1

INTRODUCTION TO GROUPS

Unit Structure

1.0 Objectives

After going through this unit you shall come to know about

- The algebraic structure called groups with its basic properties
- The concept of subgroups and types of groups
- The notion of the order and its relation with the order of the groups

We assume that a student has basic knowledge of set theory and is familiar with $\cup, \cap, \ldots$ etc. We are giving some basic concepts, which a student should go through quickly.

1.1 Prerequisites

SETS : The cardinality of a set A is denoted by $|A|$. If A and B are sets, the cartesian product of A and B is defined as, $A \times B = \{(a,b)/a \in A,\ b \in B\}$.

If $(a,b),(a',b') \in A \in B$, then $(a,b) = (a',b') \Leftrightarrow a = a',\ b = b'$

Notations for sets which we shall frequently deal with.

1) $\mathbb{N}$ = Set of natural numbers= $\{1, 2, 3, \ldots\}$

2) $\mathbb{Z}$ = Set of integers= $\{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\}$

3) $\mathbb{Q}$ = Set of rational numbers = $\left\{\frac{m}{m} : m, n \in \mathbb{Z},\ n \neq 0\right\}$

4) $\mathbb{R}$ = Set of real numbers

5) $\mathbb{C}$ = Set of Complex numbers = $\{a + ib : a, b \in \mathbb{R}\}$

FUNCTIONS :

If A, B are non-empty sets, a function f from A to B (denoted by $f : A \to B$ *or* $A \xrightarrow{f} B$) is a subset of $A \times B$ satisfying the following.

For each $a \in A$, $\exists$ unique $b \in B$ such that $(a,b) \in f$. This is denoted by $f(a) = b$.The set A is called the domain of f and B is called the codomain of f. The function f is often specified by a rule,(such as $f(x) = x^2$). When a function f is not specified an elements of the domain, it is importaut to check that f is well-defined.

For $f : A \to B$, the set $f(A) = \{b \in B/b = f(a)$ for some $a \in A\}$ is called the range of f or image of A under f.

If $f : A \to B$ and $g : B \to C$ then the composite map $g \circ f : A \to C$ is denoted by $g \circ f(a) = g(f(a))$.

Note: If $f : A \to B,\ g : B \to C,\ h : C \to D$ then

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Let $f : A \to B$

1) f is said to be injective (or one-one)

   If $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ for each $a_1, a_2 \in A$

2) f is said to be Surjective (or onto) if for each $b \in B$, $\exists$ <u>an</u> $a \in A$ such that $f(a) = b$ i.e. $f(A) = B$.

3) f is said to be bijective (or a bijection if f is both injective and surjective.

4) $f : A \to B$ is said to invertible if there exists $g : B \to A$ such that $g \circ f = id_A$ (identity map on A) and $f \circ g = id_B$ (identity map on B).

We state some importaut results without proof.

Proposition : Let $f : A \to B$

1) f is bijective if and only if f is invertible.

2) If A and B are finite sets and $|A| = |B|$. Then f is bijective if and only

   if f is injective if and only if f is surjective.

   If $f : A \to B$ and $C \subset A$, then $f / C : C \to B (C \neq \phi)$ is defined by $f/A(c) = f(c)$ $\forall$ $c \in C$ and f is called the restriction of f.

   Let A be a non-empty set. A relation R on A is a subset of $A \times A$. We shall write aRb if $(a, b) \in R$.

DEFINITIONS:

Definition: Let R be a relation on a non-empty set A, Then, R is said to be

1) Reflexive if $aRa \forall a \in A$

2) Symmetric if $aRb \Rightarrow bRa \ \forall \ a, b \in A$

3) Transitive if $aRb,\ bRc \Rightarrow aRc \ \forall \ a, b, c \in A$

Definition: 1) A relation R on a non-empty set A is called an equivalence relation if R is reflexive, symmetric and transitive.

2) If R is an equivalence relation on A, then equivalence class of $a \in A$ is defined to be $[a] = \{x \in A : xRa\}$. 'a' is called a representative of the class $[a]$.

Note: The notion of equivalence relation is very importaut in Algebra.

Definition: Let A be a non-empty set. A portion of A is a collection $\{A_i\}_{i \in I}$ of non-empty subsets of A such that

(i) $\bigcup_{i \in I} A_i = A$ (ii) $A_i \cap A_j = \phi$ for $i, j \in I,\ i \neq j$

The notion of partition and equivalence relation on a set A are same.

We state the result without proof.

Proposition: Let A be a non-empty set.

1) Let R be an equivalence relation on A. then, the set of (distinct) equivalence classes of a form a partition of A.

(We note that $a \in A \Rightarrow a \in [a]$

$$\therefore\ A \subset \bigcup_{a \in A} \{a\} \bigcup_{a \in A} [a] \subset A \quad (\because [a] \subset A)$$

Also, if $[a] \neq [b]$, then $[a] \cap [b] \neq \phi$

2) If $\{A_i\}_{i \in I}$ is a partition of A, then the relation R on A defined by aRb if and only if $a, b \in A_i$ for some $i \in I$. It is an equivalence relation whose classes are precisely A_i's.

Some Important Properties of Integers :

We next mention certain important properties of integers.

Note: For $a \in \mathbb{Z}$, $|a| = a$ if $a \geq 0$
$= -a$ if $a < 0$

1) Well-ordering Property of a set of positive integers (or set of non-negative integers)

If A is non-empty subset of $\mathbb{N}\left(\text{or } \mathbb{Z}^+ = \mathbb{N} \cup \{0\}\right)$, $\exists$ an element $\ell \in A$ such that $\ell \leq a$ for each $a \in A$. (ℓ is called the least element of A)

2) If $a, b \in \mathbb{Z}$ and $a \neq 0$, we say that a divides b (denoted by $a(b)$) if there is $\mathbb{C} \in \mathbb{Z}$ such that $b = ac$.

In case, a does not divide b, we write $a \nmid b$

3) If $a, b \in \mathbb{Z}$, not both o, there is a unique positive integer d called the greatest common divisor (g.c.d.) of a and b satisfying.

i) d/a, c/b (d is common divisor of a and b)

ii) If c/a, c/b then c/d. (If C is a common divisor of a and b, c/d)

The g.c.d. of a and b will be denoted by (a, b). If $(a, b) = 1$, then we say that a and b are relatively prime (or coprime). (Note : If one of a, b is 0, $(a, b) = |a|$ or $|b|$)

4) If a, b are non-zero integers, there is a unique positive integer ℓ (called the least common multiple or l.c.m.) of a and b if

i) a/ℓ, b/ℓ

ii) If a/m, b/m then ℓ/m

For non-zero, a, b, $|a||b| = \ell d$

5) **The division algorithm**: If $a, b \in \mathbb{Z}$ and $b > 0$, then there exist unique integers q, r (q – quotient, r – remainder) such that $a = qb + r$, $o \leq r < b$.

6) For non-zero integers a, b, $(a, b) = 1$ if and only if $\exists$ $\lambda, \mu \in \mathbb{Z}$ such that $\lambda a + \mu b = 1$.

7) A positive integer $p > 1$ is called a prime if the only positive divisors of p are 1 and p ifself.

8) An importaut property of prime numbers : If p is a prime and plab where $a, b \in \mathbb{Z}$ then p/a or p/b.

(General property : If $a, b, c \in \mathbb{Z}$ and $a \neq 0$ then a/bc, $(a, b) = 1 \Rightarrow a/c$.

9) **The Fundamental Theorem of Arithmetic :**

If n is a positive integer, $n > 1$, then n can be factored uniquely into product of primes, i.e. $n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_k^{\alpha k}$ where $p_1 \ldots p_k$ are distinct primes, $p_1 < p_2 \ldots < p_k$ and α_i are positive integers. $1 \leq i \leq k$.

10) **The Euler ϕ function is defined as follows :**

For $n \in \mathbb{N}$, $\phi(n)$ = Number of positive integers $\leq n$ which are relatively prime to n. $\phi(1)=1,\ \phi(2)=1,\ \phi(3)=2,\ \phi(4)=2$

$\phi(p)=p-1,\ \phi(p^k)=p^k-p^{k-1}$ where p is prime

If $n=p_1^{a_1}\ldots p_k^{\alpha k}$, $\phi(n)=\left(p_1^{\alpha 1}-p_1^{\alpha 1-1}\right)\ldots\left(p_k^{\alpha k}-p_k^{\alpha k-1}\right)$

$$= n\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_k}\right)$$

(11) **First and Second Principal of Induction :**

Consider a statement $p(n)$ where $n \in \mathbb{N}$ (or $\mathbb{N} \circ \{0\}$)

If 1) $p(1)$ is true and

2) $p(k)$ is true $\Rightarrow$ $p(k+1)$ is true then $p(n)$ is true $\forall$ $n \in \mathbb{N}$

OR

2) $p(k)$ is true for $1 \leq k \leq n$

$\Rightarrow$ $p(n)$ is true then $p(n)$ is true $\forall$ $n \in \mathbb{N}$.

$\mathbb{Z}_n$ (*or* $\mathbb{Z}/n\mathbb{Z}$) $\mathbb{Z}$ THE INTEGERS MODULO *n* :

Let n be a fixed positive integer $(n>1)$

Define a relation $\sim$ in $\mathbb{Z}$ by,

$a \sim b$ if and only if $n/c-b$ for $a, b \in \mathbb{Z}$.

For each $a \in \mathbb{Z}$, $a \sim a$ $(\because n/a-a \Rightarrow n/0)$

$\therefore \sim$ is reflexive –(1)

For a, b ∈ Z, a ∼ b ⇒ n / a – b

$\Rightarrow a-b=kn, k\in z \Rightarrow -(a-b)=(-k)\,n \Rightarrow -b-a=(-k)\,n\,(-k\in z)$
$\Rightarrow b\sim a$

$\therefore \sim$ is symmetinic – (2)

For $a,b,c\in z, a\sim b, b\sim c \Rightarrow n/a-b, n/b-c$

$\Rightarrow a-b=k_1\,n, \quad b-c=k_2 n, \quad k_1,k_2\in\mathbb{Z}$

$\Rightarrow a-c=(a-b)+(b-c)=(k_2+k_2)\,n,\ k_1+k_2\in\mathbb{Z}$

$\Rightarrow a\sim c$

$\therefore \sim$ *is transitive* (3)

By (1), (2), (3), $\sim$ is an equivalence relation.

Let $\mathbb{Z}_n$ denote the set of all equivalence classes w.r.t. $\sim$

Let us denote [a] by $\bar{a}$ for $a \in \mathbb{Z}$.

Then, by division algonthm, $a = qn + r$, $q \in \mathbb{Z}, 0\le r\le n-1$.

$$\therefore a-r=qn$$

$$\therefore a\sim r. \qquad o\le r\le n-1.$$

$\therefore$ For each $a\in\mathbb{Z}, \bar{a}=\bar{r}, 0\le r\le n-1$

Moreover, if o $\le r<s\le n-1$.

Then o < s – r < n

$\therefore$ s – r $\neq$ k n for any k $\in$ $\mathbb{Z}$

$\therefore \bar{r}\neq\bar{s}.$

$\therefore$ The distinct equivalence classes are $\bar{0},\bar{1},..\overline{n-1}$

$\therefore$ The set of all equivalence classes is $\mathbb{Z}_n = \{\overline{0}, \overline{1}, .. \overline{n-1}\}$ and is called the set of integers modulo n.

Let U (n) = $\{\overline{a} : 1 \le a \le n-1 . (a, n) = 1\}$ where $\overline{a} = [a] w.r.t. \sim$

For $\overline{a}, \overline{b} \in u(n)$. $(a, n) = 1, (b, n) = 1$

$\therefore \exists \lambda_1, u_1, \lambda_2, u_2 \in \mathbb{Z}$ such that $\lambda_1 a + u_1 n = 1$, $\lambda_2 b + u_2 n = 1$

$\therefore (\lambda_1 a + u_1 n)(\lambda_2 b + u_2 n) = 1$

$\therefore \lambda_1 \lambda_2 ab + (u_1 \lambda_2 b + \lambda_1 u_2 a + u_1 u_2 n) n = 1$

$\therefore (ab, n) = 1 \therefore \overline{ab} \in u / n).$

U (n) is called the set of prime residue classes modulo n.

BINARY OPERATION.

Definition: A binary operation * on a non-empty set A is a function

* : A x A $\rightarrow$ A (i.e. For each a,b $\in$ A, $\exists$unique * (a, b) $\in$ A)

We shall do note * (a, b) by a * b.

Let * be a binary operation on a non-empty set A

Then

1) * is said to be associative if for each a, b, c $\in$ G, (a * b) * c = a * (b * c)
2) * is said to be commutative if for each a,b,$\in$ G a * b = b * a (we say a and b commute if a * b = b * a
3) A is said to have an identity element e w.r.t. * if a*e = a = e a for each a $\in$ A
4) Suppose A has an identity element e w.r.t. *. Then, a $\in$ A is said to have an inverse b in A if a * b = e = b * a.

Examples

(1) + (usual addition is associative and commutative binary operation in N, Z, Q, R, G. (N has no identity element).

(2) × (usual multiplication) is associative, commutative binary operation in N, Z, Q, R, G.

(3) – (usual subtraction) is not a binary operation in 1N. However is a binary operation in Z, Q, R, C. It is neither commutative nor associative.

(4) We define addition and multiplication in Z_n as follows.

$$\text{For } \overline{a}, \overline{b} \in \mathbb{Z}_n, \quad \left.\begin{array}{ll} \overline{a} + \overline{b} = \overline{a+b} \\ \overline{a} \,.\, \overline{b} \;\; = \overline{ab} \end{array}\right\} (*)$$

We show that these operation are well defined and do not depend on the choice of representatives a and b of $\overline{a}$ and $\overline{b}$ respectively.

Suppose $\overline{a_1} = \overline{a_2}$ *and* $\overline{b_1} = \overline{b_2}$ *in* $\mathbb{Z}_n$

$\therefore a_1 - a_2 = kn, b_1 - b_2 = mn$

$\therefore (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$ = nk + mn= (k + m) n.

$\therefore \overline{a_1} + \overline{b_1} = \overline{a_2} + \overline{b_2}$

Also $(a_1 - a_2) b_1 + a_2 (b_1 - b_2) = a_1 b_1 - a_2 b_2$

$\therefore knb_1 + a_2 mn = a_1 b_1 - a_2 b_2$

$\therefore n / a_1 b_1 - a_2 b_2$

$\therefore \overline{a_1}\,\overline{b_1} = \overline{a_2}\,\overline{b_2}$

Thus, * and . defined in (*) do not depend on choice of representative and are well defined binary operations.

We note that $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$ and $(\overline{a} + \overline{b}) \,.\, \overline{c} = \overline{a} \,.\, \overline{c} + \overline{b} . \overline{c}$ check using definition.

Also $\overline{0}$ is identity w.r.t. + and $\overline{1}$ is identity w.r.t.

1.2 Groups

Definition: A group is an ordered pair (G, *) where G is a set and * is a binary operation on G satisfying the following axioms.

(1) (a * b) * c = a * (b * c) for all a, b, c, $\in$ G (* is associative)

(2) There exists e$\in$G such that a * e = a = e * a for each a $\in$G. (G has an identity element)

(3) For each a$\in$G, there exists a^1 $\in$ G such that a * a^1 = e = a^1 * a (Each element in G has an inverse in G)

Note :

It can be shown that in a group G,

$(a_1 * a_2) * (a_3 * a_4) = a_1 * (a_2 * (a_3 * a_4)$ in general, for

$a_1\, a_2, . a_n \in G, the\ product\ a_1 * a_2 *.$ * an is uniquely defined

(Proof by induction) and does not depend where brackets are written.

Properties of groups

Let (G, *) be a group

(1) For a,b,c,$\in$G, a * b = a * c $\Rightarrow$ b = c (left cancellation law)

b * a = c * a $\Rightarrow$ b = c. (right cancellation law)

(2) Identity of G is unique

(3) Each a $\in$G has a unique inverse. We shall denote inverse of a by a^{-1}.

Definition: A group (G_1*) is said to be a 1) finite group, if G is a finite set, and we say order of G (o(G)) is [g], and 2) On infinite group if G is an infinite set

Definition: A group (G,*) is said to be Abelian if a * b = b * a * a,b $\in$G

Note : We shall denote group (G,*) by G and a * b by ab

(In case, the binary operation is addition, we write a + b)

Law of indices in a group.

(1) $a^{m+n} = a^m\ a^n$ *for* $m, n \in N.$

(2) $(a^m)^n = a^{mn} = (\alpha^n)^m$ for m, n $\in$ N.

We define a^o = e

And for negative integor m, $a^m = (a^{-1})^{-m}$

In additive notation, we write na instead of a^n and 0.a = 0

ma + na = (m + n) a, m(na) = (mn) a

Result: If G is an abelian group and a, b $\in$ G, then $(ab)^n = a^n b^n \forall n \in N$

Examples of Groups

1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (P, +), (O, +)$ are infinite abelian groups.

2) $(\mathbb{Q}^*, .), (\mathbb{R}^*, .), (G^*, .)$ Where F^* =F - {O}, F = Q, R, G are infinite abelian groups.

3) $(Z_n, +)$ is a group (we have shows associability $\bar{0}$ is identity element and for $\bar{r}, 0 \le r \le n-1, \overline{n-r}$ is the inverse of $\bar{r}$.

4) $U(n)$ is a group under multiplication modulo n. we know multiplication is associative.

We have already seen, that $\bar{a}, \bar{b} \in U(n) \Rightarrow \bar{a}.\bar{b} \in U(n)$.

$\therefore \bar{1}$ is identity of $U(n)$

We show a $\in U(n) \Leftrightarrow a$ has an inverse mod n,

$a \in U(n) \Rightarrow \lambda, \eta \in \mathbb{Z}$ such that $\lambda a + \eta n = 1$

$\Rightarrow \lambda a + \eta n = \bar{1} \Rightarrow \lambda a = 1 \Rightarrow \lambda.\bar{a} = 1. \therefore \bar{a}$ is invertible

(5) $M_{m\,x\,n}$ (R) is a group under addition of m x n matrices. It is an abelian

(6) $GL_n(\mathbb{Q}), GL_n(\mathbb{R})$ are groups under multiplication of n x n matrices. Where $GL_n(R)$ ={A/A is an n x n invertible}. GL_n (R) is non-abelian.

(7) Symmetric Group Sn

If S = I_n , ie. S = {1,2 …..n}

Then T(S) = $\{f / f : I_n \to I_n, f$ objective$\}$ is called symmetric group on n symbols and is denoted by S_n . An element of S_n is denoted by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & ..... & ..... & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & ..... & ..... & \sigma(n) \end{pmatrix}$$

(8) Dihedral group: (denoted by D_n) dihedral group is group of symmetries of regular n-gon (eg. Equilateral triangle, square, regular pentagon and so on.)

In general $D_n = \{I, \rho, \rho^2, \rho^3, \rho^4 .....\rho^{n-1}, \mu, \mu\rho, \mu\rho^2, \mu\rho^3 .....\mu\rho^{n-1}\}$ where ρ denotes the rotation by $\left(\frac{2\pi}{n}\right)^c$ and μ denotes reflection about the axis of symmetry.

Clearly $|D_n| = 2n$

The binary operation is composition and the relation is $\rho^n = I, \mu^2 = I, \rho^r \mu = \mu\rho^{n-r}$

Example: $D_3 = \{I, \rho, \rho^2, \mu, \mu\rho, \mu\rho^2\}$

Order of an element in a group: Let G be a group and a $\in$ G. Then order of `a' denoted by O(a) (or by $|a|$) is

(i) the least positive integer n (if it exists) such that a^n = e

(ii) infinite if no such integer exists.

Note : O(e) is always 1 in any group.

Proposition 1:. Let G be a group and a $\in$ G. Then $(xax^{-1})^n = xa^n x^{-1} \forall n \in \mathbb{Z}$

Proof :We prove inductively, $(xax^{-1})^n = xa^n x^{-1} \forall n \in N$

The result is true for n = 1.

If the result is true for k $\in$ N,

$$(xax^{-1})^{k+1} = (xax^{-1})^k (xax^{-1}) = xa^k x^{-1} xax^{-1} = xa^k eax^{-1} = xa^{k+1} x^{-1}$$

$\therefore$ The result is true for each n$\in$ N.

$(xax^{-1})^o = e = xa^0x^{-1}\ (a^0 = e)$

$For\ n < o\ (xax^{-1})^n = ((xax^{-1})^{-n})^{-1} = (xa^{-n}x^{-1})^{-1} = (x^{-1})^{-1}\ (a^{-n})^{-1}, x^{-1}$

$= xa^n\ x^{-1}\ by\ (5)\ z^2$

Thus, $(\text{xax}^{-1})^n = xa^nx^{-1} \nvdash n \in \mathbb{Z}$

(2) Let G be a group and a,b, $\in$ GThen,

$(i)\ O\ (xax^{-1}) = O(a)$,

$(ii)\ O\ (ab) = O\ (ba)$,

$(iii)\ \text{O}(a) = \text{O}(a^{-1})$

Proof :-

(i)Suppore O(a) = n, then a^n = e and $O(xax^{-1}) = k$

$\therefore (xax^{-1})^n = xa^nx^{-1} = xex^{-1} = e \quad \therefore k \backslash n$

Now, $(xax^{-1})^k = xa^kx^{-1} = e \quad \therefore a^k = x^{-1}x = e \quad \therefore n \backslash k$

Hence n = k

If O(a) is infinite and $O(\text{xax}^{-1}) = k$, then $(\text{xax}^{-1})^k = xa^kx^{-1} = e$

$\therefore a^k = xex^{-1} = e$. This is a contradictions that o(a) is finite

$\therefore$ If O(a) is infinite, $O(\text{xax}^{-1})$ is infinite

(ii) $ba = b(ab)b^{-1} \ \therefore O(ba) = o(ab)$

(iii) Let $O(a^{-1}) = k$.

$O(a) = n \Rightarrow a^n = e \Rightarrow a^{-n} = (a^n)^{-1} = e^{-1} = e$

$\Rightarrow (a^{-1}) \leq O(a)$

By similar argument $(a^{-1})^k = e \Rightarrow (a^k)^{-1} = e \Rightarrow a^k = O(a^{-1}) \leq \text{O}(\alpha^{-1})$

Thus, we must have $O(a) = O(a^{-1})$

1.3 Subgroups

Definition: Let G be a group. A subset H of G is called a subgroup of G if

(i) $a, b \in h \Rightarrow ab \in H$ (closure property)

(ii) $e \in H$ (identity)

(iii) $a \in H \Rightarrow a^{-1} \in H$

We note that from the given condition that

(i) the law of composition of G defines a binary operation in H. The induced binary operation in H is associative. From

(ii) it follows that H is a group. Thus, a subgroup of a group is a group under induced binary operation.

Notation H is a subgroup of G is denoted by H < G.

Note

1) Any group has two obvious subgroups {e} and G itself. {e is called the trivial group.

2) A subgroup of G other than G itself is called a proper subgroup of G.

Examples of Subgroups:

1) $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$ Where n is a fixed prositive integer.

2) $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det A = 1\}$ is a subgroup of $GL_n(R)$

Subgroup Test (Necessary and sufficient condition.)

Let G be a group and H be a non-empty sub set of G,then H < G if and only if $\forall$ a, b $\in$ H, $ab^{-1} \in H$ (or a - b $\in$ H in additive notation)

Example :

1) Let G be an abelian group and

$H = \{x \in G : x^2 = e\}$, Then, H < G.

$(e \in H \therefore H \neq \varnothing.$

$a, b \in H \Rightarrow a^2 = e, b^2 = e,$

$(ab^{-1})^2 = a(b^{-1})^2 = a^2(b^2)^{-1} = e)$

2) Centre of a group :- Let G be a group and Z(G) = {a∈G: ax = xa ∀ x ∈G}

Then, Z(G) < G (Z(G) is called the centre of the group G)

Proof: ex = xe ∀ x∈G, ⇒ e∈ Z(G) and Z(G) ≠ ∅

Let a,b ∈ Z(G) and x∈G.

$\therefore ax = xa, bx^{-1} = x^{-1}b\ (\because x^{-1} \in G)$

$\therefore (bx^{-1})^{-1} = (x^{-1}b)^{-1}\ i.e.\ (x^{-1})^{-1}b^{-1} = b^{-1}(x^{-1})^{-1}\ ie\ xb^{-1} = b^{-1}x$

$b^{-1}x = xb^{-1} \Rightarrow b^{-1} \in Z(G)$

$\therefore (ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$

$\therefore ab^{-1} \in Z(G) \therefore Z(G) < G.$

Note : Z(G) is always abelian.

3) Centralizer of an element: Let G be a group and a∈G. Then, C(a) = {X∈G: ax = xa} (C(a) is called the centralizer of a)

Proof : ae = ea ⇒ e∈C(a) and C(a) ≠ ∅.

Let x, y ∈ C(a), Then $ax = xa, ay = ya$

$\therefore a^{-1}ay = a^{-1}ya \quad ie\ y = a^{-1}ya,\ y^{-1} = (aya)^{-1} = a^{-1}ya$

$a(xy^{-1}) = (ax)y^{-1} = xay^{-1} = xaa^{-1}y^{-1}a = (xy^{-1})a$

$\therefore xy^{-1} \in C(a) \therefore C(a) < G.$

4) Intersection of subgroups:-

Let H, K < G, where G is a group. Then H ∩ K < G

Proof : e∈H, e∈k ⇒ e∈H ∩ K ⇒ H ∩ K ≠ ∅

x, y ∈H ∩ K ⇒ x, y ∈ H, x, y ∈ K ⇒ xy^{-1} ∈H, xy^{-1} ∈K

⇒ xy^{-1} ∈H ∩ K

∴H ∩ K < G.

More generally, if $\{H_i\}_{i \in \mathbb{N}}$ is a family of subgroups of a group G, then $\cap H_i$ is a subgroup of G.

Finite subgroup Test

Let H be a non-empty subset of a group G. Then, H < G iff H is closed under the binary operation of G.

Proof Clearly, H < G $\Rightarrow$ H is closed under the binary operation of G.

Conversely, suppose H $\neq \varnothing$ and a, b $\in$ H $\Rightarrow$ ab $\in$ H

Now, H $\neq \varnothing$

$\therefore$ $\exists$ a $\in$ H. We show inductively $a^n \in H \forall n \in N$.

$a \in H$ given.

$a^k \in H \Rightarrow a^k\, a \in H \Rightarrow a^{k+1} \in H$

$\therefore a^n \in H \forall n \in N$

$Let\ S = \{a^n, n \in N\}, Then, S \leq H$

But H is finite.

$\therefore$ S is finite.

$\therefore \exists\, i, j \in N, i \neq j\ (i > j)\ such\ that\ a^i = a^j$

$\therefore a^{i-j} = e, \quad i - j \in N$

$\therefore e \in S \subset H.$ ie $a^o \in H$ and $a^r \in H$ for $r \in N \cup \{0\}$

$Also, a^{i-j} \in H \Rightarrow a^{i-j-1}.a \in H\ (\because i - j - 1 \geq 0).$

$But\ a^{i-j-1}.a = a^{i-j-1+1} = a^{i-j} = e.$

$and\ a.a^{i-j-1} = e$

$\therefore a^{i-j-1} = a^{-1} \in H.$

$\therefore a \in H \Rightarrow a^{-1} \in H$

e $\in$ H, and H satisfies the closure property

$\therefore$ H < G.

Theorem: Let G be a group, and H, K < G, (H, K finite), then $|HK| = \dfrac{|H||K|}{|H \cap K|}$.

Proof: HK = {hk/h ∈ H, k ∈ K} Moreover, for h ∈ H, k ∈ K , t ∈ H ∩ K,

$t \in H$ *and* $t \in K$

$ht^{-1} \in$ H and tk ∈ K

$((ht^{-1})$ (tk) ∈ HK. And $((ht^{-1})(tk) = hk.$

Thus, for each h ∈ H, k ∈ K, hk is counted $|H \cap K|$ times.

$$\therefore |HK| = \frac{|H||K|}{|H \cap K|}$$

1.4 Cyclic Groups and Cyclic Subgroups

Proposition: let G be a group and a ∈ G. Then, H = {a^n : n ∈ $\mathbb{Z}$ }

Then H is a subgroup of G. Moreover, if K < G and a ∈ K, then H ⊂ K (H is the smallest subgroup of G containing a)

Proof : We Show H < G.

a^o = e ∈ H and H ≠ ∅

$Suppose\ x, y \in H, x = a^m, y = \alpha^n, m, n \in Z$
$Then, xy^{-1} = a^m.(a^n)^{-1} = a^m.a^{-n} = a^{m-n} \in H, m - n \in Z$
$\therefore H < G$

If a ∈ K, K < G, We show inductively a^n ∈ K for n ∈ N

a^1 ∈ K,

a^k ∈ K, k ∈ N ⇒ $a^k.a \in K \Rightarrow a^{k+1} \in K$

∴ By Principle of Induction, a^n ∈ K ∀ n ∈ N

a^o = e ∈ K (K < G)

if n < 0, n ∈ Z,

$a^n = (a^{-n})^{-1}, a^{-n} \in K \Rightarrow (a^{-n})^{-1} \in K \Rightarrow a^n \in K$
$\therefore a^n \in K \forall n \in \mathbb{Z}$
$\therefore H \subset K$

Cyclic Subgroup :

Definition: Let G be a group and a∈G. Then, the subgroup $\{a^n : n \in Z\}$ is called the cyclic subgroup of G generated by `a' and is denoted by <a>.

Cyclic group :

Definition: A group G is said to be a cyclic group if there exists a ∈G such that

G = $\{a^n : n \in Z\}$ and this is denoted by G = <a> `a' is called the generator of a.

Example :

1) ($\mathbb{Z}$, +) is a cyclic group. $\mathbb{Z}$ = {n: n∈ $\mathbb{Z}$ } = {n.1: n∈Z} = <1>

Properties of Cyclic groups

Proposition 1: A cyclic group is abelian.

Proof: If G=<a>, for x, y∈G, x=a^m , x=a^n

$\therefore xy = a^m.a^m = a^{m+n} = a^{n+m} = a^n\ a^m = yx$

Note : The converse of the above result is not true. Consider U(8) = $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ mod 8 under multiplication.

e.g. U(8) is abelian, but U(8) is not cyclic.

$\because \bar{1}^2 = \bar{3}^2 = \bar{5}^2 = \bar{7}^2 = \bar{1}$

$\therefore$ we can not write U(8) as $\{a^n : n \in Z\}$

Proposition 2: A subgroup of a cyclic group is cyclic

Proof : Let G be cyclic group, G = <a> and H < G.

If H = {e}, H = <e> and H is cyclic.

Suppose H≠ {e}

Then let x ∈H, x ≠ e.

H ⊂G $\therefore x = a^k$ for some k ∈ $\mathbb{Z}$, k ≠0.

$\therefore x^{-1} \in H$ *i.e.* $a^{-k} \in H . \therefore a^k \in H$ *and* $a^{-k} \in H$, *and one of* $k, -k \in \mathbb{N}$.

$\therefore S = \{n \in N : a^n \in H\}$ *is a non − empty sub set of* N (k *or* $-k \in S$)

By well ordering Principle, S has a least element (say) m.

We show H = <a ^{m} >.

Let y $\in$ H, y = a ^{l} , $\ell \in \mathbb{Z}$,

By division algorithm,

$$\therefore a^r = (a^{qm})^{-1} \cdot a^{\ell} = \alpha^{(-q)m} \cdot a^{\ell} = (a^m)^{-q} \cdot a^{\ell} \in H. (a^m \in H \Rightarrow (a^m)^{-q} \in H, a^{\ell} \in H)$$

But m is the least positive integer such that a ^{m} $\in$ H,

$$\therefore a^r \in H, 0 \leq r < m \Rightarrow r = 0 \Rightarrow \ell = qm \Rightarrow a^{\ell} = (a^m)^q \Rightarrow a^{\ell} \in < a^m > .$$

$$\therefore y \in \mathrm{H} \Rightarrow y \in < a^m >$$

$$\therefore H \subset < a^m >, but\ a^m \in H \Rightarrow < a^m > \subset H$$

$$\therefore H = < a^m >, H\ is\ cyclic$$

1.5 Order of an Element in A Group

Let G be a group and a $\in$ G

Then, there are two possibilities

(i) O (a) is finite

(ii) O (a) is infinite.

(i) O(a) is finite,

Some more results on finite cyclic groups.

Proposition : Let G be a finite cyclic group of order n, G = < a >, then G has a unique subgroup of order a for each divisor d of n.

Proof : Let G = <a>, o(G) = o(a) = n.

Let a be a positive divisor of n,

n = d . d'

Then $< a^{d'} >$ has order d.

For

$(a^{d'})^d = a^n = e$

$\therefore o(a^{d'}) \leq d.$

$If\ o(a^{d'}) = k\ , k \leq d - (1)$

$Then\ a^{d'k} = e$

$\therefore n \leq d'k \quad ie\ d'd \leq d'k$

$\therefore d \leq k - (2)$

From (1) and (2), k = d.

$\therefore o(a^{d'}) = o(< a^{d'} >) = d.$

Thus, we have a subgroup. H = $< ad' > = < \alpha^{n/d} >$ of order d.

We show H is a unique subgroup of G of order d.

Let K be any subgroup of G of order d.

K < G and G is cyclic

$\therefore$ K is cyclic.

Let K = $<a^{\ell}>$. o(k) = d. $\therefore o(a^{\ell}) = d.$

$\therefore$ d is the least positive integer such that $(a^{\ell})^d = e.$ (*)

By division algorithm, $\exists$ q, r $\in$ z such that

$\ell = q\,d' + r \quad 0 \leq r \leq d' - 1$

$\therefore \ell d = qd'd + rd \quad = qn + rd.$

$\therefore a^{\ell d} = a^{qd'd + rd} = a^{qn + rd} = a^{qn} \cdot a^{rd} = (a^n)^q\ a^{rd} = e^q\ a^{rd} = a^{rd}$

$\therefore a^{rd} = a^{\ell d} = e\ by\ (*)$

But $0 \leq rd < d'd = n$ and n is the least positive integer such that $a^n = e$

$\therefore rd = 0$ which means r = 0 (d is positive)

$\therefore \ell = qd'\ \therefore < a^{\ell} > = < a^{qd'} > < < a^{d'} > \therefore K \subset H$

$But\ |K| = |H| = d.$

$\therefore K = H.$

$\therefore$ G has unique subgroup of order d for each positive divisor d of n.

Proposition 4: Let G be a finite cyclic group of order n, G = <a> then a^m is a generator of G if and only if (m , n) = 1.

Proof : Suppose $G = < a^m >, o(G) = n = o(a)$

Then, a $\in$ G.

$\therefore a = (a^m)^r \ for\ some\ r \in \mathbb{Z}\ \therefore a = a^{mr}\ \therefore a^{1-mr} = e.$

$\therefore n / 1 - mr$

$\therefore 1 - mr = ns\ for\ s \in \mathbb{Z}$

$\therefore 1 = mr + ns, r, s \in \mathbb{Z}.$

$\therefore (m, n) = 1.$

Conversely, suppose (m, n) = 1.

$\therefore \exists\, r, s \in \mathbb{Z}\ such\ that\ rm + sn = 1.$

$\therefore a^{rm+sn} = a^1 = a$

$\therefore (a^m)^r\ (a^n)^s = a$

$\therefore (a^m)^r . e^s = a$

$\therefore (a^m)^r = a = < a >$

$\therefore G = \{a^m / m \in \mathbb{Z}\} = \{(a^{mr})^k / k \in \mathbb{Z}\} \subset < a^m >$

$\therefore < a > \subset < a^m > \subset < a >$

$\therefore < a^m > = < a > = G.$

In particular, G has $\phi(n)$ generators.

Note : A group G of order n is cyclic if and only if G has an element of order n.

Proposition 5: Let G be a group and a $\in$ G. If o(a) = n, then

$$o(a^r) = \frac{o(a)}{g.c.d(o(a), r)} = \frac{n}{g.c.d(n, r)}$$

Proof: $a^n = e.$

$\therefore a^{nr} = e\ i.e.\ (a^r)^n = e$

$\therefore o(a^r)\ is\ finite.\ Let\ o(a^r) = k$

$Let\ d = g.c.d(n, r),\ \ n = n_1 d,\ \ r = r_1 d,\ \ g.c.d(n_1, r_1) = 1$

$(a^r)^{n_1} = (a^{r_1 d})^{n_1} = a^{r_1 d n_1} = a^{r_1 n} = (a^n)^{r_1} = e^{r_1} = e$

$o(a^r) \mid n_1 \quad ie\ k \mid n_1 \qquad (1)$

On the other hand, $(a^r)^k = e \; and \; o(a) = n$

$\therefore n \mid rk \; ie \; n, d \mid r, d \; k$

$\therefore n_1 \mid r_1 k \;\; but \; (n_1, r_1) = 1$

$\therefore n_1 \mid k \qquad (2)$

$\therefore k = n_1$

$$i.e. \; o(a^r) = n_1 = \frac{n}{d} = \frac{n}{g.cd(n,r)}$$

Proposition 6: If G is a cyclic group of order n, and $d \mid n$ then no of elements of order d is $\phi(d)$.

Proof : By Proposition 3, G has exactly one (Cyclic) subgroup of order d, say < a >. Then, every element of order d generates <a> and by proposition 4, has $\phi(a)$ generators $\therefore$ No of elements of order d in G is $\phi(n)$

Note : In G is a cyclic group of order n then G is generated by $\phi(n)$.

Proposition 1: Let G be an infinite cyclic group generated by a. Then

1) Every non-trivial subgroup of G is infinite.

2) G has infinitely many distinct subgroups.

Proof : We first note that in an infinite cyclic group < a >, i, j, $\in \mathbb{Z} \Rightarrow a^i \neq a^j$

(1) Let H be a non-trivial subgroup of G. Then H is cyclic.

$\therefore H = < a^m > \; for \; some \; m \in \mathbb{Z}, m \neq 0$

$= \{(a^m)^n : n \in Z\}$ which is infinite ($\because (a^m)^i \neq (a^m)^j$ for distinct

$i, j, \in, \mathbb{Z}$)

$\therefore$ every non-trivial subgroup of G is infinite.

(2) Let $G_k = (a^k), k \in N$ .Then are infinitely many distinct subgroups of G.

For if $G_k = G_m \Rightarrow < a^k > = < a^m > \Rightarrow a^k \in < a^m > \Rightarrow k = \ell m, \ell \in \mathbb{Z}$

$a^m \in < a^k > \Rightarrow m = \ell k, \ell \in \mathbb{Z}$

$\therefore \ell^2 = 1, \ell \in \mathbb{N}$

$\therefore \ell = 1 = and \; k = m$

Proposition 2: Let G be an infinite cyclic group generated by `a' and a^{-1} are the only generators of G.

Proof:-Suppose $G = < a^m >, m \in \mathbb{Z},$

$G = < a > = < a^m >$

$\therefore a \in < a^m >$ and $a = (a^m)^k, k \in \mathbb{Z}.$

$\therefore a = a^{mk}$ and $1 = mk$ ($\because$ distinct powers of `a' are distinct)

$\therefore m \neq 1$

$\therefore$ Generators of G are a and a^{-1}

Note : $\mathbb{Z}$ is an infinite cyclic group and 1 and -1 are the only generation of $\mathbb{Z}$

1.6 Permutation Groups

We have defined symmetric group $S_n = \{f / f : I_n \to I_n$ s.t. f is bijective$\}$ where $I_n = \{1, \ldots, n\}$. $(S_n, \circ)$ is a group of order n! where ' $\circ$ ' is composition of maps.

Reason: $\sigma \in S_n$ is determined by specifying $\sigma(1), \ldots, \sigma(n)$. $\sigma(1)$ can be choosen in n ways. After choosing $\sigma(1)$, $\sigma(2)$ can be choose in n - 1 ways and finally $\sigma(n)$ can be choose in 1 way.

$\therefore$ No of elements in $S_n = n(n-1) = n!$.

We have already seen $\sigma \in S_n$ is denoted by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}$$

It is non-abelian if $n \leq 3$

$$\text{Consider } \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 2 & 3 & 1 & 4 & \ldots & n \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 2 & 1 & 3 & 4 & \ldots & n \end{pmatrix}$$

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 3 & 2 & 1 & 4 & \ldots & n \end{pmatrix}, \quad \sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 1 & 3 & 2 & 4 & \ldots & n \end{pmatrix}$$

Cycle: $\sigma \in S_n$ is said to be a *cycle* of length r if there exists $1 \leq i_1 < i_2 < \ldots < i_r \leq n$ such that $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3 \ldots \sigma(i_{r-1}) = i_r$, $\sigma(i_r) = i_1$ and $\sigma(k) = k$ for $k \neq \{i_1, \ldots, i_r\}$. It is denoted by $(i_1 \ldots i_r)$

Note : $(i_1\, i_2 \ldots\, i_r) = (i_2\, i_3 \ldots i_r\, i_1) = (i_r\, i_1 \ldots . i_{r-1})$

A cycle of length 2 is called a **transposition**. A cycle of length 1 is denoted by (*k*), which means *k* is fixed.

Cycles x and $y \in S_n$ are said to be disjoints if $x = (i_1\, i_2 \ldots i_r)$, $y = (j_1 \ldots j_s)$ and $\{i_1 \ldots . i_r\}\{j_1 \ldots . . j_s\} = \varnothing$.

We note that if *x* and *y* are disjoint cycles then *xy* = *yx*

Reason :- $x = (i_1 \ldots i_r)\ \ y = (j_1\ \ j_s), \{i_1 \ldots i_r\} \cap \{j_1 \ldots j_s\} = \varnothing$

$$\text{Then } xy(i_\ell) = xy(i_\ell) = i_{\ell+1} \quad \text{if } \ell = 1 \ldots r-1$$
$$= i_1 \quad \text{if } \ell = r$$

$$xy(j_k) = x(j_{k+1}) \quad \text{if } 1 = k \le -1$$
$$= j_{k-1}$$
$$= j_1 \quad \text{if } k = s$$

$$xy(k) = k \ \text{ if } k\{i_1 \quad i_r\} \cup \{j_1 \quad j_s\}$$
$$yx(i_2) = y\,(i_{\ell+1}) \ \ (\text{if } 1 \le \ell \le r-1) = i_{\ell+1}$$
$$yx(i_r) = y(i_1) = i_1$$
$$yx(j_k) = y\,(j_r) = j_{k+1} \text{ if } 1 \le k \le s-1$$
$$= j_1 \quad \text{if } k = s$$
$$yx(k) = k \ \text{ for } k \notin \{i_1 \ldots i_r\} \cup \{j_i \ldots j_s\}$$
$$\therefore xy = yx$$

Theorem:

1. Every $\sigma \in S_n$ can be written as a product of disjoint cycles (unique upto order)

2. Every $\sigma \in S_n$ can be written as product of transpositions.

Proof : proof of (1) easy .

(2) Let $\sigma = \sigma_1 \ldots . \ \sigma_2$ where σ is are disjoint cycles.

Let $\sigma_1 = (i_1\ \ldots .\ i_r)$

Then $\sigma_i = (i_1\, i_r)(i_1\, i_{r-1}) \ldots . (i_1\, i_3)\,(i_1\, i_2)$

$\therefore$ Each cycle is a product of transpositions

$\therefore$ σ is a product of transposition.

Order of a cycle of length r in group S_n :

$Let\ \sigma = (i_1 \ \ ...\ i_r)$

Then we note $\sigma(i_1) = i_2, \sigma^2\ (i_1) = i_3\ k, \sigma^{r-1}\ (i_1) = i_r,\ \ \sigma^r\ (i_1) = i_1$

$\therefore \sigma\ (i_1) \neq i_1\ for\ 1 \leq k \leq r$

Similarly for $i_2, ..\ i_r$

$\sigma^k (i_m) = i_{m+k}\ for\ 1 \leq r-k$

$\sigma^k (i_m) = i_{m+k-r}\ \ for\ r-k+1 \leq m \leq r$

$\therefore \sigma^k (i_m) + i_m\ \ for\ k\ k \leq r-1$

$and\ \sigma^r (i_m) = i_m$

$\therefore \sigma^r (i_m) = i_m\ for\ i \leq m \leq r$

$\therefore \sigma^r = I,$ and r is the least positive integer such that $\sigma^{\ r} = \mathrm{I}$

$\therefore \sigma(\sigma) = r.$

2. Order of $\sigma \in S_n$ where $\sigma_1, ...\sigma_k$ are disjoint cycles of length $r_1 ....r_k$.
$O(\sigma_1 .... \sigma_k) = lcm[O(\sigma_1) .... o(\sigma_k)] = lcm[r_1 ..... r_k]$

Definition : (Even and Odd Permutation) A permutation that can be expressed as a product of an even number of 2-cycles is called an **even permutation**. A permutation that can be expressed as a product of an odd number of 2-cycles is called an **odd permutation**.

Definition: (Sign of a permutation) The sign of a permutation α is said to be 1 if α is even and – 1 if α is odd.

$$sign(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is even} \\ -1 & \text{if } \alpha \text{ is odd} \end{cases}$$

Lemma: For $\sigma_1, \sigma_2 \in S_n$, $i)\ sign\ (\sigma_1\ \sigma_2) = sign\ (\sigma_1)\ sign\ (\sigma_2)$

$ii)\ sign\ (\sigma^{-1}) = sign\ (\sigma)$

Proof: (i) If σ_1 is a product of k_1 transpositions and σ_2 is a product of k_2 transpositions then $\sigma_1.\sigma_2$ is a product of $k_1 + k_2$ transpositions.

Thus, $sign(\sigma_1.\sigma_2) = (-1)^{k_1+k_2}$

$\Rightarrow sign(\sigma_1.\sigma_2) = (-1)^{k_1}.(-1)^{k_2}$

$\Rightarrow sign(\sigma_1.\sigma_2) = sign(\sigma_1).sign(\sigma_2)$

Let $A_n = (\sigma \in S_n : \text{Sign}(\sigma) = 1)$ (This group is called **Alternating group** i.e**.** it is the group of all even permutation of S_n)

We shall prove later that $A_n < G$ and $|A_n| = \frac{|S_n|}{2}$.

Generators and relations: A group generated by a finite set S, stashing a set of relations, which give all possible finite products of elements in the group can be described by the generators and relations.

e.g. D_n = {e, a, …a^{n-1}, b, ab,…. $a^{n-1}b$} = <a,b>, $a^n = e = b^2$, $ba = ab^{n-1}$

1.7 Lagrange Theorem

This is one of the most importaut theorems for finite groups

Definition: Cosets: Let G be a group and H be a subgroup of G for a∈G, we define, Ha = $\{\lambda a : \lambda \in H\}$ to be the right coset of H in G containing a and

aH = {aλ ∈H} to be the left coset of H in G containing a

For example, if G = S_3 = {I, (123), (132), (12), (13), (23)} and H = {I, (1,2)}

Then the right cosets of H in G are,

HI = H = {I, (12)}

H (123) = {(123), (12) (123)} = {(123), (23)}

H (132) = {(132), (12) (132)} = {(132), (13)}

We now prove Lagrange theorem

Theorem: If G is a finite group and H is a subgroup of G then O (H) \ O(G).

Proof : We define a relation $\sim$ in G as follows : For a,b,$\in$ G, a $\sim$ b if and only if $ab^{-1} \in H.$ We show $\sim$ is an equivalence relation in G we note a $\sim$ a for each a $\in$ G since $aa^{-1} = e \in H. \therefore \sim$ *is is reflexive*

For $a, b \in G, a \sim b \Rightarrow ab^{-1} \in H$

$\Rightarrow (ab^{-1})^{-1} \in H \Rightarrow ba^{-1} \in H \Rightarrow b \sim a$

$\therefore \sim$ *is symmetric.*

$For\ a,b,c,\in,G, a \sim b, b \sim c \Rightarrow ab^{-1} \in H, bc^{-1} \in H$

$\Rightarrow ab^{-1}bc^{-1} \in H \Rightarrow ac^{-1} \in H \Rightarrow c \sim a$.

$\therefore \sim$ *is transitive*

Thus $\sim$ is an equivalence relation an G.

$a \in G, [a] = \{x \in G / a \sim x\} = \{x \in G / x \sim a\}$ ($\because \sim$ *is symmetric*)

$= \{x \in G / xa^{-1} = \lambda, \lambda \in H\} = \{x \in G / x = \lambda \in H\} = Ha$

2) Thus, we have the following,

For a $\in$ G, a $\in$ [a] = Ha

$\bigcup_{a \in G} a = \subseteq G$.

Moreover, as two equivalence classes [a], [b] are either disjoint or equal,

Ha $\cap$ Hb = ϕ or Ha = Hb for a, b $\in$ G.

$\therefore G = \bigcup_{a \in G} Ha$

3) Let a $\in$ G

We now define a map $\varnothing : H \to Ha\ s.t.\ \varnothing(\lambda) = \lambda a.$

The map is well-defined and for

$\lambda_1, \lambda_2 \in H, \varnothing(\lambda_1) = \varnothing(\lambda_2) \Rightarrow \lambda_1 a = \lambda_2 a \Rightarrow \lambda_1 = \lambda_2 \therefore$ The map is 1-1

The map is clearly onto.

$\therefore$ the map is bijective.

$\therefore |H| = |Ha|.$

$\therefore |G| = |Ha_1| + |Ha_2| + ... + |Ha^k|$, *where* Ha_1,

Ha_k *are distinct right cosets of* H *in* G

$\therefore |G| = k\,|H|$

ie $o(G) = k\,o(H)$ *and* $o(H) \backslash o(G)$

Definition: The number of right cosets of H in G is called index of H in G and is denoted by (G : H) or $|G:H|$.

$Note: For\ a, b \in G, Ha = Hb \Leftrightarrow ab^{-1} \in H$

We also note that the number of left gets of H in G is same as the number of right cosets of H in G.

Left coset of H contain `a' = aH = {ah : h$\in$H}.Further, aH = bH iff $a^{-1} b \in H.$

Proof:

$aH = bH \Rightarrow b = be \in b\,H$, *and hence* $b \in a\,H \Rightarrow b = a\lambda$ *for some* $\lambda \in$ H

$\Rightarrow a^{-1} b = \lambda, \lambda \in H.$

Conversely $a^{-1}b = \lambda, \lambda \in H \Rightarrow b = ah, b \in a\,H$

$\therefore x \in b\,H \Rightarrow x = b\lambda, \lambda \in H \Rightarrow x = a\lambda, \lambda \in aH$

$\therefore bH \subseteq a\,H$

$x \in a\,H \ \Rightarrow x = a\lambda', \lambda' \in H \Rightarrow x = b\lambda^{-1}\lambda' \in b\,H$

$\therefore aH \subseteq bH$

$\therefore aH = bH$ *iff* $a^{-1} b \in H.$

There is 1-1 correspondences between the set of right cosets of H in G and the set of left cosets of H in G

$Ha \rightarrow a^{-1} H.\ Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow (a^{-1})^{-1} b^{-1} \in H \Leftrightarrow \alpha^{-1} H = b^{-1}$ H

Consequences of Lagrange's Theorem:

(1) In a finite group G, order of each a $\in$ G divides the order of G i.e.

O(a) / O(G) and a $^{o(g)}$ = e

Proof: For a $\in$ G, <a> < G, and o(a) = o(<a>)

G is finite. $\therefore$ By Lagrange's Theorem o(a) $|o(G)$

$\therefore a^{o(a)} = e.$

(2) A Group of prime order is cyclic.

Proof: Let O(G) = p, where p is a prime

$\therefore G \text{ has an element } a \neq e. < a > < G.$
$o(< a >) | o(G),$
$\therefore o(< a >) = 1 \text{ or } p \text{ but } o(< a >) \neq 1 (\because a \neq e)$
$\therefore o(< a >) = p = o(G)$
$\therefore < a > = G.$

(3) Fermat's little Theorem.

For a $\in \mathbb{Z}$ and every prime p, a ^{p} = a (mod p)

Proof :- Consider the group U(p) of prime residue classes modulo p under multiplication.

$Let\ a \in \mathbb{Z}, and\ a \equiv r \bmod p$
$If\ r = 0, then,\ p \backslash a \text{ and } p \backslash a^p$
$\therefore a^p \equiv a \equiv o \bmod p$
$If\ r \neq 0. then\ \bar{a} = \bar{r} \in U(p), o(U(p)) = p - 1$
$\therefore \bar{r}^{p-1} \equiv 1 \bmod p .... by\ (1)$
$But\ a^{p-1} \equiv r^{p-1} \equiv 1 \bmod p$
$\therefore a^{p-1} \equiv 1 \bmod p$
$\therefore a^p \equiv a \bmod p.$

(4) Euler's Theorem : Let a$\in$z and n $\in$ N, (a, n) = 1,Then, a $^{\varnothing(n)} \equiv 1 \bmod e\, n.$

Proof :- $a \in U(n), O(U(n)) = \varnothing(n)$

$\therefore$ *By Lagrange's Theorem* $a^{\varnothing(n)} \equiv 1 \bmod n.$

Remark :- We shall show later that the converse of Lagrange's Theorem is not true for groups in general. However, we have already seen that it is true in case of cyclic groups.

1.8 Summary

1) **A group** is an ordered pair (G, *) where G is a set and * is a binary operation on G satisfying the following axioms.

(1) (a * b) * c = a * (b * c) for all a, b, c, $\in$ G (* is associative)

(2) There exists e $\in$ G such that a * e = a = e * a for each a $\in$ G. (G has an identity element)

(3) For each a $\in$ G, there exists $a^1 \in$ G such that a * a^1 = e = a^1 * a (Each element in G has an inverse in G)

2) **Order of an element in a group**: Let G be a group and a $\in$ G. Then order of `a' denoted by O(a) (or by $|a|$) is

(i) the least postive integer n (if it exists) such that a^n = e

(ii) infinite if no such integer exists.

3) **Subgroup:** Let G be a group. A subset H of G is called a subgroup of G if

(i) a, b $\in$ h $\Rightarrow$ ab $\in$ H (closure property) (ii) e $\in$ H (identity)

(iii) a $\in$ H $\Rightarrow$ $a^{-1} \in$ H

4) **Cyclic group** : A group G is said to be a cyclic group if there exists a $\in$ G such that

G = $\{a^n : n \in Z\}$ and this is denoted by G = <a> `a' is called the generator of a.

5) Let G be a finite cyclic group of order n, G = < a >, then G has a unique subgroup of order a for each divisor d of n.

6) Let G be a group and a $\in$ G. If o(a) = n, then

$$o(a^r) = \frac{o(a)}{g.c.d(o(a), r)} = \frac{n}{g.c.d(n, r)}$$

7) **Lagrange theorem:** If G is a finite group and H is a subgroup of G then O (H) \ O(G).

1.9 Unit and Exercises

1) If R is an equivalence relation on a non-empty set A, then show that –

a) $a \in [\, a \,]$ (by reflexivity)

b) $b \in [\, a \,] \Rightarrow [\, a \,] = [\, b \,]$

c) For $a, b \in A$, either $[\, a \,] \cap [\, b \,] = \phi$ *or* $[\, a \,] = [\, b \,]$

Thus, an equivalence relation divides the set into disjoint equivalence classes.

2) Determine if $\mathrm{f} : \mathbb{Q} \to \mathbb{Z}$ defined by $\mathrm{f}\left(\frac{\mathrm{m}}{\mathrm{n}}\right) = \mathrm{m}$ is well defined.

$\left(\text{Is } \mathrm{f}\left(\frac{1}{1}\right) = \mathrm{f}\left(\frac{2}{2}\right)?\right)$

Determine if $\mathrm{f} : \mathbb{Q} \to \mathbb{Z}$ defined by $\mathrm{f}\left(\frac{\mathrm{m}}{\mathrm{n}}\right) = \mathrm{m}$ is well defined.

$\left(\text{Is } \mathrm{f}\left(\frac{1}{1}\right) = \mathrm{f}\left(\frac{2}{2}\right)?\right)$

3) Determine whether the following functions are injective, surjective, and bijective.

i) $\mathrm{f} : \mathbb{Z} \to \mathbb{Z}$ defined by $\mathrm{f}(\mathrm{x}) = 3\mathrm{x} + 2$

ii) $\mathrm{f} : \mathbb{R}^+ \to \mathbb{R}^+$ defined by $\mathrm{f}(\mathrm{x}) = \frac{1}{\mathrm{x}}$

iii) $\mathrm{f} : \mathbb{C} \to \mathbb{R}$ defined by $\mathrm{f}(\mathrm{z}) = |\, \mathrm{z} \,|$

iv) $\mathrm{f} : \mathbb{R} \to \mathbb{R}$ defined by $\mathrm{f}(\mathrm{x}) = \mathrm{x}^2$

4) Let $\mathrm{f} : \mathrm{A} \to \mathrm{B}$ be a surjective map. Show that the relation R defined by aRb if and only if $\mathrm{f}(\mathrm{a}) = \mathrm{f}(\mathrm{b})$ is an equivalence relation. Find the equivalence classes.

5) Consider a relation R on $\mathbb{Z}$ defined by aRb if and only if $\mathrm{ab} \geq 0$. Is R an equivalence relation?

6) Find $\phi(200)$, $\phi(350)$

7) List elements of U(24).

8) Which elements in $\mathbb{Z}$ have an inverse w.r.t. multiplication.

9) Find inverse of $\bar{5}$ in $\overline{\mathbb{Z}_6}$

10) Is multiplication a binary operation in the set of odd integer?

11) List elements in $\mathbb{Z}_{10}$ which are invertible (we will prove a general result later)

12) Show that `0' is a binary operation in z where aob = a+b+5, for a, b $\in \mathbb{Z}$.
Show `o' is commutative and associative.

13) Find identity of $\mathbb{Z}_{10}$ and inverse of 2.

(14) Find generators of Z_6, Z_{20} and subgroups of Z_{10}

Ans:

(i) $<\bar{r}>=Z_6$ *iff* $(6,\bar{r})=1,\ 1\le r\le 5\,(Z_6=<i>)$

$\therefore$ *generaton of* Z_6 *are* $1,5,6=\phi(2)\,\phi(3)=1\times 2=2$

(ii) $<\bar{r}>=Z_{20}$ *iff* $(20,r)=1, 1\le r\le 20\Rightarrow \bar{r}=$

$\bar{1},\bar{3},\bar{7},\bar{9},\overline{11},\overline{13},\overline{17},\overline{19}$

$(\phi(20)=\phi(2^2)\,\phi(5)=(2^2-2)\bullet 4=8)$

(iii) Subgroups of Z_{10}, order 1, 2, 5, 10

$<\bar{0}>=\{\bar{0}\},\ <\bar{5}>=\{\bar{0},\bar{5}\},\ <\bar{2}>=\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\},\ <\bar{1}>=Z_{10}$

(15) List the elements of subgroup <20> in Z_{30}.

(16) List the elements of subgroups <3>, <7> in Z_{20}.

(Ans :- $<\bar{3}>=\{\bar{1}\,\bar{3}\,\bar{9}\,\bar{7}\}$
$<\bar{7}>=\{\bar{1}\,\bar{7}\,\overline{93}\}$

(17) Let a be a group and a$\in$G. If o(a) = 15 state orders of a^3, a^5, α^4.

(18) Let G be a group and a$\in$G. If o(a) = 24. Find a generator for $<a^{21}>\cap<a^{10}>\ Ans:-a^6$

(19) List all the elements of order 8 in $Z_{80,80,000.}$

(20) Let G be a cyclic group of order 15, G=<a> Find all subgroups of G and list generators of each of the subgroups of G.

(21) Find a cyclic group of order 4 in U(40).

(22) Show that $U_n = \{z \in G : z^n = 1\}$ under multiplication is a cyclic group of under n.

(23) Let G be a group and a,b $\in$ G. If ab = ba, o(a) = m o(b) = n. where (m,n) = 1, show that o(ab) = mn.

Hint :- Show $(ab)^{mn} = (a^m)^n\ (b^n)^m = e \therefore o(ab) \mid mn$

$(ab)^{mn} = (a^m)^n\ (b^n)^m = e \therefore o(ab) \mid mn$

$if\ o(ab) = k, (ab)^k = e, a^k = b^{-k}, (a^k)^m = e = b^{-km}, n \setminus km \Rightarrow n \mid k$

$Similarly\ m \mid k \therefore mn \mid k\ and\ o(ab) = mn.$

(24) A group G of even order has odd member of elements of order 2. In particular if has at least one element of order 2.

Hint : If there are k element of order 2, $|G|$ = 1 + k + $\in$ a(x) > 2 = 1 + k + 2m

2

ISOMORPHISM OF GROUPS

Unit Structure

2.0 Objectives

After going through this unit you shall come to know about

- Relation between the groups and the existence of isomorphisms between groups
- Special kind of subgroups called normal subgroups and its impotance in the construction of factor groups
- Classification of groups upto order 7 using various results of isomorphism theorem

2.1 Homomorphism and Isomorphism

Definition: 1] Let G, $\overline{G}$ be groups. A map f : G $\rightarrow \overline{G}$ is called a homomorphism of group G to group G if f(ab) = f(a) f(b) for each a, b $\in$ G (i.e. f preserves group operation)

Definition: 2] Let G, G be groups. A map f : G $\rightarrow \overline{G}$ is called an is isomorphism of group G to group $\overline{G}$ if i) f (ab) = f(a) f(b) for for each a,b $\in$ G (ie f is a group homomorphism) and ii) f is bijective.

This is denoted by G $\approx$ G

Properties of group homomorphisms and isomorphisms.

Let G, $\overline{G}$ be groups and f : G $\rightarrow$ $\overline{G}$ be a group homomorphism and a $\in$ G

Then

(i) f(e) = e' where e, e' are identity elements of G, $\overline{G}$ respectively.

(ii) f (a^{-1}) = (f (a))$^{-1}$

(iii) f(a^k) = (f(a))^k for each k$\in$ $\mathbb{Z}$

Proof : (i) e' = f(e) = f(e.e) = f(e) . f(e)

$\therefore$ By right cancellation law, f(e) = e'

(ii) f (aa^{-1}) = f(e) = e'

$\therefore f(a)\, f(a^{-1}) = e^1 = f(a)(f(a))^{-1}$

$\therefore f(a^{-1}) = (f(a))^{-1}$

(iii) We prove inductively, f (a^n) = (f(a))^n $\forall n \in N$

The result is true for n = 1

Suppose the result is true for k, k$\in$N

$f(a^k) = (f(a))^k$

Then, $f(a^{k+1}) = f(a^k a) = f(a^k)\, f(a) = (f(a))^k\, f(a)^1 = (f(a))^{k+1}$

$Inductively, f(a^n) = (f(a))^n \; \forall\, n \in N$

$f(a^0) = f(e) = e^1 = (f(a))^0, the\ result\ is\ true\ for\ 0,$

$for\ n \in \mathbb{Z}, \{n < 0, n = -m, m \in N\},$

$f(a^n) = f(a^{-m}) = f(a^m)^{-1}) = (f(a^m))^{-1}\ by\ (ii) = ((f(a))^m)^{-1}$

$= (f(a))^{-m} = (f(a))^n$

Thus, the result is true for each n $\in$ $\mathbb{Z}$.

Properties : Let G, $\overline{G}$ be groups and f : G $\to \overline{G}$ be an onto group homomorphism

(i) If G is abelian, so is $\overline{G}$

(ii) If G is cyclic, so is $\overline{G}$.

(iii) O(f(a)) $|o(a)$. If f is an is isomorphism, then o(f(a)) = o(a).

Proof : (i) Let $a', b' \in \overline{G}$, As f is onto, for a,b, $\in$ G such that $f(a) = a', f(b) = b'$

Then, $a'\,b' = f(a)\,f(b) = f(ab) = f(ba) = f(b)\,f(a) = b'a'$

Thus, $\overline{G}$ is abelian.

(ii) Let G = < a > = $\{a^n : n \in \mathbb{Z}\}$

$\overline{G} = f(G) = f(\{a^n : n \in \mathbb{Z}\}) = \{f(a^n) : n \in \mathbb{Z}\} = \{(f(a)^n : n \in \mathbb{Z}\} = < f(a) >$
Thus $\overline{G}$ *is cyclic*.

(iii) Suppose o(a) = n, then $a^n = e$

$\therefore (f(a))^n = f(a^n) = e'$
$\therefore\ (f(a))|o(a)$

If f : G $\to \overline{G}$ is an isomorphism, then

$o(f(a)) = m \Rightarrow (f(a))^m = e' \Rightarrow f(a^m) = (f(a))^m = e' = f(e)$

$\Rightarrow a^m = e\ (\because f\ is\ one-one) \Rightarrow n / m$

$By\ (iii) \quad m / n \qquad \therefore m = n.$

Result : If G, $\overline{G}$, are groups, and f : G $\to \overline{G}$ is an isomorphism, then $f^{-1} : \overline{G} \to G$ is an isomorphism.

Examples of homomorphism and isomorphism.

(1) For any group G, I : G $\to$ G (I = identity) and the trivial may f : G $\to$G defined by f(x) = e are group homomorphism.

(2) The map $\varnothing : R \to R$ defined by $\varnothing(x) = x^3$ is a group homomorphism.

(3) Consider the map f : $\mathbb{Z} \to \mathbb{Z}_n$ defined by f(m) = $\overline{m}$ is a group homomorphism.

Theorem 1: Any finite cyclic group of order n is isomorphic to Z_n, the group of integer residue classes modulo under addition.

Proof : Let G be a cyclic group of order n generated by `a'.

Then, G = {e, a, … a^{n-1} } and for m$\in\mathbb{Z}$, $a^m = a^r$

$0 \le r \le n-1$

$\varnothing : G \to \in \mathbb{Z}_n, a^m = a^r{}_n$ *by* *where* $m \equiv r \bmod n$

we define $\varnothing(a^r) = \bar{r}$ *for* $o \le r \le n-1\,(\bar{r} = r \bmod n)$

$\varnothing$ *is well − defined*, *for* $a^r = a^s, \mathrm{o} \le r,s \le n-1$

$\Rightarrow a^{r-s} = e, o \le |r-s| < n.$

$\Rightarrow n \setminus r-s$ *and* $r-s=0 \Rightarrow r=s \Rightarrow \bar{r}=\bar{s}$

$\varnothing$ is a group homomorphism, since

and $r+s \equiv t \bmod n$

$\Rightarrow \bar{t} \equiv \overline{r+s} = \bar{r} + \bar{s} = \varnothing(a^r) + \varnothing(a^s)$

$\varnothing$ *is clearly onto.*

$\therefore \mathbb{Z}_n = \{\bar{o}, \bar{1}, ..., \overline{n-1}\}$ *and for* $\bar{r} \in \mathbb{Z}_n, \bar{r} = \varnothing(a^r).$

$\therefore \varnothing$ *is a group isomorphism.*

$\varnothing(a^r) = \varnothing(a^s), 0 \le r, s \le n-1$

$\Rightarrow \bar{r} = \bar{s}, \Rightarrow r = s\ (\because \mathrm{o} \le |r-s| \le n-1 < n)$

$\Rightarrow a^r = a^s$

$\therefore \varnothing$ *is one one*

Corollary: Any two finite cyclic groups of same order are isomorphic

(Consider $< a > \to < b >$ *by* $a^r \to b^r$ $o \le r \le n-1$)

Theorem 2: An infinite cyclic group is isomorphic to the group of integers under addition.

Proof : Let G be an infinite cyclic group generated by `a', $G = \{a^n \mid n \in z\}$

Consider the map $\varnothing : G \to \mathbb{Z}$ *defined by* $\varnothing(a^r) = r$ *for* $r \in \mathbb{Z}$.

For $a^r, a^s \in G \ (r, s \in \mathbb{Z})$

$\varnothing(a^r, a^s) = \varnothing(a^{r+s}) = r + s = \varnothing(a^r) + \varnothing(a^s)$

$\therefore \varnothing$ *is a group homomorphism*

$\varnothing(a^r) = \varnothing(a^s) \Rightarrow r = s \Rightarrow a^r = a^s$

$\therefore \varnothing$ *is one* $-$ *one*

For $r \in \mathbb{Z}, \exists\, a^r \in G$ *such that* $\varnothing(a^r) = r \ \ \therefore \varnothing$ *is onto.*

Thus, $\varnothing$ is a group isomorphism

Corollary: Any two infinite cyclic groups are isomorphic

(If < a >, < b > are infinite cyclic groups consider $a^r \to b^r, r \in \mathbb{Z}$).

2.2 Cayley's Theorem

Cayley's Theorem: Every group is isomorphic to a group of permutations

Proof : Let G be a group

For a $\in G$, we define f_a : G $\longrightarrow$ G by f_a (x) = ax (f_a is multiplication by a on left)

We show f_a is bijective map, ie f_a is a permutations on G.

f_a (x) = f_a (y) for x, y$\in G \Rightarrow ax = ay \Rightarrow x = y$

$\therefore$ f_a is one one

For y$\in$ G, $\exists\, x = a^{-1}y \in G$ such that

$f_a(x) = ax = a^{-1}y = y$

$\therefore f_a$ *is onto.*

let $\overline{G} = \{f_a : a \in G\}$

Then $\overline{G}$ is a group under composition of maps for a, b for $a,b \in G, f_a \, o \, f_b(x) = f_a\left(f_b(x)\right) = f_a\left(bx\right) = a(bx) = (ab)\, x = f_{ab}(x)$

$\therefore f_a \, o \, f_b \in \overline{G}, f_a \, o \, f_b = f_{ab}$

f_e is the identity element of $\overline{G}$.

$\because f_e(x) = ex = x \; \forall \; x \in G = f_{ea}(x) = ax$

$f_a \, o \, f_e(x) = f_{ae}(x) = f_a(x) = f_e \, o \, f_a(x)$

f_a^{-1} is the inverse of f_a

$\because f_a^{-1} \, o \, f_a = f_a^{-1}{}_a = f_e = f_{a\,a^{-1}} = f_a \, o \, f_a^{-1}$

$\overline{G}$ is a group and $\varnothing : G \to \overline{G}$ defined by $\varnothing(a) = f_a$ is an group isomorphism.

$\because$ For $a,b \in G, \varnothing(ab) = f_{ab} = f_a \, o \, f_b = \varnothing(a) \, o \, \varnothing(b)$

$\varnothing(a) = \varnothing(b) \Rightarrow f_a = f_b \Rightarrow f_a(e) = f_b(e) \Rightarrow ae = be \Rightarrow a = b$

$\varnothing$ is clearly onto.

$\therefore$ G is isomorphic to $\overline{G}, a$ group of permutations.

Note : The group $\overline{G}$ consummated above is called the left regular representation of G

2.3 Automorphisms and Inner Automorphisms

Definition: An isomorphism of a group G onto itself is called an automorphism of G

Examples

1) Identity map is an automorphism of any group to itself

2) f : G $\longrightarrow$G defined by f(a + ib) = a – ib is automorphism of the group (G, +).

Let Aut G = {f : f : G $\longrightarrow$G, f automorphism of G }

Definition : Let G be a group and a$\in G$. The map $i_a : G \to G$ defined by $i_a(x) = axa^{-1}$ *for* $x \in G$ is called the inner automorphism of G induced by a.

Let Inn (G) $= \{i_a : G \to G / i_a(x) = axa^{-1}, a \in G\}$

Theorem: Aut G is a group and Inn G < Aut G

Proof : If f, g $\in$ aut G, f $\circ$ g $\in$ Aut G, $\circ$ is associative

i $\in$ Aut G, For f $\in$ Aut G. then map $f^{-1} \in$ Aut G,

$\therefore$ Aut G is a group

$i_e = i_d \in Inn\ G.$
$For\ i_a, i_b \in Inn\ G, where\ a, b \in G$
$i_a\ {i_b}^{-1} = i_a\ {i_b}^{-1} = {i_{ab}}^{-1} \in Inn\ G.$
$\therefore Inn\ G < Ant\ G$

2.4 External Direct Product of Groups

Definition: Let, $G_1, G_2, ..., G_n$ be finite collection of groups. The external direct product of $G_1, ... G_n$ denoted by $G_1 \oplus G_2 \oplus ... \oplus G_n$ is defined by

$G_1 \oplus G_2 \oplus \quad \oplus G_n = \{(g_1, ... g_n) / g_i \in G_i \quad 1 \le i \le n\}$ where

$(g_1, g_2, ..., g_n) \bullet (g_1', g_2', ..., g_n') = (g_1\, g', ..., g_n g_n')$

It can be easily verified that $G_1 \oplus G_2 \oplus .... \oplus G_n$ *is a group.*

$For\ (g_1, ... g_n), (g_1', g_2', ..., g_n')\ , (g_1''.. g_n'') \in G_1 \oplus ..... \oplus G_n.$
$((g_1, ..., g_n)(g_1 ..... g_n))(g_1'', ..., g_n'') = (g_1 g_1', ..., g_n\, g_n')(g_1, ".. .., g_n'')$
$= ((g_1\, g_1' g_1'', ... (g_n\, g_n'')\, g_n''$

$= (g_1(g_1' g_1''), ..., g_n(g_n' g_n''))\ (By\ associativity\ in\ G_1, .. G_n)$
$= (g_1, ..., g_n)((g_1', ... ,\ g_n')(g_1'' ..... g_n'')).$

Thus, associatively holds in $G_1 \oplus ..... \oplus G_n$

Let $e_1,.....,e_n$ *be identity elements groups of* $G_1 .....G_n$ *respectively*

$e_1,.....,e_n$ *be identity elements groups of* $G_1 .....G_n$ *respectively*

$Then, (g_1,....., g_n)\cdot(e_1, \quad e_n)=(g_1e_1,....., g_ne_n)=(g_1,....., g_n)$

$=(e_1\ g_1,.....,e_ng_n)=(e_1,.....,e_n)\,(g_1,....., g_n)$

$\therefore (e_1,...e_n)$ is identity element of $G_1\oplus \quad \oplus G_n$.

Let

$g_i\in G_i$ *for* $1\le i\le n$ *and* G_i *is a group for* $1\le i\le n$.

Let g_i^{-1} *be the inverse of* g_i *in* G_i *for* $1\le i\le n$.

$Then, (g_1,..,g_n)\,(g^{-1},....,g_n{}^{-1})=(g_1g_1{}^{-1},....., g_n\ g_n{}^{-1})$

$=(e_1,...., e_n)=(g_1{}^{-1},....., g_n{}^{-1}g_n)=(g_1{}^{-1},....., g_n{}^{-1})\,(g_1, \quad g_n)$.

Thus, $(g_1,.....,g_n)$ *has an inverse* $(g_1{}^{-1},....., g_n{}^{-1})$

in $G_1\oplus.....\oplus G_n.\therefore G_1\oplus.....\oplus G_n$ *is a group*

This is called the external direct product of $G_1\oplus.....\oplus G_n$

Examples :

1) $Z_2\oplus Z_3=\{(\bar{0},\bar{0}),(\bar{1},\bar{0}),(\bar{0},\bar{1}),(\bar{0},\bar{2}),(\bar{1},\bar{1}),(\bar{1},\bar{2})\}$

This is an abelian group.

Properties of external direct product.

Let $G_1,.....,G_n$ be finite groups and $G_1\oplus.....\oplus G_n$ be their external direct product.

(1) $O(G_1\oplus....\oplus G_n)=O(G_1)\cdot O(G_2)\cdot....\cdot O(G_n) or \left|G_1\right|\left|G_2\right|.....\left|G_n\right|$.

(2) For $g_1,..,g_n)\in G_1\oplus....\oplus G_n$, then $O(g_1,..,g_n))=lcm\,(o\,(g_1),..,o(g_n))$.

Proof : (1) is clear by property of cardinality of Cartesian product

(2) Let $O(g_i) = n_i \ for \ 1 \le i \le n$

$Let \ \ell = \ell cm\,[n_1, ..., n_k]$

$Then \ n_i \,|\, \ell \ for \ 1 \le i \le n \ , let \ \ell = n_i \ r_i \ for \ 1 \le i \le n.$

$Then \ (g_1, ..., g_n)^{\ell} = ({g_1}^{\ell}, ..., {g_n}^{\ell}) = ({g_1}^{n_1 r_1}, \quad {g_n}^{n_n r_n})$

$= (e_1^{r_1}, ..., e_n^{r_n}) = (e_1, ..., e_n)$

$\therefore O\,(g_1, \quad g_n) \setminus \ell$

Then $Let \ O(g_1, ... g_n) = k \ ie \ k \setminus \ell$

$(g_1, \quad g_n)^k = ({g_1}^k, \quad {g_n}^k)\,(*)$

$= (e_1, \quad e_n)$

$\therefore {g_2}^k = e_i \ for \ 1 \le i \le n$

$= \ell \,|\, k.$

Note, by induction, the result is true $\forall\, m \in \mathbb{N}$

Theorem : Let $G_1, ..., G_n$ be finite cyclic groups of orders $n_1, ..., n_n$ respectively, Then, $G_1 \oplus .... \oplus G_n$ is cyclic if and only if g.c.d $(n_i, \ n_j) = 1 \ for \ 1 \le i \, , \, j \le n$

Corollary: Let $m = n_1 .....n_k$. Then $\mathbb{Z}_m \cong \mathbb{Z}_{n,} \oplus ... \oplus \mathbb{Z}_{n_k}$

if and only if n_i, n_j *are relatively prime for* $i \ne j$.

Note : If G_1, G_2 are abelian groups, so is $G_1 \oplus G_2$

Theorem: Let m and n be positive integers of g.c.d (m,n) = 1, then U(mn) is isomorphic to U(m) $\oplus$ U(n).

Proof :Consider the map f : U(mn) $\longrightarrow$ U(m) $\oplus$ U(n) defined by,

f(x) = (x mod m, x mod m)

The map f is well-defined,

For if x, y $\in$ U(mn), f(xy) = (xy mod m, xy mod m)

= x mod m, y mod m, x modm, y mod m)

= (x mod m, y mod m) (y modm, y mod m)

= f(x) f(y)

Let f(x) = f(y) $\Rightarrow$ (x mod m , x mod m) = (y mod m, y mod m)

$\Rightarrow$ x mod m = y mod m x mod m = y mod m

$\Rightarrow$ x $\equiv$ y mod mn ($\because$ m, n are relatively prime)

$\therefore$ f is one – one

f is onto by Chinese Remainder Theorem.

Therefore, f is bijective

Clearly f is a homomorphism.

Thus, U(mn) is isomorphic to U(m) $\oplus$ U(n).

Corollary: Let $m = n_1, .. n_2, g.c.d\ (n_1, n_j) = 1\ for\ i \neq j$

$Then\ U(m) \cong U(n_1) \oplus U(n_2) \oplus ... \oplus U(n_k)$

2.5 Normal Sub Groups and Quotient (Factor Groups)

Normal Subgroup

Definition: Let G be a group. A subgroup H of G is called a normal subgroup of

G if aHa^{-1} $\subseteq$ H for each $a \in G$

$(or\ aha^{-1} \in H\ for\ each\ a \in G, each\ h \in H)$

This is denoted by H $\lhd$ G

Theorem 1: Let H be a subgroup of a group G.

Then, the following statements are equivalent.

1) $H \lhd G\ (ie\ aHa^{-1} \subseteq H \curlyvee a \in G)$
2) $aHa^{-1} = H\ for\ each\ a \in G$
3) $aH = H_a\ for\ each\ a \in G$
4) $H_a H_b = H_{ab}\ for\ each\ a, b \in G$

(or aHbH = abH for each a, b $\in$ G)

Proof :- $(i) \Rightarrow (ii)$

Suppose $H \lhd G$

$Let\ a \in G, then\ aHa^{-1} \subseteq H$

$Also, a^{-1} \in G, \therefore a^{-1} Ha \subseteq H \ \ (*)$

$\therefore H = a\,(a^{-1}\,\mathrm{H}\,a)\,a^{-1} \subseteq aHa^{-1}\ (by\ *)$

$\therefore aHa^{-1} = H.$

$(ii) \Rightarrow (iii)$

$Ha = aHa^{-1}a = a\ He = aH.$

$(iii) \Rightarrow (iv)$

$H_aH_b = HHab \subseteq Hab\ (\because H\ is\ closed\ under\ multiplication)$

$\therefore Hab = Heab \subseteq HHab = HaHb\ (Ha = aH)$

$\therefore Hab \subseteq HaHb$

$\therefore HaHb = Hab\ (or\ aHbH = abHH \subseteq ab\ H$

$H = eH \subseteq HH.$

$\therefore aHbH = abHH\ (abH)$

(iv)$\Rightarrow$(i)

$For\ a \in H, aHa^{-1} = eaHa^{-1} \subseteq HaHa^{-1} \subseteq Haa^{-1} = H$

$\therefore H \lhd G.$

Note : If G is abelian, and H < G, then H $\lhd$ G.

Theorem: Let H $\lhd$ G, Let $G / H = \{Ha : a \in G\}$

Then, the operation HaHb = Hab on G/H is a well defined binary operation in G/H and G/H is a group under this binary operation.

Proof : We first show that this binary operation is well defined

Let

$$Let\ aa'^{-1} = h_1 \quad bb'^{-1} = h_2, \quad h_1, h_2 \in H.$$

$$we\ show\ Hab = Ha'b'$$

$$ab(a'b')^{-1} = ab\,b'^{-1}\,a'^{-1} = ah_2a'^{-1} = aa'^{-1}a^1h_2a'^{-1} = h_1\,a'h_2a'^{-1}$$

$$= h_1h_3 \ where\ h_3 = a^1b_2a'^{-1} \in H \quad (\because H \lhd G)$$

$$\therefore ab\,(a'b'^{-1}) = h_1h_3 \in H.$$

$$\therefore Hab = Ha'b'.$$

$$ie\ HaHb = \mathrm{H}a'Hb'.$$

and the operation is well defined.

For

$$H_a, H_b, \mathrm{H}_c, \in G/H,$$

$$(H_a\mathrm{H}_b)\,\mathrm{H}_c = (\mathrm{H}_{ab})\,\mathrm{H}_c = \mathrm{H}_{(ab)c} = \mathrm{H}_{a(bc)} = \mathrm{H}_a(\mathrm{H}_{bc}) = \mathrm{H}_a(\mathrm{H}_b\mathrm{H}_c)$$

$\therefore$ The binary operation is associative:

$$H_e = H \in G/H$$

$$H_aH_e = H_{ae} = H_a = H_{ea} = H_eH_a$$

$\therefore$ He = H is, the identity element of G/H

For

$$H_a \in G/H, \exists\, H_a{}^{-1} \in G/H\ such\ that$$

$$H_aH_a{}^{-1} = H_{aa}{}^{-1} = \mathrm{H}_e = H_a{}^{-1}a = H_a{}^{-1}H_a$$

$\therefore H_a{}^{-1}$ is the inverse of H_a

Thus, G/H is a group.

It is called the quotient groups of G by H (or the factor group of G/H).

Note : If G is finite o(G/H) = o(G)/o(H) = [G : H].

Example: Let us consider $\mathbb{Z}/n\mathbb{Z}$

Let us find the cosets $\mathbb{Z}/n\mathbb{Z}$

For a $\in$ Z, we know $\exists\, q, r \in \mathbb{Z}$ such that $a = qn + r, 0 \le r \le n-1$
$\therefore a - r \in n\,\mathbb{Z}. \therefore a + n\mathbb{Z} = r + n\mathbb{Z}, 0 \le r \le n-1.$
Moreover, for $0 \le r, s \le n-1$

$r + n\mathbb{Z} = s + n\mathbb{Z} \Rightarrow r - s \in n\,\mathbb{Z}$
$\Rightarrow |r-s| = 0 \; or \; |r-s| = n \Rightarrow |r-s| = 0, \Rightarrow r = s$

$\therefore$ The distinct cosets of $Z/n\mathbb{Z}$ are o + $\mathbb{Z}$, 1 + $\mathbb{Z}$,……, (n – 1) + $\mathbb{Z}$.

Propositions 1 : Let G be a group. If G/Z(G) is cyclic, then G is abelian.

Proof : Suppose G/Z(G) = $\{(Z(G)x)^n : n \in \mathbb{Z}\}$ = <Z(a)x>

For $a, b \in Z(G)$, *let* $a \in Z(G)x^n, b \in Z(G)^m, m, n, \in, \mathbb{Z}$

$\therefore a = z_1 x^n, b = z_2 x^m, z_1, z_2 \in Z(G)$
$ab = z_1 x^n \; z_2 x^m = z_1 z_2 x^n x^m = z_2 z_1 x^m x^n = z_2 x^n z_1 x^n = ba$
$\therefore G$ *is abelian.*

Proposition 2: G/Z(G) $\approx$ Inn G

Proof : Consider f : G/Z(G) $\longrightarrow$ Inn G defined by f(Z(G)x) = i_x where

$(i_x(a) = xax^{-1})$

$\therefore Z(G)x = Z(G)y \Rightarrow xy^{-1} \in Z(G), Let\; xy^{-1} = z, z \in Z(G)$
$For\; a \in G, i_x(a) = xax^{-1} = zya\,(zy)^{-1} = zyay^{-1}z^{-1} = (yay)^{-1}\, zz^{-1} = yay^{-1} = i_y(a)$

$\therefore i_x = i_y$
$\therefore f$ *is well defined.*

f (Z(G)x. Z(G)y) = f (Z(G) = y) = i_{xy}

$For\ a \in G, i_{xy}(a) = (xy)\ a\ (xy)^{-1} = x(yay^{-1})x^{-1} = i_x i_y(a)$

$\therefore i_{xy} = i_x\ i_y$

$\therefore f(Z(G)\ x\ Z(G)y) = i_{xy} = i_x i_y = f(Z(G)x)\ f(Z(G)y)$

$\therefore f\ is\ a\ group$ hom$omorphism.$

$For\ x, y \in G, f(z(G)x) = f(z(G)y) \Rightarrow i_x = i_y \Rightarrow i_x(a) = i_y(a) \forall\ a \in G$

$\Rightarrow xax^{-1} = yay^{-1} \forall\ a \in G\ \Rightarrow y^{-1}x\ a^y = ayx^{-1} \forall\ a \in G \Rightarrow (y^{-1}x \in Z(G)$

$\Rightarrow z(G)\ y = z(G)x$

$\therefore f\ is\ one - one$

Clearly for $i_x \in$ Z(G), f(Z(G)x) = i_x and f is onto

$\therefore$ f is a group isomorphism.

Definition: Internal Direct Product :- Let $H_1, H_2, ..., H_n$ be normal subgroups of G we say G is the internal direct product of $H_1\ H_2$ if

(i) G = $H_1, H_2, ..., H_n = \{h_1\ h_2, ..., h_n / h_i \in H_i, 1 \le i \le n\}$

(ii) $H_1, H_2, ..., H_n \cap H_{i+1} = \{e\}\ for\ i = 1, 2...n - 1.$

Note : $H_i \cap H_j = \{e\}\ if\ i \ne j)$

In particular, if H, K are normal subgroups of G, then G is the internal direct product of H, K if.

(i) G = HK = $\{hk / h \in H, k \in k\}$

(ii) $H \cap k = \varnothing.$

Theorem : If a group G is the internal direct product of subgroups $H_1,..,H_n$ then $G = H_1\ H_2 \oplus .. \oplus H_n$

Proof: For $h_i \in H_i, h_j \in H_j, h_i\ h_j\ h_i^{-1} h_j^{-1} = (h_i\ h_j\ h_i^{-1})\ h_j^{-1} \in H_j$

$h_i\ h_j\ h_i^{-1}\ h_j^{1} = h_i\ (h_j\ h_i^{-1}\ h_j^{-1}) \in H_i$

$\therefore h_i\ h_j\ h_i^{-1} \in H_i\ H_j = \{e\}$

$\therefore h_i\ h_j = h_j\ h_i$

$\therefore For\ h_i, h_i^{-1} \in H_l\ , 1 \le i \le n$

$h_1\ h_2\ h_n = h_1\ h_2^{1}\quad h_n^{1}$

$\Rightarrow h_n\ h_n^{1} = h_1\ h_2\ \ h_{n-1}\ h_{n-1}\ h_{n-2}^{-1}\ h_2^{1}\ h_1^{1}$

$= (h_1\ h_1^{-1})\ (h_2\ h_2^{1-1})\ \ (h_{n-1}\ h_{n-1}^{1-1})$

$\Rightarrow h_n\ h_n^{1-1} = e$

$\Rightarrow h_n = h_n^{1}$

$\therefore h_1\ h_2\quad h_{n-1} = h_i\ \ h_{n-1}$

By similar argument, $h_{n-1} = h_{n-1}^{1}$

Proceeding in this manner, $h_i = h_i^{1}\ for\ 1 \le i \le n$

We define $\varnothing : G \to H_1 \oplus ..... \oplus H_n\ by$

$\varnothing (h_1, ..., h_n) = (h_1, ..., h_n)\ (\oplus\ is\ well\ defined)$

$\varnothing ((h_1, ..., h_n)\ (h_1^{1}, ..., h_n^{1})) = \varnothing (h_1 h_1^{1}, .., h_n h_n^{1}) = \varnothing\ (h_1 h_1^{1}, ..., h_n h_n^{1})$

$= \varnothing\ (h_1, .., h_n)\ (h_1^{1}, .., h_n^{1}) = \varnothing\ (h_1, ..., h_n)\ \varnothing\ (h_1^{1}, ..., h_n^{1})$

$\therefore \varnothing$ is a group homomorphism

$\varnothing\ (h_1, ..., h_n) = \varnothing\ (h_i^{1}, ..., h_n^{1}) \Rightarrow (h_1, ..., h_n) = (h_i^{1}, ..., h_n^{1})$

$\Rightarrow h_i = h_i^{1}\ \ for\ 1 \le i \le n \Rightarrow h_1\ \ h_n = h_i\ .h_n^{1}$

$\therefore \varnothing\ is\ one - one$

$\varnothing\ is\ clearly\ onto.$

$\therefore \varnothing$ is a group isomorphism.

2.6 Isomorphism Theorems

We recall that a homomorphism from a group G to group $\overline{G}$ is a map $f : G \to \overline{G}$ such that f(ab) = f(a) f(b) for each a, b $\in$ G.

Let G, $\overline{G}$ be groups and f : G $\to \overline{G}$ be a group homomorphism we define kernel of f (denoted by ker f) as $\ker f = \{x \in G / f(x) = e'\}$ is the identity element of $\overline{G}$.

Proposition 1: Let G, $\overline{G}$ be groups and f : G $\to \overline{G}$ be a group homomorphism. Then, Kerf $\lhd$ G.

Proof :- We know, $f(e)=e' \therefore e \in Kerf \Rightarrow Kerf \neq \varnothing$

$For\ a,b \in Ker\ f,\ f(ab^{-1}) = f(a)\ f(b^{-1}) = f(a)\ (f(b))^{-1} = e^1\ e^{1-1} = e^1$
$\therefore ab^{-1} \in Ker\ f\ and\ Ker\ f < G.$

$For\ a \in G, h \in \ker f, f(aha^{-1}) = f(a)\ f(h)\ f(a^{-1}) = f(a)\ e'(f(a))^{-1} = e'$

$\therefore aha^{-1} \in \ker f\ \ for\ a \in G, h \in \ker f$
$\therefore \ker f \lhd G$

Proposition 2: Let G, $\overline{G}$ be groups and f : G $\rightarrow \overline{G}$ be a group homomorphism. Then, f is one – one if and only if ker f = {e}.

Proof :- Suppose f is one-one

Then x $\in$ kerf

$$\Rightarrow f(x)=e' \Rightarrow f(x)=f(e)=e' \Rightarrow x=e \therefore \ker f=\{e\}$$

Conversely, suppose ker f = {e}

$Then\ for\ x, y \in, G, f(x)=f(y) \Rightarrow f(x)\ f(y)^{-1} = e' \Rightarrow f(x)\ f(y^{-1}) = e'$
$\Rightarrow f(xy^{-1}) = e' \Rightarrow xy^{-1} \in \ker f \Rightarrow xy^{-1} = e \Rightarrow x = y$
$\therefore f\ is\ one-one.$

Note: If G, $\overline{G}$ are groups and f : G $\rightarrow \overline{G}$ is a group homomorphism, then

Imf = {f(x) : x $\in G$} is a subgorup of $\overline{G}$.

Proposition: Let G be a group and H$\lhd G$, Then p: G $\rightarrow$G/H is surjective group homomorphism, where p(x) = Hx. For x $\in$ G and ker p = H

Proof: For x, y $\in$ G, (p(xy) = $H_{xy} = H_x H_y = p(x)\ p(y)$

$\therefore$p is a group homomorphism.

p is clearly onto. (For $H_x \in G/H, p(x) = H(x) \exists x \in G\ such\ that$

$x \in \ker p \Leftrightarrow H_x = H$ (identity element of G/H is H)

$\Leftrightarrow x \in H$
$\therefore \ker p = H$

Note:- Thus, if $H \lhd G$, where G is a group, then H is a kernel of a group homomorphism from G to a suitable group.

We next prove the Isomorphism Theorems.

First Isomorphism Theorem: Let $f : G \to \overline{G}$ be a homomomorphism of groups. If f is onto, G/kerf $\approx \overline{G}$ (or in general G/kerf $\approx$ Im f).

Proof : Consider the mapping $\overline{f}$: G/ker f $\to \overline{G}$ defined by,

$\overline{f}(\ker f\ a) = f(a)$ $(or\ \overline{f}(Ka) = f(a))\ where\ \mathrm{K} = \ker f$

This map is well defined

For Ka = Kb, a, b $\in$ G

$\Rightarrow ab^{-1} \in K\ (= \ker f) \Rightarrow f(ab^{-1}) = e' \Rightarrow f(a)\, f(b^{-1}) = e'$

$\Rightarrow f(a)\,(f(b))^{-1} = e' \Rightarrow f(a) = f(b)$

$\overline{f}$ (Ka.Kb) = $\overline{f}$ (Kab) = f(ab) = f(a) f(b) = $\overline{f}$ (Ka) $\overline{f}$ (Kb)

$\therefore \overline{f}$ is a group homomorphism.

$\overline{f}$ (Ka) = $\overline{f}$ (Kb) $\Rightarrow$ f(a) = f(b)

$\therefore \overline{f}$ is one – one.

If f is onto, for $a' \in \overline{G}\ \exists$ a $\in$ G such that f(a) = a'

$\therefore \overline{f}(Ka) = f(a) = a'$

$\therefore \overline{f}$ *is onto.*

Note :- 1. If f is not onto, we consider $\overline{f}$: G/ker f $\to$ Imf and G/kerf $\approx$ Imf.

2. The above theorem, is also called. The Fundamental Theorem Of Homomorphism Of Groups.

Second Isomorphism Theorem: Let H and K be subgroups of a group G and

K $\lhd$ G. Then, $\frac{H}{H \cap K} = \frac{HK}{K}$

Proof : We note H K < G and K < HK,

$K \lhd G \Rightarrow K \lhd HK$

we define a map $f : H \to HK / K$ *by* $f(h) = hK$ *for* $h \in H$

Then, for $h_1, h_2 \in H$, $f(h_1 h_2) = (h_1 h_2)\,\mathrm{K} = (h_1 K)(h_2 K) = f(h_1) f(h_2)$

$\therefore$ f is a group homomorphism.

f is onto for any element in HK / K is of the form hkk(hk)

And hk = f(h)

Ker f = {h $\in$ H : hK = K} $\Rightarrow h \in K \Rightarrow$ h = H $\cap$ K.

$\therefore$ By First Isomorphism Theorem of groups

$\frac{H}{H \cap K} = \frac{HK}{K}$

Third Isomorphism Theorem of groups:

Let G be a group and H, K be normal subgroups of G If K $\subset$ H, then

(G/K) / (H/K) $\approx$ G/H

Proof : Consider the mapping f: G/K $\longrightarrow$G/H given by f(Kx) = Hx

This map is well defined, for

$K_x = K_y \Rightarrow xy^{-1} \in k \Rightarrow xy^{-1} \in H \Rightarrow Hx = Hy$

$f(KxKy) = f(Kxy) = Hxy = HxHy = f(Kx)\, f(Ky)$

$\therefore$ f is a group homomorphism.

f is clearly onto.

$\because$ Any element of G/H is of the form Hx, x $\in$ G

$\therefore f(Kx) = Hx$

$\therefore$ *for* ker $f = \{Kx / x \in G\ f(Kx) = H\} = \{Kx / x \in G, Hx = H\} = H / K$

$\therefore$ By First Isomorphism Theorem, G/K/H/K $\approx$ G/H

Theorem: Let $G_1, G_2,$ *be groups and* $H_1 \lhd G_1, H_2 \lhd G_2$. Then

$H_1 \oplus H_2 \lhd G_1 \oplus G_2$ *and* $\dfrac{G_1 \oplus G_2}{H_1 \oplus H_2} \approx \dfrac{G_1}{H_1} \oplus \dfrac{G_2}{H_2}$

Proof : Consider the map $f : G_1 \oplus G_2 \to \dfrac{G_1}{H_1} \oplus \dfrac{G_2}{H_2}$

defined by $f(g_1 . g_2) = (H_1 g_1 , H_2 g_2)$

Then, for $(g_1, g_2), (g_1' g_2') \in G_1 \oplus G_2$

$f((g_1, g_2)(g_1', g_2')) = f(g_1 g_1', g_2 g_2') = (H_1 g_1 g_1', H_2 g_2 g_2')$

$= (H_1 g_1 \, H_1 \, g_1' , H_2 g_2 \, H_2 g_2') = (H_1 g_1, H_2 g_2)(H_1 g_1' \, H_2 \, g_2'^1)$

$= f(g_1, g_2) f(g_1', g_2')$

$\therefore f$ *is a group* hom*omorphism.*

For $(H_1 g_1 , H_2 g_2) \in \dfrac{G_1}{H_1} \oplus \dfrac{G_2}{H_2}$

$(H_1 g_1, H_2 \, g_2) = f(g_1 , g_2)$

$\therefore f$ *is onto*

$(g_1 , g_2) \in \ker f \Leftrightarrow f(g_1, g_2) = (H_1, H_2) \Leftrightarrow (H_1 g_1, H_2 g_2) = (H_1 H_2)$

$\Leftrightarrow g_1 \in H_1, g_2 \in H_2 \Leftrightarrow (g_1, g_2) \in \mathrm{H}_1 \oplus \mathrm{H}_2$

$\therefore$ By First Isomorphism Theorem,

$\dfrac{G_1 \oplus G_2}{H_1 \oplus H_2} \approx \dfrac{G_1}{H_1} \oplus \dfrac{G_2}{H_2}$

Correspondence Theorem: Let G, $\overline{G}$ be groups and f : G $\to$ $\overline{G}$ be a homomorphism of group G onto $\overline{G}$.

Then

i] H < G $\Rightarrow f(H) < \overline{G}$

ii] H < $\overline{G}$ $\Rightarrow f^{-1}(\overline{H}) < G \; f^{-1}(\overline{H}) = \{ x \in G : f(x) \in H \}$

iii] $H \lhd G \Rightarrow f(H) \lhd \overline{G}$

iv] $\overline{H} \lhd \overline{G} \Rightarrow f^{-1}(\overline{H}) \lhd G$

v] $H < G \text{ and } H \supset \ker f \Rightarrow H = f^{-1}(f(H))$.

vi] The map H $\longrightarrow$ f(H) is a 1-1 corespondence between the family of subgroups of G containing ker f and the family of subgroups of $\overline{G}$. Furthermore normal subgroups of G correspond to normal subgroups of $\overline{G}$.

Proof :

i] $e \in H, \therefore f(e) = e' \in f(H) \text{ and } f(H) \neq \varnothing$

$\text{For } a', b' \in f(H), a' = f(a), b' = f(b) \text{ for some } a, b \in H.$

$\therefore ab^{-1} \in H, \text{and } f(ab^{-1}) \in f(H)$
$f(ab^{-1}) = f(a)\, f(b^{-1}) = f(a)\,(f(b))^{-1} = a'(b')^{-1}$
$\therefore a'\left(b'\right)^{-1} \in f(H) \text{ and } f(H) < \overline{G}$

ii] $\text{Let } \overline{H} < \overline{G} \text{ and } H = f^{-1}(H)$

$\text{Then}, e' \in \overline{G} \text{ and } e' = f(e) \Rightarrow f(e) \in \overline{H} \Rightarrow e \in f^{-1}(\overline{H})$
$\therefore f^{-1}(\overline{H}) \neq \varnothing.$

Let $a, b \in f^{-1}(\overline{H}) \text{ then } f(a), f(b) \in \overline{H}, \text{and } \overline{H} < \overline{G}$

$f(a)\,(f(b))^{-1} \in \overline{H} \text{i.e. } f(a)\, f(b^{-1}) \in \overline{H},\ f(ab^{-1}) = f(a)\, f(b^{-1}) \in \overline{H}$
$\therefore ab^{-1} \in f^{-1}(\overline{H}) \therefore f^{-1}(\overline{H}) < G$

iii] Let $H \lhd G,$

$\text{Let } a' \in \overline{G}, h' \in f(H).$
$\text{Then } a' = f(a), h' = f(h), \text{where } a \in G, h \in H$
$a'h^1\, a'^{-1} = f(a)\, f(h)\,(f(a))^{-1} = f(a)\, f(h)\, f(-1)$
$= f(aha^{-1}) \in f(h)\,(\because aha^{-1} \in H)$

$\therefore f(H) \lhd G.$

iv] Let $\overline{H} \lhd \overline{G}$ *Let* $a \in G, h \in f^{-1}(\overline{H})$ *ie* $f(h) \in \overline{H}$

$\therefore f(aha^{-1}) = f(a)\, f(h)\, f(a^{-1}) = f(a)\, f(h)\, (f(a))^{-1} \in \overline{H}$
$\therefore aha^{-1} \in f^{-1}(\overline{H}) \therefore f^{-1}(\overline{H}) \lhd G$

v] Let H < G and H $\supset$ kerf.

Then, $f^{-1}(f(H)) \supset H.$

$Let\ x \in f^{-1}(f(H)) \therefore f(x) \in f(H)$
$\therefore f(x) = f(h)\ for\ some\ h \in H \quad \therefore f(x)\, f(h)^{-1} = e'$
$\therefore f(x)\, f(h^{-1}) = e'\ and\ f(xh^{-1}) = e'$
$\therefore xh^{-1} \in \ker f \subset H \therefore xh^{-1} = h_1, h_1 \in H$
$\therefore x = hh, \in H \quad and\ f^{-1}(f(H)) \subset H$
$\therefore f^{-1}(f(H)) = H.$

vi] Let $\overline{H}$ be a subgroup of $\overline{G}$.

Then, $f^{-1}(\overline{H})$ is a subgroup of G containing ker f

$\therefore f(f^{-1}(\overline{H})) = \overline{H}.$
$\therefore The\ map\ H \to f(H)\ is\ onto.$

$For\ H_1H_2 < G \Rightarrow f(H_1) = f(H_2)$
$Then\ f^{-1}(f(H_1)) = H_1\ f^{-1}(f(H_2)) = H_2$
$H_1, H_2 \supset \ker f \quad \therefore H_1 = H_2.$
$\therefore The\ map\ is\ one - one$

Corollary: Let G be a group and N G.

Given any subgroup H of G/N, there is a unique subgroup H of G containing N such that $H' = H/N, Futher, H \lhd G\ iff\ H/N \lhd G/N$

Proof : Consider the homomorphism f : G $\to$G/N defined by f(x) = Nx. f is an onto homomorphism and ker f = N $\therefore$ By correspondence Theorem, there is a unique subgroup H of G containing N such that f(H) = H/N = H'

Further H $\lhd G \Leftrightarrow H/N \lhd G/N$

Proposition : $A_n \lhd S_n$ *for* $n \geq 2$ then $o(A_n) = \frac{n!}{2}$.

Proof : Consider $\in : S_n \to \{1, -1\}$ *defined by* $\in(\sigma) = sign\,\sigma$

Then $\in(\sigma_1\sigma_2) = sign\,(\sigma_1\sigma_2) = Sign\,(\sigma_1)\,Sign\,(\sigma_2) = \in(\sigma_1) \in(\sigma_2)$
for $\sigma_1, \sigma_2 \in S_n$

$\therefore$ $\in$ is a group homomorphism.

$\in$ *is onto for* $\in((12)) = -1, \in(I) = 1,$
$\ker \in = \{\sigma \in S_n / \in(\sigma) = 1\} = A_n$
$\therefore A_n \lhd S_n$. *and by First Isomorphism Theorem of Groups*,
$S_n / A_n \approx \{1, -1\}$
$\therefore O(S_n) / o(A_n) = 2$

$$\therefore O(A_n) = \frac{O(S_n)}{2} = \frac{n!}{2}$$

Note : We have seen that by Lagrange's Theorem if G is a finite group and

H < G, then O(H)\O(G).

However, converse of Lagrange's Theorem is not true is general.

We give an example below.

Example : A_4 has no subgroup of order 6. ($O(A_4) = 12$).

Proof : Suppose A_4 has a subgroup H of order 6.

Then $[A_4 : H] = O(A_n) / o(H) = 12 / 6 = 2$

$\therefore H \lhd A_4$.
A_4 *has eight* 3 *cycles*

Let σ be a 3-cycle in A_4.

If σ/H, then $H\sigma \neq H$.

If $\sigma^2 \notin H$ *then* $H\sigma^2 = H\sigma$

$\therefore \sigma^2\sigma^{-1} \in H$. *i.e.* $\sigma \in H$, *which is not true*

If $\sigma^2 \in H$, *then* $(a^2)^{-1} = \sigma \in H$. *Which is not true*

$\therefore \sigma \in H$, *thus all* 3 *cycles are in* H.

$\therefore O(H) \geq 8$,

A contradiction.

$\therefore A_4$ has no subgroup of order 6.

2.7 Classification of Groups of Order $\leq$ 7 Upto Isomorphism.

We note that group of order 1 is a the trivial group which is unique upto isomorphism. Group of order 2, 3, 5, 7 are cyclic (as prime order) and are unique upto isomorphism.

Let G be a group of order 4. Then, any element of G has order which is divisor of 4 i.e. 1, 2 or 4.

If G has an element of order 4, then G is cyclic.

Suppose G has no element of order 4.

Then any non-trivial element in G has order 2. Let G = {e, a, b, c} which e, a, b, c and distinct elements $a^2 = b^2 = c^2 = e$

We find ab $\neq e$

$$\left(\begin{array}{l} \because ab = e \Rightarrow ab = aa \Rightarrow b = a \text{ which is not true} \\ \quad ab = a \Rightarrow ab = ae \Rightarrow b = e \text{ which is not true} \\ \quad ab = b \Rightarrow ab = eb \Rightarrow a = e \text{ which is not true} \\ \therefore ab = c, \text{similarly } ba \neq e, ba \neq a, ba \neq b \\ \therefore ba = c = ab \end{array}\right)$$

Similarly, we can show ac = b = ca

bc = a = cb.

$\therefore$ Composition table of G is

	e	a	b	c
e	e	a	b	c
a	a	e	c	a
b	b	c	e	a
c	c	b	a	e

Thus, any non-cyclic group G of order 4 is of the above type (and is called the Klein's four group V_4)

Let G be a group of order 6. Then, order of any element of G divides 6.

$\therefore$ Order of any element in G is 1, 2, 3 or 6. G is a group of even order and so has an element of order 2.

Suppose every non-trivial element of G has order 2. Then, $x^2 = e, \forall\, x \in G$

$\therefore For\ x, y \in G, (xy)^{-1} = xy$

$\therefore y^{-1}x^{-1} = xy$ i.e. $yx = xy$

$\therefore G$ is abelian

If $a, b \in G, a \neq e, b \neq e$ then $H = \{e, a, b, ab\}$ is a finite subset of G having closure property.

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

$\therefore H < G$, By Lagrange's Theorem $o(H) / o(G)$ i.e. 4/6.

A contradiction.

$\therefore G$ has an element of order 3 or 6.

Case 1: If G has an element of order 6 then G is cyclic.

Case 2 : G has no element of order 6. Let $a \in G$ have order 3 and $b \in G$ have order 2. Then $b \neq e, a, a^2$ $(o(a) = o(a^2) = 3, o(b) = 2)$. If $ab = ba$, then

$o(ab) = 6$ which contradicts that G has no element of order 6.

$\therefore ba \neq ab, ba \neq e\,(\because a^{-1} = a^2)\, ba \neq a\,(b \neq e), ba \neq a^2\,(\because b \neq a)$

$ba \neq b\,(\because a \neq e), ba \neq ab$.

We note e, a, a^2, b, ab, a^2b are distinct

$\left(a^2b \neq e \because b \neq a\right), \left(a^2b \neq a\right) \left(\because ab \neq e\right) \left(a^2b \neq a^2 \because b \neq e\right)$

$\left(a^2b \neq ab \because a \neq e\right)$

$\therefore G = \left\{e, a, a^2, b, ab, a^2b\right\}$

$\therefore ba = a^2b$

Thus, $G = \langle a, b \rangle a^3 = b^2 = e, ba = a^2b$

$\therefore G \approx S_3$

$\therefore$ There are two non isomophic groups of order 6, one is cyclic, and the other is isomorphic to S_3

Note : An abelian group of order 6 is cyclic.

2.8 Fundamental Theorem of Finite Abelian Groups

Let G be a finite abelian group of order n. Then $G \approx \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots\ldots \oplus \mathbb{Z}_{n_k}$ where $n_{i+1} \mid n_i$ for $1 \leq i \leq k-1$ and the above decomposition is unique.

This is also expressed as.

Let G be a finite abelian group of order $n > 1$ and let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ where $p_1, \ldots p_k$ are distinct primes, then

$G \approx G_1 \oplus G_2 \oplus \ldots. \oplus G_K$ _where_ $o(G_i) = p_i^{\alpha_i}$ $1 \leq i \leq k$ _and

_ $G_i \approx \mathbb{Z}_{p_i}$ $\alpha_{i1} \oplus \ldots \oplus \mathbb{Z}_{p_i}$ $\alpha_i r_i$ where $\alpha_{i1} \geq \alpha_{i2} \geq \ldots \geq \alpha_{ir} \geq 1$ and

$\alpha_{i1} + \ldots + \alpha_{ir} = \alpha_i$.

We note that if $p_i, \ldots p_k$ are primes dividing o(G), then in p_i / n for $i \leq i \leq k$.

Recall that $Z_m \oplus Z_n \approx Z_{mn}$ *if and only if* $g.c.d\ (m,n) = 1$

Example : Let us list all abelian groups (upto isomorphism) of order 180.

$180 = 2^2 \cdot 3^2 \cdot 5.$

Abelian groups.

$\mathbb{Z}_{180}$	$\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$
$\mathbb{Z}_{90} \oplus \mathbb{Z}_2$	$\mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
$\mathbb{Z}_{60} \oplus \mathbb{Z}_6$	$\mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$

Let us consider classification of abelian groups of order p^2, p^3, p^4 upto isomorphism.

	Partitions	Abelian Groups
1] p^2	2	$\mathbb{Z}_{p^2}$
	2 = 1 + 1	$\mathbb{Z}_p \oplus \mathbb{Z}_p$
2] p^3	3	$\mathbb{Z}_{p^3}$
	3 = 2 + 1	$\mathbb{Z}_{p^3} \oplus \mathbb{Z}_p$
3] p^4	4	$\mathbb{Z}_{p^4}$
	4 = 3 + 1	$\mathbb{Z}_{p^3} \oplus \mathbb{Z}_p$
	4 = 2 + 2	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$
	4 = 2 + 1 + 1	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
	4 = 1+1+1+1	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

Example: Expressing abelian groups in the form $G_{p1} \oplus G_{p2} \oplus ... \oplus G_{pn}$

And $Z_{n1} \oplus Z_{n2} \oplus \ \oplus Z_{nk}$ where $n_{i+1} \mid n_c$ for group of order 360.

$360 = 2^3 \times 3^2 \times 5$

1] $p=2 \quad p=3 \quad p=5$ *Abelian groups*

2	3	5	$\mathbb{Z}_{30} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$
2	3	1	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
2	1	1	$\oplus \mathbb{Z}_5$

2] $p=2$ $p=3$ $p=5$

2^2	3	5	$\mathbb{Z}_{60} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$
2	3	1	$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
2	1	11	$\oplus \mathbb{Z}_5$

3] $p=2$ $p=3$ $p=5$

2^2	3^2	5	$\mathbb{Z}_{180} \oplus \mathbb{Z}_2$
2	1	1	$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$

4] $p=2$ $p=3$ $p=5$

2^3	3^2	5	$\mathbb{Z}_{360}$
1	1	1	

Thus, there are 4 non-isomorphic abelian groups of order 360.

An important consequence of the Fundamental Theorem of finite abelian groups.

Theorem: If G is a finite abelian groups of order n, and m is a positive divisor of n, then G has a subgroup of order m. (This is converse of Lagrange's Theorem)

Note : The above partition may not be unique.

2.9 Summary

1) Let G, $\overline{G}$ be groups. A map f : G $\rightarrow \overline{G}$ is called a homomorphism of group G to group G if f(ab) = f(a) f(b) for each a, b $\in$ G

(i.e. f preserves group operation)

2) Let G, G be groups. A map f : G $\rightarrow \overline{G}$ is called an is isomorphism of group G to group $\overline{G}$ if i) f (ab) = f(a) f(b) for for each a,b $\in$ G (ie f is a group homomorphism) and ii) f is bijective.

3) Any finite cyclic group of order n is isomorphic to Z_n, the group of integer residue classes modulo under addition.

4) **Cayley's Theorem**: Every group is isomorphic to a group of permutations

5) An isomorphism of a group G onto itself is called an automorphism of G

6) Let G be a group and a$\in G$. The map $i_a : G \rightarrow G$ defined by $i_a(x) = axa^{-1}$ *for* $x \in G$ is called the inner automorphism of G induced by a.

7) For $g_1,..,g_n) \in G_1 \oplus .... \oplus G_n$, then $O(g_1,..,g_n)) = lcm\,(o\,(g_1),..,o(g_n))$.

8) Let G be a group. A subgroup H of G is called a normal subgroup of G if aHa $^{-1} \subseteq$ H for each $a \in G$

$(or\ aha^{-1} \in H\ for\ each\ a \in G, each\ h \in H)$

9) First Isomorphism Theorem: Let f : G $\rightarrow \overline{G}$ be a homomomorphism of groups. If f is onto, G/kerf $\approx \overline{G}$ (or in general G/kerf $\approx$ Im f).

10) **Second Isomorphism Theorem:** Let H and K be subgroups of a group G and K $\lhd$ G. Then, $\frac{H}{H \cap K} = \frac{HK}{K}$

11) **Third Isomorphism Theorem of groups:**

Let G be a group and H, K be normal subgroups of G If K $\subset$ H, then

(G/K) / (H/K) $\approx$ G/H

12) There exist unique groups of order 1, 2, 3, 5 as they are prime and 2 groups of order 4 and 6 upto isomorphism.

13) **Fundamental theorem of finite abelian groups:** Let G be a finite abelian group of order n. Then $G \approx \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus ..... \oplus \mathbb{Z}_{n_k}$ where $n_{i+1} \mid n_i$ for $1 \le i \le k-1$ and the above decomposition is unique.

2.10 Unit and Exercises

1) Show that Z(G) is a normal subgroup of a group G

2) Show that a subgroup of index 2 is a normal subgroup of any group G

(Let H < G, [G : H] = 2, Let a $\neq$ H, then H, Ha are distinct right cosets of H of G. H, aH are distinct left cosets of H in G. G = H U Ha = H UaH.

(Ha = aH = G H)

$\therefore$ For x $\in$ G, x $\in H \Rightarrow$ Hx = xH = H

x $\neq$ H $\Rightarrow$ Hx = xH = G (H).

3) What is the order of 5 + <6> in the quotient group $\mathbb{Z}_{18}/<6>$?.

4) Let G= $\{\pm 1, \pm i, \pm j, \pm k\}$ *where* $i^2 = j^2 = k^2 = -1$

$ij = -ji = k$, $jk = -kj = i, ki = -ik = j$

Construct the composition table of G.Show that every subgroup of G is normal.

5) Show that H = {I, (12)} is a not a normal subgroup of S_3 but {I, (123), (132)} is a normal subgroup of S_3.

6) If H and K are normal subgroups of a group then $H \cap K \lhd G$

7) If H is a subgroup of a group G and K $\lhd$ G, then H K < G.

$(e \in HK$, *For* $a, b \in HK$, $a = h_1k_1, b = h_2k_2, h_i \in H, k_i \in K$

$h_1k_1 \cdot (h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1kh_2^{-1}, k \in$ K

$= h_1h_2^{-1}\ h_2\ kh_2^{-1} \in H\ K)$

8) If H, K < G, where G is a group and H $\lhd$ G then $H \cap K \lhd K$

Miscellaneous problem on Group Theorem

1] Compute order of each element in the following groups

i) D_3 - Dihedral group of order 6

ii) D_4 - Dihedral group of order 8.

iii) u(30) iv) S_4 v) $\varnothing 8$

2] Let X = (1 2 3 4 .. 11 12) $\in S_{12.}$ for which integers I, $i \le i \le 12, is\ x^i$ a 12 cycle ?.

3] If X = (1 2) (3 4) (5 6) (7 8) (9 10). Is there a n cycle

$\sigma\ (n \ge 10)$ *such that* $x = \sigma^k$ for some positive integer k?

4] Show that $H = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} / n \in \mathbb{Z}\}$ is a cyclic subgroup of $GL_2(\mathbb{R})$

5] Let G be an abelian group prove or disprove

$H = \{x \in G : x^n = e$ *for some* $n \in \mathbb{N}\}$ is a subgroup of G.

6] Let G be a finite group of order $n \geq 2$, G cannot have a subgroup H of order n-1.

7] Let G_1, G_2 *be groups. Prove* $G_1 \oplus G_2 \approx G_2 \oplus G_1$

8] Show that the following are subgroups of $G_1 \oplus G_2$ where G_1, G_2 are groups then,

1] $\{(e_1, g_2) : g_2 \in G_2\}$ 2] $\{(g_1, e_2) : g_1 \in G_1\}$
3] $\{(g_1, g) : g \in G\}$ *where* $G_1 = G_2 = G$

9] i] Prove that Z $\oplus \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}$.

ii] Prove that $\varnothing \oplus \mathbb{Z}_2$ *is not isomorptic c to* $\varnothing$

10] Find the subgroup of S_n generated by {(1 2), (1 2) (3 4)}

11] Prove that S_4 = <(1 2 3 4), (1 2 4 3)>

12] Find a group which contains a, b such that o(a) = , o(b) = 5 and o(ab) = 2.

13] Let G be a group and $H \lhd G$, If o(H) = 2, Prove that H C Z(G).

14] Show that S_4 has a unique subgroup of order 12.

15] From the given pairs of subgroups, find isomorphic pairs, justify your answer

1] μ_4 *and* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ 2] $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ *and* $\mathbb{Z}_{27}$

3] $\mathbb{Z} \oplus \mathbb{Z}$ *and* $\mathbb{Z}$ 4] $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ *and* $\mathbb{Z}_{15}$

5] $\mu(8)$ *and* $\mu(10)$ 6] $\mu(8)$ *and* $\mu(12)$

7] $\mathbb{Z}$ and $2\mathbb{Z}$ (under additional)

16] Find a non-cyclic group of order 4 in $\mathbb{Z}_4 \oplus \mathbb{Z}_{10}$

17] Find all generators the following cyclic groups of

1] $30\mathbb{Z} \cap 20\mathbb{Z}$ 2] $\mathbb{Z}/30\mathbb{Z}$ 3] $\mu(13)$

18] Find a cyclic group of order 4 and a non-cyclic group of order 4 in S_4.

19] Let $G=\{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}: a,b \in G\}$ *and* $H=\{a+b\sqrt{2}: a,b \in G\}$ show that $G \approx H$ (operation being addition in both groups)

20) Prove that every subgroup of D_n of odd order is cyclic.

21] Find orders of all elements in A_n and D_n

22] Let G be a finite group and $N \lhd G$ if [G : H] and o(n) are relatively prime, then for any $x \in G, x^{o(N)} = e \; implies \; x \in N$

23] Let G be a group and N be a cyclic subgroup of G such that $N \Delta G$.

If H < N, show that H < G

24] Let =

$\{G=\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}: a,b,d \in \mathbb{R}, ad \neq o\} and \; N=\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}: b \in \mathbb{R}\}$

show that $N \lhd G$ and G/N is abelian.

25] Prove or disprove: If G is a group and K < H < G.

$K \lhd H \; and \; H \lhd G \; then \; K \lhd G$

24] Show that i) $Z(D_n)=\{e\} \; if \; n \; is \; odd$

ii) $Z(D_{2m})=\{e, a\} \; where \; a^m = e. (o(a)=m).$

25] Let $H=\{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}: a,b,c \in \mathbb{Z}_3\}$

Is H abelian? Is $H \lhd SL_3(\mathbb{Z}_3)$? Justify your answer.

26] Prove that there is no homomorphism from $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ *onto* $\mathbb{Z}_4 \oplus \mathbb{Z}_4$

27] Determine all group homomorphism from.

1] $\mathbb{Z}_{20}$ *onto* $\mathbb{Z}_8$ 2] $\mathbb{Z}_4$ *to* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

3] S_4 *to* $\mathbb{Z}_2$.

28] Suppose $\varnothing : \mu(30) \to \mu(30)$ is a group homomorphism and ker

$\varnothing = \{1, 11\}$. If $\varnothing(7) = 7,$ find all elements of $\mu(30)$ that map to 7.

29] Suppose $\varnothing : \mathbb{Z} \oplus z \to G$ (G is a group) is a group homomorphism such that $\varnothing(3, 2) = a$ and $(2, 1) = b,$ Determine $\varnothing(4, 4)$ (Assume operation in G is addition).

30] Show that a group of order 65 is cyclic.

31] Let H, K be distinct subgroups of a group G of index 2 Prove that $H \cap K \lhd G$ and $[G : H \cap K] = 4.$ In $G / H \cap K$ Cyclic? Justify your answer.

32] Let G be an abelian group of order 8. Prove or disprove. G has a cyclic subgroup of order 4.

33] Classify upto isomorphism abelian groups of under 108.

34] If G is an abelian group of order 120 and G has exactly 8 elements of order 2.

Determine the isomorphism class of G.

35] Find the number of abelian groups (upto isomorphism) of order [1] 15 [2] 42 [3] 16 [4] 48.

36] Let G be an abelian group of order 16. and $a, b, \in G$ such that o(a) = o(6) = 4 and $a^2 \neq b^2$ then determine the isomorphism class of G.

3

SYLOW THEOREMS

Unit Structure

3.0 Objectives

After going through this unit you shall come to know about

- The concept of group action and stabilizers
- The notion of the order and its relation with the order of the groups
- Classification of groups upto order 15 using various results of Sylov theorems

3.1 Centralizers and Normalizers Stabilizer

We recall that centre of a group G is defined as $Z(G)=\{x\in G / xg=gx \nvdash g\in G\}$ $Z(G)\lhd G$, Moreover, if $G/Z(G)$ is cyclic, G is abelian.

Let G be a group and A be a non-empty subset of G.

Definition: The centralizer of a $C_G(A)$ in the group G is defined as $C_G(A)=\{g\in G / g\,a\,g^{-1}=a\ \forall\ a\in A\}$.

We note $gag^{-1}=a\Leftrightarrow ga=ag$.

$C_G(A)$ is the set of all elements in G which commute with every element of A.

Proposition : $C_G(A)<G$

Proof : $e\in C_G(A)\because ea=ae=a \nvdash a\in A$

Let $x,y\in C_G(A)$ then $xa=ax,\ ya=ay \nvdash a\in A$.

$\therefore$ For $a\in A;\ y=aya^{-1},\ y^{-1}=(aya^{-1})^{-1}=\left(a^{-1}\right)^{-1}y^{-1}a^{-1}=ay^{-1}a^{-1}$

$\left(xy^{-1}\right)a=xy^{-1}a=x\,ay^{-1}\,a^{-1}\,a=xay^{-1}=axy^{-1}=a\left(xy^{-1}\right)$

$\therefore xy^{-1}\in C_G(A)$.

We note that if $A=\{a\},a^n\in C_G\left(\{a\}\right) \nvdash n\in\mathbb{N}$.

When $A=\{a\},C_G\left(\{a\}\right)$ is denoted by $C_G(a)$.

Definition: The normalizer of $A<$ G in G, is defined as

$N_G(A)=\{g\in G / g\ Ag^{-1}=A\}$.

Proposition : $N_G(A) < G$

Proof : $e\,A\,e^{-1} = A$

$$\therefore e \in N_G(A)$$

Let $x, y \in \mathrm{N}_G(A)$ then $xa\,x^{-1} = A,\ ya\,y^{-1} = A$.

$$\therefore xy^{-1}\,Ayx^{-1} = xy^{-1}\left(y\,A\,y^{-1}\right)yx^{-1} = xy^{1}yAy^{-1}yx^{-1} = xAx^{-1}A$$

$$\therefore xy^{-1} \in N_G(A)$$

$$N_G(A) < G$$

Clearly, $C_a(A) < N_G(A)$

Again, if $A = \{a\}$, we denote $N_G(A)$ by $N_G(a)$ and we shall drop a when there is no ambiguity.

i) $C_G(a) = Z(a)$

ii) $C_G(a) = \{a\}$ iff $a \in Z(G)$.

Examples :

1) If $G = S_3$ and $a = (123)$. Then $C(a) = \{I, (123), (132)\}$

   If $A = \{I, (123), (132)\}$ .Then $C_G(A) = A, N_G(A) = G$.

2) If G is a group and H < G then H, $H \subset N_G(H)$.

   $\therefore$ For $x \in H, x\,H\,x^{-1} = Hx^{-1} = H$.

3) IF G is a group and H < G then

   $H \subseteq C_a(H)$ iff H is abelian

   $H \subset C_G(H) \Leftrightarrow \nvdash h \in H, h \in C_G(H)$

   $\Leftrightarrow \nvdash h \in H, aha^{-1} = h \nvdash a \subseteq H.$

   $\Leftrightarrow ah = ha \nvdash a \in H, \nvdash h \in H \ \Leftrightarrow H$ is abelian

3.2 Group Actions

Let G be a group and S be a non-empty set. Then map $\alpha : G \times S \to S$ denoted by $(g, S) \to g \cdot S$ is an action of G on S if it satisfies the following conditions.

1) e.S = S for each $s \in S$

2) $g_1.(g_2.s) = (g_1.g_2).s$ for each $s \in S$ and each $g_1, g_2 \in G$

S is called a G - set.

Example :

1) Group acting on itself by left multiplication g.a = a a for each $g \in G, a \in G$

   i) $e.a = ea = a$ for each $a \in G$.

   ii) $g_1.(g_2.a) = g_1.(g_2.a) = g_1.(g_2.a) = (g_1 g_2)a = (g_1 g_2).a$ for each $a \in G$, for each $g_1, g_2 \in G$.

2) Group acting on itself by conjugation $g.a = gag^{-1}$ for $g \in G$ and $a \in G$

   1) $e - a = eae^{-1} = a$

   2) $g_1.(g_2.a) = g_1.\left(g_2 a g_2^{-1}\right) = g_1\left(g_2\ a\ g_2^{-1}\right)g_1^{-1} = (g_1 g_2)a\ g_2^{-1} g_1^{-1}$

   $= (g_1 g_2)a\,(g_1 g_2)^{-1} = (g_1 g_2).a$

3) A group G acts on P(G) (The set of all subsets of G) by conjugation.

   $g.S = g\ S\ g^{-1}$ for $S \in P(G)$. As in (2), it is a group action.

4) Let *n* be a positive integer. Then $G = S_n$ by $\sigma.i = \sigma(i)$ for $i \in \{1, ... n\}$. For $i \in \{1, ... n\}$ $G_i = \{\sigma \in S_n / \sigma(i) = i\}$.

5) Let *G* be a group acting on a non empty set S.

   Then, for $g \in G,$ the map $g : S \to S$ defined by $g(a) = g \cdot a$ is a permutation of S and the map $\varnothing : G \to S_n$ defined by $\varnothing(g) = \sigma_g$ is a monomorphism. (Cayley's Theorem).

3.3 Orbits and Stabilizers

If G is a group acting on a set S and $s \in S$ (is fixed) then, the stabilizer of s in G is the set $G_S = \{g \in G / g\, s = s\}$.

$G_S < G$

$e.S = S$

$\therefore e \in G_s$

Let $x, y \in G_s$ then $x - s = s, y - s = s$.

$y^{-1}.s = y^{-1}.(y.s) = \left(y^{-1}y\right).S = e.s = s$

$\left(xy^{-1}\right).s = x.\left(y^{-1}s\right) = x.s = s$

$\therefore xy^{-1} \in G_s \therefore G_s < G$

Orbit of $s \in S$ is defined as $\{g.s / s \in S\}$ and is denoted by orbit (S)

Proposition : Let G be a group and S be a subset of G. Then the number of conjugates of a subset S is $\left|G : N_a(S)\right|$ and the number $a \in S$ is $\left|G : C_G(a)\right|$.

We first prove a lemma (The proof may be read quickly)

Lemma : Let G be a group acting on a set S. Then, the relation $\sim$ on S defined by for $a, b \in S$ a $\sim b$ iff $a = g.b$ for some $g \in G$ is an equivalence relation. For each $a \in S$, the number of elements in the equivalence containing a is $\left[G : G_a\right]$, the index of the stabilizer of a.

Proof : We first prove $\sim$ is an equivalence relation. For $a \in S$, e - a = a.

$\therefore a \sim a$ ($\sim$ is reflexive)

$a, b \in S, a \sim b \Rightarrow \exists\, g \in G$ such that $a = g.b$

$\Rightarrow g^{-1}.a = g^{-1}(g - b) = \left(g^{-1}g\right).b = e.b = b$

$\Rightarrow b \sim a$ ($\sim$ is reflexive)

$a, b \in S, a \sim b, \text{b} \sim c \Rightarrow \exists\, g_1, g_2 \in G$ such that $a = g_1 \cdot b, b = g_2.c$

$\Rightarrow a = g_1.(g_2.c) = \left(g_1 g_2\right).c, g_1 g_2 \in G \Rightarrow a \sim c$ ($\sim$ is transitive)

$[a] = \{g \cdot a / g \in G\}$ (orbit of a).

Now if $b = g \cdot a \in [a]$, then $g\,G_a$ is the left cost of G_a in G and $b = g.a \to g\,G_a$

.

$\therefore$ We have a map from $[a] \to$ left costs of G_a in G defined by $g.a = gG_a$.

The map is well defined for $g.a = b.a$

$\Rightarrow h^{-1}g.a = h^{-1}.(h.a) = (h^{-1}h).a = e.a = a$

$\Rightarrow h^{-1}g \in G_a \Rightarrow hG_a = gG_a$

Similarly $hG_a = gG_a \Rightarrow h^{-1}g \in G_e \Rightarrow \left(h^{-1}g\right).a = a \Rightarrow h.a = g.a$

and the map is one - one.

The map is clearly onto, for $g \in G, g.a \in G_a \Rightarrow g.a = gG_a$.

$\therefore$ The use of elements in the equivalence classes of a = no. of left costs of G_a in G.

$\therefore$ Elements in orbit of $a = [a : G_a]$.

Proof of Proposition: $G_s = \left\{g \in G / g\,S\,g^{-1} = S\right\} = N_G(S)$.

No. of conjugates of $S = [G : N_G(S)]$ when

$S = \{a\} \Rightarrow N_G(S) = N_G(a) = C(a)$.

$\therefore$ No. of conjugates of $a = [a : G_a]$

Class equation : Let G be a finite group and let $I_1 .... I_r$ be representatives of the distinct conjugacy classes of G which are not contained in $Z(G)$. Then $|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(G_i)]$.

Proof : For $g \in G$, the conjugacy class of g is $\{g\}$ iff $g \in Z(G)$.

$\left(x\,g\,x^{-1} = g \;\forall\; x \in g \Leftrightarrow xg = gx \;\forall\; x \in G\right) \Leftrightarrow g \in Z(G)$

Let $Z(G) = \{z_1 ... z_m\}$. Let $K_1, ... K_r$ be conjugacy classes of G not contained in centre, and $I_n .... I_r$ be representatives of conjugacy classes. Then, the conjugacy classes are $\{e\}\{z_1\}...\{z_m\}, \mathrm{K}_1 ... K_r$.

This partitions G

$$\therefore |G| = \sum_{i=1}^{m} 1 + \sum_{i=1}^{r} k_i = |Z(G)| + \sum_{\substack{i=1 \\ g_o Z(G)}}^{r} |G = C(g_i)|$$

Note : $|G : (Cg_i)| O(G)$

Theorem : A group G of order p^n where p is a prime and $n \geq 1$ has non-trivial centre.

Proof : By class equation. $|G| - \sum_{\substack{i=1 \\ g_i \notin Z(G)}}^{r} |G : C(g_i)| = |Z(G)|$

As $g_i \notin Z(G)$, $|C(g_i)| \neq G$,

Now , $|G : C(g_i)| = |G| / |C(g_i)|$ so each term in $\sum_{\substack{i=1 \\ g_i \notin Z(G)}}^{r} |G : C(g_i)|$ is of the form

p^k .

Now $|G| - \sum_{\substack{i=1 \\ g_i \notin Z(G)}}^{r} |G : C(g_i)| = |Z(G)|$

$|G| = p^n$

$\therefore$ p\|G|, p\ $\sum_{i=1}^{r} |G : C(g_i)|$

$\therefore$ p\|Z (G)|

$\therefore |Z(G)| \neq 1$

$\therefore G$ has non-trivial centre.

Note : A group of order p^n , p prime, $n \geq 1$ is called a p group. A subgroup whose order is power of prime is called a p - subgroup.

Corollary: A group of order p^2 is abelian.

Proof : By class equation, $|Z(G)| \neq 1 \Rightarrow |Z(G)| = p \text{ or } p^2$

If $|Z(G)| = p^2$ then $Z(G)$=G and G is abelian.

$|Z(G)| = p$ then $G|Z(G)$ is cyclic

$\therefore G$ is abelian.

3.4 Sylow Theorems

Definition: Let G be a finite group and let p be a prime divisor of $|G|$. If p^k divides $|G|$ and p^{k+1} does not divide order $|G|$ then any subgroup of G of order p^k is called Sylow p - sub group of G.

Sylow's First Theorem :

Theorem: Let G be a finite group and p be a prime. If $p^k / |G|$ then G has a subgroup of order p^k.

Proof : We prove the result by induction on $|G|$. If $|G|$=1, the theorem is trivially true. We now assume that the theorem is true for all groups of order less than $|G|$. If G has a proper subgroup H such that p^k divides $|H|$, then by induction hypothesis H has a subgroup of order p^k, which is a subgroup of G.

So, we now assume that p^k does not divide the order of any proper subgroup of G we next consider the class equation, $|G| = |Z(G)| + \sum_{a \in Z(G)} |G : C(A)|$.

$p^k / |G|, p^k / |C(G)| \nmid a \notin Z(G)$

$\therefore \mathrm{p} / |G : (G)| \nmid a \notin Z(G)$

$\therefore$ From class equation, it follows that $p / |Z(G)|$. From the structure theorem of finite abelian groups *Z(G)* has an element *x* of order p, $x \in Z(G)$

$\therefore \langle x \rangle \lhd G$

Consider the factor group $G / \langle x \rangle, \mathrm{p}^{k-1} / |G / \langle x \rangle|$.

$\therefore$ By induction hypothesis, $G / \langle x \rangle$ has a subgroup of order p^{k-1}. This subgroup is of the form $H / \langle x \rangle$ where $H < G$ and $x \in H$.

$\left| H / \langle x \rangle \right| = p^{k-1}, |\langle x \rangle| = p$.

$\therefore |H| = p^k$ and thus *G* has a subgroup of order p^k.

Corollary 1:

Cauchy's Theorem : Let G be a finite group and p be a prime that divides the order of G. Then, G has an element of order p.

Proof : By Sylow's Theorem, G has a subgroup H of order p.

$|H| = p, \therefore H$ is cyclic and $H = \langle x \rangle$.

$\therefore O(x) = p.$

Corollary 2 : Let G be a finite group, $|G| = p^k m, k \geq 1 (p,m) = 1$ then G has a p-sylow subgroup.

Definition: **Conjugate Subgroups** :Let H, K be subgroups of a group G. We say that H, K are conjugates in G if there exists $g \in G$ such that $H = g\,k\,g$.

Sylow's Second Theorem :

Theorem : If H is a subgroup of a finite group G and $|H|$ is a power of a prime P, then H is contained in a sylow - p subgroup of G.

Proof : Let K be a Sylow p-subgroup of G. Let $C = \{K = K_1, K_2, \ldots K_n\}$ be the set of all conjugates of K in G.

Since conjugation is an automorphism, each member of C is also a Sylow p-subgroup of G. Let S_c denote the group of permutations of C.

For $g \in G$, define $\varnothing_g : C \to C$ by $\varnothing_g (K_i) = gK_i g^{-1}$.

Then, $\varnothing_g (K_i) = \varnothing_g (K_j) \Rightarrow g\,K_i g^{-1} = gK_j g^{-1}$

$\Rightarrow g^{-1} gK_i g^{-1} g = g^{-1} gK_j g^{-1} g \Rightarrow K_i = K_j$

$\therefore \phi_g$ is one one.

If $K_j \in C, K_j = hK_i h^{-1}$ for some $h \in G$

$$= gg^{-1} h\,K_i h^{-1} gg^{-1} = g\left(g^{-1}\,hK_i h^{-1} g\right) g^{-1}$$
$$= g\left(g^{-1} h\,K_i (g^{-1} h)^{-1}\right) g^{-1} = gK_i g^{-1}$$

Where $K_i = g^{-1}h\, K_i (g^{-1}h)^{-1} \in C$.

$\therefore \mathrm{K}_j = \varnothing_g(K_i), \mathrm{K}_i \in C$

$\therefore \varnothing_g$ is onto.

Thus, $\varnothing_g : C \to C$ is bijective and $\varnothing_g \in S_c$.

We define a map $T : G \to S_c$ by $T(g) = \varnothing_g$.

For $1 \le i \le n, T(gh)(K_i) = \varnothing_{gh}(K_i) = (gh)K_i(gh)^{-1} = ghK_ih^{-1}g^{-1}$

$= g\left(hK_ih^{-1}\right)g^{-1} = \varnothing_g\left(\varnothing_h(K_i)\right) = T(g)\,T(h)T(K_i)$

$\therefore \varnothing_{gh} = T(gh) = T(g)\,T(h)$.

$\therefore T$ is a group homomomorphism.

We next consider T(H).

$|H|$ is a power of p. $\therefore |T(H)|$ is also a power of p.

Now $\left|Orb_{T(H)}(K_i)\right| \backslash |\, T(H)|$

$\therefore \left|Orb_{T(H)}(K_i)\right|$ = power of p (or 1)

Now $\left|O_rb_{T(H)}(k_i)\right| = 1$ for some $i, 1 \le i \le n$

$\Leftrightarrow \varnothing_g(K_i) = K_i \nleftrightarrow g \in H \Leftrightarrow gK_ig^{-1} = K_i \nleftrightarrow g \in H$

$\Leftrightarrow g \in N(K_i) \nleftrightarrow g \in H \Leftrightarrow H < N(K_i) \Leftrightarrow H < K_i$

$\left(\because H \text{ is a } p-\text{group } a \therefore x \in N(k_i)\ \&\ x \in H \Rightarrow x \in k_i\right)$

Now $|C| = |G : N(K)|$.

$|G:K| = |G:N(K)|\,|N(K):K|, |G:K|$ is not divisible by p (K is sylow-p subgroup.

Now, $|C|$ is sum of no. of elements in the orbits.

$|G:K|$ is not divisible by p.

$\Rightarrow |G:N(K)|$ is not divisible by p. $\Rightarrow |C|$ is not divisible by p.

$|C| = \sum |orb_{T(H)} K_i|$

$\therefore$ There is at least one orbit having only one element.

$\therefore H < \mathrm{K}_i$ for some I by

Sylow's Third Theorem :

Theorem 3 : t G be a finite group and p be a prime dividing $|G|$. Then, the number of sylow p subgroups of G is equal to 1 module p and divides $|G|$.

Furthermore, any two Sylow-p subgroups of G are conjugates.

Proof : Let K be any Sylow - p - subgroups of G and $C = \{K = K, K_2, ... K_n\}$ be the set of all conjugates of K in G.

We show $n \equiv 1$ mod p.

For $g \in G$, define $\varnothing_g : C \to C$ by $\varnothing_g (K_i) = gK_i g^{-1}$.

$\varnothing_g (K_i) = \varnothing_g (K_j) \Rightarrow gK_i g^{-1} = gK_j g^{-1} \Rightarrow g^{-1} gK_i g^{-1} g = g^{-1} gK_j g^{-1} g$ $\therefore \varnothing_g$
$\Rightarrow K_i = K_j$
is one-one.

For $K_i \in C, K_i = hK_i h^{-1}$ for some $h \in G$.

$\therefore \mathrm{K}_i = gg^{-1} h \mathrm{K}_i h^{-1} gg^{-1} = g\left(g^{-1} h \mathrm{K}_i (g^{-1} h)^{-1}\right) g^{-1}$

$= g\, \mathrm{K}_j g^{-1}$ where $K_j = g^{-1} hK_j \left(g^{-1} h\right)^{-1} \in C$

$= \varnothing_g (K_j)$

$\therefore \varnothing_g$ is onto.

$\therefore \varnothing_g : C \to C$ is bijective.

$\therefore \varnothing_g \in S_c$, where S_c is the group of permutations of set C.

Let $T : G \to S_c$ be defined by $T(g) = \varnothing_g$.

Then, for $g, h \in G$.

$T(gh) = \varnothing_{gh}$

For $1 \le i \le n, \varnothing_{gh}(K_i) = (gh)K_i(gh)^{-1} = ghK_ih^{-1}g^{-1}$

$= g\left(hK_ih^{-1}\right)g^{-1} = \varnothing_g\left(hK_ih^{-1}\right) = \varnothing_g(\varnothing_h K_i) = \varnothing_g \circ \varnothing_h(K_i)$

$\therefore \varnothing_{gh} = \varnothing_g \varnothing_h$
$\therefore T(gh) = T(g)\,T(h)$

and T is a group homomorphism.

Consider $T(K)0rb_{T(K)}K_i \,/\, T(K)$.

But $|K|$ is a power of p. $|K||T(K)|$

$\therefore |T(K)|$ is a also a power of p.

$\therefore |orb_{T(K)}K_i| = 1$ when $i = 1$, and $|orb_{T(K)}K_i| =$ p otherwise

$\therefore |C| = \sum_{i-1}^{n} orb_{T(k)}\, K_i = 1 + p(n-1)m = 1 \bmod p$

We next show every sylow p subgroup is a member of C. Suppose H is a sylow p-subgroup of G which is not a member of C.

We consider T(H), then sum of the orbits size blender action of T(H) is sum of terms each divisible by p $\because |orb_{T(H)}\, k_i\, 1 \ne 1$ for any i.

$\therefore n \equiv |C| \mod p$

A contradiction.

$\therefore H \in C$

Now $n = [G : N(K)]$

$\therefore n\,|G|$

Corollary 1 :A unique sylow p - subgroup is normal.

Proof : If H is the only Sylow p - subgroup of a group G, then for each

$g \in G, g\ H\ g^{-1}$ is also a sylow - p- subgroup of G.

$\therefore g\ H\ g^{-1} = H \nrightarrow g \in G \therefore \mathrm{H} \lhd G$

Corollary 2 : A sylow - p - subgroup of a group which is normal is unique.

Proof : Let H be a sylow p - subgroup of a group G.

Then, any sylow-p-subgroup of G is conjugate to H, and is of the form gHg^{-1} for some $g \in G$.

$\mathrm{H} \lhd G \therefore g\ H\ g^{-1} = H$.

$\therefore H$ is a unique sylow p - subgroup of G.

3.5 Classification of Group of Order $\mathbb{Z}_p$ Where P is A Prime

Theorem: Let $|G| = \mathbb{Z}_p$ where p is an odd prime. Then $G \approx \mathbb{Z}_{2p}$ *or* $G \approx D_p$

Proof : By Cauchy's Theorem, G has subgroups of order 2 and p.

$\therefore G$ has an element of order 2 and an element of order p.

$G = \langle a, b \rangle, \quad |\langle b \rangle| = p$

$\therefore |G : \langle b \rangle| = 2 \ \therefore \langle b \rangle \lhd G$

$\therefore aba^{-1} \in < b >$

$\therefore ab\ a^{-1} = b^k$ *for some* $k, 1 \leq k < p$

$b^{x2} = (b^k)^k = (aba^{-1}) = ab^k a^1 = a(aba^{-1})\ a^{-1} = a^2 ba^{-2}$

$|a| = 2 \therefore b^{k^2} = b$

$\therefore b^{k^2-1} = e \Rightarrow p(k^2 - 1) \Rightarrow p(1(k+1)(k-1) \Rightarrow 1 \leq k < p$

$\Rightarrow k = 1\ or\ k + 1 = P \Rightarrow k = 1\ or\ k = p - 1$

Case 1: If k = 1,

$aba^{-1} = b \therefore ab = ba \therefore |ab| = 2p$ *and G is cyclic of order* $2p$

$\therefore G \approx Z_{2p}$

Case 2: if k = p - 1 $aba^{-1} = b^{p-1}$

$$aba = b^{p-1}$$

$$ba = ab^{p-1}$$

$\therefore G$ *is a Dihedral group*

Groups of order pq. where p,q are distinct prime.

Theorem : If G is a group of order p.q where p.q are primer, p < q and p does not divide q-1, then G is cyclic and isomorphic to Z_{pq}.

Proof : Let H be a sylow p subgroup of G and K be a sylow q subgroup of G.

The no of sylow p subgroups of G is of the form 1 + kp and divides pq.

But p x q-1

$\therefore$ k = 0 and H is the unique sylow.

p – subgroup of a $\therefore H \lhd a.$

Similarly, no of q – sylow subgroups of G are 1 + kq and divides pq.

$\therefore k = 0$

$\therefore$ K is the unique sylow subgroups of G. $\therefore K \lhd G.$

H and K are cyclic subgroups of G

Let H = <x>, k=<y>

we show xy = yx.

$xyx^{-1}y^{-1} = (yx^{-1}y^{-1}) \in H, (xyx^{-1})\, y^{-1} \in k.$

$\therefore xyx^{-1}y^{-1} \in \cap h \cap k = \{e\} \therefore |H \cap K||H||HNK|\, K$

$\therefore xy = yx$

$\therefore |< xy >| = pq = |G|$

$But < xy > \subset G$

$\therefore < xy > = G$

$\therefore G$ *is cyclic*, $\therefore G \approx Z_{pq}$

3.6 Classification 0f Groups 0f Order $\leq$ 15 Upto Isomorphism

We have already seen that groups of order 2, 3, 5, 7, 11, 13 are cyclic (prime order) and are unique upto isomorphism.

A group of order 1 is trivial and is unique upto isomorphism.

We have seen that there are two groups of order 4 upto isomorphism,

$\mathbb{Z}_4$ *and* V_4 (*or* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$) both abelian.

There are two groups of order 6 upto isomorphism cyclic $(\mathbb{Z}_6)$ or non abelian isomorphic to S_3 $(or\ D_3)$ A group of order 9 $(p^2, p = 3)$ is abelian.

There are two groups of order 10, 14 upto isomorphism cyclic and dihedral groups D_5 *and* D_7. (2p, p odd prime). The Group of order 15 is cyclic (of the form pq, 3x5) isomorphic to $\mathbb{Z}_{15}$. (Unique)

We now classify groups of order 8 and 12 upto isomorphism.

Group of order 8: There are 3 non-isomorphic abelian groups of order 8.

$\mathbb{Z}_8, \mathbb{Z}_4 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Refer to *Contemporary Abstract Algebra* by J. Gallian, pg 442.

Groups of order 12: If G is an abelian groups of order 12,

$G \approx Z_{12}$ *or* $G \approx Z_2 \oplus Z_2 \oplus Z_3$.

There are two non-isomorphic abelian groups of order 12.

There are upto isomorphism, exactly three non-abelian groups of order 12, the Dihedral group D_6 the alternating group A_4, and a group T = <a> where o(a) = 6 , o(b) = 4, $b^2 = a^3, ba = a^{-1}b$.

Note: If o(G) = 12, and G has a unique sylow 3 subgroup, G = D_6.

3.7 Summary

1) The normalizer of $A < G$ in G, is defined as $N_G(A) = \{g \in G / g\ Ag^{-1} = A\}$.

2) Let G be a group and S be a non-empty set. Then map $\alpha : G \times S \to S$ denoted by $(g, S) \to g.S$ is an action of G on S if it satisfies the following conditions.

   1) e.S = S for each $s \in S$

   2) $g_1.(g_2.s) = (g_1.g_2).s$ for each $s \in S$ and each $g_1, g_2 \in G$ S is called a G - set.

3) **Class equation :** Let G be a finite group and let $I_1....I_r$ be representatives of the distinct conjugacy classes of G which are not contained in $Z(G)$. Then $|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(G_i)]$.

4) A group G of order p^n where p is a prime and $n \geq 1$ has non-trivial centre.

5) Let G be a finite group and let p be a prime divisor of $|G|$. If p^k divides $|G|$ and p^{k+1} does not divide order $|G|$ then any subgroup of G of order p^k is called Sylow p - sub group of G.

6) **Sylow's First Theorem:** Let G be a finite group and p be a prime. If $p^k / |G|$ then G has a subgroup of order p^k.

7) **Cauchy's Theorem :** Let G be a finite group and p be a prime that divides the order of G. Then, G has an element of order p.

8) Let G be a group. A subgroup H of G is called a normal subgroup of G if aHa $^{-1} \subseteq$ H for each $a \in G$

$(or\ aha^{-1} \in H\ \ for\ each\ a \in G, each\ h \in H)$

9) **Sylow's Second Theorem :**If H is a subgroup of a finite group G and $|H|$ is a power of a prime P, then H is contained in a sylow - p subgroup of G.

10) **Sylow's Third Theorem:** If G be a finite group and p be a prime dividing $|G|$. Then, the number of sylow p subgroups of G is equal to 1 module p and divides $|G|$.

Furthermore, any two Sylow-p subgroups of G are conjugates.

11) A unique sylow p - subgroup is normal.

12) A sylow - p - subgroup of a group which is normal is unique.

13) Let $|G| = \mathbb{Z}_p$ where p is an odd prime. Then $G \approx \mathbb{Z}_{2p}$ *or* $G \approx D_p$

14) If G is a group of order p.q where p.q are primer, p < q and p does not divide q-1, then G is cyclic and isomorphic to Z_{pq}.

3.8 Unit And Exercises

1) For the given group G and the H subgroup of G. Show that $C_G(H) = H$ and $N_a(H) = G$.

   i) $G = D_4, H = \{1, b, a^2, a^2b\}$ where $a^4 = e = b^2\ ba = a^3b$

   ii) $G = S_3, H = \{1, (123), (132)\}$.

2) Find all groups (up to isomorphism) of order 99.

   Answer : Let G be a group of order 99. Let H be a sylow 3 subgroup of G and K be a sylow 11 subgroup of G Then, no of sylow 11 subgroups of G is congruent to 1 mod 11 and divides 99 $\therefore$ K is unique sylow subgroup of G.

$\therefore K \lhd G.$
Similarly $H \lhd G, H \cap K = \{e\}$

It follows that elements from H and K commute and therefore $G = H \times K$

$\therefore G$ *is abelian*
$G \approx Z_3 \oplus Z_{33}$ *or* $G \approx Z_{99}$

3) Determine all groups of order 66 upto isomorphism.

   Answer: Let G be a group of order 66. Let H be a sylow 3 subgroup of G and K be a sylow 11 subgroup 8 G.

Then, 1 is the only positive divisor of 66 which is congruent to 1 mod 11,

Therefore , $K \lhd G.$

$\therefore HK < G$ *and* $O(HK) = 33\ (33 = 3 \times 11$ *and* $3 \times 11 - 1)$
$\therefore HK$ *is cyclic*

Let HK = < x >, HK has index 2 in G $\therefore HK \lhd G.$

Let $y \in G$ *and* $|y| = 2.$

$yxy^{-1} \in < x >$

Let $yxy^{-1} = x^i$ *for some* i *for* 1 *to* 32, *Now* $|x^i| = |x|$

$yx = x^i y,\ x = y^{-1}(x^i)\ y = \left(y^{-1}xy\right)^i = \left(x^i\right)^i = x^{i^2}$

$x^{i-2} = e,$

$\therefore 33 \setminus i^2 - 1$
$\therefore 11 / i + 1 \text{ or } 11 / i - 1$

$\therefore i = 0,\ \pm 1,\ i = 11 \pm 1, i = 11 \pm 1 \text{ or } i = 33 \pm 1.$

$\therefore\ i = 1, 10, 23 \text{ or } 32.$

$\therefore$ There are at most 4 groups of order 66. we observe that $Z_{66}, D_{33}, D_{11} \oplus Z_3 \text{ and } D_3 \oplus Z_4$ are of order 66, and no two of them are isomorphic.

4) Show that the only group of order 255 is Z_{255}.

Proof:- Let G be a group of order 255.

255 = 3.5.17.

Let H be a 17 sylow sub group of G Then, number of 17 sylow subgroups of G is congruent to 1 mod 17 and divides 255.

The 17 sylow subgroup is unique.(Divisors of 255 are 1,3,5,15,51,85)

$\therefore H \lhd G\ (H \approx Z_{17})$
$\therefore N(H) = G$

$\therefore \left|N(H) / C(H)\right| \text{ divides } \left|Aut\ (H)\right| = \left|Aut\ \mathbb{Z}_{17}\right| = \left|U(17)\right| = 16$

Since $\left|N(H) / C(H)\right| = \left|G / C(H)\right| / 16$ we have $\left|N(H) / C(H)\right| = 1$

$\therefore G = C(H)$

$\therefore$ every element of G commutes with every element of H.

$\therefore H \subset Z(G)$
$\therefore 17 \left|Z(G)\right|, \left|Z(G)\right| 255$

$\therefore \left|G / Z(G)\right| = 15, 5, 3 \text{ or } 1$
$\therefore G / Z(G) \text{ is cyclic}$

$\therefore G$ *is abelian*

$\therefore G$ *is cyclic*

5) Show that a group of order pqr, where p,q,r are distant primer is cydic.

6) If (G) = 36 and G is non-abelian, probe that either G has more than one 2 sylow subgroup or more than one 3 sylow subgroup.

7) Show that a group of order 56 has a proper non-triral normal subgroup.

8) Let G be a group of order 60. If the sylow 3 subgroup is normal, show that the 5 sylow subgroup is also normal.

❖❖❖❖

4

INTRODUCTION TO RING

Unit Structure

4.0 Objective

The objective of the this unit is to introduce the concepts of

- Ring integral domain and fields with example.
- The characteristic of ring.
- How to check a given subset of ring is subring?

4.1 Introduction

Basically there are two operations '+' and '**.**' which we can apply on scalars & vectors. We know how to add and multiply two scalars. In vector space, we saw two operation vector addition and scalar multiplication. In group theory we have seen a set with one operation whether addition or multiplication satisfying certain property. So for we had not seen any set with both operation addition as well as multiplication. Ring is one such algebraic structure which has both these operation.

Loosely speaking ring means closed structure that is why (may be) an algebraic structure which is closed with addition and vector multiplication is called as ring.

4.2 Ring

A ring R is set together with two binary operations + (addition) and '$\cdot$' (Multiplication) satisfying

i) *(R, +)* is an abelian group.

ii) `.' is associative : i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all *a, b, c,* $\in R$.

iii) The distributive laws hold in R.

i.e. *for all* $a, b, c \in R$ $(a+b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b+c) = a \cdot b + a \cdot c$

Before we see example of ring let understand versions terms involved in ring with the help of following remarks.

Remarks:

1) If R is ring, then (R, +) is abelian group. Multiplication ($'\cdot'$) need not be commutative. When $'\cdot'$ is commutative we say R is commutative Ring.

2) As (R,+) is abelian group, $\exists$ on element say `0', such that $a + o = o + a = a \; \forall \; a \in R$. This element `0' is called as zero element or additive identity of R. A ring may, may not have multiplicative identity. But when it has, i.e. if ring R has an element 1 such that $a \cdot 1 = 1 \cdot a = a$ for all a $\in$ R then such element `1' is called as unity in R & R is said to be ring with unity. Note that $0 \neq 1$. Throughout the course we assume R is ring with unity otherwise

3) For each a in $R, \exists\, b \in R$ such that $a + b = 0$ such element is called additive inverse of '*a*' and is unique.

4) A non zero element *'a'* of *R* is said to be unit if there exists *b* in *R* such that *a .b = 1. b* is said to multiplicative inverse of *a*. Multiplicative inverse of element may or may not exists.

5) An element $a \in R$ is said to be zero divisor if there exists $b \neq o$ such that $a \cdot b = o$. Note that zero divisor cannot be unit.

(as if *a* is unit and zero divisor then $\exists\, b, c$ *such that* $a \cdot b = 1 = b \cdot a$ and $ac = 0$

$\Rightarrow b \cdot a \cdot c = b \cdot c \Rightarrow 1 \cdot c = 0 \Rightarrow c = 0$ a contradiction.

6) A commutative ring (with unity) is said to Integral domain (ID) if it has no non zero zero divisor. (i.e. in *R* the only zero divisor is zero element 0).

One more way is there to define ID is that, whenever $ab = 0$ in $ID \Rightarrow a = 0$ or $b = 0$. Not that if R is not ID above relation may not be satisfied as in $\mathbb{Z}_6$ $\bar{2}.\bar{3} = \bar{0}$ but $\bar{2} \neq 0, \bar{3} \neq 0$.

In case of ID cancellation law hold.

as if $ab = a.c \Rightarrow ab - ac = 0 \Rightarrow a.(b-c) = 0 \Rightarrow a = 0 \; or \; b - c = 0 \; (since \; ID)$
$if \; a \neq o \Rightarrow b = c \; \therefore ab = ac \Rightarrow b = c$ if $a \neq o$

7) In the definition of units we have seen that every element of ring R need not be unit.

A commutative ring in which every non zero element is unit is called as field.

A commutative ring R (with unity) is said to be field if for all $a \neq 0$, in R, there exists b in R such that $a.b = 1$.

They are some standard examples of ring which are easy to show. We will list then without proving.

1)

Set	Commutative Ring	Zero element	Unity	Zero Divisor	ID	Units	Field
$(\mathbb{Z}, +, \cdot)$	Yes	0	1	No	Yes	± 1	No.
$(\mathbb{Q}, +, \cdot)$	Yes	0	1	No	Yes	all non Zero element	Yes
$(\mathbb{R}, +, \cdot)$	Yes	0	1	No	Yes	All non Zero element	Yes
$(\not\subset, +, \bullet)$	Yes	0	1	No	Yes	all non zero element	Yes
$M_n(\mathbb{R})$	No.	Null Matrix	Identify Matrix	Yes	No	$A \in M_n(\mathbb{R})$ $s.t. \lvert A \rvert \neq 0$	No.
$\mathbb{Q}[x]$, $\mathbb{R}[x]$ & $\mathbb{Z}[x]$	Yes	Zero Polynomial	1	No	Yes	Non Zero Constant Poly.	No

2) IF R is a ring than the set $R \times R = \{(a,b) : a, b \in R\}$ with + and $\cdot$ define as $(a,b) + (a,d) = (a+c, b+d)$ & $(a,b) \cdot (c,d) = (ac, bd)$ is not integral domain as if a,b $\in$ R, $a \neq 0, b \neq 0 \; then \; (a,0).(0,b) = (0,0)$ Hence not ID. (a,0) is zero element of this ring and if 1 is unity in R. then (1,1) is unity in R x R. If R is commutative, R x R is also commutative.

3) Let R = $\mathbb{Z}$ [i] = $\{a+bi : a,b \in \mathbb{Z}, i=\sqrt{-1}\}$ is also ring with 0 as zero element and 1 as unity. This is commutative ring with no non zero divisor and hence integral domain. Note that only ± 1 and $\pm i$ has multiplicative inverse (as ($\pm$ 1) ($\pm$ 1) = 1, *i (-i)* = 1). So it is not field.

This ring is known as ring of Gaussian integers.

These are some important example of rings. Many examples can be found in reference books. We end this section by given two more important class of ring.

4) Consider $\mathbb{Z}_n = \{\bar{0}, \bar{1}, .. \overline{n-1}\}$ the set of residue classes modulo *n*. define + and $\cdot$ as $\bar{a}+\bar{b}=\overline{a+b}$ and $\bar{a}.\bar{b}=\overline{ab}$ Then $\mathbb{Z}_n$ is ring.

Some important results about $\mathbb{Z}_n$.

i) Every non zero element of $\mathbb{Z}_n$ is either zero divisor or unit.

Proof: - Let $\bar{a} \in \mathbb{Z}_n$ such that $\bar{a} \neq \bar{0}$ suppose $\bar{a}$ is not zero divisor.

We will show that $\bar{a}$ is unit.

Claim: *(a,n) = 1*. ((a, n) means G.C.D. of *a* and *n*)

Suppose *(a, n) = d, d > 1*. Then *d/a* and *d/n*.

Let $b = \frac{n}{d}, \bar{b} \in \mathbb{Z}_n$ *and* $\bar{b} \neq \bar{0}$ and

$$\overline{ab} = \bar{a}\left(\overline{\frac{n}{d}}\right) = \left(\overline{\frac{a}{d}}\right)\bar{n} = \left(\frac{\bar{a}}{d}\right)\bar{0} = \bar{0}.$$

$\Rightarrow$ $\bar{a}$ is zero divisor which is not the case.

Hence *(a, n) = 1*.

Therefore there exists *x, y* $\in$ $\mathbb{Z}$ such that

$ax + yn = 1$

$\therefore \bar{a}\bar{x} + \bar{y}\bar{n} = \bar{1} \Rightarrow \bar{a}\bar{x} = \bar{1}$ $\left(\because \overline{yn} = \bar{o}\right)$

$\therefore \bar{x}$ is multiplicative inverse of $\bar{a}$.

$\therefore \bar{a}$ is unit.

Hence if $\bar{a}$ is not zero divisor then $\bar{a}$ is unit.

(ii) If *n* is prime then $\mathbb{Z}_n$ is field.

$\because$ *n* is prime, therefore $(a,n)=1$, for all *a*, *1 < a < n*.

Hence for any *a* in $\mathbb{Z}_n$ multiplicative inverse of *a* exists.

5) **Polynomial Ring**: The polynomial plays very important role in Algebra. Finding root of polynomial is one of the central problems of Algebra. Set of all polynomial over $\mathbb{R}$ with respect to operation polynomial addition and multiplication from a ring. Let we recognize it's important and discuss it separately.

Definition: Let *R* be a commutative ring. The set of formal symbols

$R[x]=\{a_n\,x^n+a_{n-1}x^{n-1}+..+a_1\,x+a_o : a_i :\in R, n$ is non negative integer$\}$ is called the ring of polynomials over *R* in indeterminate *x*.

Remark:

i) Let $f(x)=a_n\,x^n+a_{n-1}\,x^{n-1}+..+a_1\,x+a_o$ and

$$g(x)=b_m\,x^m+b_m\,x^{m-1}+..+b_1\,x+b_o$$

Then

$$f(x)+g(x)=(a_s+b_s)\,x^s+(a_{s-1}+b_{s-1})\,x^{s-1}+..+(a_1+b_1)\,x+a_o+b_o$$

where *s = max {m, n}*

and $f(x).g(x)=c_{m+n}\,x^{m+n}+c_{m+n-1}x^{m+n-1}+..+c_1x+c_o$

were $c_i=\sum_{k=o}^{i} a_{i-k}\,b_k$

Definition: Let $f(x)=a_n\,x^n+a_{n-1}x^{n-1}+..+a_1x+a_o$

If $n\neq 0$ then *n* is called degree of *f(x)*, and a_n is called leading coefficient of *f(x)*. If $a_n=1$, then polynomial is called monic polynomial. The degree of polynomial is denoted by deg $f(x)$. The polynomial $f(x)=0$ has no degree and is called zero polynomial. The polynomial $f(x)=a_0$ is called constant polynomial.

If *R* is commutative ring with 0 as zero element and 1 as unity then $R[x]$ is also commutative ring with zero element as zero polynomial 0 and unity as constant polynomial $f(x)=1$. If *R* is integral domain then $R[x]$ is also. But $R[x]$ is not field even though *R* is field as the only units in $R[x]$ are constant polynomial.

In this next unit we have one separate chapter for polynomial ring where we discuss one important concept of ring irreducible polynomial.

Let we discuss some theorems giving relationship between integral domain and fields.

Theorem 1: Every field is integral domain.

Proof : Let *R* be a field and let $a, b \in R$ such that $ab = 0 \quad \rightarrow (1)$

Let assume $a \neq 0$. We will show *b = 0*.

Since $a \neq 0$. and R is field.

$\therefore \exists\, x \in R$ such that $a \cdot x = 1 = x \cdot a$.

Multiply both side of (1) by x we get

$x \cdot a \cdot b = x \cdot 0$

$\therefore (xa)\, b = 0$

$\Rightarrow 1.b = 0 \Rightarrow b = 0$

And as R field, therefore R is commutative ring.

Therefore R is integral domain.

Note : Every field is integral domain. But every integral domain need not be field. For example $\mathbb{Z}$ which integral domain but not field.

A ring R is said to be finite ring if R is finite Set.

Theorem 2: Every finite integral domain is field.

Proof : Let *R* be finite integral domain.

Therefore *R* is commutative ring.

Let a $\in$ R be such that $a \neq 0$

then $a, a^2, a^3, \ldots \in R$. But as R is finite all this indices may not be distinct.

That is there exist $i \neq j$ such that $a^i = a^j$

let i > j then $a^i \,.\, a^{-j} = a^j \,.\, a^{-j}$

$$\Rightarrow a^{i-j} = 1$$

Also note that *i – j > 0*

Therefore $a^{i-j-1} \in R$ such that $a.a^{i-j-1} = a^{i-j} = 1$

Therefore a^{i-j-1} is multiplicative inverse of a. $a \neq 0$

Therefore all non zero element of R has multiplicative inverse.

Therefore R is a field ·

4.3 Charctristic of Ring

Let R be a finite ring. Then (R, +) is a finite abelian group. If $O(R) = m$ then for all $a \in R$, $ma = 0$. Hence for finite ring $(R, +)$ there exist $m \in \mathbb{N}$ such that $m \cdot a = 0$ for all $a \in R$.

Note that such number is not unique. If m is one such number then, all multiple of m satisfies same condition. We are interested smallest positive integer n such that $n \cdot a = 0$, such number is called characteristic of ring.

Definition: Let R be a ring. A least positive integer n such that $n \cdot a = 0$ for all a $\in$ R is called characteristic of R & is denoted by char R. If no such number exists then char $R = 0$.

For example char $\mathbb{Z}$ = char $\mathbb{Q}$ = char $\mathbb{R} = 0$, char $\mathbb{Z}_n = n$.

Characteristic of infinite ring is obviously zero. But characteristic of finite ring is also not easy to find. The theorem given below helps to find characteristic of ring.

Theorem 3: The characteristic of ring R with unit 1 is n if and only if n is least positive integer such that $n \cdot 1 = 0$.

Proof : Let assume that char $R = n$

$\therefore$ n is least positive integer such that $n.a = o$ for all $a \in R$.

$\therefore$ $n \cdot 1 = 0$

Conversely let n is least positive integer such that $n \cdot 1 = 0$.

To prove that char R = n.

Let $a \in \mathbb{R}$ be arbitrary.

Consider $n \cdot a = n \cdot 1 \cdot a = (n \cdot 1) \cdot a = 0 \cdot a = 0$ and n is least such positive integer.

$\therefore$ char $R = n$.

Theorem 4: The characteristic of integral domain is (hence field) is either zero or prime.

Proof: Let R be an integral domain.

If char $R = 0$ Then nothing to prove.

Hence assume char $R = n$, $n \neq 0$

To prove n is prime number,

Let assume $n = x.y$ where $1 < x, y < n$

$\because$ char $R = n$

$\therefore$ for each $a \in R$, $n \cdot a = 0$

i.e. $n.a^2 = 0$

i.e. $(xy)a^2 = 0$

$\therefore (xa)(ya) = 0$

$\therefore x.a = o$ or $y.a = o$ (since R is integral domain)

which is not possible as $x, y < n$ and char $R = n$.

Hence no such x, y exists

$\therefore$ n is prime

Corollary 1: Characteristic of a finite field is prime.

Proof: Let F be a field.

$(F, +)$ is a finite group.

Hence order of F exist & Let $o(F) = m$

$\therefore m \cdot 1 = 0$.

Let n be least positive integer such that $n \cdot 1 = 0$ as F is field and hence integral domain. Therefore by above theorem n is prime.

4.4 Subring

Subrings are non empty subset of a ring which itself is ring with respect to the operation of ring.

So if we want to prove a non empty subset S of ring R is subring, one has to prove all the property of ring, which is a lengthy procedure. The following theorem gives a easy method to determine whether a given subset of Ring R is subring or not.

Subring Test:

Theorem 5: Let s be a non empty subset of ring R. Then S is subring of R if for any $a, b \in S$,

$a\text{-}b \in S$ and $a \cdot b \in S$.

Proof: Let S be subring of R.

Then S be itself a ring.

Therefore for any $a, b \in S$, $a\text{-}b \in S$ and $a.b \in S$

Conversely let assume that S be non empty subset of R, such that $a - b$ and $a.\ b \in S$ whenever

$a, b \in S$.

To prove S is subring.

$\because$ for a, b $\in$ S a-b $\in$ S

$\therefore$ (S, +) is subgroup of (R, +)

$\therefore$ (S, +) is abelian group.

For $a, b \in S,\ a \cdot b \in S$

S is closed under multiplication .

Also as multiplication ($'\cdot'$) distribute over addition in R and therefore in S also.

Therefore S is a ring.

Hence S is subring of R

Eg:- 1) Let $R = M_2(\mathbb{Z})$

i) $S_1 = \left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} : a, b \in \mathbb{Z} \right\}$

Let $A, B \in S,$ *and let* $A = \begin{bmatrix} a & a \\ b & b \end{bmatrix} B = \begin{bmatrix} x & x \\ y & y \end{bmatrix}$

then $A - B = \begin{bmatrix} a-x & a-z \\ y-b & y-b \end{bmatrix} \in S_1$

and $AB = \begin{bmatrix} ax+ay & ax+ay \\ bx+by & bx+by \end{bmatrix} \in S_1$

$\therefore S_1$ is subring of R

ii) $S_2 = \left\{ \begin{bmatrix} a & a-b \\ a-b & a \end{bmatrix} : b, a \in \mathbb{Z} \right\}$

Let $A=\begin{bmatrix} a & a-b \\ a-b & a \end{bmatrix}$ and $B=\begin{bmatrix} x & x-y \\ z-y & x \end{bmatrix}\in S_2$

$$A-B=\begin{bmatrix} a-x & a-b-x+y \\ a-b-x+y & a-x \end{bmatrix}\in S_2$$

$$A.B=\begin{bmatrix} ax+(a-b)(x-y) & a(x-y)+(a-b)x \\ (a-b)x+a(x-y) & (a-b)(x-y)+ax \end{bmatrix}\in S_2.$$

$\therefore S_2$ is subring

2) Let $R=\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}$

$S=\{(a,b,c)\in R \,/\, a+b=c\}$

Take a = (1, 2, 3), b = (4, 2, 6) then a, b $\in$ S

a.b = (1, 2, 3)$\cdot$ (4, 2, 6) = (4, 4, 18)

but 4 + 4 $\neq$ 18 $\therefore$ (4, 4, 18) $\notin$ S

Hence S is not subring.

4.5 Summary

1) A ring R is set together with two binary operations + (addition) and '$\cdot$' (Multiplication) satisfying

   i) *(R, +)* is an abelian group.

   ii) '$\cdot$' is associative : i.e. $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ for all *a, b, c,* $\in R$.

   iii) The distributive laws hold in R.

   i.*e. for all* $a,b,c\in R\,(a+b)\cdot c=a\cdot c+b\cdot c$ and $a\cdot(b+c)=a\cdot b+a\cdot c$

2) Every field is integral domain.

3) Every finite integral domain is field.

4) Smallest positive integer n such that $n\cdot a=0$, such number is called characteristic of ring.

5) The characteristic of ring R with unit 1 is n if and only if n is least positive integer such that $n\cdot 1=0$.

4.6 Unit and Exercises

1) Show that $\mathbb{Z}\times\mathbb{Z}$ under component wise addition and multiplication is a ring. Is it an integral domain? Justify.

2) Let $(R+,\cdot)$ be a ring with multiplicative identity 1_R. Show that $(R_1,\oplus,\odot)$ is a ring where, $a\oplus b=a+b-1_R$ and $a\odot b=a+b-ab$

3) Show that the ring

(i) $\mathbb{Z}\left[\sqrt{d}\right]=\left\{a+b\sqrt{d}:a,b,\in\mathbb{Z}\right\}$ d is an integer is integral domain.

(ii) $\mathbb{Q}\left[\sqrt{d}\right]=\{a+b\sqrt{d}:a,b\in\mathbb{Q}\}$, d is an integer is field.

4) Let $R = \{0,2,4,6,8\}$ under addition and multiplication modulo 10. Prove that R is field.

5) Let F be a field of order 2^n. Prove that char $F = 2$.

6) Let D be an integral domain of characteristic P. For any $x,y\in D$ show that

(i) $(x+y)^p=x^p+y^p$ (ii) $(x+y)^{p^n}=x^{p^n}+y^{p^n}$ for all $n\in N$

(ii) Find element x and y in a ring of characteristic 4 such that $(x+y)^4\neq x^4+y^4$.

7) Let F be a field and let K be a subset of F with at least two elements. Prove that K is subfield. (i.e. prove that for any $a,b\in F,b\neq 0$ in K, $a-b$ and $a\cdot b^{-1}\in K$)

(This is known as subfield Test)

8) An element $a \in R$ is said to be nilpotent element if there exist $n\in\mathbb{N}$ such that $a^n=0$. Prove that a $\in$ R is nilpotent then 1 – a is unit in R.

(Hint : $a^n=o\therefore 1-a^n=1$

9) An element a $\in$ R is said to be idempotent if $a^2=a.$ Prove that

(i) The set of idempotent of a commutative ring is closed under multiplication.

(ii) The only idempotent in an integral domain is 0 and 1..

10) Determine all zero- divisors, units & idempotent elements in (i) $\mathbb{Z}_{18}$ (ii) $\mathbb{Z}_3 \times \mathbb{Z}_6$ (iii) $\mathbb{Z} \times \mathbb{Q}$.

11) Let *d* be a positive integer. Prove that $\mathbb{Q}[\sqrt{d}\,] = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ is a field.

12) In the following examples, show that S is a subring of the given Ring R.

(i) $S = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a + c = b + d \right\} \quad R = \mathrm{M}_2(\mathbb{R})$

(ii) $S = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} : a, b \in Q \right\} \quad R = M_2(\mathbb{Q})$

13) Determine which of the following are subrings of $(\mathbb{Q}, +, \cdot)$. Justify your answer.

(i) $S = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ (a, b) = 1, b \text{ is odd} \right\}$

(ii) $S = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, (a, b) = 1, b \neq 0, b \text{ is even} \right\}$

(iii) $S = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0, (a, b) = 1, a \text{ is odd} \right\}$

(iv) $S = \left\{ x^2 : x \in \mathbb{Q} \right\}$

(v) $S = \left\{ x : x \in \mathbb{Q}, x > o \right\}$

14) Let $H = \left\{ \begin{bmatrix} z & w \\ w & z \end{bmatrix}, z, w \in \mathbb{R} \right\}$ Show H is a non commutative subring of $M_2(\mathbb{R})$ in which every non zero element has an inverse with respect to multiplication.

❖❖❖❖

5

IDEAL AND QUOTIENT RING

Unit Structure

5.0 OBJECTIVE:

- The objective of this chapter is to introduce the concept of
- Ideal and its importance.
- Theorem used to determine whether given set is ideal or not.
- Quotient ring
- Types of ideal i.e. Prime and maximal ideal.
- Their relation with Quotient ring.

5.1 Ideals

Our aim is to define something similar to quotient space (in case of vector space) and quotient group (in case of group). Note that if W is any subspace of vector space we can very well defined quotient space which itself a vector space. To define quotient group of group G we need special type of subgroup called as normal subgroup. In group theory we have seen that if H is normal subgroup of G then G/H is defined.

Quotient ring is also similar to quotient space (or group). It is denoted as *R/I* where *R* is ring and *I* must be similar to normal subgroup (not just subring).

This leads to concepts of ideal.

Definition (Ideals): Let *R* be a ring a subring *I* of *R* is said to be ideal of *R* if for $x \in R,\ a \in I, xa$ and $ax \in I$

That is ideals are those subring of *R* which absorbs the element of *R*.

If *I* is proper subset of *R* then *I* is said to be proper ideal of *R*.

A ring having no proper ideals is called as simple ring.

Ideal Test: A non empty subset *I* of ring *R* is an ideal of *R* if

(i) a-b $\in$ I whenever a, b $\in$ I

(ii) (ii) $x \cdot a, a \cdot x \in I$ whenever $a \in I$ and $x \in R$.

Example :

1) For any $n \in \mathbb{Z}, n\mathbb{Z}$ is ideal of $\mathbb{Z}$ as $n\mathbb{Z}$ are only subgroup of $\mathbb{Z}$.

2) Let $R = \mathbb{R}[x]$ the set of all polynomial with real coefficient.

Let A be subset of all polynomials with constant term zero. Then *A* is ideal of *R*. As let *f(x), g(x)* $\in$ *A*

Therefore $f(0) = 0 = g(0)$ (since constant term of f & g is zero)

therefore if $h(z) = f(x) - g(x)$ *then* $h(0) = 0$

Also for any $k(x) \in \mathbb{R}[x]$

$k(0) \cdot f(0) = k(0) \cdot 0 = 0$, there fore $k(x) f(x) \in I$

Therefore I is ideal of $\mathbb{R}$.

Note that $\mathrm{I} = \{f(x) \in R : f(x) = a_n x^n + ... + a_1 x\}$

$= \{f(x) \in R : f(x) = x(a_n x^{n-1} + ... + a_1)\}$

$= \{f(x) \in R : f(x) = x.g(x)\}$

$= < x >$

3) Let R be ring of the real valued functions of real variable. The subset of S of all differentiable functions is a subring of R but not an ideal of R.

$|x| \in R$, $|x|$ is not differentiable, $x \in$ S, since x is differentiable but $|x| \cdot x \notin S$ as $|x| \cdot x$ is not differentiable hence S is not an ideal.

4) Let R be a ring and $a \in R$. Then, $aR = \{ar : r \in R\}$ is ideal of R, known as principal ideal of R generated by a.

Principal ideal plays very important role in ring theory. An integral domain in which every ideal is principal ideal is known as principal Ideal Domanin which we will see in coming chapters.

Theorem 1: Let I, J be any ideal of ring R.

Then $I + J = \{x + y : x, \in I, y \in I\}$, $IJ = \left\{ \sum_{n=1}^{k} x_n\, y_n : x_n \in I, y_n \in J \right\}$

(i.e., IJ is sum of finite product of element of I and J), and $I \bigcap J$ is ideal of R.

Proof:

(i) Let a, b $\in$ I + J

$\therefore a = x_1 + y_1$ *and* $b = x_2 + y_2$

then $a - b = (x_1 - x_2) + (y_1 - y_2 \in I + J$

Also for any $r \in R$, $a.r = (x_1 + y_1) \cdot r = x_1\, r + y_1\, r \in I + J$

as I, J *are ideals, therefore* $x_1 r \in I$ *and* $y_1 r \in J$)

Similarly r.a $\in$ I + J

Hence I + J is ideal.

(ii) Let a, b $\in$ I, J

$a = \sum_{i=1}^{n} x_i\, y_i$ *and* $b = \sum_{j=1}^{m} p_j\, q_j$ where $x_i, p_j \in I$ *and* $y_i, q_j \in J$

then a – b = $\sum_{i=1}^{n} x_i\, y_i - \sum_{j=1}^{m} p_j\, q_j = \sum_{l=1}^{n} x_1\, y_i + \sum_{j=1}^{m} (-p_j)\, q_j \in IJ$

Let r $\in$ R

$ar = \left(\sum_{L=1}^{n} x_1\, y_1 \right) r = \sum_{i=1}^{n} (x_i\, r)\, y_i \in IJ$ $(Since\ I\ is\ ideal, therefore\ xr \in I)$

Similarly ra $\in$ IJ.

Therefore IJ is ideal

Theorem 2: A Field is simple ring. That is the only ideal in a Field is {0} and F itself.

Let A be any non zero ideal of field F.

Let $a \in A$, a $\neq$ 0. F is field therefore $\exists$ b $\in F$

Such that a.b = 1

But A is ideal also.

$\therefore 1 = a.b \in A$ (Since I is ideal, r.a$\in$ I for r $\in$ F)

$\therefore$ for any $x \in R$, F x.1 = x $\in$ A

$\therefore F \subseteq A$

$\Rightarrow F = A.$

5.2. Quotient Ring

Let R be a ring and I be its ideal define R/I = $\{x + I : x \in R\}$

Define `+' and `.' as

$(x+I)+(y+I) = (x + y) + I$ and $(x + I)(y + I) = x y + I$

We claim that R / I is a ring with respect to above operation, called quotient ring.

(i) First we prove that '+' and '$\cdot$' defined as above is well defined.

Let assume that $x+I=x'+I \text{ and } y+I=y'+I$

$therefore \Rightarrow x - x' \in I \text{ and } y - y' \in I$ (By definition of cosets)

$\Rightarrow x - x' + y - y' \in I \Rightarrow (x + y) - (x' + y') \in I$

$\Rightarrow x + y + I = x' + y'^{1} + I \Rightarrow (x + I) + (y + I) = (x' + I) + (y' + I)$

$\therefore$ + is well defined.

also as $x - x', y - y' \in I$

$therefore \text{ let } x - x' = a, y - y' = b \text{ for some } a, b \in I$

$\therefore x = x' + a \text{ and } y = y' + b$

$\therefore xy = (x' + a)(y' + b) = x' y' + x' b + y' a + ab$

$\therefore \quad xy + I = x'y' + x' b + y' a + ab + I = x' y' + I$ (Since I is ideal therefore $x' b + y' a + ab \in I$, hence $x' b + y' a + ab + I = I.$

$\therefore (x + I)(y + I) = (x' + I)(y' + \mathrm{I})$

$\therefore$ '$\cdot$' is well defined.

As $(R, +)$ is abelian group

$\therefore (R / I, +)$ is also abelian group.

and $\big((x + I)(y + I)\big)(z + I) = (xy + I)(z + I) = xyz + I$

Similarly $(x + I)\big((y + I)(z + I)\big) = xyz + I$

$\therefore$ '$\cdot$' is associative.

$$\big((x + I) + (y + I)\big) \cdot (z + I) = \big((x + y) + I\big)(z + I)$$
$$= (x + y) \cdot z + I = (xz + yz) + I = (xz + I) + (yz + I)$$
$$= (x + I)(z + I) + (y + I)(z + I)$$

Therefore '$\cdot$' is distribute over '+'.

Hence *(R / I, +, ·)* is ring.

Remark :

1) If I is subring only, R/I is not defined.

2) If 0 is zero element of R then 0 + I = I is zero element of R/I.

3) If R is commutative ring then quotient ring R/I is also commutative.

4) If R is ring with unity 1, then R/I is also ring with unity 1 + I.

Examples :

1) $\mathbb{Z}/4\mathbb{Z} = \{4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$

2) $2\mathbb{Z}/6\mathbb{Z} = \{6\mathbb{Z}, 2\mathbb{Z}+6\mathbb{Z}, 4\mathbb{Z}+6\mathbb{Z}\}$

3) Let R = $\mathbb{Z}[i]$, the ring of Gaussian integer and $I = \langle 2-i \rangle$

then $R/I = \{a+bi+\langle 2-1 \rangle : a + bi \in R\}$

$\therefore\ 2 - i \in \langle 2 - i \rangle = I$

$\therefore\ 2 - i + I = I$ *in* $R/I\ \ \therefore 2 - i = 0$ *in* R/I

$\therefore 2 = i$ *in* $R/I \therefore 4 = -1$ *in* R/I

$\therefore 5 = 0$ *in* $R/I \therefore$ *Let* $13 + 51i \in R$

using 2 = i, and 5 = 0 we get

$13 + 51i + I = 3 + 5 \times 2 + (5 \times 10 + 1)(2) + I$

$= 3 + 2 + I = 5 + I$ *(Since 5 = 0 in R/I)* $= I$

Thus using 2 = *i*, 5 = 0 in *R/I* any element $a + bi + I$ of *R/I* is reduced to one of the element $I,\ 1 + I,\ 2 + I,\ 3 + I$ *or* $4 + I$.

Also note that all this elements are distinct as additive order of $1 + I$ is *5* Hence $R/I = \{I,\ 1 + I,\ 2 + I,\ 3 + I,\ 4 + I\}$

4) Let $R = M_2(\mathbb{Z})$ *and* $S = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in 2\mathbb{Z}\right\}$ then *S* is ideal of *R*.

Let we find *R/S:*

Take one example. Consider on element

$$A = \begin{bmatrix} 3 & -4 \\ 1 & 7 \end{bmatrix} \in S$$

$$A + S = \begin{bmatrix} 3 & -4 \\ 1 & 7 \end{bmatrix} + S = \begin{bmatrix} 1+2 & -4 \\ 1 & 1+6 \end{bmatrix} + S$$

$$= \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 2 & -4 \\ 0 & 6 \end{bmatrix} + S = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} + S, \left(since \begin{bmatrix} 2 & -4 \\ 0 & 6 \end{bmatrix} \in S \right)$$

This means that it $\begin{bmatrix} l & m \\ n & p \end{bmatrix} + S$ is element of *R/S* then the only choice of *l, m ,n , p* are *0* and *1* Hence there total $2^4 = 16$ element in *R/S*, therefore |*R/S*|=*16.*

5) Let $\mathbb{R}[x]$ denote the ring of polynomials with real coefficient and let $I = < x^2 + 1 >$

$R = R[x] / \left(x^2 + 1\right) = \{f(x) + < x^2 + 1 > : f(x) \in R[x]\}$

Let us see what quotient ring R is;

By Division algorithm, for any $f(x) \in \mathbb{R}[x]$, $\exists\, p(x)\, and\, r(x)\, in\, \mathbb{R}[x]$

Such that $f(x) = p(x) \cdot (x^2 + 1) + r(x)\ where\ r(x) = 0$

$\deg r(x) < \deg (x^2 + 1) = 2\ \ i.e.\, r(x) = 0\ or\ r(x) = ax + b, a, b \in R.$

$\therefore f(x) + I = \left(p(x)\left(x^2 + 1\right) + r(x) + I\right)$

$= \left(p(x)\,(x^2 + 1) + I\right) + r(x) + I$

$= r(x) + I\,, \left(Since\ \ x^2 + 1 \in I,\ therefore\ p(x)\,(x^2 + 1) \in I,\ \ p(x)\,(x^2 + 1) + I = I\right.$

$\therefore R = \mathbb{R}[x] / < x^2 + 1 > = \{ax + b + \mathrm{I}.\, a, b \in \mathbb{R}\}$

5.3 Types of Ideal

Prime Ideal: Let *R* be a commutative ring. An ideal *P* of *R* is said to be prime ideal if whenever *a, b* $\in P \Rightarrow$ either *a* $\in P$ or *b* $\in P$.

Maximal Ideal: Let R be a commutative ring An ideal M of R is said to be maximal ideal if (i) M $\neq$ R (ii) $M \subseteq \underline{T} \subseteq R$ then either M = I or I = R.

Before we see example of prime and maximal ideal we just prove two theorems. These theorem use to characterise ideal with the help of quotient ring.

Theorem 3: (*P* is prime $\Rightarrow$ *R* / *P* is integral domain)

Let *R* be a commutative ring. An ideal *P* of *R* is prime ideal if and only if *R/P* is integral domain.

Proof: Let *R* be commutative ring and P is prime ideal of R.

To prove R/P is Integral domain.

Let $\bar{a} = a + P \text{ and } \bar{b} = b + p \in R / P$

Such that $\bar{a} . \bar{b} = P \text{ in } R / P$ (*P* is zero element in R/P)
$i.e. (a+P)(b+P) = P \text{ in } R / P \text{ i.e. } ab + P = P \Rightarrow ab \in P$

But *P* is prime ideal

Therefore $ab \in P \Rightarrow a \in P$ or $b \in P \Rightarrow a + P = P \text{ or } b + P = P$

Hence if $\bar{a} . \bar{b} = P \Rightarrow \bar{a} = P \text{ or } \bar{b} = P$

Conversely let assume that R/P is integral domain To prove *P* is prime ideal.

Let $a, b \in R$ such that $ab \in P \Rightarrow ab + P = P \Rightarrow (a + P)(b + P) = P$

But *R/P* is integral domain.

$(a + P) . (b + P) = P \Rightarrow a + P = P \text{ or } b + P = P \Rightarrow a \in p \text{ or } b \in p$

$\therefore a.b \in P \Rightarrow a \in P \text{ or } b \in P$

$\therefore$ *P* is Prime ideal.

Theorem 4: *M* is Maximal ideal $\Leftrightarrow$ *R/M* is Field.

Let *R* be a commutative ring with unity. An ideal *M* of *R* is maximal ideal of R if and only if *R/M* is field.

Proof: Let *R* be a commutative ring with unity and *M* is Maximal ideal of *R*.

To prove R / M is field. Let $a + M \in R / M$ such that $a + M \neq M \Rightarrow a \notin M$

Consider the ideal $aR = \{ a : r : r \in R \}$ of R.

$\therefore$ *M* is ideal, *aR* is ideal.

Then *N* = *M* + *aR* is also ideal such that $M \subseteq \mathrm{N} \subseteq R$

But M is maximal ideal and $M \neq N$.

Therefore $N = R$, hence $1 \in R \Rightarrow 1 \in N$

$\therefore \exists x \in M,\ r \in R$ such that $1 = x + ar$

$\therefore (x+ar)+M=1+M \therefore (x+M)+ar+M=1+\mathrm{M}$

$\therefore (a+M)(r+M)=1+M \ (\because x\in M \therefore x+M=M)$

Hence $a + M$ has multiplicative inverse.

$\therefore$ Every non zero element of R/M has multiplicative inverse.

$\therefore$ *R/M* is field.

Conversely, let assume that *R/M* is field.

To prove *M* is Maximal ideal.

Let assume that *N* is any ideal of *R* such that $M \subseteq \mathrm{N} \subseteq R$

then N/M is ideal in *R/M*

but *R/M* is field & hence the only ideals in R/M is zero ideal which M or *R/M* itself.

$If\ N/M=M \Rightarrow N=M$

$if\ N/M=R/M \Rightarrow N=R$

If $M \subseteq \mathrm{N} \subseteq R$ either M = N or N = R

$\therefore$ M is maximal ideal of R/M

Remark :

1) Since every field is integral domain therefore if M is maximal ideal $\Rightarrow$ R/M is field $\Rightarrow$ R/M is integral domain $\Rightarrow$ M is prime ideal

Hence every maximal ideal is prime ideal. But every prime ideal need not be maximal ideal which we will see in the examples let see some examples of prime and maximal ideals.

Examples:

1) Let R = $\mathbb{Z}$[x] and I = <x> = set of all polynomial with constant term zero.

Claim : I is prime ideal.

Let $f(x)\cdot h(x)\in\langle x\rangle$

$\therefore there\ exist\ g(x)\in\mathbb{Z}[x]\ s.t.\ f(x)\ g(x)=x.g(x)$

$\therefore f(0)\ h(0)=0\cdot g(0)=0$

$\Rightarrow f(0)=0\ or\ h(0)=0$ ($\because \mathbb{Z}$ is integral domain)

$\Rightarrow f(x)\in\langle x\rangle\ or\ h(x)\in\langle x\rangle$

$\therefore <x>\ is\ prime\ ideal\ in\ \mathbb{Z}[x]$

2) Let R = $\mathbb{Z}[x]$ and M = <x, 2> = set of all polynomial with even constant term.

Note that M = <x, 2> = {x.f(x) + 2g(x) : f(x), g(x) $\in$ $\mathbb{Z}$ [x]}

Claim : M is maximal ideal in R

Clear $M \neq R$

Let N be any other ideal of R such that $M \subseteq N \subseteq R$

we will prove that M = N or N = R

Let assume that $M \neq N$

Therefore we prove that N = R

$\because M \neq N, \therefore \exists\, f(x) \in N$ *such that* $f(x) \notin M$

$\therefore$ constant term of f(x) i.e. f(o) is not even

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + .. + a_1 x + a_o$ where a_0 is odd.

$= a_n x^n + .. + a_1 x + 2b_o + 1 \; (\because a_o \; is \; odd)$ = g(x) + 1

where $g(x) = a_n x^n + .. + a_1 x + 2b_o \in M \subseteq N$

$\therefore g(x) \in N$, $f(x) \in N$

$\therefore 1 = f(x) - g(x) \in N$

$\therefore$ *for any* $k(x) \in R, \quad 1 \cdot k(x) \in N$

$\therefore R \subseteq N$ *But* $N \subseteq R$

$\therefore N = R$

$\Rightarrow$ M is maximal ideal of R

(i) Note that $I = \langle x \rangle \subset M = \langle x, 2 \rangle$ $\therefore$ <x> is not maximal ideal.

Hence prime ideal need not be maximal ideal.

(ii) By same argument we can show for any prime <x, p> is maximal ideal of $\mathbb{Z}$[x]

(iii) Since there are infinitely many prime, hence there are infinitely many maximal ideal in $\mathbb{Z}$[x]

3) Let p is prime, then $p\mathbb{Z}$ is prime ideal of $\mathbb{Z}$.

As $Let\ x.y \in p\mathbb{Z} \Rightarrow x \cdot y = pk\ for\ some\ k \in \mathbb{Z}$

$\therefore p / x.y \therefore p / x\ or\ p / y \Rightarrow x = pk_1, or\ y = p.k_2 \Rightarrow x \in p\mathbb{Z}\ or\ y \in p\mathbb{Z}$

$\therefore p\mathbb{Z}\ is\ prime\ ideal.$

Also note that $\mathbb{Z}/p\mathbb{Z}$ is $\mathbb{Z}p$ which ring of residue modulo p. And as p is prime it is field. Hence $p\mathbb{Z}$ is maximal ideal also. Thus in $\mathbb{Z}$, prime and maximal ideal are some.

4) Let $R = \mathbb{Z} \oplus \mathbb{Z}\ and\ I = \{(a, 0) : a \in \mathbb{Z}\}$ consider R/I,

Let $(a, b) \in R\ then\ (a, b) + I = ((a, 0) + (0, b)) + I = (a, 0) + I + (a, b) + I$

$= (0, b) + I\ (Since\ \ (a, 0) \in I, \because (a, 0) + I = I)$

$\therefore R / I = \{(0, b) + I : b \in \mathbb{Z}\}$

Let ((x, y) + I) . ((p, q) + I) = I (I is zero element in I)

$\Rightarrow (xp, yq) + I = I \Rightarrow (xp, yq) \in I \Rightarrow y.q. = 0$

$\Rightarrow y = 0\ or\ q = 0\ (\because \mathbb{Z}\ is\ Integral\ domain)$
$\Rightarrow (2, 0) \in I\ or\ (p, 0) \in I$

$\Rightarrow (x, 0) + I = I\ or\ (p, 0) + I = I$

Hence R/I is Integral domain

$\therefore$ I is prime ideal

$\because$ (1, 1) is unity in $\mathbb{Z} \oplus \mathbb{Z}$

and R/I = {(0, b) + I : b $\in$ $\mathbb{Z}$} does not contain unity hence it is not field.

$\therefore$ I is not maximal ideal

5) Let us find maximal ideal of

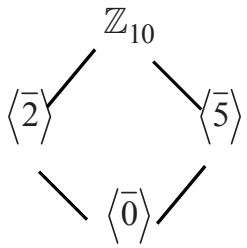
(i) $\mathbb{Z}_8$ (ii) $\mathbb{Z}_{10}$ (iii) $\mathbb{Z}_{12}$

Let us see lattice of ideals for $\mathbb{Z}_8$

I) $\mathbb{Z}_8$

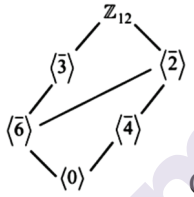
Clearly $\langle\bar{2}\rangle$ is maximal ideal of $\mathbb{Z}_8$.

II)



Clearly $\langle\bar{2}\rangle$ and $\langle\bar{5}\rangle$ is maximal ideal of $\mathbb{Z}_{10}$.

III)



Clearly $\langle\bar{2}\rangle$ and $\langle\bar{3}\rangle$ is maximal ideal of $\mathbb{Z}_{12}$.

Thus in general for any prime divisor p of n, <p> is maximal ideal of $\mathbb{Z}_n$.

5.4 Unit and Exercises

1) Let S = {a + bi : a, b $\in \mathbb{Z}$, b is even}. Show that S is subring of $\mathbb{Z}[i]$ but not on ideal.

2) Check whether the following set I is ideal of ring R?

$i)\ I=\{(a,a):a\in\mathbb{Z}\}\quad R=\mathbb{Z}\times\mathbb{Z}\quad ii)\ I=\{(a,-a):a\in\mathbb{Z}\}\ \ R=\mathbb{Z}\times\mathbb{Z}$

$iii)\ I=\{(2a,2b):a,b\in\mathbb{Z}\}\quad R=\mathbb{Z}\times\mathbb{Z}$

(In all three problems R is ring under component wise addition and multiplication.)

(iv) $I = \{f(x) \in \mathbb{Z}[x] : f(x) = a_n x^n + .. + a_1 x + a_0 \ : \ 3 \mid a_0\}$ $R = \mathbb{Z}[x]$

(v) $I = \{f(x) \in K = \mathbb{Z}[x] : f(x) = a_n x^n + .. + a_1 x + a_0 :$

$a_n + .. + a_1 + a_0 = 0\}$ and $R = \mathbb{Z}[x]$

(vi) $I = \left\{\begin{pmatrix} o & a \\ o & o \end{pmatrix} : a \in R\right\}, R = \left\{\begin{pmatrix} a & b \\ o & d \end{pmatrix} : a, b, d \in \mathbb{R}\right\}$

(vii) $I = \{4a + bi : a, b \in \mathbb{Z}\}, R = \mathbb{Z}[i]$

3) Determine the number of element in quotient ring

(i) $3\mathbb{Z} / 9\mathbb{Z}$ (ii) $\mathbb{Z}[i] / \langle 3 + i \rangle$

4) Let $I = \langle 2 + 2i \rangle$. Determine $R = \mathbb{Z}[i]/<2+2i>$.

What is characteristic of R? Is R is Integral domain? Is I = <2 + 2i> is prime ideal.

5) Show that the following ideals are prime ideals in the given ring

(i) $\langle x^2 + x + 1 \rangle$ *in* $\mathbb{Z}_2[x]$

(ii) I = {(3x, y) : *x, y* $\in \mathbb{Z}$} in $\mathbb{Z}$ x $\mathbb{Z}$ under component wise addition and multiplication.

6) Show that <1 – i> is maximal ideal in $\mathbb{Z}$[i]. (Show that $\mathbb{Z}$[i]/<1-i> is field. Note that *i =1* and 2 = 0 in $\mathbb{Z}$[i]/<1-i>)

7) Let R be the ring of continuous functions from $\mathbb{R}$ *to* $\mathbb{R}$. Show that *A = {f* $\in R$ */ f(0) = 0}* is a maximal ideal of *R*.

8) Prove that every prime ideal is maximal ideal.

6

RING HOMOMORPHISM AND ISOMORPHISM

Unit Structure

6.0 Objective

After going through this unit you shall come to know about

- The concept of ring homomorphism and isomorphism.
- Fundamental Theorem of isomorphism and its application.
- Method to construct ring of fraction and Quotient field.

One way to study property of a ring is to examine its interaction with other ring by finding some relation between them. This relation is something which must preserve the operation of the respective ring. Such relation is called as ring homomorphism.

6.1 Ring Homomorphism

Let R, S be any two ring. A map $f: R \to S$ is said to be ring homomorphism from R to S if for any $a, b \in R$ $\mathrm{f}(a+b) = \mathrm{f}(a) + \mathrm{f}(b)$ and $\mathrm{f}(ab) = \mathrm{f}(a)\,\mathrm{f}(b)$ i.e. f is operation preserving mapping.

Properties of Ring Homomorphisms :

Let $\varnothing : R \to S$ be a ring homomorphism. Let A be a subring of R and B is an ideal of S.

1. For any $r \in R$ and any positive integer $n, \varnothing(nr) = n\varnothing(r)$ and $\varnothing(r^n) = (\varnothing(r))^n$.

2. $\varnothing(A) = \{\varnothing(a) : a \in A\}$ is a subring of S.

3. If A is ideal and $\varnothing$ onto S, then $\varnothing(A)$ is an ideal.

4. $\varnothing^{-1}(B) = \{r \in R / \varnothing(r) \in B\}$ is an ideal of R.

5. If R is commutative, then $\varnothing(R)$ is commutative.

Proof :

1) $\varnothing(nr) = \varnothing(r + r + ... + r)$ (n times) $= \varnothing(r) + ... + \varnothing(r) = n\varnothing(r)$

2) $\varnothing(r^n) = \varnothing(r.r...r)$ (n times) $= \varnothing(r).\varnothing(r)..\varnothing(r) = (\varnothing(r))^n$

Let $x, y \in \varnothing(A)$

$\therefore \exists\, a, b \in A$ such that $x = \varnothing(a), y = \varnothing(b)$

$\therefore x - y = \varnothing(a) - \varnothing(b) = \varnothing(a - b) \in \varnothing(A)$ $\quad (\because a - b \in A)$

$\therefore \varnothing(A)$ is subring

3) $\varnothing : R \to S$ is onto. $\therefore$ for any $y \in S, \exists\, x \in R$ such that $\varnothing(x) = y$

To prove: $\varnothing(A)$ is ideal of S. From (2), $\varnothing(A)$ is subring.

Hence it is enough to show that for any $x \in \varnothing(A), y \in S, x \cdot y \in \varnothing(A)$.

$\because x \in \varnothing(A). \therefore \exists\, a \in A$ such that $\varnothing(a) = x, y \in S, \varnothing$ is onto, $\exists\, b \in R$ such that $\varnothing(b) = y$.

Hence $x.y = \varnothing(a)\varnothing(b) = \varnothing(ab) \in \varnothing(A)$ (Since in ideal A ideal, therefore $ab \in A$)

$\therefore \varnothing(A)$ is ideal of S.

4) $\varnothing^{-1}(B)=\{r\in R/\varnothing(r)\in S\}$

Let $x, y\in\varnothing^{-1}(B)\therefore\varnothing(x),\varnothing(y)\in B$ as B is ideal $\therefore\varnothing(x)-\varnothing(y)\in B$

$\therefore\varnothing(x-y)\in B$

$\therefore x-y\in\varnothing^{-1}(B)$

Hence $\varnothing^{-1}(B)$ is subring.

Let $r\in R$ be arbitrary. $\therefore\varnothing(r)\in S$

As B is ideal of S

$\therefore\varnothing(x)\varnothing(r)\in B$ therefore $\varnothing(xr)\in B$

$\therefore\varnothing(xr)\in B,$ therefore $xr\in\varnothing^{-1}(B)$

Similarly we can show that $r.x\in\varnothing^{-1}(B)$

Hence $\varnothing^{-1}(B)$ is ideal of R.

V) Let R is commutative ring.

$\therefore$ for any $x, y\in R, x.y=y.x$

$\therefore\varnothing(x.y)=\varnothing(y.x)$

$\therefore\varnothing(x)\varnothing(y)=\varnothing(y).\varnothing(x)$

$\Rightarrow\varnothing(R)$ is commutative ring.

Kernel of Ring homomorphism: Let $\varnothing: R\to S$ be a ring homomorphism then Kernel of $\varnothing$, denoted as ker $\varnothing$ and is defined as $Ker\,\varnothing=\{r\in R/\varnothing(r)=0\}$.

Note that ker $\varnothing$ is ideal of R.

Example:

1) Let $R=\left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} : a,b \in \mathbb{Z}\right\}$. Let $\varnothing : R \to \mathbb{Z}$ be defined by $\varnothing\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right)=a-b$ then $\varnothing$ is ring homomorphism.

As let $A=\begin{bmatrix} a & b \\ b & a \end{bmatrix}$, $B=\begin{bmatrix} x & y \\ y & x \end{bmatrix}$

then $\varnothing(A-B)=\varnothing\left(\begin{bmatrix} a-x & b-y \\ b-y & a-x \end{bmatrix}\right)=a-x-b+y$

$$=(a-b)-(x-y)$$
$$=\varnothing(A)-\varnothing(B)$$

$$A.B=\begin{bmatrix} a & b \\ b & a \end{bmatrix}\begin{bmatrix} x & y \\ y & x \end{bmatrix}=\begin{bmatrix} ax+by & ay+bx \\ bx+ay & ax+by \end{bmatrix}$$

$\therefore \varnothing(A.B)=(ax+by)-(ay+bx)$ ..... (1)

Also $\varnothing(A)\varnothing(B)=\varnothing\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right)\varnothing\left(\begin{bmatrix} x & y \\ y & x \end{bmatrix}\right)$

$$=(a-b)(x-y)=ax-ay-bx+by$$
$$=(ax+by)-(ay+bx) \text{ ..... (2)}$$

From (1) and (2)

$\varnothing(A.B)=\varnothing(A)\varnothing(B)$

Hence $\varnothing$ is homomorphism.

Let us find Ker $\varnothing$,

Ker $\varnothing=\left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix}\in R : \varnothing\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right)=0\right\}$

$$=\left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix}\in R / a-b=0\right\}=\left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix}\in R / a=b\right\}$$

$$=\left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} : a\in\mathbb{R}\right\}=\left\{a\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} / a\in R\right\}=\left\{\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\right\}$$

2) Define $\varnothing : \mathbb{Z} \to \mathbb{Z}_n,\ \varnothing(k) = k \bmod n$. Then $\varnothing$ is an homomorphism known as natural homomorphism.

3) Let R be commutative ring of prime characteristic P.

Define $\varnothing : R \to R$ as $\varnothing(x) = x^p$ is ring homomorphism

as $\varnothing(x+y) = (x+y)^p = x^p + {}^pC_1 x^{p-1}y + {}^pC_2 x^{p-2}y^2 + ... + {}^pC_{p-1} xy^{p-1} + y^p \therefore$

Each of ${}^pC_1\ 1 \le i \le p-1$ is multiple of p and char R = p $\therefore C_1^p x^{p-i} y^i = 0$ for all $i,\ 1 \le i \le p-1$

$$\therefore \varnothing(x+y) = x^p + y^p = \varnothing(x) + \varnothing(y)$$

$$\varnothing(xy) = (xy)^p = x^p . y^p = \varnothing(x) . \varnothing(y)$$

Therefore $\varnothing$ is ring homomorphism, known as Frobenius homomorphism.

4) Let R be a ring and A be its any ideal.

Define a map $f : R \to R/A$ as $f(r) = r + A$, then f is ring homomorphism known as a natural homomorphism.

Ring Isomorphism: A ring homomorphism $\varnothing : R \to S$ which is one-one and onto is known as ring isomorphism.

If $\varnothing : R \to S$ is ring isomorphism we say that ring R and S is isomorphic to each other and this is denoted by $R \approx S$.

Isomorphic rings are exactly similar in terms of property of element and their behavior. In Other words isomorphic rings are nothing but different way of looking of same ring.

Theorem 1. First Isomorphism Theorem of Ring:

Statement: Let $\varnothing : R \to S$ be a onto ring homomorphism then $R / \ker \varnothing \approx \varnothing(R)$.

Proof : Let Ker $\varnothing$ = W.

To prove $R/W \approx \varnothing(R)$

Clearly $W = Ker\ \varnothing$ is ideal of R.

Define a map $f : R/W \to \varnothing(R)$ as $f(r+W) = \varnothing(r), r \in R$.

Claim :

1) is well defined one - one map.

Let assume that

$r+W=\mathrm{s}+W, \quad r,s\in R \Leftrightarrow r-s\in W=Ker\varnothing \Leftrightarrow \varnothing(r-s)=0$ (By Definition of Ker $\varnothing$)

$\Leftrightarrow \varnothing(r)-\varnothing(s)=0$ (By definition of homomorphism)

$\Leftrightarrow \varnothing(r)=\varnothing(s) \Leftrightarrow f(r+w)=f(r+W)$

$\therefore$ f is well defined one-one map.

2) f is onto.

Let $y\in\varnothing(R)$

Therefore there exist $x\in R$ such that $\varnothing(x)=r$.

Therefore there exist $x+W\in R/W$ such that $f(x+W)=\varnothing(x)=y$.

Therefore f is onto.

3) f is homomorphism.

Consider $f(x+W+y+W)=f(x+y+W)$

$=\varnothing(x+y)$ (By definition of f)

$=\varnothing(x)+\varnothing(y)$ ($\varnothing$ is homomorphism)

$=f(x+W)+f(y+W)$

$f(x+W)(y+W)=f(xy+W)=\varnothing(xy)=\varnothing(x)\varnothing(y)$

$=f(x+W).f(y+W)$

$\because f$ is homomorphism

Hence f is isomorphism.

$\therefore R/W\approx\varnothing(R)$

Theorem 2. Second Isomorphism Theorem for Rings :

Statement: Let A be a subring and let B be an ideal of R. Then $A+B=\{a+b:a\in A,b\in B\}$ is a subring of R, $A\cap B$ is an ideal of A and $(A+B)/B\approx A/A\cap B$

Proof : Let we give sketch of the proof.

To prove this we use first isomorphism theorem of rings.

Let $x\in A+B$

$\therefore x=a+b, a\in A, b\in B$

$\therefore x+B=a+b+B=a+(b+B)=a+B\left(\because b\in B\right)$

Hence define a map $\varnothing: A\to\left(A+B\right)/B$ such that $\varnothing(a)=a+B$.

You prove this map $\varnothing$ is onto homomorphism.

Then apply first isomorphism theorem, according to which $A/\ker\varnothing\approx\left(A+B\right)/B$.

Now prove that $\ker\varnothing=A\cap B$.

Theorem 3. Third Isomorphism Theorem of Ring:

Statement : Let I and J be ideals of R with $I\subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I)\approx R/J$.

Proof : This proof is also similar to proof of second isomorphism theorem.

Here define $\varnothing: R/I\to R/J$ as $\varnothing(r+I)=r+J$.

Show that $\varnothing$ is onto homomorphism.

Then by first isomorphism theorem $R/I\,|Ker\varnothing\approx R/J$.

Show that $Ker\varnothing=J/I$.

The first isomorphism theorem has lot of application. One of the application is to prove that a field contains $\mathbb{Z}_p$ or $\mathbb{Q}$. We prove this by following steps.

Theorem 4: Let R be a ring with unity e. The mapping $\varnothing : \mathbb{Z} \to R$ given by $\varnothing(n) = n.e$ is a ring homomorphism.

Proof : Let $m, n \in \mathbb{Z}, m, n > 0$

$$\varnothing(m+n) = (m+n)e = e + e + ... + e\,(m+n\ times)$$

$$= \underbrace{(e+e+..+e)}_{m\ times} + \underbrace{(e+..+e)}_{n\ times} = me + ne = \varnothing(m) + \varnothing(n)$$

Let assume $m, n < 0$

Then Let $m = -p, n = -q$ where $p, q > 0$.

$$\therefore \varnothing(m+n) = (m+n)\,e = (-p-q)\,e = (p+q)\,(-e)$$
$$= (p)\,(-e) + q(-e)$$
$$= (-p)\,e + (-q)\,e = me + ne = \varnothing(m) + \varnothing(n)$$

Similarly if $m \geq 0$ $n < 0$ we can prove $\varnothing(m+n) = \varnothing(m) + \varnothing(n)$.

Also $\varnothing(mn) = \varnothing(mn)e = (mn)\,(e.e) = (me)(ne) = \varnothing(m).\varnothing(n)$

$\therefore \varnothing$ is ring homomorphism.

Corollary 1: Let R is the ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If the characteristic of R is 0, then R contains a subring isomorphic to $\mathbb{Z}$.

Proof: Let $S = \{ke : k \in \mathbb{Z}\}$

Claim : S is subring of R.

Let $a, b \in S$

$\therefore \exists\, n, m \in \mathbb{Z}$ such that $a = ne$ and $b = me$

$\therefore a - b = ne - me = (n-m)e \in s$

$a.b = (ne)\,(me) = n(em)e = nmee = (nm)e \in S.$

Hence S is subring of R.

Define $\varnothing : \mathbb{Z} \to S$ such that $\varnothing(n) = ne$.

Then $\varnothing$ is onto and above theorem $\varnothing$ is homomorphism.

Hence by first isomorphism theorem $\mathbb{Z} / Ker\,\varnothing \approx S$.

If Char $R = n$

Then Ker $\varnothing = \{m \in \mathbb{Z} / \varnothing(m) = 0\} = \{m \in \mathbb{Z} / me = 0\}$

$= \{m \in \mathbb{Z} : n / m\} (\because char\ R = n) = \langle n \rangle$

$\therefore \mathbb{Z} / \langle n \rangle \approx S$

$\therefore S \approx \mathbb{Z}_n$

Hence *R* contains subring isomorphic to $\mathbb{Z}_n$.

If char *R = 0* $\Rightarrow$ There exist no integer *n* such *ne=0*.

$Ker\ \varnothing = \{m \in \mathbb{Z} / \varnothing(m) = 0\} = \{m \in \mathbb{Z} / me = 0\} = \{0\}$ (Since $char\ R = 0$)

$\therefore \mathbb{Z} / \ker \varnothing \approx S$

$\therefore \mathbb{Z} \approx S$

Hence R contains a subring isomorphic to $\mathbb{Z}$.

Corollary 2: A field contains $\mathbb{Z}_p$ or $\mathbb{Q}$.

Proof: Characteristics of a field is either zero or prime. Let *R* be a field.

Case I: Char *R = p, p* is prime.

Then by previous corollary R contains a subring isomorphic to $\mathbb{Z}_p$, $\mathbb{Z}_p$ is field, as *p* is prime

Hence *R* contains $\mathbb{Z}_p$.

Case II: Char *R = 0*

Then subring *S* of *R* is isomorphic to $\mathbb{Z}$.

Let $T = \{a.b^{-1} : a, b \in S, b \neq 0\}$

The *T* is subfield of *R* and isomorphic to $\mathbb{Q}$.

Hence a field contains $\mathbb{Z}_p$ or $\mathbb{Q}$.

6.3 Ring Of Fractions

The aim of this section is to prove that a commutative ring *R* is always a subring of a larger ring $\mathbb{Q}$ in which every non zero zero divisor of *R* is unit in $\mathbb{Q}$. In case of integral domain such ring is field and called as field of fraction or Quotient field. Construction of quotient field $\mathbb{Q}$ from ring *R* is exactly as construction of $\mathbb{Q}$ from $\mathbb{Z}$.

Theorem 6 : Let *D* be an integral domain. Then there exists a field *F* (called the field of fraction of *D*) that contains a subring isomorphic to *D*.

Proof: Let *S* be the set of all formal symbols of the form *a/b,* where $a, b \in D$ and $b \neq 0$. Define an equivalence relation $\equiv$ on S by $a/b \equiv c/d$ if $ad = bc$. Let *F* be the set of equivalence classes of *S* under the relation $\equiv$ and denote the equivalence class that contains x/y by $[x/y]$. We define addition and multiplication on *F* by $[a/b]+[c/d]=[(ad+bc)/bd]$ and $[a/b].[c/d]=[ac/bd]$.

We will prove *F* is field with respect to the operation $+ \; and \; \cdot$ define above.

To prove this first of all the operation $+ \; and \; \cdot$ is well defined.

Let assume that $\frac{a}{b}=\frac{a^1}{b^1}$ and $\frac{c}{d}=\frac{c^1}{d^1}$.

To prove $\frac{a}{b}+\frac{c}{d}=\frac{a^1}{b^1}+\frac{c^1}{d^1}$

$\because \frac{a}{b}=\frac{a^1}{b^1} \Rightarrow ab^1 = a^1 b$

$\frac{c}{d}=\frac{c^1}{d^1} \Rightarrow cd^1 = c^1 d$

$\because$ To prove $\frac{a}{b}+\frac{c}{d}=\frac{a^1}{b^1}+\frac{c^1}{d^1}$ i.e. to prove $\frac{ad+bc}{bd}=\frac{a^1d^1+c^1d^1}{b^1d^1}$

i.e. to prove that $(ad+bc)b^1d^1 = (a^1d^1 + c^1d^1)\,bd$.

i.e. to prove that $adb^1d^1 + bcb^1d^1 = a^1d^1bd + c^1d^1bd$

In LHS put $ab^1 = a^1b$ and $cd^1 = c^1d$ we get RHS.

Hence + is well defined.

Similar To prove $\frac{a}{b}.\frac{c}{d} = \frac{a^1}{b^1}.\frac{c^1}{d^1}$ which is obvious as $\frac{a}{b} = \frac{a^1}{b^1}$ and $\frac{c}{d} = \frac{c^1}{d^1}$

$\Rightarrow \frac{ac}{bd} = \frac{a^1c^1}{b^1d^1}$

It is trivial to prove that (F, +) is abelian group with zero element as $\left[0/1\right]$ and additive inverse of $\left[a/b\right]$ as $\left[-a/b\right]$.

Multiplication is obviously distributive over addition and associative.

The unity element of F is $\left[1/1\right]$ and multiplicative inverse of non zero element $\left[a/b\right]$ is $\left[b/a\right]$ for $a,\ b \neq 0$.

Hence F is field. Finally let we define a map $\varnothing : D \to F$ as $\varnothing(x) = \left[x/1\right]$ then $\varnothing$ is ring isomorphism from D to $\varnothing(D)$ as,

$$\varnothing(x+y) = \left[(x+y)/1\right] = \left[x/1 + y/1\right] = \left[x/1\right] + \left[y/1\right] = \varnothing(x) + \varnothing(y)$$

$$\varnothing(xy) = \left[xy/1\right] = \left[x/1\right] = \left[y/1\right] = \varnothing(x)\varnothing(y)$$

$$Ker\ \varnothing = \left\{x \in D : \varnothing(x) = 0\right\}$$

$$= \left\{x \in D : \left[x/1\right] = 0\right\} = \left\{x \in D : x = 0\right\} = \left\{0\right\}$$

$\therefore$ By first isomorphism theorem,

$$D / Ker\varnothing \approx \varnothing(D)$$
$$\therefore D \approx \varnothing(D)$$

Hence F contains a subfield isomorphic to D.

Examples :

1) Show that the ring $\mathbb{Z}\left[\sqrt{2}\right]$ and H are isomorphic where $H=\left\{\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} : a,b \in \mathbb{Z}\right\}$ under addition and multiplication of 2×2 matrixes.

Solution : $\varnothing : \mathbb{Z}\left[\sqrt{2}\right] \to H$ as $\varnothing\left(a+b\sqrt{2}\right)=\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$

Claim :

1) $\varnothing$ is well defined, one-one map

Let $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}=\begin{bmatrix} x & 2y \\ y & x \end{bmatrix}$

$\therefore \Leftrightarrow a=x \,\&\, b=y$

$\Leftrightarrow a+b\sqrt{2}=x+y\sqrt{2}$

$\therefore \varnothing\left(a+b\sqrt{2}\right)=\varnothing\left(x+y\sqrt{2}\right) \Leftrightarrow a+b\sqrt{2}=x+y\sqrt{2}$

$\therefore \varnothing$ is well defined one-one map.

2) $\varnothing$ is onto

For any $\begin{bmatrix} x & 2y \\ y & x \end{bmatrix} \in H, x+\sqrt{2}\, y \in \mathbb{Z}\left[\sqrt{2}\right]$ such that

$\varnothing\left(x+\sqrt{2}\, y\right)=\begin{bmatrix} x & 2y \\ y & x \end{bmatrix}$. Hence $\varnothing$ is onto.

3) $\varnothing$ is homomorphism.

$$\varnothing\left[\left(a+b\sqrt{2}\right)+\left(x+y\sqrt{2}\right)\right]=\varnothing\left(a+x+(b+y)\sqrt{2}\right)$$

$$=\begin{bmatrix} a+x+ & (b+y)\sqrt{2} \\ b+y & a+2 \end{bmatrix}=\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}+\begin{bmatrix} x & 2y \\ y & x \end{bmatrix}$$

$$=\varnothing\left(a+b\sqrt{2}\right)+\varnothing\left(x+y\sqrt{2}\right)$$

$$\varnothing\left[\left(a+b\sqrt{2}\right)+\left(x+y\sqrt{2}\right)\right]=\varnothing\left(ax+2by+(ay+bx)\sqrt{2}\right)$$

$$= \begin{bmatrix} ax+2by & 2ay+2bx \\ ay+bx & ax+2by \end{bmatrix}$$

$$\varnothing\left(\left(a+b\sqrt{2}\right)\left(x+y\sqrt{2}\right)\right) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}\begin{bmatrix} x & 2y \\ y & x \end{bmatrix} = \begin{bmatrix} ax+2by & 2ay+2bx \\ ay+bx & ax+2by \end{bmatrix}$$

$$= \varnothing\left(\left(a+b\sqrt{2}\right)\left(x+y\sqrt{2}\right)\right)$$

Hence $\varnothing$ is homomorphism.

$\therefore \varnothing$ is isomorphism.

$\therefore \mathbb{Z}\left[\sqrt{2}\right] \approx H$.

2) Let $R = \left\{\begin{bmatrix} a & b \\ b & a \end{bmatrix} : a,b \in \mathbb{Z}\right\}$. Let $\varnothing : R \to \mathbb{Z}$ defined $\varnothing\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = a-b$. Show that $\varnothing$ is a ring homomorphism. Determine Ker$\varnothing$. Is Ker$\varnothing$ a prime ideal? Is it a maximal ideal? Justify.

Solution: Let $A = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$ and $B = \begin{bmatrix} x & y \\ y & x \end{bmatrix} \in R$

$$\varnothing(A+B) = \varnothing\begin{bmatrix} a & b \\ b & a \end{bmatrix} + \begin{bmatrix} x & y \\ y & x \end{bmatrix} = \varnothing\left(\begin{bmatrix} a+x & b+y \\ b+y & a+x \end{bmatrix}\right) = a+x-(b-y)$$

$$= (a-b)+(x-y) = \varnothing(A)+\varnothing(B)$$

$$\varnothing(AB) = \varnothing\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\begin{bmatrix} x & y \\ y & x \end{bmatrix}\right) = \varnothing\left(\begin{bmatrix} ax+by & ay+bx \\ ay+bx & ax+by \end{bmatrix}\right)$$

$$= \varnothing(ax+by-(ay+bx)) = a(x-y)+b(y-x) = (a-b)(x-y) = \varnothing(A).\varnothing(B)$$

$\therefore \varnothing$ is homomorphism

Ker$\varnothing = \{A \in R : \varnothing(A) = 0\}$

$$= \left\{A \in R : \varnothing\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = 0\right\} = \{A \in R : a-b=0\} \qquad = \left\{\begin{bmatrix} a & a \\ a & a \end{bmatrix} . a \in \mathbb{Z}\right\}$$

$\therefore$ First Isomorphism theorem

$R / Ker\varnothing \approx \mathbb{Z}$ as $\mathbb{Z}$ is Integral domain, $R / Ker\varnothing$ is integral domain.

$\therefore Ker\varnothing$ is prime ideal.

Also as $\mathbb{Z}$ is not field. $\therefore R / Ker\varnothing$ is not field.

$\therefore Ker\varnothing$ is not maximal ideal.

3)Prove that $M_2(\mathbb{R})$ contains a subring that is isomorphic to $\mathbb{C}$.

Solution : $M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R} \right\}$.

Define a map $\varnothing : \mathbb{C} \to M_2(\mathbb{R})$ as $\varnothing(a+ib) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

Claim : $\varnothing$ is homomorphism.

$$\varnothing(a+ib+c+id) = \varnothing(a+c+i(b+d)) = \begin{bmatrix} a+c & -(b+d) \\ b+d & a+c \end{bmatrix}$$

$$= \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \varnothing(a+ib) + \varnothing(c+id)$$

$$\varnothing\left((a+ib).\varnothing(c+id)\right) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}\begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{bmatrix}$$
$$= \varnothing\left((a+ib)(c+id)\right)$$

Hence $\varnothing$ is homomorphism.

Ker $\varnothing = \{a+ib \in \not\subset : \varnothing(a+ib) = 0\}$

$$= \left\{ a+ib \in \not\subset : \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\} = \{a+ib \in \not\subset : a=0, b=0\} = \{0\}$$

$\therefore$ By First isomorphism theorem

$\mathbb{C}/\text{Ker } \phi \approx M_2(\mathbb{R})$. i.e. $\mathbb{C} \approx \varnothing(M_2\mathbb{R})$.

Hence $M_2(\mathbb{R})$ contains a subring that is isomorphic to $\varnothing$.

4) Is $2\mathbb{Z}$ is isomorphic to $3\mathbb{Z}$

Solution : No. Let $\varnothing : 2\mathbb{Z} \to 3\mathbb{Z}$ is isomorphism & $\varnothing(2) = a$.

$\therefore \varnothing(4) = \varnothing(2+2) = \varnothing(2) + \varnothing(2) = 2\varnothing(2) = 2a$ ..... (I)

Also $\varnothing(4) = \varnothing(2.2) = \varnothing(2).\varnothing(2) = (\varnothing(2))^2 = a^2$ ..... (II)

Therefore From (I) & (II).

$$a^2 = 2a \Rightarrow a^2 - 2a = 0 \Rightarrow a(a-2) = 0$$

$\Rightarrow a = 0$ or $a = 2$ if $a = 0$ then $\varnothing(2.n) = \varnothing(2)\varnothing(n) = 0$.

Hence $\varnothing$ is zero map which is not isomorphism.

$\therefore \varnothing \neq 0 \therefore a = 2$ but then $a \notin 3\mathbb{Z}$.

Hence $2\mathbb{Z}$ is not isomorphic to $3\mathbb{Z}$.

5) Is $\mathbb{Z}\left[\sqrt{-2}\right]$ isomorphic to $\mathbb{Z}\left[\sqrt{-5}\right]$.

Solution : No, $\mathbb{Z}\left[\sqrt{-2}\right]$ is not isomorphic to $\mathbb{Z}\left[\sqrt{-5}\right]$. As if $\varnothing : \mathbb{Z}\left[\sqrt{-2}\right] \to \mathbb{Z}\left[\sqrt{-5}\right]$ is isomorphism $\varnothing(1) = a$.

$\therefore \phi(x) = \phi(x.1) = \phi(x).\phi(1) = a.\phi(x)$

$\Rightarrow \phi(x) = a.\phi(x)$

$\Rightarrow$ Hence a is multiplicative identity in $\mathbb{Z}\left[\sqrt{-5}\right]$.

$\therefore a = 1$

$\therefore$ *for any* $a \in \mathbb{Z}, \phi(a) = a$

Let assume $\phi\left(\sqrt{-2}\right) = \alpha + \beta\left(\sqrt{-5}\right)$

$$\therefore \quad -2 \quad = \phi\left(\sqrt{-2} : \sqrt{-2}\right) = \left(\phi\left(\sqrt{-2}\right)\right)^2 = \left(x + \beta\sqrt{-5}\right)^2$$

$$\therefore -2 = x^2 - 5\beta^2 + 2\alpha\beta\sqrt{-5}$$

Comparing we get $\alpha\beta = o$

$\Rightarrow \alpha = o \quad$ or $\quad \beta = o$

if $\alpha = o \quad \Rightarrow -2 = -5\beta^2 \Rightarrow \beta^2 = 2/5$

But no such β in $\mathbb{Z}$ exists

if $\beta = o$ then $\alpha^2 = -2$

again so such α exists.

Hence no such ϕ exists

$\therefore \phi\, \mathbb{Z}[\sqrt{-2}]$ is not isomorphic to $\mathbb{Z}\left[\sqrt{-5}\right]$.

6.4 Summary

1) **First Isomorphism Theorem of Ring:** Let $\varnothing : R \to S$ be a onto ring homomorphism then $R / \ker \varnothing \approx \varnothing(R)$.

2) **Second Isomorphism Theorem for Rings:** Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b : a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \approx A / A \cap B$

3) **Third Isomorphism Theorem of Ring:** Statement : Let I and J be ideals of R with $I \subseteq J$. Then J / I is an ideal of R / I and $(R / I)/(J / I) \approx R / J$.

4) Let D be an integral domain. Then there exists a field F (called the field of fraction of D) that contains a subring isomorphic to D.

6.5 Unit and Exercises

Exercises :

1) Let $R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$ under addition and multiplication of 2 x 2 matries. Prove that R is isomorphic to $\not\subset$.

2) Show that the map $\phi : \mathbb{R}[x] \to M_2(\mathbb{R})$ defined as $\phi(a_o + a\ x + .. + a_n x^n) = \begin{pmatrix} a_o & a_1 \\ o & a_o \end{pmatrix}$ is ring homomorphism. Find ker ϕ.

3) Let $R = \left\{ \begin{bmatrix} a & b \\ o & d \end{bmatrix} : a, b\ d \in \mathbb{Z} \right\}$. Show that $\phi : R \to \mathbb{Z} \times \mathbb{Z}$ defined by $\phi\left(\begin{bmatrix} a & b \\ o & d \end{bmatrix} \right) = (a, d)$ is a ring homomorphism. Find Ker ϕ.

4) Let ϕ be a ring homomorphism from a commutative ring R onto a commutative ring S and let A be un ideal of S.

(i) If A is prime in S, show that $\phi^{-1}(A) = \{x \in R : \phi(x) \in A\}$ is pprime in R.

(ii) If A is maximal in S, show that $\phi^{-1}(A)$ is maximal in R.

5) Let $\mathbb{Z}[i]$ = {a + bi : a, b $\in \mathbb{Z}$ }. Show that the field of quotients of $\mathbb{Z}[i]$ is ring – isomorphic to $\mathbb{Q}[i] : \{r + si / r, S \in \mathbb{Q}\}$ (Hint: Let F is field containing $\mathbb{Z}$ and *i*, then for any $a \in \mathbb{Z}, a \neq 0, \frac{1}{a} \in F,$ Hence F contain $\mathbb{Q}$ and *i*. Also prove that for any $a + bi, c + di \neq 0 \in \mathbb{Z}[i], \quad \frac{a + bi}{c + di} \in \mathbb{Q}[i]$.

7

EUCLIDEAN DOMAIN, PRINCIPAL IDEAL DOMAIN UNIQUE FACTORIZATION DOMAIN

Unit Structure

7.0 Objective

The Objective this chapter is to make you understand

- Prime and irreducible elements and difference between them.

  Euclidean domain *(ED)*
- Principal ideal domain *(PID)*
- Unique factorization domain *(UFD)*
- Difference between *E D, PID, UFD*

7.1 Introduction

Primes plays central role in theory of integers. Lots of famous theorems are there for prime. For example, there are infinite numbers of primes; there are infinite numbers of prime of the type *4n-1* (or *4n+1).* Euclid lemma which states that *p* is the prime, *plab* then either *pla* or *pla,* etc.

There some conjectures which are simple to state but yet not proved. One of them is twin prime theorem. Prime like *3* and *5*, *11* and *13*, *17* and *19* are called twin prime. Twin prime theorem states that "there are infinitely many twin primes". This conjecture yet to be proved.

We want to introduce same notion of prime to general ring. That is we want find element in general ring which has property similar to prime of integers.

Note that in case of integer we define prime as positive integers which are divisible by 1(unity) and itself but in case of general ring this definition may not be appropriate. As if *u* is unit in ring *R* and *a*

a|*b* then *ua*|*b*. Hence in a ring if there more than one unit then definitely there more than two divisors.

Hence we need different approach to define prime. One such approach given by Euclid lemma.

7.2 Prime and Irreducible Element

Definition: Let *R* be an integral domain. A non zero non unit element *p* of *R* is said to be *prime element in R* if whenever $p \mid a \cdot b \Rightarrow p \mid a \text{ or } p \mid b$.

Definition: A non zero non unit element *P* of integral domain *R* is said to be irreducible element if whenever $p = a \cdot b$ then either *a* is unit or *b* is unit.

Two elements *a* and *b* of integral domain *R* is said to be *associates* of each other if they differ by unit (i.e., *a=ub* for some unit *u*). The other way to say same thing is *a/b* and *b/a.*

Theorem 1: In an integral domain prime element are irreducible.

Proof: Let *R* be an integral domain and let $p \in R$ be prime element in *R*. To Prove *P* is irreducible.

Let $p = a \cdot b$

Hence To prove either *a* or *b* is unit.

Since $p \mid p \Rightarrow p \mid a.b \Rightarrow p \mid a \text{ or } p \mid b$ (Since *p* is prime element)

If $p \mid a$ then $a = kp$ for some $k \in R$

$\therefore p = ab \Rightarrow p = kpb \Rightarrow kb = 1 \Rightarrow b$ is unit in *R*

Similarly if $p \mid b$ then we can prove *a* is unit in *R*. Hence whenever $p = a \cdot b \Rightarrow$ either *a* or *b* is unit.

Therefore *p* is irreducible.

Remark:

1. In case of $\mathbb{Z}$, the prime and irreducible are same.
2. The above theorem say that prime and irreducible are same in an integral domain. But converse need not be true.

That is there are integral domain in which irreducible need not be prime.

Let see one such example. Consider the ring $\mathbb{Z}\left[\sqrt{d}\right]$ where *d* is square free integer. (That is *d* is not divisible by square of any number).

We define a function $N : \mathbb{Z}\left[\sqrt{d}\right] \to \mathbb{Z}$ define as $N\left(a + b\sqrt{d}\right) = a^2 - b^2 d.$ this function is called as norm function.

This function has some trivial property which is easy to prove (of course involve some calculation)

1. $N(xy) = N(x).N(y)$ for all $x, y \in \mathbb{Z}\left[\sqrt{d}\right]$.
2. If *u* is unit in $\mathbb{Z}\left[\sqrt{d}\right]$ if and only if *N(u) = 1*

(This is clear because the only unit in $\mathbb{Z}\left[\sqrt{d}\right]$ are ± 1 and $\pm 1, \pm i$ in case *d = i*)

3. If $x, y \in \mathbb{Z}\left[\sqrt{d}\right]$ such that *x*|*y* then $N(x) \mid N(y)$.

4. If $p \in \mathbb{Z}\left[\sqrt{d}\right]$ is prime then *N(p)* is prime number (This can be proved from III property and Euclid Lemma)

Now consider particular example $\mathbb{Z}\left[\sqrt{-3}\right]$

Consider $1+\sqrt{-3} \in \mathbb{Z}\left[\sqrt{-3}\right]$

Claim: $1+\sqrt{-3}$ is irreducible element

Let $1+\sqrt{-3} = xy$ for some $x, y \in \mathbb{Z}\left[\sqrt{-3}\right]$

$\therefore N\left(1+\sqrt{-3}\right) = N(xy)$

$\therefore 1-1(-3) = N(x)\,N(y)$

$\therefore N(x).\,N(y) = 4$

$\therefore N(x) = 1,\ \ N(y) = 4$ or $N(x) = 4, N(y) = 1$, or $N(x) = 2, N(y) = 2$

But in this case either *x* or *y* is unit in $\mathbb{Z}\left[\sqrt{-3}\right]$

Hence $1+\sqrt{-3}$ become irreducible.

The other possible case is $N(x) = 2, N(y) = 2$

Let $x = a+b\sqrt{-3} \in \mathbb{Z}\left[\sqrt{-3}\right]$ then $N(x) = a^2+3b^2 = 2$ but this is not possible for any value of $a, b \in \mathbb{Z}$. Hence this case is not possible.

Thus we have shown that $1+\sqrt{-3}$ is irreducible.

Also $\left(1+\sqrt{-3}\right)\ \left(1-\sqrt{-3}\right) = 4 = 2.2$

Thus $\left(1+\sqrt{-3}\right) | 2.2$ but $1+\sqrt{-3}\ \nmid 2$ as if $1+\sqrt{-3}\ | 2$ then

$2 = \left(1+\sqrt{-3}\right)\ \left(a+b\sqrt{-3}\right)$

$\Rightarrow 2 = a-3b+\left(a+b\right)\sqrt{-3} \Rightarrow a-3b = 2$ and $a+b = o$

But the above equations have no integer solution $1+\sqrt{-3} \dagger 2$

Hence $1+\sqrt{-3}\ | 2\cdot 2$ but $\left(1+\sqrt{-3}\right) \dagger 2$

$\therefore 1+\sqrt{-3}$ is not prime

3. If p is a prime element in an integral domain $R \leftrightarrow \langle p \rangle$ is prime ideal.

as let $a \cdot b \in \langle p \rangle \Rightarrow a \cdot b = kp \Rightarrow p | a \cdot b \Rightarrow p | a \text{ or } p | b$ [Since p is prime element]

$\Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle$

$\therefore a \cdot b \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle$

$\therefore \langle p \rangle$ is prime ideal.

Conversely, let $\langle p \rangle$ is prime ideal.

Let $p | a \cdot b \Rightarrow a \cdot b \in \langle p \rangle \Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle$ (Since $\langle p \rangle$ is prime ideal)

$\Rightarrow p | a \text{ or } p | b \Rightarrow p$ is prime element.

There are different classes of ring. Let we study them. In first year we study division algorithm in $\mathbb{Z}$ and in $\mathbb{R}[x]$. Actually they are Euclidean algorithm. The integral domain having Euclidean algorithm is called Euclidean domain *(ED)*. Similarly in F.Y.B.S.c we study the fundamental theorem of Arithmetic (i.e. Unique factorization theorem) applicable in $\mathbb{Z}$ and $\mathbb{R}[x]$.

The integral domain having this property is called unique factorization domain *(UFD)*. The class of integral domain in which every ideal is principal ideal is called principal ideal domain *(PID)*. We will study these class of ring one by one.

7.3 Euclidean Domain (ED)

An integral domain R is said to be Euclidean domain (ED). If there exist a function $d : R \to \mathbb{Z}^+ \cup \{0\}$ such that

(i) $d(a \cdot b) \geq d(a)$ for all $a, b \in R$.

(ii) For any $a, b \in \mathbb{R}, b \neq o$ there exist $p, r \in R$ such that $a = bp + r$ with $r = 0$ or $d(r) < d(b)$.

Note: Such function d is called Euclidean function.

Example:

1. $\mathbb{Z}$ is an Euclidean domain.

   In $\mathbb{Z}$, the Mod Function $|\ |$ is an Euclidean Function and division algorithm is Euclidean algorithm.

2. $\mathbb{R}[x]$, the ring of polynomial over $\mathbb{R}$ is Euclidean domain.

   In $\mathbb{R}[x]$, the degree function, degree of polynomial is Euclidean Function and division algorithm of polynomials are Euclidean algorithm.

3. Any Field is by default Euclidean domain. In a field multiplication is Euclidean Function. If $a, b \in F, b \neq o$ then $a = b\left(b^{-1}a\right)$ this is nothing but Euclidean algorithm.

4. Consider the ring of *Gaussian* integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Then $\mathbb{Z}$ [i] is Euclidean domain.

Define the function $N : \mathbb{Z}[i] \to \mathbb{N}U\{o\}$ as $\therefore N(a+ib) = a^2 + b^2$.

Then for any $x, y \in \mathbb{Z}[i]$

$N(x.y) = N(x)\,N(y)$

To See Euclidean algorithm.

Let $x = a + ib$ and $y = c + id \in \mathbb{Z}[i]$ such that $c + id \neq 0$. Consider the Quotient $\frac{x}{y}$.

Let $\frac{x}{y} = \mathrm{s} + it$ where $s, t \in \mathbb{Q}$.

Let *m, n* be the integers closest to s and t respectively such that $|m - \mathrm{s}| \leq 1/2$ and $|n - t| \leq 1/2$

Then $\frac{x}{y} = \text{s+it} = (m-m+s)+i(n-n+t)i$

$$=(m+in)+\left[(s-m)+i(t-n)\right]$$

Then $x=(m+in)+\left[(s-m)+i(t-n)\right]y$

We claim thath the division algorithm of the definition of a Euclidean domain is satisfied si satisfied with $q = m + ni$ and $r=(m+in)+\left[(s-m)+i(t-n)\right]$

Clearly, q belongs to Z[i], and since $r = x - qy$, so does r. Finally

$$N(r)=N\left((s-m)+i(t-qn)i\right)\cdot N(y) \quad =\left((s-m)^2+(t-n)^2\right)N(y)$$

$$\leq\left(\frac{1}{4}+\frac{1}{4}\right)N(y)<N(y)$$

Hence for any $x, y\in\mathbb{Z}[i], y\neq 0\ \exists\ \text{q, r}\in\mathbb{Z}[i]$ Such that $x=\text{q}y+\text{r}$ with $N(\text{r})<N(y)$.

Hence $\mathbb{Z}[i]$ has Euclidean algorithm. $\therefore \mathbb{Z}[i]$ is Euclidean domain.

These are some example of Euclidean domain. Let us understand the importance of being Euclidean domain.

Theorem 2: In an Euclidean domain every ideal is principal ideal (i.e generated by single element).

Proof: Let *R* be an Euclidean domain and let *I* be any non zero ideal of *R*.

Let *d* be an Euclidean function of *R* choose $a\in I$ such that *d(a)* is minimum.

Claim : $I=\langle a\rangle$.

Let $b\in I$ be arbitrary. Then by Euclidean algorithm there exist $p, r\in R$. Such that $b = ap + r$ with $r = 0$ or $d(r)<d(a)$. If $r\neq 0$ then $r=b-ap\in I$ $\left(\text{since } I \text{ is ideal }\right)$ but then *d(r) < d(a)* will contradiction as *a* is the element of I such that *d(a)* is minimum.

$\therefore r = 0 \therefore b = aq \quad \Rightarrow b \in \langle a \rangle$

but $b \in I$ be arbitrary.

Hence $I \subseteq \langle a \rangle$

$\therefore I = \langle a \rangle$

$\therefore I$ *is principal ideal*

The Integral domain in which every ideal is principal is known as *Principal ideal domain (PID).* Thus above theorem says that every Euclidean domain is principal ideal domain.

Now we see this class of ring in details.

7.4 Principal Ideal Domain

An Integral domain *R* is said to be *principal ideal domain (PID)* if every ideal of R is Principal ideal.

Example:

1. Every field is by default Principal ideal domain.

   Since only ideal in field *F* is zero ideal and *F* itself. (Since fields are *simple ring*). The zero ideal is generated by zero elements and F is generated by unity.

2. $\mathbb{Z}$ is *PID*.Since any ideal of $\mathbb{Z}$ are of the form $m\mathbb{Z}, m \in \mathbb{Z}$.

3. $\mathbb{R}[x]$ is *PID*.One can argue like, as $\mathbb{R}[x]$ is Euclidean domain, every Euclidean domain is PID, hence $\mathbb{R}[x]$ is PID. But we can prove directly that $\mathbb{R}[x]$ is PID. Proof is exactly similar to the way we prove "In Euclidean domain every ideal is principal". We request the students to understand the similarity between two proofs.

Proof: Let *I* be any nonzero ideal of $\mathbb{R}[x]$ Since Let $f(x) \in I$ such that *f(x)* is monic and deg *f(x)* is minimum.

Claim:- $I = \langle f(x) \rangle$

Let $g(x) \in I$ be arbitrary.

Let $\mathbb{R}[x]$ is Euclidean domain, then by division algorithm, there exist $p(x)$ and $r(x) \in \mathbb{R}[x]$ such that $g(x) = p(x) f(x) + r(x)$ with $r(x) = o$ or $deg\ r(x) < deg\ f(x)$.

If $r(x) \neq O$ then $r(x) = g(x) - p(x) f(x) \in I$ (Since I is ideal)

But this is contradiction to minimality of $deg\, f(x)$ as $f(x) \in I$, $f(x)$ is monic & $deg\ f(x)$ is minimum.

Hence $r(x) = 0$

$\therefore g(x) = p(x) f(x) \Rightarrow g(x) \in \langle f(x) \rangle \Rightarrow I \subseteq \langle f(x) \rangle$

$\therefore I = \langle f(x) \rangle$

Hence *I* is principal ideal.

$\therefore$ Every ideal of $\mathbb{R}[x]$ is principal Hence $\mathbb{R}[x]$ is *PID*.

4. $\mathbb{Z}[x]$ is not *PID*.

Consider the ideal $I = \{ f(x) : f(0) \text{ is even} \}$ i.e. *I* is ideal of $\mathbb{Z}[x]$ with even constant term.

$$I = \{ a_n x^n + .. + a_1 x + a_o : a_2 \in \mathbb{Z}, a_o \text{ is even} \}$$

$$= \{ x(a_n x^{n-1} + .. + a_1) + 2b_o : a_o = 2b_o \} = \langle x, 2 \rangle$$

Let assume that $\langle x, 2 \rangle = \langle f(x) \rangle$ for some $f(x) \in \mathbb{Z}[x]$.

$\therefore x \in \langle f(x) \rangle$
$\therefore x = f(x) g(x)$ for some $g(x) \in \mathbb{Z}[x]$

$\therefore$ 1 = *deg* x = $deg\ (f(x) g(x)) = deg\ f(x) + deg\ g(x)$

$\Rightarrow deg\ f(x) + deg\ g(x) = 1$ but as degree is non negative number,

Hence either $deg\ f(x)=1,\ deg\ g(x)=0$

or $deg\ f(x)=0,\ deg\ g(x)=1$.

If deg *f(x)* = 1, then *f(x)* = $ax + b$, for some $a,b\in\mathbb{Z}$ but then $2\in\langle f(x)\rangle\Rightarrow 2\in\langle ax+b\rangle$ is not possible. Hence $deg\ f(x)\neq 1$.

$\therefore deg\ f(x)=0\Rightarrow f(x)$ is constant polynomial.

Let $2=f(x)h(x)$ for some $h(x)\in\mathbb{Z}(x)$ then $2=f(1)h(1)$

$\Rightarrow f(1)=\pm 2\ (\because 1\notin I)$ but $\Rightarrow f(x)=\pm 2$ (As *f(x)* is constant polynomial but then $x=\pm 2g(x)$ which is nonsense.

Hence $\langle x,2\rangle=\langle f(x)\rangle$ is not possible.

$\therefore$ *I* is not principal ideal.

A ring being Principal ideal domain has lots of advantage. We see them one by one. We already seen "In an integral domain primes are irreducible". But we also seen the example of integral domain where irreducible are not prime. The one advantage of being *PID* is that irreducible are also prime.

Theorem 3: In Principal ideal domain irreducible are prime,

Proof: Let *R* be principal ideal domain, and let *r* be irreducible element of *R*.

To prove *r* is prime.

Let $r\mid bc,\ c,\ b\in R$.

Clearly *r* is non zero, non unit element.

To prove $r\mid b$ or $r\mid c$ consider the ideal $I=\{xr+by\ /\ x,\ y\in R\}$ Since *R* is *PID*

$\therefore I=\langle d\rangle$ for some $d\in R$

Since $r\in I=\langle d\rangle$

$\therefore r=ad$ for some *a* in *R*. (as *r* is irreducible)

$\therefore$ either *a* or *d* is unit.

If d is unit then $I = R$ and as $1 \in R \therefore \exists\, \alpha, \beta \in R$ such that $1 = \alpha r + \beta b$

$\therefore c = (\alpha c) r + \beta (bc) \therefore r \mid (\alpha c) r , r \mid bc \Rightarrow r \mid \beta bc$

$\therefore r \mid \alpha cr + \beta bc \Rightarrow r \mid c$

Now if a is unit then $< r > = < d >$ and as $b \in \langle d \rangle \Rightarrow b \in \langle r \rangle \Rightarrow r \mid b.$

$\therefore r$ is prime

1. In short we say that in *PID*, prime and irreducible are same.
2. We had seen that in $\mathbb{Z}\left[\sqrt{-3}\right]$, irreducible are not prime from this and above theorem we conclude that $\mathbb{Z}\left[\sqrt{-3}\right]$ is not PID.
3. One more advantage of being *PID* is existence of *GCD*. Before we see let recall the definition.

Definition:

(i) Let R be a ring. We say that element a of R divides $b \in R$ or b is divisible by a if there exist $c \in R$ such that $b = ac$ and this we denote by $a \mid b$.

(ii) Let R be a ring $a, b \in R$. We say that $d \in R$ is greatest common divisior (GCD) of a and b if (i) $d \mid a$ and $d \mid b$ (ii) If $d \in R$ such that $d' \mid a$ and $d' \mid b$ then $d' \mid d$. It is denoted by (a, b).

In short the greatest common divisor of *a, b* at is the largest among all common divisor.

In school, even if in F.Y.B.Sc. we seen how to find GCD of two positive integer. The Euclidean algorithm is powerful technique to find GCD. We also seen how to GCD of two polynomial with the help of division algorithm.

Do you think GCD of any two number exists in all integral domain. To surprise you the answer is no.

Let see this example.

Let $a = 4$ & $b = 2\left(1+\sqrt{-3}\right)$ in $\mathbb{Z}\left[\sqrt{-3}\right]$

as $a = (2)(2) = \left(1+\sqrt{-3}\right)\left(1-\sqrt{-3}\right)$

$b = 2(1-\sqrt{-3})$ then $2|a$ and $2|b$ and $\left(1+\sqrt{-3}\right)|a$ and $\left(1+\sqrt{-3}\right)|b$

$\therefore$ Both 2 and $\left(1+\sqrt{-3}\right)$ are common divisor of a & b. But $2 \nmid (1+\sqrt{-3})$ and $\left(1+\sqrt{-3}\right) \nmid 2$ as both are irreducible.

Like this you can see so many example of non existence of GCD, Note that $\mathbb{Z}\left[\sqrt{-3}\right]$ is not PID.

So we hope you can guess the second advantage being yes. PID guarantees the existing of GCD.

Theorem 4: Let R Principal ideal domain. Then for any $a, b \in R$, greatest common divisor of a and b exists.

Proof: R is *PID* and $a, b \in R$. Consider the ideal $I = \{ax + by : x, y \in R\}$ As R is PID,

$\therefore$ there exist d $\in$ R such that I=< d >.

Claim: d is gcd of a, b.

(1) $\because b, a \in I = \langle d \rangle$

$\therefore a = a_1 d$ & $b = b_1 d, a_1, b_1 \in R \Rightarrow d|a$ & $d|b$

$\because d \in \langle d \rangle = I$

$\therefore \exists\, m, n \in R$ such that $d = am + bn$.

Now let assume that $d^1 \in R$ such that $d^1|a$ and $d^1|b$.

$\Rightarrow \exists\, \alpha_1 \beta \in R$ such that $a = \alpha d^1$ *and* $b = \beta d^1$.

then $d = am + bn = \alpha m d^1 + \beta n d^1 = (\alpha m + \beta n) d^1 \Rightarrow d^1 | d$

Hence *d* is GCD of *a* and *b*.

1. Note that the GCD *d* of *a* and *b* is generator of ideal generated by *a* and *b*. This may the reason why GCD is denoted by (a,b).

2. Every Euclidean domain is PID. Hence in Euclidean domain also GCD of any two elements exists. In fact Euclidean algorithm is best way to calculate the GCD.

3. We have shown that Euclidean domain $\Rightarrow$ PID but PID does not mean Euclidean domain. For example it shown that the ring $R=\left\{a+b\theta \mid a,b\in\mathbb{Z},\ \theta=\frac{1+\sqrt{-19}}{2}\right\}$ is PID but not Euclidean domain, but detail is beyond the scope of syllabus. So we skip that.

Now let we move to next advantage of being PID. That is PID every ascending chain of ideal is finite.

Theorem 5: Let *R* be PID and $I_1\subset I_2\subset \mathrm{I}_3\subset\cdots I_n\subset\cdots$ be strictly increasing chain of ideals. Then this chain must be at finite length.

Proof: Let $I=\underset{n}{U} I_n$

Claim:*I is ideal of R.*

$I_1\subset I_2\subset \mathrm{I}_3\subset\cdots I_n\subset\cdots$

$Let\ a,\ b\in I=\underset{n}{U} I_n$

$\therefore \exists\ p,\ q$ such that $a_1\in I_p,\ b\in I_p,\ b\in I_q$

if $p\neq q$ let $p<q$ then $I_p\subset I_q$

$\Rightarrow a,b\in I_q\Rightarrow a-b\in I_q\ \left(\because I_q \text{ is ideal}\right)\quad\Rightarrow a-b\in I=\underset{n}{U} I_n$

Let $r\in R$ then clearly *ar* and $ra\in I_p$

$\therefore ar\ and\ ra\in I=\underset{n}{U} I_n.$

Hence *I* is ideal.

But as R is PID, therefore there exist $d \in R$ such that $I = \langle d \rangle$

Since $d \in \langle d \rangle = I = \underset{n}{U} I_n$

$\therefore$ there exist k such that $d \in I_k$

but then $I = \langle d \rangle \subseteq I_k \Rightarrow \underset{n}{U} I_n \subseteq I_k$

Hence $I_1 \subset I_2 \subset \mathrm{I}_3 \subset \cdots I_n \subset \cdots$

$\therefore$ chain of ideal is finite.

This is important theorem which helps us (in future) to prove that $PIDs$ have property called unique factorization as a product of irreducible. The class of ring having this property is called as unique factorization domain (UFD). Let we study this in details.

7.5 Unique Factorization Domain (UFD)

An integral domain R is said to be unique factorization domain (UFD) if

(i) Every non zero non unit element R can be expressed as a product of irreducible of R.

(ii) The factorization into irreducible is unique up to associates and the order in which the factors appear.

Now let we prove $PID \Rightarrow \mathrm{U}FD.$

Theorem 5: Every principal ideal domain is Unique factorization domain.

Proof: Let R be a principal ideal domain and let a_o be any non zero non unit element of R.

We will prove that a_o can be expressed as product of irreducible

Claim: a_o has at least one irreducible factor.

If a_o is itself irreducible, then we are done. So assume $a_o = a_1 b_1$ where neither of a_1, b_1 are unit and a_1 is non zero.

If a_1 is irreducible then a_1 become irreducible factor of a_o.

So assume $a_1 = a_2 b_2$ where neither of a_2 and b_2 are unit. It a_2 is irreducible then we done otherwise we continue some step so that sequence of element a_n, b_n of R such that $a_{n-1} = a_n b_n$.

Thus we have $\langle a_0 \rangle \underset{\neq}{\subset} \langle a_1 \rangle \underset{\neq}{\subset} \langle a_2 \rangle \underset{\neq}{\subset} ....$

Thus we have strictly increasing sequence of ideal in R. But R PID. There for this Chain must be finite.

That is there exist $a_r \in R$ such that $\langle a_1 \rangle \subset \langle a_2 \rangle \subset ... \langle a_r \rangle$

In particular a_r is irreducible factor of a_o.

Thus every non zero non unit element of R has irreducible factor.

Let $a_0 = p_1 q_1$ where p_1 is irreducible if q_1 is also irreducible we get a_0 as product of irreducible.

Let assume q_1 is not irreducible. clearly q_1 is not unit otherwise $\underline{a_0}$ become irreducible which is not the case.

Hence let $q_1 = p_2 q_2$ where p_2 where q_2 is irreducible & q_2 is not unit. If q_2 is also irreducible then $a_0 = p_1 q_1 = p_1 p_2 q_2$, product of irreducible and we done. If not we continue same process. Thus again getting ascending chain of ideal $\langle a_0 \rangle \subset \langle q_1 \rangle c \subset ....$ Being PID this chain must be finite. Hence $\exists q_m \in R$ such that $\langle a_0 \rangle c \langle q_1 \rangle C ... C \langle q_m \rangle$, q_m being irreducible as product of irreducible.

Thus every non zero non unit element of R can be written as product uniqueness.

Let $a = p_1 p_2 ... p_k = q_1 q_2 ... q_r$ where p_i and q_j are irreducible in R for all i and j.

$\therefore p_1 p_2 ... p_k = q_1 q_2 ... p_r$

$\because p_1 \mid p_1 \; p_2 ... p_k$

$\therefore p_1 \mid q_1 \; q_2 ... q_r$

And as irreducible are prime in PID.

$\therefore p_1 \mid q_j$ for some j. Without loss of generality let $p_1 \mid q_1$

$\therefore q_1 = p_1 a_1$ but both p_1 and q_1 are irreducible $\Rightarrow a_1$ is a unit.

$\therefore p_1$ is associate of q_1.

$\therefore p_1\ p_2 \ldots p_k = q_1 q_2 \ldots q_r \Rightarrow p_2 \ldots p_k = a_1\ q_2 \ldots q_r \Rightarrow p_2 \ldots p_k = a_1\ q_2 \ldots q_r$

Similarly canceling $p_2, p_3 \ldots$ and if $K < r$ we get

$1 = a_1\ a_2 \ldots a_k\ q_{k+1} \ldots q_r \Rightarrow 1$ as product of irreducible.

This is contradiction.

Hence $r = k$ and $p_i's$ are associate of $q_j's$. Hence proved.

Example :

1) A field $F, \mathbb{Z}, \mathbb{R}[x]$ as being PID, there are UFD.

   One can prove directly. In case of field, there is no non zero non unit element. Hence by default field are UFD.

   In case of $\mathbb{Z}\left(and\ \mathbb{R}[x]\right)$ we can prove unique factorization in prime (irreducible polynomial) as in F.Y.B.Sc.

2) A part from this one can show that it D is UFD then $D[x]$ also.

   Thus as $\mathbb{Z}$ is UFD, there fore $\mathbb{Z}[x]$ also.

   This theorem is proved in next chapter.

Remark : Since $PID \Rightarrow UFD$ but converse need not be true that is $UFD \not\Rightarrow PID$.

For example we seen that $\mathbb{Z}[x]$ is not PID but it is UFD as $\mathbb{Z}$ is UFD.

Being UFD will also has lots of benefit. One such benefit is given in following theorem.

Theorem : In unique factorization domain irreducibles are primes.

Proof :

Let R be a UFD and $a \in R$ be irreducible.

To show that *a* is prime.

As *a* is irreducible. $\therefore a$ is non zero non unit.

Let $a \mid bc$ for some $b, c \in R$.

$\therefore bc = ka$ for some $k \in R$.

As *R* is UFD, therefore b, c, k can be written as product of irreducible.

Let $b = b_1 b_2 b_3 \ldots b_\ell$, $c = c_1 c_2 \ldots c_{jn}$, $k = k_1 k_2 \ldots k_n$ where b_i, c_j and k_p are irreducibles in *R* for all i, j and *p* then

$$bc = ka \Rightarrow b_1 b_2 \ldots b_\ell \ldots c_1 c_2 \ldots c_m = k_1 k_2 \ldots k_n a .$$

As factorization is unique upto associates. Hence a must be associates of some b_i or c_j if a is associate of b_i then $a \mid b_i$ and hence $a \mid b$ if *a* is associate of some c_j then $a \mid c_j$ and hence $a \mid c$.

$\therefore a \mid bc \Rightarrow a \mid b$ or $a \mid c$

$\therefore a$ is prime.

Thus we see in case of PID and UFD primes and irreducibles are essentially same.

This is the one reason why interval domain like $\mathbb{Z}\left[\sqrt{-3}\right]$ is no UFD (Note that $\mathbb{Z}\left[\sqrt{-3}\right], 1+\sqrt{-3}$ is irreducible but not prime).

One more advantage of being UFD is that it also guarantees the existence of GCD of any two element of UFD. This is given as an exercise.

7.6 Summary

1) Let R be an integral domain. A non zero non unit element p of R is said to be *prime element in R* if whenever $p \mid a \cdot b \Rightarrow p \mid a \text{ or } p \mid b$.

2) In an integral domain prime element are irreducible.

3) An integral domain R is said to be Euclidean domain (ED). If there exist a function $d : R \to \mathbb{Z}^{+} U \{0\}$ such that

   (i) $d(a \cdot b) \geq d(a)$ for all $a, b \in R$.

   (ii) For any $a, b \in \mathbb{R}, b \neq o$ there exist $p, r \in R$

   such that $a = bp+r$ with $r=0$ or $d(r) < d(b)$.

4) In an Euclidean domain every ideal is principal ideal (i.e generated by single element).

5) An Integral domain R is said to be *principal ideal domain (PID)* if every ideal of R is Principal ideal.

6) Let R be PID and $I_1 \subset I_2 \subset \mathrm{I}_3 \subset \cdots I_n \subset \cdots$ be strictly increasing chain of ideals. Then this chain must be at finite length.

7) An integral domain R is said to be unique factorization domain (UFD) if

   (i) Every non zero non unit element R can be expressed as a product of irreducible of R.

   (ii) The factorization into irreducible is unique up to associates and the order in which the factors appear.

8) Every principal ideal domain is Unique factorization domain.

9) In unique factorization domain irreducibles are primes.

7.7 Unit and Exercises

1. Define

   (i) Euclidean domain

   (ii) Principal ideal domain. Show that a Euclidean domain is a principal ideal domain.

2. Show that the following rings are Euclidean domain:

   (i) The ring $\mathbb{Z}[i]$, ring of Gaussian integer

   (ii) The polynomial ring *F[x],* where F is a Field.

3. Show the polynomial ring $\mathbb{R}[x]$ is OID.

4. Prove or disprove

   If *F* is PID then *F[x]* is also PID.

5. Show that every ascending chain of ideals

   $I_1 \subset I_2 \subset ... \subset I_n \subset I_{n+1} ...$ in a PID R is finite.

6. Prove that in a PID R, an element $a \in R$ is prime

   if and only if a is irreducible.

7. Show that a PID is a UFD.

8. Show that any prime element in integral domain is irreducible.

   Is converse true? Justify your answer.

9. Explain why $\mathbb{Z}\left[\sqrt{-5}\right]$ is not PID.

10. Show that any two elements a & b in a PID *R* have a GCD which can be expressed in the form $\lambda a + \mu b$ where $\lambda, \mu, \in, R$.

11. Show that every irreducible element in a UFD is prime.

12. Is $\mathbb{Z}\left[\sqrt{-5}\right]$ is UFD? Justify your answer.

13. Show that $\mathbb{Z}$ is PID but $\mathbb{Z}[x]$ is not.

    (Hint : show that (2, x) is not principal ideal)

14. Let R be an integral domain in which every non zero, non unit element can be expressed as a product of irreducible and every irreducible element is prime. Show that R is UFD.

15. (Hint : Note that factorization is unique upto associate.

    Take two factorization of an element & use the fact that irreducible is prime.)

16. Let $\mathbb{R}$ be an UFD. Show that for any $a, b, \in R,$ gcd of a and b exist.

(Hint : let $a = p_1^{\ell 1} P_2^{\ell 2} \ldots p_k^{\ell k}$, $b = p_1^{m1} p_2^{m2} - .. p_k^{mk}$ where all ℓ_i and m_j need not be non zero then take $d = p_1^{n_i} p_2^{n2} .... p_k^{nk}$ where $n_i = \max\{\ell_i, m_i\}$ then show that d is gcd of a and b.

❖❖❖❖

8

IRREDUCIBILITY IN POLYNOMIAL RING

Unit Structure

8.0 Objective

This chapter makes you to understand

- Irreducible, reducible polynomials
- Classification of irreducible polynomials in $\mathbb{R}$ [x] and $\not\subset[x]$
- Various criteria to check irreducibility.
- Gauss lemma and Eisenstein's criteria.

8.1 Introduction

In the chapter of ring we had deals with polynomial ring in detail. In high school students spend much time factoring polynomials and finding their roots. This is what we going to learn in this chapter but in abstract manner. Let us understand FIRST which polynomial we can factorize and which cannot. We start with definition.

8.2 Definition and Example of Irreducible and Reducible Polynomial

Definition: Let *D* be an integral domain. A polynomial *p(x)* in *D[x]* is said to be *irreducible polynomial* if whenever *p(x) = f(x) g(x)* then either *f(x)* or *g(x)* is unit (i.e. constant polynomial) in *D[x]*.

Definition: A non zero – non unit polynomial of *D[x]* which is not irreducible is said to *reducible*.

Example:

1. The polynomial $2x^2-3$ is irreducible in $\mathbb{Q}[x]$ but reducible in $\mathbb{R}$ [x].

2. The polynomial x^2+1 is irreducible over $\mathbb{R}$ but reducible over $\mathbb{C}$.

3. The polynomial x^2+1 is irreducible over $\mathbb{Z}_3$ but reducible over $\mathbb{Z}_5$

Note that $\mathbb{Z}_3=\{\bar{0},\bar{1},\bar{2}\}$ $f(x)=x^2+1$ then

$f(\bar{0})=1, f(\bar{1})=\bar{2}, \quad f(\bar{2})=\bar{5} \bmod 3=\bar{2}.$

but if we take element from $\mathbb{Z}_5$

$f(0)=1\, f(1)=\bar{2}\, f(2)=4+1=5=\bar{0}\,(\text{mod } 5)$

$\therefore f(\bar{2})=\bar{0}$

Hence $x=\bar{2}$ is root x^2+1 *in* $\mathbb{Z}_5$

$\therefore x^2+1$ is reducible.

4. The only irreducible polynomial in $\mathbb{R}$[x] are linear polynomial or the polynomial x^2+bx+c such that $b^2-4c<o$.

Proof: Clearly the linear polynomial *ax + b,* $a,b\in\mathbb{R}$ are irreducible polynomial because they cannot be factorize.

Similarly for polynomial $x^2-bx+c, if\ b^2-4c<o$ then it has complex root hence cannot be factorize. Now we will prove polynomial of any other degree must be reducible. Let f(x) is any polynomial of degree *n, n>2.*

Case I: *deg f(x)* is odd.

As complex roots are always come with conjugate pair and number of roots is equal to degree of polynomial, therefore a polynomial of odd degree must have one real root.

Let α be real root of *f(x)*.

$\therefore f(x)=(x-\alpha)g(x)$ where degree of $g(x)=n-1$

$\therefore f$ is reducible.

Case II: deg *f(x)* is even.

In worst case let assume all roots of *f(x)* are complex.

Let $a + ib$ be one root of *f(x)* then $a-ib$ must be other roots.

$\therefore f(x)=(x-(a+ib))(2-(a-ib))g(x).$

$=((x-a)-ib)((x-a)+ib)g(x)=\left((x-a)^2+b^2\right)g(x)$

$\therefore (x-a)^2+b^2$ and $g(x)$ are two factors of $f(x)\, in\, \mathbb{R}[x]$

$\therefore f(x)$ is reducible.

5. The only irreducible polynomial in $\mathbb{C}$ are linear polynomials.

   The other way of saying this is every polynomial over

   One of important problem in mathematics is to find root of polynomials. These roots have different meaning and application in different context. Lots of techniques are developed in order to find the root of polynomial.

   Suppose we had applied one technique to find root. But we haven't got, then we apply second technique to find root but we havn't got, then third, and so on. And then we came to know that this polynomial has no solution.

   If in advance we get to know that the polynomial has no root or in other word it is irreducible then lots of our efforts can be saved. So we are going to see some test to check whether given polynomial are reducible or not.

Reducibility test for Degrees 2 and 3.

Theorem 1: Let *F* be a field. If $f(x) \in F[x]$ and $\deg f(x) = 2$ or *3* then f(x) is reducible over *F* if and only if *f(x)* has a zero in *F*.

Proof : Suppose that $f(x) = g(x)h(x)$

Where $g(x), h(x) \in F[x]$.

as $\therefore \deg f(x) = \deg g(x) + \deg h(x)$

as $\deg f(x) = 2$ or *3*

$\therefore$ one of the polynomial *g(x)* or *h(x)* must be of degree one.

Let assume deg *g(x)* = 1.

$\therefore g(x) = ax + b, \quad a \neq 0$

then clearly $x = 1 - b.a^{-1} \in F$ is root of *g(x)* and hence of *f(x)*.

$\therefore$ Conversely let assume that *f* has root α in *F* then *f(x) = (x-α) g(x)*

where deg *g(x) = 1 or 2* $\therefore$ *f(x)* is reducible.

The above theorem is particularly used when the underlying Field is $\mathbb{Z}_p$. because in this case, we can check for reducibility of *f(x)* by simply checking that *f(a) = 0* or not for *a = 0, 1, ..., p-1*.

Note that the polynomials of degree larger than *3* may be reducible over a field, even though they do not have zeros in field. For example in

$\mathbb{Q}$ [x], the polynomial $x^4 + 2x^2 + 1$ is equal to $\left(x^2 + 1\right)^2$, but has no zeros in $\mathbb{Q}$.

To see next tests for inedibility we need following definition.

Content of Polynomial

Definition: The content of a non zero polynomial $a_n x^n + a_{n-1}x^{n-1} + .. + a_o$, where $a_i \in \mathbb{Z}$ is the greatest common divisor of $a_n, a_{n-1}, .. a_1, a_o$.

Definition: A polynomial $a_n\, x^n + .. + a_1 x + a_o, a_i \in \mathbb{Z}$ is said to be *primitive polynomial* if its content is one.

8.3 Gauss Lemma

Theorem 1: The product of two primitive polynomials is Primitive.

Proof: Let *f(x)* and *g(x)* be primitive polynomials and suppose that *f(x)g(x)* is not primitive. Let *p* is prime divisor of content of *f(x) g(x)*. Let $\overline{f}(x), \overline{g}(x)$ and $\overline{f(x)\,g(x)}$ be the polynomials obtained from *f(x), g(x)* and *f(x) g(x)* by reducing the coefficient modulo p

then $\overline{f}(x), \overline{g}(x) \in \mathbb{Z}_p[x]$ and $\overline{f(x), g(x)} = 0 \text{ in } \mathbb{Z}_p[x]$

($\because$ Each coefficient of *f(x) g(x)* is divisible by *p*)

$\Rightarrow \overline{f(x)}\,\overline{g(x)} = 0 \; in \; \mathbb{Z}_p[x]$

$\Rightarrow \overline{f(x)} = 0 \quad or \quad \overline{g(x)} = 0.$ ($\because$ p is prime, $\therefore \mathbb{Z}_p$ is integral domain and hence $\mathbb{Z}_p[x]$ is integral domain.)

$\Rightarrow$ Either *p* divides coefficient of *f(x)* or *p* divides coefficient of g(x).

Which is contradiction as *f(x)* and *g(x)* is primitive.

$\therefore f(x)g(x) \; is \; primitive.$

Theorem 2: Let $f(x) \in \mathbb{Z}[x]$. If *f(x)* is reducible over $\mathbb{Q}$,

then it is reducible over $\mathbb{Z}$.

Proof: Suppose that *f(x) = g(x) h(x),* where *g(x)* and *h(x)* $\in \mathbb{Q}[x]$.

We may assume that *f(x)* is primitive because we can divide both *f(x)* and *g(x) h(x)* by content of *f(x)*. Let *a* and *b* be the least common multiple of the denominators of the coefficients of *g(x)* and *h(x)* respectively.

Then *ab f(x) = ag(x) bh(x)* where $ag(x), bh(x) \in \mathbb{Z}[x]$.

Let c_1 and c_2 be the content of *ag(x)* and *bh(x)* respectively.

$\therefore ag(x) = c_1 g_1(x)$ and $bh(x) = c_2\, h_1(x)$. where $g_1(x)$ and $h_1(x)$ are primitive polynomial in $\mathbb{Z}[x]$

$\therefore ab\, f(x) = c_1\, c_2\, g_1(x).\, h_1(x).$

Note that *f(x)* is of content 1, Hence content *abf(x)* is *ab*.

By Gauss lemma $g_1(x).h_1(x)$ is also primitive.

$\therefore$ content at $c_1\, c_2\, g_1(x)\, g_2(x)$ *is* $c_1\, c_2$.

$\therefore abf(x) = c_1\, c_2\, g_1(x).h_1(x) \Rightarrow ab = c_1\, c_2$

$\therefore f(x) = g_1(x).h_1(x)$ *where* $g_1(x), h_1(x) \in \mathbb{Z}[x]$

$\therefore f(x)$ is reducible over $\mathbb{Z}[x]$.

Theorem 3: Let *P* be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with deg $f(x) \geq 1$. Let $\overline{f}(x)$ be a polynomial in $\mathbb{Z}_p[x]$ obtained from *f(x)* by reducing all coefficients of *f(x)* modulo *p*. If *f(x)* is irreducible over $\mathbb{Z}_p$ and deg $\overline{f}(x) = \deg f(x)$ then *f(x)* is irreducible over $\mathbb{Q}$.

Proof: Since by previous theorem we know that if *f(x)* is reducible over $\mathbb{Q}$ then it is reducible over $\mathbb{Z}$.

Hence let assume *f(x) = g(x). h(x)* where *g(x), h(x)* $\in \mathbb{Z}[x]$.

Let $\overline{f}(x), \overline{g}(x)$ and $\overline{h}(x)$ be the polynomials obtained from *f(x)*, *g(x)* and *h(x)* by reducing all the coefficients modulo *p*. And $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p$.

Since deg *f(x)* = deg $\overline{f}(x)$

$\therefore \deg \overline{g}(x) \leq \deg g(x) < \deg \overline{f}(x)$ and $\deg \overline{h}(x) \leq \deg h(x) < \deg \overline{f}(x)$

But $\overline{f}(x) = \overline{g}(x).\overline{h}(x)$

This means that $\overline{g}(x)$ *and* $\overline{h}(x)$ are proper factor $\overline{f}(x)$, but this is contradiction to our assumption that $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p$.

Hence our assumption that *f(x)* reducible over $\mathbb{Q}$ is wrong.

$\therefore f(x)$ is irreducible over $\mathbb{Q}$.

Example:

Let $f(x) = 21x^3 - 3x^2 + 2x + 7$

Then over $\mathbb{Z}_2$, $\overline{f}(x) = x^3 + x^2 + 1$

Since $\overline{f}(0) = 1 = \overline{f}(1)$

then $\overline{f}(x)$ is irreducible over $\mathbb{Z}_2$

and as deg f= deg $\overline{f}$

$\therefore f(x)$ is irreducible over $\mathbb{Q}$.

8.4 Eisenstein's Criterion

Theorem 4: Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + .. + a_o \in \mathbb{Z}[x]$ if there is a prime p such that $P \dagger a_n, P \mid a_{n-1}, ..., P \mid a_o$ but $P^2 \dagger a_o$ then *f(x)* is irreducible over $\mathbb{Q}$.

Proof: Let assume that *f(x)* is reducible over $\mathbb{Q}$. Then by previous theorem *f(x)* is reducible over $\mathbb{Z}$ also.

Let assume that *f(x) = g(x) h(x)* where $1 < \deg g(x), \deg h(x) < n.$

Let $g(x) = b_r x^r + .. + b_1 x + b_o$ and $h(x) = c_k x^k + .. + c_1 x + c_o.$

Since *f(x) = g(x). h(x)*

$\therefore a_n = b_r c_k$ and $a_o = b_o c_o.$

Since $P \mid a_o \Rightarrow p \mid b_o . c_o \Rightarrow p \mid b_o \; or \; p \mid c_o$ (Since *P* is prime)

but $p^2 \dagger a_0$, p does not divide both b_o & c_o. Hence Let assume $p \mid b_o \; but \; p \dagger c_0$

Also $p \mid a_n \Rightarrow p \mid b_r . c_k \Rightarrow p \mid b_r$ & $p \mid c_k.$

$p \dagger a_n \Rightarrow p \dagger b_r c_k \Rightarrow p \dagger b_r \; and \; p \dagger c_k$

$\because p \dagger b_r$

Therefore there exist least integer t such that $p \dagger b_t$ but the

$a_t = b_t c_o + b_{t-1} c_1 + ... + b_o c_t$
$as\ p \mid a_t$

Now by choice of *t, p* must divide each term of right hand side except the first one.

$p \mid \left(a^t - \left(b_{t-1} c_1 + ... b_o c_t\right)\right) ie.\ p \mid b_t . c_o.$ Which is not possible as $p \mid b_t, p \mid c_o.$

Hence *f(x)* is irreducible over $\mathbb{Q}$.

Example: Irreducibility of p^{th} **Cyclotomic polynomial** for any prime *p*,

The p^{th} Cyclotomic polynomial.

$\varnothing_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1$ is irreducible over $\mathbb{Q}$.

As consider the polynomial

$$f(x) = \varnothing_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{\left(x^p + px^{p-1} + .. px + 1\right) - 1}{x} = x^{p-1} + px^{p-1} + .. + p$$

Note that *p* divides all coefficient of *f(x)* except for leading coefficient 1 and also p^2 does not divide constant term which *p*.

Hence by Eisenstein's criteria *f(x)* is irreducible over *Q*.

But if $\varnothing(x) = g(x).h(x)$ were a non trivial factorization of $\phi_p(x)$ over $\mathbb{Q}$ then $f(x) = \phi_p(x+1) = g(x+1)h(x+1)$ will we a non trivial factorization of *f(x)*.

Since this is impossible, hence we conclude that $\phi_p(x)$ is irreducible over $\mathbb{Q}$.

Let us understand the importance of irreducible polynomials.

1. The irreducible polynomial plays exactly same role as prime plays in case of integer. For example the fundamental theorem of arithmetic (or unique factorization theorem) irreducible polynomial are treated as prime.
2. One more reason which makes irreducible polynomial important, which is given in terms of next theorem.

Theorem 5: Let *F* be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in *F[x]* if and only if *p(x)* is irreducible over *F*.

Proof: Let assume that $\langle p(x) \rangle$ is maximal ideal in *F[x]*.

Let assume that *p(x)* is reducible then *p(x) = f(x) . g(x)*

$\Rightarrow p(x) \in \langle f(x) \rangle \Rightarrow \langle p(x) \rangle \subseteq \langle f(x) \rangle$

but $\langle p(x) \rangle$ is maximal ideal.

Hence it either $\langle p(x) \rangle = \langle f(x) \rangle$ or $\langle f(x) \rangle = F[x]$ if $\langle p(x) \rangle = \langle f(x) \rangle$ then $p(x)$ and $f(x)$ are associate of each that therefore $p(x) = f(x)\, g(x)$ implies *g(x)* is unit.

And if $\langle f(x) \rangle = F[x]$ this implies *f(x)* is unit.

$\therefore$ $p(x)$ is irreducible.

Conversely, let *p(x)* is irreducible.

Let assume I is ideal of *F[x]* such that $\langle p(x) \rangle \subseteq I \subseteq F[x]$

As *F[x]* is PID,

Therefore there exists $g(x) \in F[x]$ such that

$I = \langle g(x) \rangle \Rightarrow p(x) \in \langle g(x) \rangle \Rightarrow p(x) = f(x).\, g(x)$ for some $f(x) \in F[x]$

Now as *p(x)* irreducible.

$\therefore p(x) = f(x)\, g(x)$ implies either *f(x)* is unit or *g(x)* is unit.

If *f(x)* is unit *p(x)* and *g(x)* are associates of each other.

$\therefore \langle p(x) \rangle = \langle g(x) \rangle = I$

If g(x) is unit then $I = \langle g(x) \rangle = F(x)$

Hence $\langle p(x) \rangle$ is maximal.

Corollary 1: Let F be a field and let $p(x), a(x), b(x) \in F[x]$. If *p(x)* is irreducible over *F* and $p(x) \mid a(x)b(x)$, *then* $p(x) \mid a(x)$ *or* $p(x) \mid b(x)$.

Proof: Let since *p(x)* is irreducible, $\therefore \dfrac{F[x]}{< p(x) >}$ is a field and therefore integral domain.

Let $\bar{a}(x)$ *and* $\bar{b}(x)$ be the images of *a(x)* and *b(x)* under the natural homomorphism from *F[x]* to $\dfrac{F[x]}{< p(x) >}$. Since $p(x) \mid a(x)b(x)$.

$\therefore \bar{a}(x).\bar{b}(x) = \bar{0}$ in $\dfrac{F[x]}{< p(x) >}$, but then $\bar{a}(x) = \bar{0}$ or

$\bar{b}(x) = 0 \left(\text{Since } \dfrac{F[x]}{< p(x) >} \text{ is integral domain} \right)$.

Therefore it follows that $p(x) \mid a(x)$ *or* $p(x) \mid b(x)$.

Now we conclude this chapter by proving $\mathbb{Z}[x]$ is unique factorization domain.

Theorem 5: Every non zero non unit polynomial in $\mathbb{Z}[x]$ can be written as $b_1 b_2 .. b_s p_1(x) ... p_m(x)$ where $b_i's$ are irreducible polynomials of degree zero and $p_i's$ are irreducible polynomials of positive degree.

More over if $b_1 b_2 .. b_s \; p_1(x) ... p_m(x) = c_1 c_2 .. c_k g_1(x) .. q(x)$ where $b_i's$ *and* $c_j's$ are irreducible polynomial of degree zero and $p_i(x)s$ and $q_j(x)'s$ are irreducible polynomial of positive degree then s = k, m=t and after renumbering $p_i(x) = \pm q_j(x)$ and $b_i = c_j$.

Proof: Let $f(x)$ be a nonzero non unit polynomial from $\mathbb{Z}[x]$. If deg $f(x) = 0$, then $f(x)$ is constant and we are through, by Fundamental Theorem of Arithmetic.

If deg $f(x) > 0$, let *b* denote the content of $f(x)$, and let $b_1 b_2 ... b_s$ be the factorization of *b* as a product of primes. Then $f(x) = b_1 b_2 ... b_s f_1(x)$, where $f_1(x)$ belongs to $\mathbb{Z}[x]$, is primitive and deg $f_1(x) = \deg f(x)$.

Thus to prove the existence portion of the theorem it suffices to show that a primitive polynomial $f(x)$ of positive degree can be written as a product of irreducible polynomials of positive degree. We proceed by induction on deg $f(x)$. If deg $f(x)=1,$ then $f(x)$ is already irreducible and we are done.

Now suppose that every primitive polynomial of degrees less than deg $f(x)$ can be written as product or irreducible of positive degree. If $f(x)$ is irreducibles, there is nothing to prove. Otherwise Let $f(x)=g(x).h(x)$ where both $g(x)$ and $h(x)$ are primitive and have degree less than that of $f(x).$ Thus by induction both $g(x)$ and $h(x)$ can be written as a product of irreducibles of positive degree. Clearly then $f(x)$ is also such a product.

To prove the uniqueness portion of the theorem, suppose that

$$f(x)=b_1b_2\ldots b_s\ p_1(x)\ldots p_m(x)=c_1\,c_2\ldots c_k\ q_1(x)\ldots q_t(x)$$

where $b_i's$ and $c_j's$ are irreducible polynomial of zero and $p_i(x)'s$ and $q_j(x)'s$ are irreducible polynomials of positive degree.

$$\text{Let } b=b_1b_2\ldots b_s \quad \& c=c_1c_2\ldots c_k$$

Since $p_i(x)'s$ and $q_j(x)'s$ are primitive therefore by Gauss Lemmas

$p_1(x)\,p_2(x)\ldots p_m(x)$ and $q_1(x)\ldots q_t(x)$ are primitive.

Hence both *b* and *c* must equal plus or minus the content of $f(x)$ and therefore are equal in absolute value. It their follows from the fundamental Theorem of Arithmetic that *s* = *k* and after renumbering $b_i=\pm c_i \text{ and } 1\le i\le k.$

Thus by cancelling the constant terms in the two factorizations for we get, $p_1(x)\,p_2(x)\ldots p_m(x)=\pm q_1(x)\ldots q_t(x).$

By viewing $p_i(x)$ and $q_j(x)$ as element of $\mathbb{Q}$[x] & noting that $p_1(x)\mid p_1(x)\,p_2(x)\ \ldots.\ p_m(x)$

Therefore $p_1(x) \mid q_1(x) \ldots q_t(x)$, and by corollary of previous theorem $p_1(x) \mid q_j(x)$ for some j. by renumbering we get, $p_1(x) \mid q_1(x)$ $\Rightarrow q_1(x) = f(x)\, p_1(x)$ but as both $q_1(x)$ and $p_1(x)$ are irreducible therefore $f(x)$ is unit in $\mathbb{Q}[x]$ say f_1

$\therefore q_1(x) = f_1, p_1(x)$ but both $q_1(x)$ and $p_1(x)$ are primitive which implies $f_1 = \pm 1$, so $q_1(x) = \pm p_1(x)$.

Also after canceling we get

$p_2(x)\, p_3(x) \cdots p_m(x) = \pm q_2(x) \cdots q_t(x)$. After repeating above argument if $m < t$ then we get 1 on left side and non constant polynomial in right which leads to contradiction. Hence $m = t$ and $p_i(x) = \pm q_i(x)$.

8.5 Summary

1) Let *D* be an integral domain. A polynomial *p(x)* in *D[x]* is said to be *irreducible polynomial* if whenever *p(x) = f(x) g(x)* then either *f(x)* or *g(x)* is unit (i.e. constant polynomial) in *D[x]*.

2) A non zero – non unit polynomial of *D[x]* which is not irreducible is said to *reducible*.

3) The content of a non zero polynomial $a_n x^n + a_{n-1} x^{n-1} + .. + a_o$, where $a_i \in \mathbb{Z}$ is the greatest common divisor of $a_n, a_{n-1}, .. a_1, a_o$.

4) **Gauss Lemma:** The product of two primitive polynomials is Primitive.

5) **Eisenstein's Criterion:** Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + .. + a_o \in \mathbb{Z}[x]$ if there is a prime *p* such that $P \nmid a_n, P \mid a_{n-1}, ..., P \mid a_o$ but $P^2 \nmid a_o$ then *f(x)* is irreducible over $\mathbb{Q}$.

6) Let *F* be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in *F[x]* if and only if *p(x)* is irreducible over *F*.

8.6 Unit and Exercises

1) Show that x^2+1 and x^2+x+4 are irreducible polynomial in $Z_{11}[x]$. Show that $\frac{Z_{11}[x]}{(x^2+1)}$ and $\frac{Z_{11}[x]}{(x^2+x+4)}$ are fields having 121 elements.

Solution :- Let $f(x)=x^2+1$

$f(0)=1, f(1)=2, f(2)=5, f(3)=10$

$f(4)=17=6 \pmod{11}$, $f(5)=26=4 \pmod{11}$,

$f(6)=37=4 \pmod{11}$, $f(7)=50=6 \pmod{11}$,

$f(8)=10 \pmod{11}$, $f(9)=5 \pmod{11}$,

$f(10)=2 \pmod{11}$.

Hence *f(x)* is irreducible over $\mathbb{Z}_{11}[x]$

$\therefore \langle f(x) \rangle$ is maximal ideal in $\mathbb{Z}_{11}[x]$

$\therefore \mathbb{Z}_{11}[x] / \langle f(x) \rangle$ is field.

Now for any $h(x) \in \mathbb{Z}_{11}[x]$, by division algorithm

$h(x)=g(x)(x^2+1)+r(x)$

where $r(x)=o$ or deg $r(x)=1$

$\therefore r(x)=ax+b, a,b \in \mathbb{Z}_{11} \quad \therefore h(x)=g(x)(x^2+1)+ax+b$

$h(x)+\langle x^2+1 \rangle = (g(x)(x^2+1)+ax+b)+\langle x^2+1 \rangle = ax+b+\langle x^2+1 \rangle$

$\therefore \mathbb{Z}_{11}[x] / \langle f(x) \rangle = \{ax+b+\langle x^2+1 \rangle : a,b \in \mathbb{Z}_{11}[x]\}$

$\therefore$ There are 11 choice for a and 11 choice for b. Hence total 121 polynomials are there of the form $ax + b$.

Hence $\left|\mathbb{Z}_{11}[x] \Big/ \langle x^2+1 \rangle\right| = 121.$

Similarly we can prove that $\left|\mathbb{Z}_{11}[x] \Big/ \langle x^2+x+4 \rangle\right| = 121.$

2) Show that $(3x^2+4x+3) \in \mathbb{Z}_5[x]$ factors as $(3x+2)(x+4)$ and $(4x+1)(2x+3)$. Is $\mathbb{Z}_5[x]$ a UFD?

Justify your answer. Is the above factorization is unique upto multiplication by a unit?

Solution: $f(x) = 3x^2 + 4x + 3$

$f(0) = 3 \quad f(1) = 10 = \bar{0}$

$\therefore (3x+2)(x+4) = 3x^2 + 2x + 12x + 8 = 3x^2 + 14x + 8 = 3x^2 + 4x + 3 \pmod 5$

Similarly $(4x+1)(2x+3) = 8x^2 + 14x + 3 = 3x^2 + 4x + 3 \pmod 5$

Hence $(3x^2+4x+3) = (3x+2)(x+4) = (4x+1)(2x+3)$

$\therefore$ Since $(3x+2)(x+4)$ and $(4x+1)(2x+3)$ are two factors of $3x^2 + 4x + 3$.

$\because 4 \equiv -1 \pmod 5$

$1 = -4 \pmod 5$

$\therefore 4x + 1 = -x - 4 \pmod 5$

$= -(x+4) \pmod 5$

$\therefore 4x+1$ is associate of $(x+4)$ $in\ \mathbb{Z}_5[x]$ Similarly 2x+3 = - (3x+2) (mod 5).

Hence 2x+3 is associate of (3x+2) in $\mathbb{Z}_5[x]$

$\therefore$ Hence the above factorization is unique upto multiplication by a unit.

$\because \mathbb{Z}_5$ is field $\therefore \mathbb{Z}_5[x]$ us UFD.

3. Determine which of the following polynomials are irreducible in the indicated rings.

   (i) $x^2+x+1 \ in \mathbb{Z}_2[x]$

   (ii) $x^4+x \ in \mathbb{Z}_5[2]$

   (iii) $x^4+10x^2+1 \ in \mathbb{Z}[x]$

4. Show that if $\langle f(x)\rangle$ is maximal ideal in $\mathbb{R}[x]$, then *f(x)* is irreducible.

5. Let F be a field. Show that the $F[x]/\langle f(x)\rangle$ is field if and only if *f(x)* is irreducible over F.

6. Show that the only maximal ideals of $\mathbb{R}[x]$ are of the form

   (x-a), $a \in \mathbb{R}$ *or* x^2+bx+c where b,c $\in \mathbb{R}$ with $b^2+4ac<0$.

7. Show that maximal ideals of $\mathbb{C}[x]$ are *x-*α where $\alpha \in \mathbb{C}$.

8. Show that if D is UFD then D[x] is also (Proof is on similar line of proving $\mathbb{Z}[x]$ is UFD)