrt{6}) | a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$.

Now $[K : F] = 2 \times 2 = 4$. Since K is the splitting field of $f(x)$, and is normal extension of F , we get,

$o(G(K, F)) = [K : F] = 4$.

Let us find the 4 elements $\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ of $G(K, F)$.

$$\sigma_1 = \begin{pmatrix} i\sqrt{2} & -i\sqrt{2} & i\sqrt{3} & -i\sqrt{3} \\ i\sqrt{2} & -i\sqrt{2} & i\sqrt{3} & -i\sqrt{3} \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} i\sqrt{2} & -i\sqrt{2} & i\sqrt{3} & -i\sqrt{3} \\ i\sqrt{3} & -i\sqrt{3} & i\sqrt{2} & -i\sqrt{2} \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} i\sqrt{2} & -i\sqrt{2} & i\sqrt{3} & -i\sqrt{3} \\ -i\sqrt{3} & i\sqrt{3} & -i\sqrt{2} & -i\sqrt{2} \end{pmatrix}$$

and

$$\sigma_4 = \begin{pmatrix} i\sqrt{2} & -i\sqrt{2} & i\sqrt{3} & -i\sqrt{3} \\ -i\sqrt{2} & i\sqrt{2} & -i\sqrt{3} & i\sqrt{3} \end{pmatrix}.$$

Therefore, $G(K,F) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$.

Summary of this unit.

In this unit we have studied the following:

- Let K be a field. A mapping $\sigma : K \to K$ is said to be an automorphism on K if
  1. σ is 1 - 1
  2. $\sigma(x+y) = \sigma(x) + \sigma(y)$
  3. $\sigma(xy) = \sigma(x)\sigma(y), \forall x, y \in K$.

- Two automorphisms σ and τ on K are said to be equal if $\sigma(x) = \tau(x), \forall x, \in K$.
  Two automorphisms σ and τ on K are said to be distinct if $\sigma(x) \neq \tau(x)$, for some x in K.

- Let K be a field. Let $\sigma_1, \sigma_2, \cdots, \sigma_n$, be distinct automorphisms on K, then it is impossible to find elements $a_1, a_2, \cdots a_n$ in K, not all zero such that
  $a_1\sigma_1(u) + a_2\sigma_2(u) + a_3\sigma_3(u) + \cdots + a_n\sigma_n(u) = 0, \forall u \in K$.

- Let G be a group of all automorphisms on K. Then the fixed field of G is denoted by K_G and is defined as follows.
  $K_G = \{x \in K | \sigma(x) = x, \forall \sigma \in G\}$

- The fixed field of G is a subfield of K.

- Let K be a field and let F be the subfield of K. The set of all automorphisms on K leaving every element of F is fixed is called the group of all automorphisms on K relative to F. This is denoted by $G(K,F)$. That is, the automorphism σ of K is in $G(K,F)$ iff $\sigma(\alpha) = \alpha, \forall \alpha \in F$.

- If K is a finite extension of F, then $G(K,F)$ is a finite group

and its order $o(G(K,F))$ satisfies the condition $o(G(K,F)) \leq [K:F]$.

- Let K be a field and let F be the subfield of K. Let $G(K,F)$ be the group of all automorphisms on K relative to F. If the fixed field of $G(K,F)$ is F then the extension K is called the normal extension of F.

- Suppose K is a finite extension of F. Let H be a subgroup of $G(K,F)$.
  Let $K_H = \{x \in K | \sigma(x) = x, \forall \sigma \in H\}$ be the fixed field of H. Then,

  1. $[K:K_H] = o(H)$
  2. $G(K,K_H) = H$

- If K is a normal extension of F, then K is a splitting field of some polynomial over F.

- Suppose $f(x)$ is a polynomial in $F[x]$, and let K be the splitting field of $f(x)$, and let $p(x)$ is an irreducible factor of $f(x)$. If $\alpha_1, \alpha_2, \cdots \alpha_r$ are the roots of $p(x)$ then for each i , there exists an automorphism σ_i in $G(K,F)$ such that $\sigma_i(\alpha_1) = \alpha_i$.

- If K is a splitting field of some polynomial over F, then K is a normal extension of F.

- A field K is a normal extension of F if and only if it is a splitting field of some polynomial over F.

- Let $f(x) \in F[x]$ and let K be the splitting field of $f(x)$. Let $G(K,F)$ be the Galois group of $f(x)$. For any subfield T of K which contains F, there is a one to one correspondence between the set of all subfields of K which contains F on to the set of all subgroups of $G(K,F)$

Multiple Choice Questions

1. Let K be an extension of F.Two automorphisms σ and τ on K are said to be distinct if
   a) $\sigma(x) \neq \tau(x)$, for some x in K
   b) $\sigma(x) \neq \tau(x)$, for all x in K
   c) $\sigma(x) \neq \tau(x)$, for some x in F
   d) $\sigma(x) \neq \tau(x)$, for all x in F

2. Let G be a group of all automorphisms on K. Then the fixed field of G is
   denoted by K_G and is defined as follows.
   a) $K_G = \{x \in K | \sigma(x) = x, \text{for some} \sigma \in G\}$
   b) $K_G = \{x \in G | \sigma(x) = x, \text{for all} \sigma \in K\}$
   c) $K_G = \{x \in K | \sigma(x) = x, \text{for all} \sigma \in G\}$
   d) $G_K = \{x \in K | \sigma(x) = x, \text{for all} \sigma \in G\}$

3. The fixed field of G is
   a) always a subfield of K.
   b) for some times a subfield of K.
   c) never be a subfield of K.
   d) None of the above

4. Find Galois group of the polynomial $x^4 - 5x^2 + 6$ over Q
   a) Z_2 b) Z_3 c) Klein 4 group d) Z_5

5. Find Galois group of the polynomial $x^2 - 3$ over Q
   a) Z_2 b) Z_3 c) R d) Z_5

6. Find Galois group of the polynomial $x^2 - 1$ over Q
   a) Z_2 b) Z_3 c) Q d) Z_5

7. If K is the field of complex numbers and F is the field of real numbers, then $o(G(K, F))$ and $K_G(K, F)$ respectively are

a) $2, K$

b) $2, F$

c) $3, K$

d) $3, F$

8. The number of elementary symmetric functions in x_1, x_2, x_3 and x_4 is

   a) 2 b) 4 c) 8 d) 16

9. If $[K : F] = 11$, then

   a) $o(G(K, F)) < 11$

   b) $o(G(K, F)) \leq 11$

   c) $o(G(K, F)) > 11$

   d) $o(G(K, F)) \geq 11$

10. An extension K is a normal extension of F if

    a) If K is a splitting field of some polynomial over F

    b) the fixed field of $G(K, F)$ is F

    c) both (a) and (b) is true

    d) (a) is true but (b) is not true.

Answers:

1	2	3	4	5	6	7	8	9	10
a	c	a	c	a	a	b	b	b	c

Exercise:

1. Prove directly that any automorphism of K must leave every rational number fixed.

2. If K is a field and S a set of automorphisms of K, prove that the fixed field of S and that of $\overline{S}$ (the subgroup of the group of

all automorphisms of K generated by S) are identical.

3. Prove that the Galois group of $x^3 - 2$ over Q is isomorphic to S_3, the symmetric group of degree 3.

4. Find the splitting field, K, of $x^3 - 2$ over Q

5. For every subgroup H of S_3 find K_H and check the correspondence given in Fundamental Theorem on Galois Theory.

6. Prove that a symmetric polynomial in $x_1, \cdots, x_n$ is a polynomial in the elementary symmetric functions in $x_1, \cdots, x_n$.

7. Express the $x_1^2 + x_2^2 + x_3^2$ as polynomial in the elementary symmetric functions in x_1, x_2 and x_3.

8. Write $x_1^3 + x_2^3 + x_3^3$ as polynomial in the elementary symmetric functions in x_1, x_2 and x_3.

9. Express the $(x_1 - x_2)^2 + (x_1 - x_3)^2 + (x_2 - x_3)^2$ as polynomial in the elementary symmetric functions in x_1, x_2 and x_3.

Block 5 - UNIT 10

Solvability by Radicals

Objectives

- We try to learn about solvable groups
- To study about commutator subgroups
- Try to learn about solvability by radicals over F
- We study Abel's Theorem

In this unit first we discuss about solvable groups.

10.1 Solvable Groups

Definition 10.1.1. *A group G is said to be solvable if there exists a nested sequence of subgroups (chain of subgroups) of the form $G = N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_k = (e)$ such that,*

i) N_{i+1} is a subgroup of N_i

ii) $\frac{N_i}{N_{i+1}}$ is abelian.

Definition 10.1.2. *Let G be a group and let $a, b \in G$. Then define, $S = \{aba^{-1}b^{-1} \mid a, b \in G\}$. The set S is called commutator set.*

Definition 10.1.3. *Let S be a nonempty subset of a group G and let $H = \{x_1x_2\cdots x_n \mid x_i \in S \ (or)\ x_i^{-1} \in S\}$. If this H is a subgroup of G, then we say that it is generated by S.*
If $H = G$, then we say that G is generated by S. This set S is called the generating set of G.

Definition 10.1.4. *Let G be a group and let S be a set of commutators of G. The subgroup G' generated by S is called the commutator subgroup of G (or) the derived subgroup of G.*

Lemma 10.1.1. *Let G' be the commutator subgroup of G. Then*
i) G' is normal in G
ii) $\frac{G}{G'}$ is abelian
iii) G' is the smallest subgroup of G such that $\frac{G}{G'}$ is abelian

Proof. Let $x \in G'$ and $g \in G$.
Claim: $g^{-1}xg \in G'$.
Since $x \in G'$, we have, $x = c_1c_2c_3\cdots c_n$, where n is finite and $c_i \in S$ or $c_i^{-1} \in S$, where S is the set of commutators of G.
Let $c_i \in S$. Then, $c_i = a_i^{-1}b_i^{-1}a_ib_i$ for some $a_i, b_i \in G$
Then $c_i^{-1} = (a_i^{-1}b_i^{-1}a_ib_i)^{-1} = b_i^{-1}a_i^{-1}b_ia_i \Rightarrow c_i^{-1}$ is a commutator.
Consider $g^{-1}xg = g^{-1}(c_1c_2c_3\cdots c_n)g$
= $g^{-1}(c_1gg^{-1}c_2gg^{-1}c_3gg^{-1}\cdots gg^{-1}c_n)g$
That is,
$g^{-1}xg = (g^{-1}c_1g)(g^{-1}c_2g)(g^{-1}c_3g)\cdots(g^{-1}c_ng)\ \cdots(1)$
Consider $g^{-1}c_ig = g^{-1}(a_i^{-1}b_i^{-1}a_ib_i)g$ for some $b, a \in G$.
= $g^{-1}(a_i^{-1}gg^{-1}b_i^{-1}gg^{-1}a_igg^{-1}b_i)g$
= $(g^{-1}a_i^{-1}g)(g^{-1}b_i^{-1}g)(g^{-1}a_ig)(g^{-1}b_ig)$
= $(g^{-1}a_ig)^{-1}(g^{-1}b_ig)^{-1}(g^{-1}a_ig)(g^{-1}b_ig)$
= $\alpha^{-1}\beta^{-1}\alpha\beta$ where, $\alpha = (g^{-1}a_ig)\ and\ \beta = (g^{-1}b_ig)$
Thus $g^{-1}c_ig$ is a commutator.
Hence $g^{-1}c_ig \in G'$, for all i.

Therefore their product is also in G'.

Hence by equation (1), we have, $g^{-1}xg \in G'$.

That is G' is normal. This proves part (i).

Proof of (ii): We know that $\frac{G}{G'} = \{aG' \quad | \, a \in G\}$.

Let $aG', bG' \in \frac{G}{G'}$.

To prove $\frac{G}{G'}$ is abelian, it is enough to prove that $aG'bG' = bG'aG'$

Now $aG'bG'$

$= abG'$

$= eabG'$

$= (baa^{-1}b^{-1})abG'$

$= ba(a^{-1}b^{-1}ab)G'$

$= baG'$. (since $(a^{-1}b^{-1}ab) \in G'$).

Thus, $aG'bG' = bG'aG'$

Hence, $\frac{G}{G'}$ is abelian.

Proof of (iii) : Suppose $\frac{G}{K}$ is abelian.

Claim : $G' \subseteq K$.

Let $aK, bK \in \frac{G}{K}$. Then, $aK.bK = ab.K$. But $bK.aK = ba.K$.

Since $\frac{G}{K}$ is abelian, we have,

$ab.K = ba.K \Rightarrow a^{-1}b^{-1}ab.K = K$

Thus $S \subseteq K$. (S is the set of all commutators).

Hence G' is the smallest subgroup of G such that $\frac{G}{G'}$ is abelian. ■

10.2 Derived subgroups

We present now following notation to describe derived subgroups.

Notation: Let G be a group.

$G^{(1)}$ is the derived subgroup of G.

That is, $G^{(1)} = G'$

$G^{(2)}$ is the derived subgroup of $G^{(1)}$.

That is, $G^{(2)} = (G^{(1)})'$

$G^{(3)}$ is the derived subgroup of $G^{(2)}$.

That is, $G^{(3)} = (G^{(2)})'$

$G^{(4)}$ is the derived subgroup of $G^{(3)}$.

That is, $G^{(4)} = (G^{(3)})'$

.....

.....

.....

$G^{(n)}$ is the derived subgroup of $G^{(n-1)}$.

That is, $G^{(n)} = (G^{(n-1)})'$

Theorem 10.2.1. *A group G is solvable if and only if $G^{(k)} = \{e\}$, for some integer k .*

Proof. Let G be the group. We know that

$G^{(k)} = (G^{(k-1)})'$.

Let $G^{(k)} = N_k$. Then N_k is the normal subgroup of N_{k-1} .

Let $G^{(k)} = \{e\}$, for some integer k .

Claim : G is solvable

Let $G = N_0$ $G' = N_1$

$G^{(2)} = N_2$

$G^{(3)} = N_3$

.....

.....

$G^{(k)} = N_k = e$

Clearly, N_1 is a normal subgroup of N_0

N_2 is a normal subgroup of N_1

N_3 is a normal subgroup of N_2

N_4 is a normal subgroup of N_3

.....

.....

N_k is a normal subgroup of N_{k-1}

More over $\frac{N_0}{N_1}$ is abelian .

$\frac{N_0}{N_1}$ is abelian .

$\frac{N_1}{N_2}$ is abelian .

$\frac{N_2}{N_3}$ is abelian .

.....

.....

.....

$\frac{N_{k-1}}{N_k}$ is abelian .

Also, $G = N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_k = (e)$. Hence G is solvable.

Converse part: Suppose G is solvable. Then there exists a chain of subgroups $N_0, N_1, N_2, \cdots, N_k$ such that ,

$N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_k = (e)$ for some k

and such that,

N_1 is a normal subgroup of N_0

N_2 is a normal subgroup of N_1

N_3 is a normal subgroup of N_2

N_4 is a normal subgroup of N_3

.....

.....

N_k is a normal subgroup of N_{k-1}

and

$\frac{N_0}{N_1}$ is abelian .

$\frac{N_1}{N_2}$ is abelian .

$\frac{N_2}{N_3}$ is abelian .

.....

.....

.....

$\frac{N_{k-1}}{N_k}$ is abelian .

Take, $G = N_0$, $G' = N_1$, $G^{(2)} = N_2$, $G^{(3)} = N_3, \cdots, G^{(k)} = N_k = e$.

Hence the Theorem. ■

Theorem 10.2.2. *The homomorphic image of a solvable group is solvable.*

Proof. Let G is a solvable group and let f be a homomorphism from G onto G^* . We have to prove that $f(G)$ is solvable.

Let us denote $f(G) = \overline{G} \quad \cdots (1)$

We have to prove that $\overline{G}$ is solvable.

Since G is solvable, there exists an integer k such that $G^{(k)} = e$.

Since f is a homomorphism, $f(e) = \overline{e}$.

That is, $f(G^{(k)}) = \overline{e} \Rightarrow \overline{f(G^{(k)})} = \overline{e}$.

But $\overline{(G^{(k)})} = \overline{(G)}^{(k)})$

Hence, $\overline{(G)}^{(k)} = \overline{e}$.

That is, $\overline{G}$ is solvable. ■

Lemma 10.2.1. *Let $G = S_n$, where $n \geq 5$, then $G^{(k)}$, for $k = 1, 2, 3, \cdots$, contains every 3-cycles of S_n .*

Proof. It is given that, $G = S_n$, for $n \geq 5$. Let us take $G = N$. Let $a = (1, 2, 3)$ and $b = (1, 4, 5)$ be any two 3-cycles of N .

Claim : $a, b \in N'$.

It is obvious that N is a normal subgroup of N itself.

Let $\alpha = (1 \;\; 2 \;\; 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Then, $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

Let $\beta = (1\ \ 4\ \ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$.

Then, $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}$ Let $x = \alpha^{-1}\beta^{-1}\alpha\beta =$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix} = (1\ \ 4\ \ 2)\ \ (3)\ \ (5)$

$\Rightarrow \quad x = \quad (1\ \ 4\ \ 2\ )$

Clearly $x \in N'$. Let $\pi \in N_0 = G$ and $x \in N'$.

Since N' is a normal subgroup of N_0, we have that $\pi^{-1}x\pi \in N'$.

Let $\pi = \begin{pmatrix} 1 & 2 & 4 \\ i_1 & i_3 & i_2 \end{pmatrix}$ for any three distinct integers i_1, i_2, i_3.

Then, $\pi^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 \\ 1 & 2 & 4 \end{pmatrix}$. Then,

$\pi^{-1}x\pi = \begin{pmatrix} i_1 & i_2 & i_3 \\ 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 4 & 2 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 4 \\ i_1 & i_3 & i_2 \end{pmatrix}$

$= \begin{pmatrix} i_1 & i_2 & i_3 \\ i_2 & i_3 & i_1 \end{pmatrix}$

$\Rightarrow \pi^{-1}x\pi \in N'$.

That is, $i_1\ \ i_2\ \ i_3\ \in N'$.

Thus, N' has all the 3-cycles of N.

$N^{(2)}$ has all the 3-cycles of N' and so of N.

$N^{(3)}$ has all the 3-cycles of $N^{(2)}$ and so of N.

$N^{(4)}$ has all the 3-cycles of $N^{(3)}$ and so of N.

.....

.....

$N^{(k)}$ has all the 3-cycles of $N^{(k-1)}$ and so of N.

Hence the Theorem. ■

Theorem 10.2.3. *The group S_n for $n \geq 5$, is not solvable .*

Proof. Let $G = S_n$. Then $G^{(k)}$ has all the 3-cycles of G. Therefore there exists no integer k such that $G^{(k)} = (e)$. Hence G is not solvable. ■

10.3 Solvability of Galois groups

In this section we now interrelate the solvability by radicals of $p(x)$ with the solvability, as a group, of the Galois group of $p(x)$. The terminology is highly suggestive that such a relation exists.
Now we need a result about the Galois group of a certain type of polynomial. We assume for the rest of the section that F is a field which contains all n^{th} roots of unity for every integer n. We have

Definition 10.3.1. *A polynomial $p(x)$ is said be solvability by radicals over F if there exists a finite sentence of fields $F_1 = F(\omega_1), F_2 = F_1(\omega_2), \cdots, F_k = F_{k-1}(\omega_k)$ such that*
$\omega_1^{r_1} \in F$, $\omega_2^{r_2} \in F_1, \cdots, \omega_k^{r_k} \in F_{k-1}$ such that all the roots of $p(x)$ are lie in F_k.

Theorem 10.3.1. *If F has all the n^{th} roots of unity and suppose that $a \neq 0$ is in F. Let $x^n - a \in F[x]$ and let K be its splitting field over F. Then*
i) $K = F(u)$, where u is any root of $x^n - a$.
ii) The Galois group of $x^n - a$ is abelian.

Proof. Since F has all the n^{th} roots of unity , it contains $\xi = e^{\frac{2\pi i}{n}}$. Then , $\xi^n = 1$ but $\xi^m \neq 1$, for $0 < m < n$.
It is also given that u is a root of $x^n - a$ and K is the splitting field of $x^n - a \quad \cdots(1)$
Therefore , $u^n - a = 0 \quad \cdots(2)$.
Substitute $u = \xi^i u$ in (2). Then we have , $(\xi^i u)^n - a = (\xi^n)^i u^n - a = 1^i u^n - a = u^n - a = 0$.

This implies, $\xi^i u$ is also a root of $x^n - a$, for $i = 1, 2, \cdots, n-1$.

i.e , $u, \xi u, \xi^2 u \cdots \xi^{n-1} u$, are all the roots of $x^n - a$.

We claim that all the above roots are distinct.

Suppose $\xi^i u = \xi^j u, (i > j)$.

$\xi^i u - \xi^j u = 0$

$(\xi^i - \xi^j)u = 0, (u \neq 0)$.

Therefore we must have $(\xi^i - \xi^j) = 0$

$\Rightarrow \xi^i = \xi^j \Rightarrow \frac{\xi^i}{\xi^j} = 1 \Rightarrow \xi^{i-j} = 1$, which is a contradiction.

Therefore all the roots are distinct.

Now $x \in F, u \in K$. Hence we have $u, \xi u, \xi^2 u, \cdots, \xi^{n-1} u \in F(u)$.

Therefore $F(u)$ is a splitting field of $x^n - a \quad \cdots (3)$.

So from (1) and (3) , we have $K = F(u)$. This proves the first part.

Now let us prove the second part.

Let σ, τ be any two elements in the Galois group of $x^n - a$.

Since u is a root of $x^n - a$, we have $u^n - a = 0$. Now $\sigma(u^n - a) = \sigma(0) = 0$

$\Rightarrow \sigma(u^n) - \sigma(a) = 0 \Rightarrow \sigma(u^n) - a = 0 \Rightarrow \sigma(u)^n - a = 0$

$\Rightarrow \sigma(u)$ is a root of $x^n - a$.

Similarly , $\tau(u)$ is also a root of $x^n - a$.

Therefore let us take , $\sigma(u) = \xi^i u$ and $\tau(u) = \xi^j u$, for some i, j.

Now, $\tau(\sigma(u)) = \tau(\xi^i u) = \tau(\xi^i)\tau(u) = \xi^i \xi^j u = \xi^{i+j} u$.

That is, $\tau(\sigma(u)) = \xi^{i+j} u \quad \cdots (4)$.

Again now, $\sigma(\tau(u)) = \sigma(\xi^j u) = \sigma(\xi^j)\sigma(u) = \xi^j \xi^i u = \xi^{i+j} u$.

That is, $\sigma(\tau(u)) = \xi^{i+j} u \quad \cdots (5)$.

Therefore from (4) and (5), we have $\tau(\sigma(u)) = \sigma(\tau(u))$. Therefore, $\tau\sigma = \sigma\tau$. Hence the Galois group is abelian. ■

Note that the Theorem says that when F has all nth roots of unity, then adjoining one root of $x^n - a$ to F , where $a \in F$, gives us the whole splitting field of $x^n - a$; thus this must be a normal extension

of F. We have

Theorem 10.3.2. *If $p(x) \in F[x]$ is solvable by radicals over F, then the Galois group of $p(x)$ is a solvable group.*

Proof. Let K be the splitting field of $p(x)$ over F and let $G(K,F)$ be the Galois group of $p(x)$ over F.

We claim that $G(K,F)$ is a solvable group.

It is given that $p(x)$ is solvable by radicals over F.

Therefore there exists a finite sentence of fields

$F_1 = F(\omega_1), F_2 = F_1(\omega_2), \cdots, F_k = F_{k-1}(\omega_k)$ such that

$\omega_1^{r_1} \in F$, $\omega_2^{r_2} \in F_1, \cdots, \omega_k^{r_k} \in F_{k-1}$ such that all the roots of $p(x)$ are lie in F_k.

Without loss of generality, we assume that F_k is a normal extension of F.

As a normal extension of F , F_k is also a normal extension of any intermediate field. Hence F_k is a normal extension of F_i for $i = 1, 2, \cdots, (k-1)$.

Also each F_i is a normal extension of F_{i-1} , for $i = 1, 2, \cdots, (k-1)$.

Thus , F_1 is a normal extension of $F \Rightarrow G(F_k, F_1)$ is a normal subgroup of $G(F_k, F)$.

F_2 is a normal extension of $F_1 \Rightarrow G(F_k, F_2)$ is a normal subgroup of $G(F_k, F_1)$.

F_3 is a normal extension of $F_2 \Rightarrow G(F_k, F_3)$ is a normal subgroup of $G(F_k, F_2)$.

Thus in general,

F_i is a normal extension of $F_{i-1} \Rightarrow G(F_k, F_i)$ is a normal subgroup of $G(F_k, F_{i-1})$.

Now consider the chain $G(F_k, F) \supseteq G(F_k, F_1) \supseteq G(F_k, F_2) \supseteq G(F_k, F_3) \supseteq \cdots \supseteq G(F_k, F_{k-1}) = (e)$.

It is given that each subgroup in this chain is the normal subgroup

of the preceding one. Since F_i is a normal extension F_{i-1}, By Fundamental Theorem on Galois Theory , we have,

$G(F_i, F_{i-1}) \simeq \dfrac{G(F_k, F_{i-1})}{G(F_k, F_i)}$

But by Theorem 10.3.1 , the Galois group $G(F_i, F_{i-1})$ is abelian.

Therefore , each quotient group , $\dfrac{G(F_k, F_{i-1})}{G(F_k, F_i)}$ is abelian.

Hence the group $G(F_k, F)$ is a solvable group.

Also we have $K \subseteq F_k$ and K is a normal extension of F. Therefore

$G(K, F) \simeq \dfrac{G(F_k, F)}{G(F_k, K)}$

Here $G(K, F)$ is the homomorphic image of a solvable group $G(F_k, F)$. Hence $G(K, F)$ is solvable. ■

Note that the converse of above theorem is also true; that is,

Theorem 10.3.3. *If the Galois group of $p(x) \in F[x]$ is a solvable group then $p(x)$ is solvable by radicals over F.*

It is important to mention here that above two theorems are true even if F does not contain roots of unity.

Now we recall the definition of general polynomial of degree n over F, $p(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$ where $F(a_1, a_2, \cdots, a_n)$ is the field of rational functions in the n - variables $a_1, a_2, \cdots, a_n$. We close this section with the great, classic theorem of Abel:

Theorem 10.3.4. ***(Abel's Theorem:)***

The general polynomial of degree $n \geq 5$ is not solvable by radicals.

Proof. In earlier theorems we saw that if $F(a_1, \cdots, a_n)$ is the field of rational functions in the n variables $a_1, \cdots, a_n$ then the Galois group of the polynomial $p(t) = t^n + a_1t^{n-1} + a_2t^{n-2} + \cdots + a_n$ where over $F(a_1, \cdots, a_n)$ was S_n, the symmetric group of degree n.

But we know that, S_n is not a solvable group when $n \geq 5$, thus by

Theorem 10.3.2, $p(t)$ is not solvable by radicals over $F(a_1, \cdots, a_n)$ when $n \geq 5$. Hence the theorem. ■

10.4 Galois Groups over the Rationals

In earlier chapters, we have seen that, given a field F and a polynomial $p(x)$, of degree n, in $F[x]$, then the splitting field of $p(x)$ over F has degree at most $n!$ over F. But we have seen that this upper limit of $n!$ is, indeed, taken on for some choice of F and some polynomial $p(x)$ of degree n over F. In fact, if F_0 is any field and if F is the field of rational functions in the variables $a_1, a_2, \cdots, a_n$ over F_0 , it was shown that the splitting field, K, of the polynomial $p(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$ over F has degree exactly $n!$ over F.

Moreover, it was shown that the Galois group of K over F is S_n, the symmetric group of degree n. This turned out to be the basis for the fact that the general polynomial of degree n, with $n \geq 5$, is not solvable by radicals. We will show that for any prime number p, at least, we can find polynomials of degree p over the field of rational numbers whose splitting fields have degree $p!$ over the rationals.

This way we will have polynomials with rational coefficients whose Galois group over the rationals is S_p. Therefore by well known theorems, we will conclude from this that the roots of these polynomials cannot be expressed in combinations of radicals involving rational numbers. We shall make use of the fact that polynomials with rational coefficients have all their roots in the complex field. We now prove that the Galois group of an irreducible polynomial of degree p, p a prime is S_p the symmetric group of degree p.

Theorem 10.4.1. *Let $q(x)$ be an irreducible polynomial of degree*

p, p a prime, over the field $\mathbb{Q}$ of rational numbers. Suppose that $q(x)$ has exactly two nonreal roots in the field of complex numbers. Then the Galois group of $q(x)$ over $\mathbb{Q}$ is S_p the symmetric group of degree p. Thus the splitting field of $q(x)$ over $\mathbb{Q}$ has degree $p!$ over $\mathbb{Q}$.

Proof. Let K be the splitting field of the polynomial $q(x)$ over $\mathbb{Q}$.

If α is a root of $q(x)$ in K, then, since $q(x)$ is irreducible over Q, by a well known theorem we have $[Q(\alpha) : Q] = p$.

Since $K \supset Q(\alpha) \supset Q$ and, according to Theorem 6.2.1, $[K : Q] = [K : Q(\alpha)][Q(\alpha) : Q] = [K : Q(\alpha)]p$, we have that $p \mid [K : Q]$.

If G is the Galois group of K over Q, by Theorem 9.3.1, $o(G) = [K : F]$.

Thus $p \mid o(G)$. Hence, by Cauchy's theorem on groups, G has an element σ of order p.

It is given that $q(x)$ has exactly two non real roots. Let these two non real roots be α_1, α_2.

Therefore $\overline{\alpha_1} = \alpha_2$ and $\overline{\alpha_2} = \alpha_1$, where the bar denotes the complex conjugate.

If $\alpha_3, \alpha_4, \cdots, \alpha_{p-1}, \alpha_p$ are the other roots, then, since they are real, $\overline{\alpha_3} = \alpha_3, \overline{\alpha_4} = \alpha_4, \cdots, \overline{\alpha_p} = \alpha_p$.

Thus the complex conjugate mapping takes K into itself, is an automorphism τ of K over Q, and interchanges α_1 and α_2, leaving the other roots of $q(x)$ fixed.

Now, the elements of G take roots of $q(x)$ into roots of $q(x)$, so induce permutations of $\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_p$.

In this way we imbed G in S_p. The automorphism τ described above is the transposition $(1, 2)$ since $\tau(\alpha_1) = \alpha_2, \tau(\alpha_2) = \alpha_1$, and $\tau(\alpha_i) = \alpha_i$ for $i \geq 3$.

Since G is imbedded in S_p and σ is in G, we can view σ is in

S_p. Since σ is of order p, and the elements in S_p of order p are exactly $p-$ cycles, we must have σ is a $p-$ cycle.

Therefore G, as a subgroup of S_p , contains a transposition and a $p-$ cycle.

It is very clear that that any transposition and any $p-$ cycle in S_p generate S_p.

Thus τ and σ generate S_p.

But since they are in G, the group generated by τ and σ must be in G.

The net result of this is that $G = S_p$. In other words, the Galois group of $q(x)$ over Q is S_p. This proves the theorem. ■

The above theorem gives us a general criterion to get S_p as a Galois group over Q. Now we obtain a polynomial of degree p over the rationals which is irreducible over Q and have exactly two nonreal roots. We do it for $p = 5$.

Let us consider the polynomial $q(x) = 2x^5 - 10x + 5$.

By the Eisenstein criterion, $q(x)$ is irreducible over Q.

If we draw the graph of this polynomial $q(x) = 2x^5 - 10x + 5$, we can see that the curve intersects the $x-$ axis in three places.

Therefore it must have three real roots.

Since this polynomial is of degree 5, the remaining two roots must be complex roots.

Thus, this $q(x)$ has exactly two non real roots.

Therefore the Galois group of $q(x)$ over Q is S_5 the symmetric group of degree 5.

But by Abel's theorem, S_5 is not solvable by radicals over Q.

That is, it is not possible to express the roots of $q(x)$ in a combination of radicals of rational numbers.

Example 10.4.1. *Show that* $f(x) = x^5 - 6x^3 - 27x - 3 \in \mathbb{Q}[x]$ *is*

not solvable.

Solution: We claim that the Galois group of $f(x)$ over $\mathbb{Q}$ is S_5. By Eisenstein's Criterion, $f(x)$ is irreducible and, therefore, must be separable. The derivative of $f(x)$ is $f'(x) = 5x^4 - 18x^2 - 27$, hence, setting $f'(x) = 0$ and solving, we find that the only real roots of $f'(x)$ are $x = \pm\sqrt{\frac{6\sqrt{6}+9}{5}}$.

Therefore, $f(x)$ can have at most one maximum and one minimum. It is easy to show that $f(x)$ changes sign between -3 and -2, between -2 and 0, and once again between 0 and 4.

Therefore, $f(x)$ has exactly three distinct real roots. The remaining two roots of $f(x)$ must be complex conjugates. Let K be the splitting field of $f(x)$. Since $f(x)$ has five distinct roots in K and every automorphism of K fixing $\mathbb{Q}$ is determined by the way it permutes the roots of $f(x)$, we know that $G(K,\mathbb{Q})$ is a subgroup of S_5. Since $f(x)$ is irreducible, there is an element $\sigma \in G(K,\mathbb{Q})$ such that $\sigma(a) = b$ for two roots a and b of $f(x)$. The automorphism of $\mathbb{C}$ that takes $a + bi \mapsto a - bi$ leaves the real roots fixed and interchanges the complex roots; consequently, $G(K,\mathbb{Q}) \subset S_5$. Since S_5 is generated by a transposition and an element of order 5, we get, $G(K,\mathbb{Q})$ must be all of S_5. By Abel's Theorem, S_5 is not solvable. Consequently, $f(x)$ cannot be solved by radicals.

Summary of this unit.

In this unit we have studied the following:

- A group G is said to be solvable if there exists a nested sequence of subgroups (chain of subgroups) of the form $G = N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_k = (e)$ such that,

  i) N_{i+1} is a subgroup of N_i

ii) $\frac{N_i}{N_{i+1}}$ is abelian.

- Let G be a group and let S be a set of commutators of G. The subgroup G' generated by S is called the commutator subgroup of G (or) the derived subgroup of G.

- Let G' be the commutator subgroup of G. Then

  i) G' is normal in G

  ii) $\frac{G}{G'}$ is abelian

  iii) G' is the smallest subgroup of G such that $\frac{G}{G'}$ is abelian .

- A group G is solvable if and only if $G^{(k)} = \{e\}$, for some integer k.

- Let $G = S_n$, where $n \geq 5$, then $G^{(k)}$, for $k = 1,2,3,\cdots$, contains every 3-cycles of S_n.

- The group S_n for $n \geq 5$, is not solvable .

- A polynomial $p(x)$ is said be solvability by radicals over F if there exists a finite sentence of fields $F_1 = F(\omega_1), F_2 = F_1(\omega_2), \cdots, F_k = F_{k-1}(\omega_k)$ such that
  $\omega_1^{r_1} \in F$, $\omega_2^{r_2} \in F_1, \cdots, \omega_k^{r_k} \in F_{k-1}$ such that all the roots of $p(x)$ are lie in F_k.

- If F has all the n^{th} roots of unity and suppose that $a \neq 0$ is in F. Let $x^n - a \in F[x]$ and let K be its splitting field over F. Then

  i) $K = F(u)$, where u is any root of $x^n - a$.

  ii) The Galois group of $x^n - a$ is abelian.

- If $p(x) \in F[x]$ is solvable by radicals over F, then the Galois group of $p(x)$ is a solvable group.

- If the Galois group of $p(x) \in F[x]$ is a solvable group then $p(x)$ is solvable by radicals over F.

- **Abel's Theorem:** The general polynomial of degree $n \geq 5$ is not solvable by radicals.

- Let $q(x)$ be an irreducible polynomial of degree p, p a prime, over the field $\mathbb{Q}$ of rational numbers. Suppose that $q(x)$ has exactly two nonreal roots in the field of complex numbers. Then the Galois group of $q(x)$ over $\mathbb{Q}$ is S_p the symmetric group of degree p. Thus the splitting field of $q(x)$ over $\mathbb{Q}$ has degree $p!$ over $\mathbb{Q}$.

Multiple Choice Questions

1. Subgroup G generated by all commutators $[u,v]$ such that $u,v \in G$ then it is known as
   a) Abelian
   b) Normal subgroup
   c) Commutator subgroup
   d) Commutator and Normal subgroup

2. Let G' be the commutator subgroup of G. Then
   a) G' is normal in G
   b) G' is not normal in G
   c) G' is not cyclic
   d) G' is cyclic

3. If G' be the commutator subgroup of G then
   a) $\frac{G}{G'}$ is abelian
   b) G' is normal in G
   c) both (a) and (b) is true
   d) None of the above

4. The symmetric group S_n , is not solvable for
   a) $n \geq 5$ b) $n = 5$ c) $n \neq 5$ d) $n \leq 5$

5. Consider the statements.

   I. If the Galois group of $p(x) \in F[x]$ is a solvable group then $p(x)$ is solvable by radicals over F

   II. If $p(x) \in F[x]$ is solvable by radicals over F, then the Galois group of $p(x)$ is a solvable group.

   a) Only (I) is true

   b) Only (II) is true

   c) (I) is true but (II) is not true

   d) both (I) and (II) is true.

6. The general polynomial $p(x)$ of degree n is not solvable by radicals if

   a) $n \leq 5$ b) $n = 5$ c) $n \neq 5$ d) $n \geq 5$

Answers:

1	2	3	4	5	6
c	a	c	a	d	d

Exercise:

1. Prove that a subgroup of a solvable group is solvable.

2. Prove that S_4 is a solvable group.

3. If G is a group, prove that all $G^{(k)}$ are normal subgroups of G.

4. If N is a normal subgroup of G prove that N' must also be a normal subgroup of G.

5. If $p(x)$ is solvable by radicals over F, prove that we can find a sequence of fields $F \subset F_1 = F(\omega_1) \subset F_2 = F_1(\omega_2) \subset \cdots \subset F_k = F_{k-1}(\omega_k)$ where

$\omega_1^{r_1} \in F$, $\omega_2^{r_2} \in F_1, \cdots, \omega_k^{r_k} \in F_{k-1}$, F_k containing all the roots of $p(x)$, such that F_k is normal over F.

6. If the Galois group of $p(x) \in F[x]$ is a solvable group prove that $p(x)$ is solvable by radicals over F.

7. Prove that the above problem is true even if F does not contain all the n^{th} roots of unity.

8. In S_5 show that $(1\ 2)$ and $(1\ 2\ 3\ 4\ 5)$ generate S_5

9. In S_5 show that $(1\ 2)$ and $(1\ 3\ 2\ 4\ 5)$ generate S_5

10. If $p > 2$ is a prime, show that $(1\ 2)$ and $(1\ 2 \cdots\ p)$ generate S_p

11. Prove that any transposition and $p-$ cycle in S_p , p a prime, generate S_p

12. Show that the polynomial $p(x) = x^3 - 3x - 3$, over Q is irreducible and have exactly two nonreal roots.

13. Prove that the polynomial $p(x) = x^5 - 6x + 3$, over Q is irreducible and have exactly two nonreal roots.

14. Show that the polynomial $p(x) = x^5 + 5x^4 + 10x^3 + 10x^2 - x - 2$, over Q is irreducible and have exactly two nonreal roots

15. Find the Galois group over Q of the polynomial $p(x) = x^3 - 3x - 3$

16. Obtain the Galois group over Q of the polynomial $p(x) = x^5 + 5x^4 + 10x^3 + 10x^2 - x - 2$

17. Find the Galois group over Q of the polynomial $p(x) = x^5 - 6x + 3$

Block 5 - UNIT 11

Finite fields

Objectives

- We try to learn about finite fields
- To study about the existence of a unique field for every prime number p and for every positive integer m.
- Try to learn about Wedderburn theorem
- We study Jacobson's Theorem

In this unit we investigate the nature of fields having only a finite number of elements. Such fields are called finite fields. Finite fields do exist, for the ring J_p of integers modulo any prime p, provides us with an example of such.

11.1 The properties of fields

In this section we shall determine all possible finite fields and many of the important properties which they possess. We begin with

Lemma 11.1.1. *Let F be a finite field consists of q elements and*

let K be an extension of F such that $[K : F] = m$, then K has q^m elements.

Proof. It is given the $[K : F] = m$. Therefore $dim_F K = m$.
Hence we can obtain a basis for K over F consisting of m elements, say, $\{v_1, v_2, \cdots, v_m\}$. Let $w \in K$.
Then $w = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \cdots + \alpha_m v_m$.
Since each coefficient has q values, we conclude that K has q^m elements.
Result: If F is of characteristic p, where p is a prime, then there exists a field F_0 such that $F_0 \subset F$ and $F_0 \simeq J_p$. ■

Corollary 11.1.1. *If F is a finite field,then F has p^m elements, where the prime p is the characteristic of F.*

Proof. It is given that F is a finite field of characteristic p, where p is a prime number.
Then by the above result, there exists a proper sub field F_0 isomorphic to J_p.
Since J_p has p elements we have F_0 has p elements.
But F is a finite extension of F_0. Let $[F : F_0] = m$.
Hence by Lemma 11.1.1, we have F has p^m elements. ■

Corollary 11.1.2. *If F is a finite field having p^m elements, where p is a prime, then every element $a \in F$ satisfies $a^{p^m} = a$.*
In other words, every element of F is a root for the polynomial $x^{p^m} - x$ for some $m > 0$.

Proof. Let $a = 0$. Then, $0^{p^m} = 0$. This implies $0 = 0$, which is true.
There fore let us prove this corollary for the nonzero elements of F.
Let $G = F - \{0\}$. Then G is group with respect to multiplication of order $p^m - 1$.

That is, $o(G) = p^m - 1$.

By corollary to Lagrange's Theorem, for any $a \in G$, $a^{o(G)} = 1$.

That is, $a^{p^m-1} = 1$.

Multiply by a on both sides, we have, $a^{p^m} = a$. ■

Lemma 11.1.2. *If F is a finite field consisting of p^m elements, then the polynomial $x^{p^m} - x \in F[x]$ factors in $F[x]$ as $x^{p^m} - x = \prod_{\lambda \in F} (x - \lambda)$.*

Proof. The polynomial $x^{p^m} - x \in F[x]$ has p^m roots.

But every element in F is a root for $x^{p^m} = x$.

Hence the polynomial $x^{p^m} = x$ has all the roots in F itself.

Since F has p^m elements and since $x^{p^m} = x$ has p^m roots in F we have each element of F is a root of $x^{p^m} = x$.

Thus, F has all the roots of the polynomial $x^{p^m} = x$ and no proper subfield of F has all the roots of the polynomial $x^{p^m} = x$.

Therefore F is splitting field of the polynomial $x^{p^m} = x$.

Thus $x^{p^m} = x$ can splits in $F[x]$. ■

Corollary 11.1.3. *If the field F has p^m elements then F is the splitting field of the polynomial $x^{p^m} - x$.*

Proof. By Lemma 11.1.2, $x^{p^m} - x$ certainly splits in F. But, it cannot split in any smaller field for that field would have to have all the roots of this polynomial and so would have to have at least p^m elements. Thus F is the splitting field of $x^{p^m} - x$. ■

As we have seen in earlier chapters any two splitting fields over a given field of a given polynomial are isomorphic. We can state

Lemma 11.1.3. *Any two finite fields having the same number of elements are isomorphic.*

Proof. Let F and K be any two finite fields.

Let F contains p^m elements and let K contains p^m elements.

Then by Lemma 11.1.2, the polynomial $x^{p^m} = x$ has all the p^m roots in F.

Therefore F is the splitting field of the polynomial $x^{p^m} = x$.

Similarly, the polynomial $x^{p^m} = x$ has all the p^m roots in K.

Therefore K is the splitting field of the polynomial $x^{p^m} = x$.

Since a polynomial $x^{p^m} = x$ has two splitting fields, they are isomorphic.

Hence F and K are isomorphic. Hence the proof. ■

Result: If F is of characteristic p, where p is a prime, then the polynomial $x^{p^m} = x$ has distinct roots.

Thus for any integer m and any prime number p there is, up to isomorphism, at most one field having p^m elements. The purpose of the next lemma is to demonstrate that for any prime number p and any integer m there is a field having p^m elements. Once we done this, we shall know that there is exactly one field having p^m elements where p is an arbitrary prime and m an arbitrary integer.

Lemma 11.1.4. *For every prime number p and for every positive integer m, there exists a field F consisting of p^m elements.*

Proof. It is given that p is a prime number. So, J_p is the ring of integers modulo prime p.

Let $J_p[x]$ be the set of all polynomials in x over J_p.

Then $x^{p^m} - x \in J_p[x]$.

Let K be the splitting field for the polynomial $x^{p^m} - x$.

Clearly F be the set of all the roots of $x^{p^m} - x$.

Thus F has p^m elements.

Claim: F is a field.

Let $a, b \in F$. Then $a^{p^m} = a$ and $b^{p^m} = b$.

$(ab)^{p^m} = (a)^{p^m}.(b)^{p^m} = ab.$

Thus F is closed with respect to multiplication.

Consider $(a \pm b)^{p^m} = (a)^{p^m} + p^m C_1 (a^{p^m-1})b + \cdots + (b)^{p^m}$

$(a \pm b)^{p^m} = (a)^{p^m} \pm (b)^{p^m} = a \pm b.$

Hence $a \pm b \in F$.

Consequently F is a subfield of K and F itself is a field consisting of p^m elements. ■

Theorem 11.1.1. *For every prime number p and for every positive integer m, there exists a unique field F consisting of p^m elements.*

Proof. Write the proofs of Lemma 11.1.3 and Lemma 11.1.4. ■

Theorem 11.1.2. *Let G be finite abelian group enjoying the property that the relation $x^n = e$ is satisfied by atmost n elements of G for every integer n. Then G is a cyclic group.*

Proof. Our aim is to show that G is cyclic.

Case (i): Let $o(G) =$ Power of some prime number q.

Let $a \in G$ such that a is of maximum order.

Let $o(a) = q^r$ for some integer r. Therefore $a^{q^r} = e$.

Consider the elements $A = \{e, a, a^2, a^3, \cdots, a^{q^r-1}\}$.

Clearly these elements are distinct because these are distinct solutions of $x^{q^s} = e$.

Let $b \in G$ such that $o(b) = q^s$ where $s < r$.

Consider $(b)^{q^r} = \left(b^{q^s}\right)^{q^{r-s}} = e$.

Thus b is a root for $x^{q^r} = e$.

Since b is a element of A, we have $b = a^i$ for $0 \leq i \leq q^{r-1}$.

Thus b can be expressed as some integral powers of a.

That is a is a generator of G. Hence G is cyclic.

Case(ii): Suppose G is a finite abelian group of general order.

We know that every finite abelian group can be expressed as a

direct product of its Sylow subgroups.

Thus, $G = S_{q_1}S_{q_2}S_{q_3}\cdots S_{q_k}$ where each S_{q_i} is a Sylow subgroup such that $q_1, q_2, \cdots, q_k$ are distinct prime numbers, which are divisors of G.

Let $g \in G$ be arbitrary.

Therefore $g = s_1s_2s_3\cdots s_k$ where each $s_i \in S_{q_i}$.

Now each solution of $x^n = e$ in S_{q_i} is also a solution of $x^n = e$ in G.

Thus each Sylow sub group satisfies the hypothesis of the theorem.

Hence each Sylow sub group is Cyclic.

Let a_i be the generator of $S_{q_i}, i = 1, 2, 3, \cdots, k$.

Let $c = a_1a_2\cdots a_k$. Clearly $c \in G$.

We claim that c is the generator for G.

Let $o(c) = m$.

Therefore $c^m = e$ and $m|o(G) \quad \cdots(1)$

Now $c^m = (a_1a_2\cdots a_k)^m = e$.

That is, $a_1^m a_2^m \cdots a_k^m = e$.

This implies, $a_1^m = e, a_2^m = e, \cdots, a_k^m = e$.

Thus, $o(a_1)|m, o(a_2)|m, o(a_3)|m, \cdots o(a_k)|m$.

Therefore,

$o(a_1) = o(S_{q_1}), o(a_2) = o(S_{q_2}), o(a_3) = o(S_{q_3}), \cdots, o(a_k) = o(S_{q_k})$.

Therefore, $o(S_{q_1})|m, o(S_{q_2})|m, o(S_{q_3})|m, \cdots, o(S_{q_k})|m$.

Therefore $o(S_{q_1})o(S_{q_2})o(S_{q_3})\cdots o(S_{q_k})|m$.

That is $o(G)|m \quad \cdots(2)$.

From (1) and (2), we have $o(G) = m = o(c)$.

Therefore c is the generator for G. Hence G is cyclic. ■

Lemma 11.1.5. *Let K be a finite field and let G be a finite subgroup of the multiplicative group of nonzero elements of K. Then G is a cyclic group.*

Proof. Since K is a field, any polynomial of degree n in $K[x]$ has atmost n roots in K.
In particular for the polynomial $x^n - 1 \in K[x]$ has atmost n roots in K and hence in G, where $G = K - 0$.
Since each root is non zero, all these roots are in G.
Thus atmost n elements of G satisfies the property, $x^{p^m} = 1$;
Hence by a known Lemma, we have G is cyclic. ■

Theorem 11.1.3. *The multiplicative group of nonzero elements of a finite field is a cyclic group.*

Proof. By Lemma 11.1.5, F is cyclic. ■

We conclude this section by using a counting argument to prove the existence of solutions of certain equations in a finite field. We shall need the result in one proof of the Wedderburn theorem.

Lemma 11.1.6. *If F is a finite field and $\alpha \neq 0, \beta \neq 0$ are in F, then we can find elements $a, b \in F$ such that $1 + \alpha a^2 + \beta b^2 = 0$.*

Proof. We know that for every prime number p and for every positive integer m, there exists a unique field F consisting p^m elements.
Case(i): Let $p = 2$. Then F has 2^n elements, where n is any positive integer.
Therefore $\forall x \in F$ we have $x^{2^n} = x$.
Hence every element in F is a square .
Let $\alpha \neq 0$ in F. Therefore α^{-1} exists in F.
Therefore $\alpha^{-1} = a^2$, for some $a \in F$. Now,
$1 + \alpha a^2 + \beta b^2 = 1 + \alpha(\alpha^{-1}) + \beta(0) = 1 + 1 = 2(\mod 2) = 0$.
Case(ii): If F is a characteristic p, where p is odd prime, then F has p^m elements, for some positive integer n.
Let us define a subset $W_\alpha = \{1 + \alpha x^2 | x \in F\}$.

When $x \neq 0$ for both x and $-x$ we get only one element in W_α.
So, for all nonzero elements of F, we have $\frac{p^n-1}{2}$ elements.
Therefore W_α has $1+\frac{p^n-1}{2}$ elements.
That is, W_α has $1+\frac{p^n-1}{2}=\frac{2+p^n-1}{2}=\frac{p^n+1}{2}$ elements.
Thus W_α has more than half of the elements of F.
Let us define a subset $W_\beta=\{-\beta x^2 | x \in F\}$.
Here also W_β has $\frac{p^n+1}{2}$ elements.
Thus W_β has more than half of the elements of F.
Since W_α and W_β are subsets of F and each of them having more than half of elements of F, we have that their intersection nonempty.
Let $c \in W_\alpha \cap W_\beta$.
Now, $c \in W_\alpha \Rightarrow c = 1+\alpha a^2$, for some $a \in F$.
Similarly, $c \in W_\beta \Rightarrow c = -\beta b^2$, for some $b \in F$.
Therefore, $1+\alpha a^2 = -\beta b^2$.
Hence $1+\alpha a^2+\beta b^2 = 0$. Hence the theorem. ■

Definition 11.1.1. *The nonzero elements of J_p form a cyclic group under multiplication. We denote this group as J_p^*. Any generator of this group is called a primitive root of p.*

Example 11.1.1. *Now let us find the primitive root of 11. The non zero residues of 11 are $J_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$. It is clear that 2 is a generator of J_{11}^*, since $2^1=2, 2^2=4, 2^3=8, 2^4=16=5, 2^5=32=10, 2^6=64=9, 2^7=128=7, 2^8=256=3, 2^9=512=6, 2^{10}=1024=1$. Therefore 2 is a primitive root of 11.*
Clearly $o(J_{11}^*)=10$.
The positive integers which are less than 10 but relatively prime to 10 are $\{1,3,7,9\}$.
There fore the cyclic group J_{11}^* has 4 generators.
Therefore 11 has 4 primitive roots.

11.2 Wedderburn's Theorem

In 1905 Wedderburn proved the theorem, now considered a classic, that a finite division ring must be a commutative field.

Cyclotomic polynomials

Now we discuss the concept of primitive n^{th} root of unity and cyclotomic Polynomials.

Definition 11.2.1. *A complex number θ is said to be a primitive n^{th} root of unity if $\theta^n = 0$ but $\theta^m \neq 0$ for any positive integer $m < n$.*

The complex numbers satisfying $x^n = 1$ form a finite subgroup, under multiplication, of the complex numbers, so by a known theorem this group is cyclic. Any cyclic generator of this group must then be a primitive n^{th} root of unity, so we know that such primitive roots exist. (Alternatively, $\theta = e^{\frac{2\pi i}{n}}$ yields us a primitive n^{th} root of unity.)

$\phi_1(x) = x - 1$

$\phi_2(x) = x + 1$

$\phi_3(x) = x^2 + x + 1$

$\phi_4(x) = x^2 + 1$

$\phi_5(x) = x^4 + x^3 + x + 1$

$\phi_6(x) = x^2 - x + 1$

The divisors of 2 are 1,2. Therefore

$\phi_1(x)\phi_2(x) = (x-1)(x+1) = x^2 - 1.$

This can be written as $x^2 - 1 = \prod_{d|2} \phi_d(x)$

The division of 3 are 1,3. Therefore

$\phi_1(x)\phi_3(x) = (x-1)(x^2+x+1) = x^3 - 1.$

This can be written as $x^3 - 1 = \prod_{d|3} \phi_d(x)$

The divisors of 4 are 1,2,4. Therefore

$\phi_1(x)\phi_2(x)\phi_4(x) = (x-1)(x+1)(x^2+1) = x^4 - 1.$

This can be written as

$x^4 - 1 = \prod_{d|4} \phi_d(x) = \prod_{d|4,(d\neq 4)} \phi_d(x)\phi_4(x)$

In general,

$x^n - 1 = \prod_{d|n} \phi_d(x) = \prod_{d|n,(d\neq n)} \phi_d(x)\phi_n(x)$

Theorem 11.2.1. *A finite division ring is necessarily a commutative Field.*

Proof. Let K be a finite division ring. Let $a \in K$.

Define $N(a) = \{x \in K | ax = xa\}$

Define the centre of K as $Z = \{z \in K | zx = xz, \forall x \in K\}$.

It is clear that $Z \subseteq N(a) \subseteq K$.

Since K is a division ring, Z is a subdivision ring of K.

$N(a)$ is a subdivision ring of K. Also Z is a subdivision ring of $N(a)$.

Let Z has q elements.

Viewing K as a vector space over Z such that $[K : Z] = n$, we have K has q^n elements.

Viewing $N(a)$ as a vector space over Z such that $[N(a) : Z] = n(a)$,we have $N(a)$ has $q^{n(a)}$ elements.

Claim: $Z = K$ or $n = 1$.

Being a division ring the nonzero elements of K form a group with respect to multiplication.

Let this group be D^*. Then $o(D^*) = q^n - 1$. $D^* = K - \{0\}$.

Being a division ring the nonzero elements of $N(a)$ form a group with respect to multiplication.

Let this group be N^*. Then $o(N^*) = q^{n(a)} - 1$.

Being a division ring the nonzero elements of Z form a group with respect to multiplication.

Let this group be Z^*. Then $o(Z^*) = q - 1$.

By class equation on groups, we have

$o(D^*) = o(Z^*) + \sum \frac{o(D^*)}{o(N^*)}$

$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^{n(a)} - 1} \quad \cdots (1)$

Consider the cyclotomic polynomials $\phi_n(x) = \prod(x - \theta)$, where θ is a primitive nth root of unity.

Also it is easy to see that

$x^n - 1 = \prod_{d|n} \phi_d(x) = \prod_{d|n,(d\neq n)} \phi_d(x)\phi_n(x) \quad \cdots (2)$

First we show that $\phi_n(x)$ is a monic Polynomial with integer coefficients.

Let us prove this by method of induction on n.

Let $n = 1$. Then $\phi_1(x) = x - 1$.

Clearly it is a monic polynomial with integer coefficients.

Induction Hypothesis: Let us assume that this result is true for all polynomials of degree upto $n - 1$.

That is $\phi_{n-1}(x)$ is a monic polynomial with integer coefficients.

Consider $\phi_n(x)$. From (2), we have

$x^n - 1 = \prod_{d|n} \phi_d(x) = \prod_{d|n,(d\neq n)} \phi_d(x)\phi_n(x).$

But $d|n, d \neq n \Rightarrow d < n$.

i.e, $\phi_n(x) = \frac{x^n - 1}{\prod_{d|n,(d\neq n)} \phi_d(x)}$.

Here $x^n - 1$ is integer monic and $\prod_{d|n,(d\neq n)} \phi_d(x)$ is integer monic.

Therefore $\phi_n(x) = \frac{x^n - 1}{\prod_{d|n,(d\neq n)} \phi_d(x)}$ is also integer monic.

Secondly now we prove that $\phi_n(x) | \frac{x^n - 1}{x^d - 1}$, where $d|n, d \neq n \quad \cdots (2)$

We know that $x^n - 1 = \prod_{d|n} \phi_d(x)$ and $x^d - 1 = \prod_{k|d} \phi_k(x)$

Since $d < n, x^d - 1$ does not involve the term $\phi_n(x)$, we have all

the divisors of d are also divisors of n, Therefore there may be some divisors for n which are not divisors of d. Therefore we have,

$$x^n - 1 = (x^d - 1)\left[\prod_{k|n,(k\neq n)} \phi_k(x)\right]\phi_n(x)$$

$$x^n - 1 = (x^d - 1)g(x)\phi_n(x) \text{ where } g(x) = \prod_{k|n,(k\neq n)} \phi_k(x)$$

Therefore we have,

$$\frac{x^n - 1}{x^d - 1} = g(x)\phi_n(x).$$

Hence, $\phi_n(x)|\frac{x^n - 1}{x^d - 1}$.

Note that $\phi_n(x)|(x^n - 1)$ is true for all x. Let t be an integer.

Therefore $\phi_n(t)$ is also an integer.

Thus by (2), we have, $\phi_n(t)|\frac{t^n - 1}{t^d - 1}$, where $d|n, d \neq n$

In particular, for the integer q, we have,

$\phi_n(q)|\frac{q^n - 1}{q^{n(a)-1}}$, where $n(a)|n, n(a) \neq n$

Also, $\phi_n(q)|(q^n - 1)$.

That is, $q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^{n(a)} - 1}, n(a)|n, n(a) \neq n$

In particular, $\phi_n(q)|\frac{q^n - 1}{q^{n(a)-1}}$

Also, $\phi_n(q)|(q^n - 1)$.

This implies $q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^{n(a)} - 1}$ and $\phi_n(q)|(q^n - 1)$

This implies, $\phi_n(q)|(q - 1) \quad \cdots (3)$

Finally we show that $n = 1$.

Indeed, if $n > 1$, then $\phi_n(q) = \prod(q - \theta)$.

Now $|q - \theta| > |q| - |\theta| > q - 1$.

$|\phi_n(q)| = \prod|(q - \theta)| > \prod|(q - 1)|$

$\phi_n(q) > (q - 1)$ and therefore $\phi_n(q) > (q - 1)$ which is a contradiction to (3). Therefore $n = 1$ and thus the claim is established. Now $o(Z) = o(K)$ and $Z \subseteq K \Rightarrow Z = K$. Since Z is commutative, K is commutative. Therefore K is a commutative field. Hence the theorem. ■

11.3 Jacobson's Theorem

In this section, in the division ring case, we will prove a beautiful theorem due to Jacobson.

The central elements

Definition 11.3.1. *An element $x \in R$ is called idempotent if $x^2 = x$. The center of R is $Z(R) = \{x \in R : xy = yx \text{ for all } y \in R\}$.*

It is easy to see that $Z(R)$ is a subring of R. An element $x \in R$ is called central if $x \in Z(R)$. Obviously R is commutative iff $Z(R) = R$, that is, every element of R is central.

Theorem 11.3.1. *If D be a division ring such that for every element $a \in D$, there exists a positive integer $n(a) > 1$ such that $a^{n(a)} = a$, then D is a commutative field.*

Proof. Let $a \in D$. Then there exists a positive integer n such that $a^n = a, (n > 1)$.

Let $a \neq 0$. Since $a \neq 0, \quad 2a \in D,$ there exists a positive integer say, m, such that $(2a)^m = 2a, (m > 1)$.

Clearly $(n-1)(m-1)+1 > 1$.

Let $s = (n-1)(m-1)+1$.

That is $s = nm - n - m + 2$.

Then $s > 1$. Now,

$$\begin{aligned} a^s &= a^{nm-n-m+2} \\ &= a^{n(m-1)+2-m} \\ &= a^{n(m-1)}a^{(2-m)} \\ &= (a^n)^{(m-1)}a^{(2-m)} \end{aligned}$$

$$\begin{aligned} &= a^{(m-1)}a^{(2-m)} \\ &= a^{(m-1+2-m)} \\ &= a \end{aligned}$$

Thus $a^s = a$. Again, now consider,

$$\begin{aligned} (2a)^s &= (2a)^{(nm-n-m+2)} \\ &= (2a)^{m(n-1)}(2a)^{(2-n)} \\ &= ((2a)^m)^{(n-1)}(2a)^{(2-n)} \\ &= (2a)^{(n-1)}(2a)^{(2-n)} \\ &= (2a)^{(n-1+2-n)} \\ &= 2a \end{aligned}$$

Thus $(2a)^s = 2a \quad \cdots (1)$

But $(2a)^s = 2^s a^s = 2^s a \cdots (2)$

Therefore from (1) and (2) we have $2^s = 2a$.

That is, $2^s - 2a = 0$. That is, $(2^s - 2)a = 0$.

Let $(2^s - 2) = p$. Therefore $p > 0$. Hence D is of characteristic $p > 0$.

Let Z be the centre of D. Then $Z \subseteq D \quad \cdots (3)$.

Claim: $D \subseteq Z$.

Let P be a sub field of Z which is isomorphic to J_p.

Therefore P has p elements.

Since $a^n = a$, we have $a^n - a = 0$. This implies, a satisfies the polynomial $x^n - x \in J_p[x]$.

This implies a is algebraic over J_p (over P).

Therefore $[P(a) : P]$ is finite.

Let us assume that a algebraic of degree n.

Therefore $[P(a) : P] = n$.

Therefore $P(a)$ has p^n elements.

Since $a \in P(a)$ and since $P(a)$ has p^n elements, we have a satisfies a polynomial $x^{p^n} - x$.

That is $a^{p^n} - a = 0$. That is $a^{p^n} = a$. Here $p^n > 1$.

Similarly we can show that $b^{p^k} = b$.

Now we define

$$W = \left\{ x \in D | x = \sum_{i=1}^{p^n} \sum_{j=1}^{p^k} p_{ij} a^i b^j \right\}$$

It is easy to see that, W is a finite subdivision ring of D.

Therefore by Wedderburn's Theorem we have W is a commutative field.

Moreover $a, b \in W \Rightarrow ab = ba \quad \cdots (4)$

Now we have, D and $a \notin Z$, by the above result, there exists an element b such that $bab^{-1} \neq a$. That is $ab \neq ba$, which is a contradiction to (4).

Therefore for every $a \in D$ we have $a \in Z$.

Hence $D \subseteq Z \quad \cdots (5)$.

From (1) and (5) we have $Z = D$.

Since Z is commutative we have D is commutative.

Therefore D is a commutative division ring. Hence it is a field. ■

Jacobson's theorem actually holds for every ring R satisfying $a^{n(a)} = a$ for every $a \in R$, not just for division rings.

Summary of this unit.

In this unit we have studied the following:

- Let F be a finite field consists of q elements and let K be an extension of F such that $[K : F] = m$, then K has q^m elements.
- If F is a finite field,then F has p^m elements, where the prime p is the characteristic of F.

- If F is a finite field having p^m elements, where p is a prime, then every element $a \in F$ satisfies $a^{p^m} = a$.
  In other words, every element of F is a root for the polynomial $x^{p^m} - x$ for some $m > 0$.

- If F is a finite field consisting of p^m elements, then the polynomial $x^{p^m} - x \in F[x]$ factors in $F[x]$ as $x^{p^m} - x = \prod_{\lambda \in F} (x - \lambda)$.

- If the field F has p^m elements then F is the splitting field of the polynomial $x^{p^m} - x$.

- Any two finite fields having the same number of elements are isomorphic.

- For every prime number p and for every positive integer m, there exists a field F consisting of p^m elements.

- For every prime number p and for every positive integer m, there exists a unique field F consisting of p^m elements.

- Let G be finite abelian group enjoying the property that the relation $x^n = e$ is satisfied by atmost n elements of G for every integer n. Then G is a cyclic group.

- Let K be a finite field and let G be a finite subgroup of the multiplicative group of nonzero elements of K. Then G is a cyclic group.

- The multiplicative group of nonzero elements of a finite field is a cyclic group.

- If F is a finite field and $\alpha \neq 0, \beta \neq 0$ are in F, then we can find elements $a, b \in F$ such that $1 + \alpha a^2 + \beta b^2 = 0$.

- A complex number θ is said to be a primitive n^{th} root of unity if $\theta^n = 0$ but $\theta^m \neq 0$ for any positive integer $m < n$.

- The nonzero elements of J_p form a cyclic group under multiplication. We denote this group as J_p^*. Any generator of this group is called a primitive root of p.
- **Wedderburn theorem:** A finite division ring is necessarily a commutative Field.
- **Jacobson's Theorem**: If D be a division ring such that for every element $a \in D$, there exists a positive integer $n(a) > 1$ such that $a^{n(a)} = a$, then D is a commutative field.

Multiple Choice Questions

1. Number of elements in the Galois group of p^{th} cyclotomic polynomial over Q is
   a) 2 b) p c) $p-1$ d) $p+1$
2. Which of the following is a Fermat prime
   a) 2 b) 6 c) 5 d) 8
3. Which of the following is not a Fermat prime
   a) 3 b) 5 c) 17 d) 8
4. Find the number of elements less than and relatively prime to 10
   a) 3 b) 5 c) 4 d) 8
5. Which of the following is an order of a finite field
   a. 16 b) 20 c. 26 D. 15
6. Which of the following is not an order of a finite field
   a) 16 b) 20 c) 3 d) 5
7. If F has 6561 elements, then the splitting field of $x^{6561} = x$ is
   a) Q b) F c) $Q(\sqrt{2})$ d) $F(\sqrt{2})$
8. The number of primitive roots of 17 is
   a) 4 b) 6 c) 8 d) 10

9. A complex number θ is a primitive n^{th} root of unity if
   a) $\theta^n = 1$ and $\theta^m = 1$, $m < n$
   b) $\theta^n = 1$ and $\theta^m \neq 1$, $n < m$
   c) $\theta^n = 1$ and $\theta^m = 1$, $n < m$
   d) $\theta^n = 1$ and $\theta^m \neq 1$, $m < n$

Answers:

1	2	3	4	5	6	7	8	9
c	c	d	c	a	b	b	c	d

Exercise:

1. If the field F has p^n elements prove that the automorphisms of F form a cyclic group of order n.
2. If F is a finite field, by the quaternions over F we shall mean the set of all $\{\pm 1, \pm i, \pm j, \pm k\}$, such that $ijk = i^2 = j^2 = k^2 = -1, ij = -ji, ik = -ki, jk = -kj$. Prove that the quaternions over a finite field do not form a division ring.
3. Find primitive roots of: 17, 23, 31.
4. How many primitive roots does a prime p have?
5. If $t > 1$ is an integer and $(t^m - 1) \mid (t^n - 1)$, prove that $m \mid n$.
6. If D is a division ring, prove that its dimension (as a vector space) over its center cannot be 2.
7. Show that any finite subring of a division ring is a division ring.
8. If R is a finite ring in which $x^n = x$, for all $x \in R$ where $n > 1$ prove that R is commutative.
9. If R is a finite ring in which $x^2 = 0$ implies that $x = 0$, prove that R is commutative.

10. If $W = \left\{ x \in D | x = \sum_{i=1}^{p^n} \sum_{j=1}^{p^k} p_{ij} a^i b^j \right\}$, prove that, W is a finite subdivision ring of D where D is given as in statement of Jacobson's theorem.