COUNCILE OF SCIENTIFIC & INDUSTRIAL RESEARCH

Unit – 4 : ABSTRACT ALGEBRA

SYLLABUS

SL NO.	TOPICS
1	4.1 Set
2	4.2 Cartesian Product
3	4.3 Relations
4	4.4 Functions
5	4.5 Binary Operation
6	4.6 Groups
7	4.7 Sub group
8	4.8 Cyclic Group
9	4.9 Co-set and Lagrange's Theorem
10	4.10 Normal Subgroup and Qutient Groups
11	4.11 Homomorphism of Groups
12	4.12 Direct Product of Group
13	4.13 Simple Group
14	4.14 Rings
15	4.15 Subrings
16	4.16 Ideal
17	4.17 Simple Ring
18	4.18 Quotient Ring
19	4.19 Ring Homomorphism
20	4.20 Polynomial Rings
21	4.21 Divisibility Rings
22	4.22 Extension Field

4. Abstract Algebra

4.1 Set:

4.1.1 Set: A well defined collection of distinct objects is called a set.

Well-defined: Either an object belongs to a set or it does not belongs to a set i.e. there should be no ambiguity what so ever regarding the membership of such collection of a set.

Example (4.1) : Collection of all positive integers is a set but a collection of some positive integers is not a set, as is not clear whether a particular positive integer, say 5, is a member of this collection or not.

4.1.2. Power Set: $P(X) = \{A : A \text{ is a subset of } X\}$

$$|P(X)| = 2^k \text{ where } |X| = k$$

Null Set$(\emptyset)$ **:** $\emptyset = \{x \in 2 : x^2 + 1 = 0\}$

4.1.3. Ordered Pair : Let $x \in X$ and $y \in Y$. The ordered pair of elements x and y denoted by (x, y), is the set $\{\{x\}, \{x, y\}\}$.

Clearly, $(x, y) = \{\{x\}, \{x, y\}\} \neq \{\{y\}, \{x, y\}\} = (x, y), where\ x \neq y$

$$(x, y) = (z, w) \Leftrightarrow x = z, y = w.$$

4.2. Cartesian Product :

4.2.1. Cartesian Product: $X \times Y = \{(x, y) : x \in X, y \in Y\}$

(i) Assume $X \times \emptyset = \emptyset = \emptyset \times X$ *for any set* X.

(ii) If $|X| = m, |Y| = n, then\ |X \times Y| = mn.$

(iii) $X \times Y$ is called diagonal of X and it is denoted by Δ_x.

4.3. Relations:

4.3.1. Relations: A binary relation or simply a relationρ from a set A into a set B is a subset of $A \times B$.

Domain of: $D(\rho) = \{a \in A : \exists\, b \in B \text{ such that } (a, b) \in \rho\}$

Range or Image of : $R(\rho) = \{b \in B : \exists\, a \in A \text{ such that } (a, b) \in \rho\}$

Inverse relation$(\boldsymbol{\rho^{-1}})$**:**$(\rho^{-1}) = \{(b, a) : (a, b) \in \rho\}$, $(\rho^{-1})^{-1} = \rho$

4.3.2.Composition : Let ρ_1 be a relation from A into B and ρ_1 be a relation from B to C then the composition of ρ_1 and ρ_2 is denoted by $\rho_2 \circ \rho_1$is a relation from A to C.

4.3.3. Definition : Let A be a set and ρ be a relation of A. Then ρ

i. reflexive if for all $a \in A, (a, a) \in \rho$

ii. symmetric, if for all $a, b \in A, whenever\ (a, b) \in \rho \Rightarrow (b, a) \in \rho$

iii. transitive, if for all $a, b, c \in A, whenever\ (a, b) \in \rho\ wher\ (b, c) \in \rho \Rightarrow (a, c) \in \rho$

4.3.4. Definition (Equivalence relation): A relation ρ on a set A is called an equivalence of ρ in reflexive, symmetric and transitive.

4.3.5. Definition (Anti symmetric): ρ is said to be anti symmetric if $\forall\ a, b \in A\ where\ (a, b) \in \rho\ and\ (b, a) \in\ \rho\ \Rightarrow a = b$.

Examples (4.2):

$\forall\ x, y, \in\ \mathbb{R}$therefore the following reasons

		Reflexive	Symmetric	Transitive	Antisymmetric
1	$y = 2x$	×	×	×	
2	$x < y$	×	√	×	√
3	$x \neq y$	×	√	×	
4	$xy > 0$	× (0,0)	√	√	
5	$y\ \neq x + 2$	√	× (3,5)	×	
6	$x \leq y$	√	×	√	√
7	$xy \geq 0$	√	√	× (5,0), (0, −2)	×
8	$x = y$	√	√	√	√

4.3.6. Definition (Partially order set or poset): A relation ρ on a set A is said to be a partial order on A if ρ is reflexive, anti symmetric and transitive. The set A with the partial order defined on it is called a partially order set or poset and it is denoted by (A, ρ).

Example (4.3): $(\mathbb{R}, \leq), (P(X),\ \subseteq)$.

4.3.7. Definition (Linearly ordered set or chain): A poset(A, ρ) is called a linearly ordered set or chain if $\forall\ a, b \in A\ either\ a, b \in \rho\ or\ (b, a) \in\ \rho$ must hold.

Example (4.4): $(\mathbb{R}, \leq)$ but not $(P(X),\ \subseteq)$, since for some $a, b\ \in X\ \ \{a\}, \{b\} \in P(X)\ such\ that\ \{a\} \nsubseteq \{b\}\ and\ \{b\} \nsubseteq \{a\}$.

Examples (4.5): Let S be a finite set and $|S| = n$. Then

i. The number of reflexive relation defined on S is 2^{n^2-n}

ii. The number of symmetric relation defined on S is $2^{\frac{n^2+n}{2}}$

iii. The number of relation that are both reflexive and symmetric is $2^{\frac{n^2-n}{2}}$

4.4. Functions:

Definition: For two nonempty sets A and B, a relation f from A into B is called a function from A into B if

i. $D(f) = A$

ii. $f$is well defined (or, single valued) in the series that $\forall\ (a,b),(a',b') \in f, a = a' \Rightarrow b = b'\ i.e,\ a = a' \Rightarrow f(a) = f(a')$.

Identity mapping:$f: A \to A, f(x) = x\ \forall\ x \in A$.

Constant mapping: $f: A \to B, f(x) = c\ \ \forall\ x \in A,\ some\ c \in B$.

Examples (4.6): Let A and B be two finite sets and $|A| = n\ \ and\ |B| = m\ (n \geq m)$. Then

(i). The number of distinct functions defined from A to B is m^n.

(ii). The number of onto functions defined from A to B is $\emptyset(n,m) \times m!$, where $\emptyset(n,m)$ is the number of partitions of a set A with n elements into m subsets (1$\leq m \leq n$) , $\emptyset(n,m)$ is known as stirlling number of 2nd kind and it can be calculated from the formula:

$$\emptyset(n,m) = \begin{cases} 1 & if\ m = 1\ or\ n \\ \emptyset(n-1,m-1) + m\emptyset(n-1,m) & otherwise \end{cases}$$

(iii). The number of injective function defined from$A(|A| = n)\ to\ B(|B| = m, n \leq m)$ is ${}^mP_n$ and bijective is $n!$(if $m\ \ =\ \ n$) otherwise 0.

4.4.1. Definition: Let us consider a function $f: A \to B$. Then

a) $f$is called injective (one-one) where $\forall\ a_1, a_2 \in A\ if\ a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_{d2})$.

b) $f$is called subjective if $Im\ (f) = B$.

c) f is called bijective if f is both injective and subjective

4.4.2. (Theorem): Composition of functions is associative, provided the requisite composition make sense.

4.4.3. (Theorem): Suppose that $f: A\ \ \to B\ and\ g: B \to C$. Then

(i). if f and g are both injective then $g \circ f$ is also so,

(ii). if f and g are both surjective then $g \circ f$ is also so,

(iii). if f and g are both bijective then $g \circ f$ also so,

(iv). if$g \circ f$ is injective then f is injective.

(v). if$g \circ f$ is surjective then g is surjenctive.

(vi). if$g \circ f$ is bijective, then f is injective and g is surjective.

4.4.4. (Theorem): Let A be any set and $f: A \to A$ be an identity injective function. Then $f: A \to A$ is an injective $\forall\ n\ \ \geq 1$.

4.4.5. (Theorem): For any finite set A if $f: A \to A\ is\ injective$, then f is bijective.

If A is infinite this is not true. Example $f: [1,2] \to [1,2]$by $(x) = \frac{x}{2}$. Then f is one – one but there in number of $x \in [1,2] such\ that\ 2 = f(x), i.e.\ \ f$ is not onto and hence not bijective $(f: \mathbb{R} \to \mathbb{R}, f(x) = e^x$.

4.4.6.Definition : Consider a function $f: A \to B$ then f is called

(i). Left invertible, if $\exists\ g: B \to A$ *such that* $g \circ f = i_A$ *and* g is called left inverse of f.
(ii). Right invertible if $\exists\ h: B \to A$ such that $f \circ h = i_B$ and then h is called right inverse of f.
(iii). Invertible if f is both left and right invertible.

Example (4.7): $f : \mathbb{N} \to \mathbb{N}, f(n) = n + 1\ \forall\ n \in \mathbb{N}$ and $g: \mathbb{N} \to \mathbb{N}, g(1) = 1$ and $g(n) = n - 1, n > 1$. Now $(g \circ f)(n) = g\big(f(n)\big) = g(n + 1) = n \Rightarrow$ g is left inverse of f.

But $f \circ g(1) = f\big(g(1)\big) = f(1) = 2\ \Rightarrow g$ *is not right inverse of* f.

4.4.7. (Theorem): Let $f: A \to B$ be a function. Then –

(i). f is left invertible $\Leftrightarrow f$ is injective.

(ii). f is right invertible $\Leftrightarrow f$ is surjective.

(iii). f is invertible $\Leftrightarrow f$ is bijective.

4.5 Definition (Binary Operation) : Let A be a nonempty set. A binary operation $*$ *on* A is a function from $A \times A \to A$.

Example (4.8):$(\mathbb{Z}, +), (\mathbb{N}, +), (\mathbb{R}, \cdot), (\mathbb{R}, +)$ not binary operation $(\mathbb{N}, -)$ since $1 - 2 = -1 \not\subset \mathbb{N}$.

4.5.1. (Multiplication Table): $A = \{1, \omega, \omega^2\}$, $*: A \times A \to A$ is complex multiplication.

$M \equiv$

$*$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Note: $*$ is commutative (-) M is symmetry.

4.5.2. (Theorem): An identity of a mathematical system $(A,*)$, if it exists unique.

Example (4.9):

(i). (No identity): $(\mathbb{Z},*)$, where $a \times b = |a + b| \quad \forall\ a, b \in \mathbb{Z}$ *and* $a \times b = a$.
(ii). Right identity but no left identity $(\mathbb{Z},*), a * b = a - b \quad \forall\ a, b \in \mathbb{Z}$. Here 0 is such element.
(iii). (No identity) $(\mathbb{Z},*), a * b = a$.
(iv). (No identity): $(\mathbb{N}, +)$.
(v). (Not cancellation) $(\mathbb{Z},*)$, *with* $a * b = a$.

4.5.3. (Semi group): Let S be a non-empty set and $*: S \times S \to S$ be a binary operation on S and $*$ is associative. Then $(S,*)$ is called semi group.

Example (4.10):$(\mathbb{Z}, -)$.

4.5.4. (Monoid): Semi group with identity.

Example (4.11):$(\mathbb{N}, +)$ is a semi group but not monoid and $(\mathbb{N} \cup \{0\}, +)$ is monoid.

4.5.5. (Quasi group): A mathematical system $(G,*)$ i.e, G is used under $*$ is called a quasi group, if $\forall\ a, b, \in G$ each of the equations $a \times x = b\ and\ y - a = b$ has a unique solution in G.

Example (4.12):

(i). $(\mathbb{Z}, -), a - x = b\ and\ y - a = b\ have\ solution\ x = a - b, y = a + b.$

(ii). $(\mathbb{Z},*),\ a * b = |a + b|$. Not a quasi group. Since $a * b = b \Rightarrow |a + x| = b > 0$ has two solution $x = -a + b\ and\ x = -a - b$

Example (4.13): Let $|S| = n$. How many different binary operations can be defined on S?

Answer: Total number of binary operations $= n^{n^2}$

Number of commutative binary operations $= 2^{\frac{n^2+n}{2}} = number\ of\ symmetric\ realtion.$

4.6. Groups :

Definition (Group): A group is an ordered pair $(G,*)$, where G is a non-empty set and $*$ is a binary operation on G such that following properties hold :

(i). $\forall\ a, b, c \in G, a * (b * c) = (a * b) * c\ (\ associative\ law)$.

(ii). $\exists\ e \in G\ such\ that\ \forall\ a \in G, a * e = a = e * a\ (\ existence\ of\ identity)$.

(iii). for each $a \in G\ \exists\ b \in G\ such\ that\ a * b = e = b * a\ (\ existence\ of\ an\ inverse)$.

4.6.1. (Theorem): Let $(G,*)$ be a group. Then identity and inverse are unique.

4.6.2. Abelian (Commutative): $\forall\ a\ , b \in G, a * b = b * a \quad i.e. (\mathbb{Z}, +)$.

4.6.3. (Non commutative) : $(S_3, 0),\ (GL(2, \mathbb{R}),\ \cdot)$.

Example (4.14):

(i). $(\mathbb{Z}_n, +) = \{\bar{0}, \bar{1}, \ldots\ldots\ldots, \overline{n-1}, +\}, \forall\ \bar{a}, b \in \mathbb{Z}_n,\ a + = a + b$ is a commutative group and $n \in \mathbb{Z}^+$.

(ii). $V_w,\ \cdot) = \{\bar{a} \in \mathbb{Z}_n | \{\bar{0}\} : \gcd(a, n) = 1\}\ and\ \bar{a}.\bar{b} = \overline{ab}$ is also a commutative group.

(iii). $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}\,b : a\ .\ b \in \mathbb{Q}\}\ Then\big(\mathbb{Q}[\sqrt{2}], +\big)\ and\ (\ \mathbb{Q}[\sqrt{2}] | \{\bar{0}\},\ \cdot)$ are commutative groups.

(iv). $(P(X), \Delta)$ where X be a set and $P(X)$ is the power set of X and for all $A, B \in P(X), A\Delta B = (A \backslash B) \cup (B \backslash A)$ is a commutative group and $\Delta(A) = 2\ \forall\ A \in P(X)$.
Note : If X is infinite then $(P(X), \Delta)$ is an infinite group but order of every element is finite, namely 1 and $A^{-1} = A$.

(v). $(S_n, 0)$ is non-commutative for $n > 2$ where δ_n is the collection of all bijeciton mapping (permutation) from $X\ to\ X$ where $|X| = x$.

(vi). $GL(2, \mathbb{R}) = (G,*)$ where $G = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0\right\}$ and $*$ is the matrix multiplication. Then $GL(2, \mathbb{R})$ is a $SL(2, \mathbb{R}) = \left(\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1\right\}, *\right)$

4.6.4. (Theorem): Let $(G,*)$ be a group, then

(i). $\forall\, a \in G, (a^{-1})^{-1} = a$
(ii). $\forall\, a, b \in G, (a * b)^{-1} = b^{-1} * a^{-1}$
(iii). $[cancellation\ law]\ \forall\, a, b, c \in G\ if\ either\ a * c = b * c\ or\ c * a = c * b,$ $then\ a = b.$
(iv). $\forall\, a, b \in G, the\ equation\ a * x = b\ and\ y * a = b$ have unique solution in G for $x\ and\ y.$

4.6.5. (Corollary): Let $(G,*)$ be a group and $a \in G$. If $a * a = a$, then $a = e$ and a is idempotent element and in a group e is the only idempotent element.

4.6.6.(Theorem): A semi group $(S,*)$ is a group if only if

(i). $\exists\, e \in S\ such\ that\ e * a = a\ \forall\, a \in S\ \ (left\ identity)$
(ii). $\forall\, a \in S, \exists\, b \in S\ such\ that\ b * a = e(left\ identity)$

4.6.7. (Theorem): A semi group $(S,*)$ in a group $\Leftrightarrow \forall\ a, b \in S,$ the equation $a * x = b$ and $y * a = b$ have solutions in $S\ for\ x\ and\ y.$

4.6.8. (Theorem): A finite semi group $(S,*)$ is a group $\Leftrightarrow$ $(S,*)$ satisfies the cancellation laws.

$*$ Finite is necessary. Example (4.15) $(\mathbb{Z}\{0\}, \cdot)$ is a semi group and satisfies cancellation laws but inverse of an element $1 \neq a \in \mathbb{Z}\{0\}$ does not exist.

4.6.9. Definition(Order): Let $(G,*)$ be a group and $a \in G$. If $\exists$ a positive integer n such that $a^n = e$, then the smallest such positive integer is called the order of a.

4.6.10. (Theorem): Let $(G,*)$ be a group and $a \in G$ such that $O(a) = n$

(i). If $a^m = e$ for some positive integer m, then n divides m.
(ii). For any positive integer t,

$$O(a^t) = \frac{O(a)}{\gcd(t, n\,)} = \frac{n}{\gcd(t, n\,)}$$

Example (4.16): Give a counter example to justify that in a semi group with, left identity, if every element has a right inverse with respect to the left identity, it need not be a group.

Solution: Consider $\mathbb{Z} \times \mathbb{Z}$ endowed with the operation $(a, b) * (c, d) = (c, b * d)\forall(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$.Then $\mathbb{Z} \times \mathbb{Z},*)$ is a semi group.

Now, $(0,0) * (a, b) = (a, b)\forall(a, b) \in \mathbb{Z} \times \mathbb{Z}$ where $(0,0)$ is a left identity and $(0, -b) \in \mathbb{Z} \times \mathbb{Z}\ and\ (a, b) * (0, -b) = (0,0) \Leftrightarrow (0, -b)$ is a right $(0,0)$ – inverse of $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.But($\mathbb{Z} \times \mathbb{Z},*)$ has no identity and hence $(\mathbb{Z} \times \mathbb{Z},*)$ is not a group.

4.6.11. If $(G,*)$ is an even order group, then there must exist at least one non-identity element $a \in G\ such\ that\ a^2 = e.$

4.6.12. A group G is commutative $\Leftrightarrow$ $(a * b)^n = a^n * b^n$ for any three commutative integer n and for all $a, b \in G$.

4.6.13. Definition(Permutation): Let A be a set (non-empty). A permutation of A is a bijecitive mapping of A onto itself.

4.6.14. Definition: A group $(G,*)$ is called a permutation group, on a non-empty set A if the elements of G are some permutations of A and the operation $*$ is the composition of two mapping.

Example (4.17): $S_3, 0)$, S_n symmetric group and $|S_n| = n!$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \ Then\ \alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 1 \end{pmatrix}$$

4.6.15. (Theorem): If n is positive integer such that $n \geq 3$, then the symmetric group S_n is a non-commutative group.

4.6.16. Definition: Cycle of length 2 is called transposition.

4.6.17. Definition: A permutation is called even permutation is called even permutation if it can be expressed as a product of even number of transpositions.

4.6.18. (Theorem): If $\alpha\ and\ \beta$ be the disjoint cycles in $S_n\ i.e. \alpha \cap \beta = \{i_1, i_2, \ldots \ldots \ldots, i_k\} \cap \{j_1, j_2, \ldots \ldots \ldots, j_p\} = \phi, then\ \alpha \circ \beta = \beta \circ \alpha.$

4.6.19. (Theorem): Any non-identity permutation $\alpha \in S_n$ $(n \geq 2)$ can be expressed as a product of disjoint cycles where cycle is of $length\ \geq 2$.

4.6.20. (Theorem): Any cycle of $length\ \geq 2$ is either a transposition or can be expressed as a product of transpositions.

Example (4.18):

$$\alpha = \begin{pmatrix} 1 & 2 & 34 & 5 & 67 & 8 \\ 8 & 5 & 63 & 7 & 42 & 1 \end{pmatrix} = (1 \quad 8)(2 \quad \overset{*}{5} \quad 7)(3 \quad 6 \quad 4)$$

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

4.6.21. (Theorem: Order and length): Let $n \geq 2$ and $\sigma \in S_n$ be a cycle. Then σ is a

$$k - cycle \Leftrightarrow order\ of\ \sigma\ is\ k.$$

4.6.22. (Theorem): Let $\sigma \in S_n,\ n \geq 2\ and\ \sigma = \sigma_1 \circ \sigma_2 \circ \ldots \ldots \circ \sigma_k$ be a product of disjoint cycles and suppose $O(\sigma_i) = n_i, i = 1,2, \ldots \ldots, k.\ Then\ O(\sigma) = (n_1, n_1 \ldots \ldots, n_k)$

Example (4.19):

(i). $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, Then $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

(ii). The number of even permutations in $S_n(n \geq 2)$is the same as that of the odd permutations.

4.7. Subgroups :

Definition : Let $(G,*)$ be a group and H be a non-empty sub-set of G. Then H called a subgroup of $(G,*)$, if H is closed under the binary operation $*$ and $(H,*)$ is a group.

Note: $\{e\}$ and G are two trivial subgroup of G.

Example(4.20): $(E, +) of\ (\mathbb{Z}, +) where\ E = \{2x : x \in \mathbb{Z}\}.$

4.7.1. (Theorem): All subgroups of $(G,*)$ have the same identity.

4.7.2. (Theorem): Let G be a group and H be a non-empty subset of G. Then H is a subgroup of $G \iff \forall\, a, b \in H, ab^{-1} \in H$.

4.7.3. (Corollary): Let G be a group and H be a non-empty finite subset of G. Then H is a subgroup $\iff \forall\, a, b \in H, ab \in H$.

4.7.4. (Theorem): The intersection of any collection of subgroups of a group G is a subgroup of G.

- Union of two subgroups of a group G may not be a subgroup of$G$.

Example (4.21): Consider $G = S_3$ *and* $H = \{e, (2,3)\}$ *and* $K = \{e, (1,2)\}$

Then H, K are two subgroup ofS_3. Now, $H \cup K = \{e, (1 \quad 2), (2 \quad 3)\}$ is not a group. Since

$$(1 \quad 2) \circ (2 \quad 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3) \notin H \cup K$$

4.7.5. (Theorem): Let $n \geq 3$. Then A_n is generated by the set of all $\exists\, cycle$. Number of cycle length r in S_n is $\frac{n!}{r \times (n-r)!}$

4.7.6. Definition: Let H and K be two non-empty subsets of a group$G$. Then the product of H *and* K is defined to be the set

$$H_k = \{hk : h \in H, x \in K\}$$

Product of two subgroups may not be a subgroup. Let $H = \{e, (1 \quad 2)\} \quad K = \{e, (1 \quad 3)\}$.

Now, $H_k = \{e, (1 \quad 2), (1 \quad 3), (1 \quad 3 \quad 2)\}$ *but* $(1 \quad 3)(1 \quad 2) = (1 \quad 2 \quad 3) \in H_k$

4.7.7. (Theorem) Let H *and* K be two subgroup of a group$G$. Then the following are equivalent:

(i). H_k *is a subgroup of* G.
(ii). $HK = KH$
(iii). KH is a subgroup of$G$

4.7.8. (Corollary): If H *and* K are two subgroup of a commutative group G, then HK is a subgroup of G.

4.7.9. (Centre of G):$Z(G) = \{x \in G : gx = xg \;\forall\, g \in G\}$

(i). $Z(G)$ *is a subgroup of* G.
(ii). *If* G *is commutative, then* $Z(G) = G$.

- Let H be a subgroup of G. Then for any $g \in G, K = gHg^{-1} = \{gHg^{-1} : h \in H\}$ in a subgroup of G and $|H| = |K|$.
- All subgroups of the group $(\mathbb{Z}, +)$ are $T_n = \{r_n : r \in \mathbb{Z}\}, n \in \mathbb{N}_0$

4.8. (Cyclic Groups):

Definition: A group G is called cyclic group if $\exists$ an element $a \in G$ such that $G = < a \geq \{a^n : n \in \mathbb{Z}\}$. Such an element a is called a generator of G.

Example (4.22):

(i). $G = \{1, -1, i, -i\}, G = < i > = < -i >$
(ii). $(\mathbb{Z}, +) = (< 1 >, +)$
(iii). $(\{2n : n \in \mathbb{Z}\}, +) = (< 2 >, +)$
(iv). $(\mathbb{Z}, +) = \{[1], +\}$

4.8.1. (Theorem): Every cyclic group G is commutative.

4.8.2. (Theorem): A finite group g is cyclic $\Leftrightarrow \exists\ a \in G\ such\ that\ O(a) = |G|$

4.8. 3.(Corollary): Let $< a >$ be a finite cyclic group. Then $O(a) = |G|$

4.8.4. (Theorem): Let $G =< a >$ be a cyclic group of order n. Then for any integer k where $1 \leq k < n, a^k\ is\ a\ generator\ of\ G \ \Leftrightarrow \gcd(n, k) = 1$

4.8.5. (Theorem): Every subgroup of a cyclic group is cyclic.

4.8.6. (Theorem): Let $G =< a >$ be a cyclic group of order n

(i). If H is a subgroup of G, then $|H|$ divides $|G|$.(For any group).
(ii). If m is a positive integer such that$m\ divides\ n$, the $\exists$ a unique subgroup of G of order n.(True for also any commutative group).
(iii). If $G =< a >$ is an infinite cyclic group, then any subgroup $H \neq \{e\}$ of G is also infinite order.
(iv). Let $G =< a >$ be an infinite cyclic group. Then
(a) $a^r = a^t \Leftrightarrow r = t, r, t \in \mathbb{Z}$
(b) Ghas only two generators.

4.9. Co-sets and Lagrange's Theorem :

Definition: Let H be a subgroup of G. If $a \in G$, the subset $aH = \{ah : h \in H\}$ is called a left co-sets of Hin G. Similarly, $Ha = \{ha : h \in H\}$ is called a right co-set of $H\ in\ G$.

Note: $eH = H = He \Rightarrow H$ is a left and right co-set of itself in G

- $aH \neq H$always example(4.23) $H = \{e, (1 \quad 2)\}$ in S_3. Then
  $(2 \quad 3)H = \{(2 \quad 3), (1 \quad 3 \quad 2)\ and\ Ha = \{(2 \quad 3), (1 \quad 2 \quad 3)$
  i.e.$(2 \quad 3)H \neq H(2 \quad 3)$

4.9.1. (Theorem): Let H be a subgroup of a group G and let $a, b \in G$

(i). $aH = H \Leftrightarrow a \in H\ (i*) Ha = H \Leftrightarrow a \in H$
(ii). $aH = bH \Leftrightarrow a^{-1}b \in H (ii*)\ Ha = Hb \Leftrightarrow ba^{-1} \in H$
(iii). Either $aH \cap bH = \phi\ or\ aH = bH\ (iii*) Either\ Ha \cap Hb = \phi\ or\ Ha = Hb$

$\Rightarrow$ Left co-set or right co-sets gives a partition of G is $\{aH : a \in G$ forms a partition of G.

4.9.2. (Theorem):$|aH| = |H| = |Ha|\ \forall\ a \in G\ and\ any\ subgorup\ H\ of\ G.$

4.9.3. (Theorem): Let H be a subgroup of G. Then $|L| = |R|, where\ L(represent\ R)$ denotes the set of all left (represents right) co-sets of Hin G.

4.9.4. Index of subgroup: Let H be a subgroup of G. Then the number of distinct left (or right) co-sets of Hin G, written $[G, H]$ is called the index o f a H in G.

4.9.5. (Lagrange's Theorem): Let H be a subgroup of a finite group G. Then $|H|$divides $|G|$. In particular, $|G| = |H|[G, H]$.

4.9.10. (Corollary): (i) Every group of prime order is cyclic and hence commutative.

(ii) Let $|G| = n$ and $a \in G$.Then $\phi(a)$ divides $n = \ |G|\ and\ a^n = e$.

4.9.11. (Fermat Theorem): Let p be a prime integer and $a$be an integer such that p does not divide a. Then $a^{p-1} \equiv 1(mod\ p)$.

4.9.12. (Theorem): Let H and K be two finite subgroup of G. Then

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

4.9.13. (Corollary): If $|H| > \sqrt{|G|}\ and\ |K| > \sqrt{|G|}\ , then\ H \cap K \neq \{e\}$.

Converse of Lagrange's Theorem not true:

Example(4.23) consider the symmetric group S_4. In this group A_4 of all even permutation is a subgroup and $|A_4| = 6, H$ can not contain all these $\exists$ −cycles. Let $\alpha = (a \quad b \quad c) \notin H$. Now, $O(\alpha) = 3$.Hence $K = \{e, \alpha, \alpha^2\}$ is a subgroup of A_4.

Note that $\alpha^2 = \alpha^{-1}$.

Hence $H \cap K = \{e\}$. Then $|HK| = \frac{|H|\ .\ |K|}{|H \cap K|} = \frac{6.3}{1} = 18$. But $HK \subseteq\ A_4$and $A_4 = 12, a\ contradiction.$

- But the converse of Langrage's theorem true for any abelian group.

4.10. Normal Subgroups and Quotient Groups :

4.10.1. Definition: Let H be a subgroup of G. $H$is said to be normal subgroup of G if $aH = Ha\ \forall\ a \in G$. Note that G and $\{e\}$ are normal subgroup of G which are trivial.

4.10.2. Let H be a subgroup of G. The following conditions are equivalent:

(i). $H$is a normal subgroup.
(ii). $gHg^{-1} \subseteq H \quad \forall\ g \in G$
(iii). $gHg^{-1} = \ H \quad \forall\ g \in G$

4.10.3. Theorem: Let $H\ and\ K$ be two subgroups of G. Then

(i). if$H$ is a normal subgroup of G, then $HK = KH$ is a subgroup of G.
(ii). if$H\ and\ K$ are both normal subgroups, then $HK = KH$ is a normal subgroup o f G.
(iii). if $H\ and\ K$ are both normal subgroups, then $H \cap K$ is a normal subgroup.

Note: If one of H and K be normal then$H \cap K$ is normal in another. It follows from second isomorphism theorem.

4.10.4. Theorem (Quotient group or factor group): Let H be a normal subgroup of G. Denote $G|H$ by $\forall\ aH, bH \in G|H\ ,\ aH * bH = abH$. Then$(G|H,*)$ is group and it is known as quotient or factor group.

4.10.5. Results:

(i). Let H be a subgroup of G such that $[G : H] = 2$. Then H is normal in G.
(ii). The centre $of\ G, Z(G)$ is normal in G.
(iii). Let H be a subgroup of G. Then $W = \bigcap_{g\in G} gHg^{-1}$ is normal in G.
(iv). If $x^2 \in H\ \ \forall\, x \in G,$ then H is normal and $G|H$ is commutative.
(v). If every cyclic subgroup of G is normal, then every subgroup $H\ of\ G$ is normal.
Proof: Let $a \in H, then\ for\ any\ g \in G, gag^{-1} \in < a >\subseteq H.$

(vi). If H is the only subgroup of order $x\ in\ G$, then H is normal.

Proof:$|gHg^{-1}| = |H|\ \Rightarrow\ gHg^{-1} = H\ \ \Rightarrow H\ is\ normal.$

(vii). Let $x, y \in G|H$ and $xy \in H$. Then H is normal in G.

Proof : Let $a \in H,\ g \in\ G|H\ \ \Rightarrow\ g^{-1} \in\ G|H \Rightarrow ga, g^{-1} \in\ G|H\ \Rightarrow gag^{-1} \in H.$

(viii). Let H be a subgroup of a group G. If the product of two left co-sets of $H\ in\ G$ is again a left co-set of G, then it is normal.

proof: Let $g \in G$. Then $gH\ g^{-1}H = tH\ for\ some\ t \in G$. Thus $e = gg^{-1}e \in tH$

$\Rightarrow e = th\ for\ some\ h \in H\ \ \Rightarrow t = h^{-1} \Rightarrow tH = H.$ Now, $gHg^{-1} \subseteq gHg^{-1}H = H.$

(a). Let $H\ and\ K$ be two normal subgroups of G such that $H \cap K = \{e\}$. Then $hk = kh\ \ \forall\, h \in H, \forall\, k \in K.$

(b). If $If\ G|Z(G)\ is\ cyclic, then\ G\ is\ abelian.$

4.11. Homomorphisms of Groups :

4.11.1 Definition (Homomorphisms): Let $(G,*)$ and $(G_1,*_1)$ be two groups and $f : G \to G_1$ be a function. Then f is called a homomorphism of $G\ into\ G_1$ if $\forall\, a, b \in G,\ \ f(a * b) = f(a) *_1 f(b).$

Example(4.24):

(i). $f : \mathbb{R} \to \mathbb{R}^+,\ f(x) = e^x\ \forall\, x \in \mathbb{R}.\ f\ is\ a\ homomorphism\ form\ (\mathbb{R},+) to\ (\mathbb{R}^+,\ \cdot).$
(ii). Definition(Trivial homomorphism): $f : G \to G_1 by\ f(a) = e_1 \forall\, a \in G.$
(iii). Define: $f : G|(2,\mathbb{R}) \to \mathbb{R}^*$by $f(A) = detA\ \ \forall\, A \in G|(2,\mathbb{R}).$
Note :$\left|G|(n, F_p)\right| = (p^n - p^0)(p^n - p^1) \ldots\ldots\ (p^n - p^{n-1})\ and\ \left|S|(n, F_p)\right| = \frac{|G|(n,F_p)|}{p-1}$

4.11.2. (Theorem): If f is a homomorphism form a group G into a group G_1 and e, e_1 are the identity element of G and G_1 respectively, then

(i). $f(e) = e_1$
(ii). $f(a^{-1}) = f(a)^{-1}\ \forall\, a \in G.$
(iii). $f(a^n) = f(a)^n\ \ \forall\, a \in G\ and\ \forall\ \ x \in \mathbb{Z}.$

4.11.3. (Theorem): If f be a homomorphism of a group G into a group G_1. Then the following results hold :

(i). if H is a subgroup of G, then $f(H) = \{f(h): h \in H\}$ $in\ subgroup\ of\ G_1$.
(ii). if H_1 is a subgroup of G_1, then $f^{-1}(H_1) = \{g \in G : f(g) \in H_1\}$ is a subgroup of G and if H_1 in normal, then $f^{-1}(H_1)$ is also normal.
(iii). if $a \in G$ is such that $O(a) = n, then\ O\big(f(a)\big)\ divides\ n.$
(iv). (Epimorphism): if f is onto, then $f(H)$ is normal in G_1 where H is normal in G.

Example (4.25): (In general if H is normal in G, then $f(H)$ may not normal in G_1).

Definition: $f : \mathbb{Z}_3 \to S_3$ by $f(\delta) = e, f(\bar{1}) = (1\quad 2), f(\bar{2}) = (1\quad 2)$. Then f is homomorphism and $f(\mathbb{Z}_3) = \{e, (1\quad 2)\} = H_1$ which is not normal in S_3 but $H = \mathbb{Z}_3$ is normal in $\mathbb{Z}_3$.

4.11.4. (Kernel): Let $f : G \to G_1$ be a homomorphism. The Kernel of f is defined by

$Ker\ f = \{x \in G : f(x) = e_1\}$.

4.11.5. (Theorem): Let $f : G \to G_1$ be a homomorphism. Then –

(i). $Im\ f$ is a subgroup of G_1.
(ii). $Ker\ f$ is a normal subgroup of G.
(iii). f is one – one (monomorphism) $\Leftrightarrow kerf = \{e\}$.

4.11.6. (Theorem): Let $G\ and\ G_1$ be two groups such that G_1 in a homomorphic image of G i.e. $f(G) = G_1$ i.e. f is onto (epimorphism).

(i). If G is commutative, then so is G_1.
(ii). If G is cyclic, then so is G_1 and i_b $G > \langle a \rangle, then\ G_1 = \langle f(a) \rangle$.

4.11.7. (Isomorphism): A homomorphism $f : G \to G_1$ is called an isomorphism if f is a bijective function.

A group G_1 is said to be isomorphic to a group G, if $\exists$ an isomorphism $f : G \to G_1$. In this case we write $G \simeq G_1$.

Example (4.26):

(i). Let $G = (\mathbb{R}, +),\ G_1 = (\mathbb{R}^+, \ \cdot)\ and\ f : G \to G_1, by\ f(a) = e^a\ \forall\ a \in G.$
(ii). $I : G \to G\ by\ I(x) = x\ \forall\ x \in G.$

4.11.8. (Theorem): Let $f : G \to G_1$ be an isomorphism. Then

(i). $f^{-1} :\ G \to G_1$ is an isomorphism.
(ii). G is commutative $\Leftrightarrow$ G_1 is commutative.
(iii). G is cyclic $\Leftrightarrow$ G_1 is cyclic.
(iv). For all $a \in G, O(a) = O(f(a))$

Following are the consequences of the above theorem :

I. A finite group can never isomorphic with an infinite group as $\nexists$ a one – one mapping and hence bijective.
II. Two groups of same order may not be isomorphic.
Example(4.27): $S_3\ and\ \mathbb{Z}_6$ where S_3 is non-commutative and $\mathbb{Z}_6$ is commutative.
III. Two groups of same order, commutative may not be isomorphic.
Example(4.28): $\mathbb{Z}_4$ cyclic and k_4 is non-cyclic.

IV. Two groups of infinite order and commutative may not be isomorphic.
Example(4.29): $(\mathbb{Z},+)$ cyclic and $(\mathbb{Q},+)$ non cyclic.

V. Two groups of infinite order, non-cyclic and commutative may not be isomorphic.
Example (4.30): $(\mathbb{R}^*, \cdot)$ has number of element of order 4 but $(\mathbb{C}^*, \cdot)$ has i of order 4.

4.11.9. (Theorem): Any infinite cyclic group is isomorphic to $(\mathbb{Z},+)$.

Proof: $G = \langle a \rangle \quad f : \mathbb{Z} \to G \quad by\ f(n) = a^n$.

4.11.10. (Theorem(Cayley)) : Every group is isomorphic to some subgroup of the group $A(S)$ of all permutations of some set.

4.11.11. (Corollary): Let G be a group of order n. $G$is isomorphic to a sub group of the symmetric group S_n.

Example (4.31):

(i). Find all homomorphisms of the group $(\mathbb{Z},+)$ to itself.

Ans : (Define): $f_n : \mathbb{Z} \to \mathbb{Z}$ by $f_n(t) = nt\ \forall\ t \in \mathbb{Z},\ n \in \mathbb{Z}$. Any homomorphism $f : \mathbb{Z} \to \mathbb{Z}$ is of the form f_n. Since $m \in \mathbb{Z},\ f(m) = f(m_1) = mf(1)$ and f is completely determined if we know $f(1) = n$. Then $f(m) = nm = f_n(m) \Rightarrow f \equiv f_n, n = 1, \pm 1, \pm 2, \ldots\ldots\ldots$

(ii). Find all homomorphisms from $(\mathbb{Z}_8,+)$into $(\mathbb{Z}_6,+)$.

Solutions: Let $[a] \in \mathbb{Z}_8 = \langle [1] \rangle$. $f([a]) = af([1])$. Then f is completely determined if we know $f([1])$. Now,$O(f([1]))$ divides $O([1])$ and $|(\mathbb{Z}_6|$i.e. $\delta$and 6. So, $O(\delta[1]) = 1\ or\ 2$. Thus $f([a]) = [0], or\ [3]$. If $f([1]) = 0$, then f is trivial homomorphism.
If $f([1]) = [3]$ then $f([a]) = [3a]$.

(iii). (a) There does exist any isomorphism from $(\mathbb{R},+)\ to\ (\mathbb{R}^*,\cdot)$
ans: $-1 \in \mathbb{R}^*$ with order 2 but $\nexists\ a \in \mathbb{R}$ whose order is 2.
(b) $(\mathbb{Q},+)$ is not isomorphic to $\mathbb{Q}^+, \cdot)$
Ans: Let $f : \mathbb{Q} \to \mathbb{Q}^+$ is an isomorphism. Now, $2 \in \mathbb{Q}^+$. Hence$\exists\ x \in \mathbb{Q}\ such\ that\ 2 = f(x) = f\left(\frac{x}{2}+\frac{x}{2}\right) = f\left(\frac{x}{2}\right)f\left(\frac{x}{2}\right) = \left\{f\left(\frac{x}{2}\right)\right\}^2 = y^2, y = f\left(\frac{x}{2}\right) \in \mathbb{Q}$ which is not possible.

4.11.12. (Theorem of First Isomorphism): Let $f : G \to G_1$ be a homomorphism of groups. Then the quotient group $G|Ker\ f \simeq Im\ f\ of\ G_1$.

4.11.13. (Corollary): For any group G, $G|\{e\} \simeq G.(I : G \to G, Ix = x\ \forall\ x \in G)$.

4.11.14. (Theorem): If G is a finite cyclic group of order n, then $G \simeq \mathbb{Z}|n\mathbb{Z} \simeq \mathbb{Z}_w$.

Example(4.32):

(i). Upto isomorphism, there are only two group of order 4, $\mathbb{K}_4\ and\ \mathbb{Z}_4$.
(ii). Upto isomorphism, there are only two groups of order 6, $\mathbb{Z}_6\ and\ S_3$.
(iii). If $\gcd(m,n) = 1, then\ m\mathbb{Z}|mn\mathbb{Z} \simeq \mathbb{Z}w$.
(iv). $U(m) = U(n_1) \oplus \quad U(n_2) \oplus \quad \ldots\ldots\ldots\ldots \oplus U(n_k)\ where\ m = n_1, n_2, \ldots\ldots n_k\ and\ gc\,d(n_i, n_j) = 1, i \neq j$.
(v). Consider S_3, its normal sub groups are $\{e\}, S_3, A_3$. Hence all homomorphic images of S_3 are $S_3|S_3,\quad S_3|\{e\} = S_3,\ S_3|A_3 = \mathbb{Z}_2$.

4.11.15. Theorem (Second Isomorphism): Let H and K be sub groups of G with K normal in G. Then, $H|(H \cap K) \simeq (HK)|K$.

4.11.16. Theorem (Third Isomorphism) : Let H_1 *and* H_2 *be two normal subgroups of* G *such that* $H_1 \subseteq H_2$. Then−

$(G|H_1)\,|(H_2|H_1) \simeq G|H_2$.

Example(4.33):

- Find all homomorphic image of$(\mathbb{Z},+)$.

  Solution: The subgroups of $\mathbb{Z}$ and $n\mathbb{Z}$, $n \in \mathbb{N}_0$.Since$\mathbb{Z}$ is commutative and the subgroups of $\mathbb{Z}$ are normal. Thus the homomorphic images of $\mathbb{Z}$ are the groups $\mathbb{Z}|n\mathbb{Z} \simeq \mathbb{Z}n, n = 0,1,2,\ldots\ldots$

  Note: Index of $n\mathbb{Z}$ in $\mathbb{Z}$ is n namely, $n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots \ldots \ldots (n-1) + n\mathbb{Z}$.

- $\mathbb{Z}_9$is not homomorphic image of $\mathbb{Z}_{16}$. Since $\mathbb{Z}_{16}|\ker f \simeq \mathbb{Z}_9 \Rightarrow |\mathbb{Z}_{16}||\ker f| = |\mathbb{Z}_9| \Rightarrow 16 = |\ker f|.9$ − absurd.

4.12. Direct Product of Groups:

Theorem: Let G and G be two groups. Then the set $G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1 \text{ and } g_2 \in G_2\}$

is a group under the binary operation $*\,[(a_1,b_1)*(a_2,b_2) = (a_1a_2, b_1b_2)\;\forall\,(a_1,b_1)(a_2,b_2) \in G_1 \times G_2]$. Further more

(i). $H_1 = \{(a_1, e_2) \in G_1 \times G_2\}$is normal in $G_1 \times G_2$ and $G_1 \simeq H_1$.
(ii). $H_2 = \{(e_1, b_2) \in G_1 \times G_2\}$is normal in $G_1 \times G_2$ and $G_2 \simeq H_2$.
(iii). $G_1 \times G_2 = H_1H_2 = H_2H_1,\; H_1 \cap H_2 = \{(e_1, e_2)\}$

4.12.1. Definition (Direct Product of groups): The group $(G_1 \times G_2, *)$ of the above theorem is called the direct products of the groupsG_1 *and* G_2 *(or external direct product of the groups* G_1 *and* G_2*)*.

4.12.2. Definition(Internal direct product): Let H and K be two subgroup of G. G is said to be an internal direct product of H and K if

a) $G = HK$
b) $H \cap K = \{e\}$
c) $hk = kh\;\forall\, h \in H \text{ and } k \in K$

Example(4.34):$k_4 = \{e, a, b, ab\}, H_1 = \{e, a\}, H_2 = \{e, b\}, -$

(a) $k_4 = H_1H_2$(b) $H_1 \cap H_2 = \{e\}$ (c)$hk = kh\;\forall\; h \in H_1, k \in H_2$

4.12.3. (Theorem): Let H and k be any subgroups of a group G. G is an internal direct product of H and $k \Leftrightarrow$

(i). $G = Hk$
(ii). H *and* k *are normal in* G.
(iii). $H \cap k = \{e\}$.

4.12.4. (Theorem): Let G be a group and H, K be two normal subgroups of G. If G is an internal direct product of H *and* K then

(i) $G \simeq H \times K$

(ii) $G|H \simeq K$ *and* $G|K \simeq H$

4.12.5. (Theorem): Every finite abelian group is the direct product of cyclic groups.

4.12.6. (Theorem): The number of non-isomorphic abelian groups of order p^n, p a portion equals to the number of partition $p(n)$ *of* n.

4.12.7. (Theorem): The number of non-isomorphic abelian of order$p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots \ldots, p_r^{\alpha_r}$, where $p(u)$ denoted the number of partitions of u.

Example (4.35): Let G be a abelian group of order 18. Then $18 = 2^1, 3^2 = 2^1 3^1 3^1$ So, G is one of $\mathbb{Z}_{18} = \mathbb{Z}_2 \times \mathbb{Z}_9 \; or \; \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ ($\because \gcd(2,9) = 1$).

(i). Find the number of elements of order 5 in $\mathbb{Z}_{15} \times \mathbb{Z}_5$

Ans: $5 \subset O(a,b) = lcm\,\{O(a), O(b)\}$

Case –I : Since $\mathbb{Z}_{15}$ is cyclic, it contains only one subgroup of order 5. In any subgroup of order 5, except identity element, every element is of order 5. Hence there are 4 choices of a and 4 choices of b. This gives 16 elements of order 5 in $\mathbb{Z}_{15} \times \mathbb{Z}_5$.

Case – II :$4\; choices\; of\; a\; and\; 1\; choices\; of\; b \Rightarrow$ 4 elements of order 5 in $\mathbb{Z}_{15} \times \mathbb{Z}_5$.

Case – III :$1\; Choices\; of\; a\; and\; 4\; choices\; of\; b \Rightarrow$ 4 elements of order 5 in $\mathbb{Z}_{15} \times \mathbb{Z}_5$.

Thus $16 + 4 + 4 = 24$ is the number of elements of order 5 in $\mathbb{Z}_{15} \times \mathbb{Z}_5$.

(ii). Let G be an abelian group of order b. Then $|G| = b = 2 \times 3$

$$\Rightarrow G \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6 \; (\because \gcd(2,3) = 1)$$
$$|not\; \mathbb{Z}_m \times \mathbb{Z}_n\; in\; cyclic \;\Leftrightarrow \gcd(m,n) = 1|$$

(iii). Find number of non-isomorphic non-abelian groups of order $n \geq b$.

Solution:

Case – I : If $n = r!$

Case – II :if $n = 2m(m > 3)$. Then $D_3\; and\; if\; n = r!$ then S_r

Case – III : If $mr = n$, then find a non-commutative group H of order m andH_m take direct product to $\mathbb{Z}_r$. This $G \simeq H \times \mathbb{Z}_r\; and\; |G| = n$.

Case –IV: If $n = 4k, then\; Q_{2k}, k \geq 2$

4.12.8. (Conjugacy class of a $\boldsymbol{a} \in \boldsymbol{G}$):

$$cl(a) = \{b \in G : x\,a\,x^{-1} = b\; for\; some\; x \in G\} = \{xax^{-1} : x \in G\}$$

Conjugacy classes gives a partition of G. Let $|G| = n$. Then $\exists$ aistients $a_1, a_2, \ldots \ldots \ldots, a_k \in G$ such that $G = \bigcup_{i=1}^{k} cl(a_i)$.

Now, let $a \in \mathbb{Z}(G) \cup cl(a_1) \cup cl(a_2) \cup \ldots \ldots \ldots \ldots \cup cl(a_k)$. Hence $|G| = |Z(G)| + \sum_{i=1}^{k} |cl(a_i)|$

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

Example(4.39):$S_3, cl(e) = \{e\}, cl(1 \quad 2) = \{(1 \quad 2), (1 \quad 3), (2 \quad 3)\}$

$cl(1 \quad 2 \quad 3) = \{(1 \quad 2 \quad 3), (1 \quad 3 \quad 2)\}$ Then $S_3 = cl(e) \cup cl(1 \quad 2) \cup cl(1 \quad 2 \quad 3)$

and$6 = |S_3| = |cl(e)| + |cl(1 \quad 2)| + |cl(1 \quad 2 \quad 3)| = 1 + 3 + 2$

4.12.9. Definition(Centralizer of a): Let $a \in G$. Then centralizer of a is the subset

$$C(a) = \{\, x \in G : ax = xa\}$$

Clearly, $C(a)$ is a subgroup of G and $\mathbb{Z}(G) \subseteq C(a)$.

4.12.10. (Theorem): Let G be a finite group and $a \in G$. Then $[G : C(a)] = |cl(a)|$

4.12.11. (Theorem): If G is a group and $|G|p^n (n > 0), then\; Z(G) \neq \{e\}\; i.e. |\mathbb{Z}(G)| \geq p \;\; (p\; is\; prime)$.

Proof : Follows from class equation and above theorem.

4.12.12. (Theorem): Every group of order p^2 is commutative and it is either a cyclic or a direct product of cyclic groups.

4.12.13. Theorem (Cauchy): Let G be a finite group and $p||G|$. Then G has an element of order p and hence a subgroup of order p.

Proposition (i) : Every group of order p^n $(n > 0)$ contains a normal subgroup of order p.

Proposition (ii): If $|G| = px$, where p is prime such that $p > n$ their G has a normal subgroup of order p.

⇒ If $|G| = pq$ where p *and* q are both primes and $p > q$ then G has a normal subgroup of order p.

⇒ If $|G| = pq$ where p, q, r are primes and $p > q > r$ then G has a normal subgroup of order p.

4.12.14. (Theorem): Let G be a finite abelian group of order n. If m is a positive integer such that $m|n$, then G has a subgroup of order m.

Note: The converse of Lagrange's theorem hold for finite abelian group.

4.12.15. Theorem (Sylow's First Theorem): Let G be a group of order $p^n m$, where p is a prime and $\gcd(p, m) = 1$ $for\ 0 \le i \le n, G$ has a subgroup of orderp^i.

4.12.16. Definition (Sylow p-subgroup): If $|G| = p^n m\ and\ \gcd(p, m) = 1$, then any subgroup of G of order p^n is called a Sylow $p - subgroup$.

4.12.17. Theorem (Sylow's second Theorem): If $H\ and\ K$ are any two Sylow $p - subgroup$of a finite group G, then $H = gkg^{-1}\ for\ some\ g \in G$.

4.12.18. Theorem (Sylow's Third Theorem): If $|G| = p^n m$ and $\gcd(p, m) = 1$, then the number of $k_p$of Sylow $p - subgroup$ of G is of the form $k_p + 1\ (k \ge 0)\ and\ n_p||G|$.

Proposition (i): A finite group G contains only one Sylow$p - subgroup\ H \iff H\ is\ normal\ in\ G$.

Proposition (ii): If $|G| = pq$ where p, q are primessuch that $p > q\ and\ q$ does not divide – 1 , then G is a cyclic group.

Example(4.37.):

(i) If $|G| = 15, 35, 77, then\ G\ is\ cyclic$.

(ii) Show that every group of order 14 contains only 6 elements of order 7.

Ans: Let $|G| = 14 = 2.7$ By Sylow's first theorem G has a subgroup oforder 7 and ahas Sylow 7-subgorup H. Now, $n_7 = 7k + 1\ (k \ge 0) and\ n_7|14 \Rightarrow n_7 = 1$. Hence$H$ is unique and hence normal and $O(H) = 7 \Rightarrow H$ is cyclic. So, it has 6 elements of order 7.

(iii) A finite abelian group is cyclic ⇔ all of its Sylow subgroups of are cyclic.

(iv) A finite abelian group of order n is cyclic if n is not divisible by p^2 for any prime p.

(v) Let $H\ and\ K$ be subgroups of commutative group G. Let $|H| = m\ \ |K| = n, l = lcm(m, n)$. Then G has a subgroup of order l.

(vi) Let G be a non-commutative group of order $p^3 (p - prime)$.Then $|Z(G)| = p$.

(vii) Let G be a group of order $p^n (p - prime)\ and\ n \in \mathbb{Z}, n \ge 1$.Then any subgroup of G of order $p^{n-1}$is normal in G.

(viii)Let H be a normal subgroup of a finite group $G\ and\ p$ be a prime dividing $|G|$. If $[G : H]$ and p are relatively prime, then H contains all Sylow $p - subgroup$ of G.

4.13. Simple Groups :

Definition: A group G is called a simple group if $G \neq \{e\}$ and G has no non trivial normal subgroups.

4.13.1. Theorem: A commutative group G is simple $\Leftrightarrow G \simeq \mathbb{Z}_p$ for some prime p.

Proposition(i): If $|G| = 2n$ and n is off, then G has a normal subgroup of order n and hence G is not simple, for $n > 1$.

Proposition(ii): Let H be a subgroup of G with $[G : H] = m$. If $|G|$does not divide $m!$, then G has a non-trivial normal subgroup. $\therefore G$ is not simple.

Note: (i) A group of order 60 is the smallest simple non-commutative group.

(ii) Let $n \in \mathbb{Z}$ such that $1 \leq n < 60$ $and\ n\ is\ not\ prime$. Then number of group order n is simple.

4.14. Rings

4.14.1. Definition (Ring): A ring R is an algebraic structure $(R, +, \cdot)$ consists of a non-empty set R together with two binary operations $+\ and\ *$ (called addition and multiplication) such that $(R, +)$ is an abelian group and $(R, .)$ is a semi group and

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), (b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

(i) R is commutative if $ab = ba\ \forall a, b \in R$

(ii) $R$is said to have an identity if $\exists\ 1 \in R\ such\ that\ a \cdot 1 = a\ \forall\ a \in R$

Example (4.38):

(i) $(\mathbb{Z}, +, \cdot)$is a commutative ring with identity.

(ii) $(\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot). (\mathbb{C}, +, \cdot)$ are all commutative ring with 1.

(iii) Finite ring :$\mathbb{Z}_n, +, \cdot)$

(iv)Let$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}, i = \sqrt{-1}\}$ with complex $*\ and \cdot$ is a ring known as ring of Gaussian integers.

(v) Let $(G, +)$ be an abelian group and R be the set of all endomorphisms (homomorphism on G) of G. Define $(f + g)(x) = f(x) + g(x)$ and $(f \circ g)(x) = f(g(x))\ \forall\ f, g \in R\ and\ \forall\ x \in G$. Then$(R, +, 0)$ is a ring (which is called the ring of endomorphisms of G).

(vi) Let$R_1\ and\ R_2$ be two rings. Define $R = R_1 \times R_2, (a, b) + (c, d)$

$$= (a + c, b + d)\ and\ (a, b); (c, d) = (ac, bd).$$

Then $(R, +, \cdot)$ is a ring where (OR_1, OR_2) is the additive identity (R is called the direct product of rings $R_1\ and\ R_2$).

(vii) $(\mathbb{R}[x], +, \cdot)$is a ring where $\mathbb{R}[x]$ set of all polynomial with real coefficients.

(viii) $R = P(X) and\ A, B \in P(X)\quad A + B = A \Delta B\ and\ A \cdot B = A \cap B.\ There\ (R, +, \cdot)$is a ring.

(ix) $(M_x(\mathbb{R}), +, \cdot)$is a ring where $M_x(\mathbb{R})$ is the set of all $n \times n$ real matrices.

4.14.2. Theorem: Let R be a ring and $a, b \in R$. Then –

(i) $a \cdot 0 = 0 = 0 \cdot a$

(ii) $a(-b) = (-a)b = -ab$

(iii) $(-a)(-b) = ab$

(iv)$(a+b)(c+d) = ac + ad + bc + bd, \quad c, d \in R$

(v) $(a-b)(c-d) = ac - bc - ad + bd$

(vi)$(a+b)^2 = a^2 + ab + ba + b^2$

4.14.3. (Idempotent): An element $x \in R$ is called idempotent if $x^2 = x$.

4.14.4. (**Boolean Ring**): A ring R is called Boolean ring if every element of R is idempotent i.e. $x^2 = x \ \forall\, x \in R$.

Example (4.39): See example (viii) of (4.38) .

4.14.5. Theorem: Let R be a Boolean ring. Then –

(i) $2x = 0 \ \forall \ x \in R$

(ii) $xy = yx \ \forall\, x, y \in R$

Note : Boolean is a commutative ring.

4.14.6. (Unit): Let R be a ring with identity $1(\neq 0)$. Then $u \in R$ is called a unit (or invertible) if $\exists \ v \in R \ \ such\ that\ uv = vu = 1.$ $v$is called the inverse of u and is denoted by u^{-1}.

Example (4.40):

(i) Non-singular matrices are units in $M_n(\mathbb{R})$

(ii) Any non-zero rational number in $\mathbb{Q}$ is a unit.

4.14.7. (Nilpotent): An element $x \in R$ is called nilpotent if $x^n = 0$ for some positive integer n. The smallest $n(for\ x)$ is called degree of nilpotent of x.

4.14.8. Theorem: The sum of two nilpotent elements of a commutative ring is also nilpotent.

4.14.9. (Zero divisor): Let $0 \neq a \in R$. Then a is called a zero divisor if $\exists\ 0 \neq b \in R$

$$such\ that\ ab = 0\ or\ ba = 0.$$

Example(4.41):

(i) $(M_n(\mathbb{R}), +, \ \cdot)$has zero divisor (ii) $\mathbb{Z}_6, +, \ \cdot)$ $\qquad \bar{2} \cdot \bar{3} = 0\ in\ \mathbb{Z}_6$

4.14.10. (Cancellation Law): A ring R is said to satisfy left (right) cancellation property if

$$\forall\ a, b, c \in R, \qquad a \neq 0\ \ and\ \ ab = ac\ [represent\ \ ba = ca]\ \Rightarrow b = c$$

4.14.11. Theorem: Let R be a ring. Then the followings are equivalent:

i. R has no zero divisors.
ii. R satisfies left cancellation property.
iii. R satisfies right cancellation property.

4.14.12. (Integral Domain): A commutative ring with identity $1 \neq 0$ is called on integral domain(ID) if R has no zero divisors.

Examples (4.42):

(i) $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$

(ii) $R = R_1 \times R_2$ is not an integral domain even if both R_1 and R_2 are Integral Domain. Since $(0, b) \cdot (a, 0) = (0,0)$.

4.14.13. Theorem: For any positive integer n, the ring $\mathbb{Z}_n$of all integers modules n is an integral domain $\Leftrightarrow n$ is prime.

4.14.14. Theorem: A commutative ring R with identity $1 \neq 0$ is an integral domain $\Leftrightarrow$ the cancellation law holds for multiplication.

4.14.15. (Division ring): A ring R with identity $1 \neq 0$ is called a division ring if every non-zero element of R is a unit.

Example(4.43):$R = \{\left(\frac{\alpha}{\beta}, \frac{\beta}{\alpha}\right) \in M_2(\mathbb{C}): \bar{\alpha}, \bar{\beta}\ are\ conjugate\ of\ \alpha, \beta$

4.14.16. (Field): A commutative division ring is called field. For field $(F, +, \cdot)$ we have $(F, +)\ and\ (F, \cdot)$ are both abelian groups.

Examples(4.44):$(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$

4.14.17. Theorem: Any field is an integral domain.

4.14.18. Theorem: Any finite integral domain is a field.

4.14.19. (Corollary): $\mathbb{Z}_n$ is a field $\Leftrightarrow n$ is prime.

4.14.20. (Characteristic of Ring): Let R be a ring. If there exists a positive integer n such that $na = 0\ \forall\ a \in R$, then the least such n is called the characteristic of the ring.

Note: If there is not exists positive integer n with $na = 0\ \forall\ a \in R$, then the ring is said to be of characteristic $0\ (Zero)$.

Example(4.45)

(i) The characteristic of $\mathbb{Z}_n$in n.

(ii) The ring $\mathbb{Z}$ and the fields $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are of characteristic zero.

4.14.21. Theorem: The characteristic of an integral domain is either prime or zero. In particular characteristic of a field is either prime or zero.

4.14.22. (Corollary): The characteristic of a finite field is prime.

4.15. Subring: A non-empty subset S of a ring $(R,+,\cdot)$is called a subring of R if $(S,+)$ is a subgroup of the abelain group $(R,+)$ and S closed under multiplication i.e. $\forall\ a,b\in S\ \Rightarrow ab\in S$.

Example(4.46.):

(i) The smallest subring of R is $\{0\}$ and the greatest one is R itself.

(ii) In the following chain, the former is a subring of the later $\mathbb{Z}\subseteq\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}$

Note: $\mathbb{Z}_n$ is not a subring of $\mathbb{Z}$, but $n\mathbb{Z}-\{nr : r\in\mathbb{Z}\}$ is a subring of $\mathbb{Z}$.

(iii) The set $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\in\mathbb{R} : a,b,\in\mathbb{Z}\}$ is a subring of $\mathbb{R}$.

(iv) LetR_1 *and* R_2 be two rings and S_1 *and* S_2 be two subrings of R_1 *and* R_2 respectively. Then $S_1\times S_2$ is a subring of $R_1\times R_2$.

(v) The set of even polynomial R is a subring of $\mathbb{R}[x]$.

(vi) The Gaussian integers $\mathbb{Z}[i]=\{a+bi\in\mathbb{C} : a,b\in\mathbb{Z},\ i^2=-1\}$ is a subring of $\mathbb{C}$.

4.15.1. Theorem: Let R be a ring and S be an non-empty subring of R. A necessary and sufficient condition that S is a subring of R is $a,b\in S\ \Rightarrow a-b,ab\in S$.

4.15.2. Theorem: Let $\{S_\alpha : \alpha\in\wedge\}$ be a collection of subrings of a ring R. Then $S=\bigcap_{\alpha\in\wedge}S_\alpha$ is a subring of R *and* S is the smallest subring.

Note: Union of two subrings may not be a subring. Consider the subrings $2\mathbb{Z}$ *and* $3\mathbb{Z}$ *of* $\mathbb{Z}$. Since $2+3\notin 2\mathbb{Z}\cup 3\mathbb{Z}$ *we have* $2\mathbb{Z}\cup 3\mathbb{Z}$ is not a subring of $\mathbb{Z}$.

4.15.3. (Centre of R): Let R be a ring. Define

$C(R)=\{a\in R : x_a=a_x\ \forall\ x\in R\}$, $C(R)$ is called the centre of R.

Note that $C(R)=R\ \Leftrightarrow R$ *is commutative*.

4.15.4. Theorem: The centre of a ring R is a subring of R.

4.15.5. (Sub field): Let F be a field. A subring S of F is called a subfield of if $1\in S$ and for each $0\neq a\in S, a^{-1}\in S$.

Clearly a subfield S in itself a field.

Example(4.47):

(i) In the following chain the former is the subfield of the later

$$\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}$$

(ii) $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}\in\mathbb{R} : a,b\in\mathbb{Q}\}$is a subfield of $\mathbb{R}$.

(iii) Let A be the set of all complex number which satisfy a polynomial equation with rational co-efficient, i.e.$A=\{\alpha\in\mathbb{C} : a_0+a_1\alpha+a_2\alpha^2..........+a_n\alpha^n=0, a_i\in\mathbb{Q},\ n\in\mathbb{N}_0\}$

Then A is a subfield of $\mathbb{C}$. Elements of A are called algebraic numbers.

4.15.6. Theorem: Let S be a subset of a field F. Then is a subfield of $F \Leftrightarrow S$ satisfies the following conditions:

i. $|S| \geq 2$
ii. $a - b \in S\ \forall\, a, b \in S$
iii. $ab^{-1} \in S\ \forall\, a \in S, b \in S\ |\{0\}$.

4.15.7. Theorem: Let $\{S_\alpha\ : \alpha \in \Lambda\}$ be a collection of subfield of a field F.Then$S = \bigcap_{\alpha\in\Lambda} S_\alpha$ is also a subfield of F.

- Note that
  (i) $\mathbb{Q}$is the smallest subfield over $\mathbb{R}$.
  (ii) The characteristic of a subfield is same as the characteristic of the field. $\Rightarrow \mathbb{R}$has no finite subfield.
  (iii) The union of two subfields may not be a subfield consider $\mathbb{Q}[\sqrt{2}]$ *and* $\mathbb{Q}[\sqrt{3}]$ two subfield of $\mathbb{R}$.Then $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}[\sqrt{2}] \cup \mathbb{Q}[\sqrt{3}]$. So, $\mathbb{Q}[\sqrt{2}] \cup \mathbb{Q}[\sqrt{3}]$ is not a subfield of$\mathbb{R}$.

4.16. (Ideal) : A subring I of ring R is called a left [right] ideal of R, if $\forall\ r \in R \text{ and } \forall\, x \in I, rx \in I\ [respectively\ xr \in I]$. If I is both left and right ideal, then I is called an ideal of R.

Examples(4.48):

i). $\{0\}$*and* $R$are two trivial ideal of R.
ii). $2\mathbb{R}$is an ideal of $\mathbb{R}$.
iii). *Let* R be a ring and consider $S = R \times R$. Then $R \times \{0\}$ *and* $\{0\} \times R$ are ideals of $R \times R = S$.
iv). Every field has only two trivial ideals $\{0\}$ *and* F.

4.16.1. Theorem: Let $\{I_\alpha\ : \alpha \in \Lambda\}$ be a collection of left [right ideal] of a ring R. Then $I = \bigcap_{\alpha\in\Lambda} I_\alpha$is a left [respectively right ideal] ideal of R.

Note that union of two ideals may not be an ideal consider $2\mathbb{Z}$ *and* $3\mathbb{Z}$ *of* $\mathbb{Z}$ ($As\ 2\mathbb{Z} \cup 3\mathbb{Z}$ *is a subring of* $\mathbb{Z}$.).

4.16.2. Definition: Let I and J be two ideas of R. Define

$$I + J = \{a + b : a \in I, b \in J\} \text{ and}$$

$$IJ = \{\textstyle\sum_{i=1}^{m} a_i b_i\ :\ a_i \in I, b_i\ \in J, n \in \mathbb{N}\}.$$

4.16.3. Theorem: Let R be a ring and I, J be two ideals of R. Then $I + J$ and IJ are ideals of R. Moreover $IJ \subseteq I \cap J$ *and* $I \cup J \subseteq I + J$. Ideal $I + J$ is the smallest ideal containing $I \cup J$.

4.16.4. Theorem: Let R be a ring and $x \in R$.Denote the smallest ideal containing x by (x). Then

$$(x) = \{ rx + rs + \sum_{i=1}^{m} s_i \ x \ t_i + nx : r, s, s_i, t_i \in R; m \in \mathbb{N}, n \in \mathbb{N}\}$$

If R has m identity, then –

$(x) = \{\sum_{i=1}^{m} s_i \ x \ t_i : s_i, t_i \in R; m \in \mathbb{N}\}$and

if$R$ is a commutative ring with identity, then –

$$(x) = Rx = \{rx : r \in R\}$$

4.16.5. (Principal ideal): The ideal (x) of a ring R is called the principal ideal generated by the element $x \in R$.

4.16.6. (Principal ideal ring): A ring R with identity is called a principal ideal ring if every ideal of $R$is a principal ideal.

- An integral domain (ID) in which every ideal is a principal ideal is called a principal ideal domain(PID).

Example (4.49):

i). $\mathbb{Z}$is a principal ideal domain(PID). Since its every ideal is of the form $n\mathbb{Z} = (n), n \in \mathbb{N}_0$.

Note that in a ring R with identity, $R = (1)$ and hence for any ideal I of $R, 1 \in I \Leftrightarrow I = R$. Thus in this case R has trivial ideals (0) and (1).

ii). $\mathbb{Z}(n > 1)$ is a PIR

iii). $\mathbb{Q}[x]$ is a PID.

4.17. (Simple ring): A ring R is called simple if $R^2 \neq \{0\}$ and R has no non-trivial ideal.

Example(4.50): (i) $\mathbb{Z}_p$ (ii) $M_2(\mathbb{R})$ (iii) Any field.

4.17.1. Theorem: A commutative ring R with identity is simple $\Leftrightarrow$ R is a field.

4.18. (Quotient ring/ Factor ring): Let R be a ring and I be an ideal of R. Then the ring

$R/I = \{a + I : a \in R\}$is called the quotient ring of R by I. Where –

$$(a + I) + (b + I) = (a + b) + I \ and \ (a + I)(b + I) = ab + I \ \forall \ a, b \in R$$

Example(4.51): Consider the ring $\mathbb{Z}$ and in this ring $5\mathbb{Z} = \{5k : k \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. Then $\mathbb{Z}/5\mathbb{Z} = \{n + 5\mathbb{Z} : n \in \mathbb{Z}\}$ is a quotient ring.

4.18.1. Theorem: If R is a commutative ring with identity $1 \neq 0$ and I be a proper ideal of R, then the quotient ring R/I is also a commutative ring with identity.

4.19. (Homomorphism): Let R and S be two rings. A mapping $f : R \to S$ is called a homomorphism of R $into$ S, if it satisfies the following –

i). $f(a + b) = f(a) + f(b)$

ii). $f(ab) = f(a)f(b) \quad \forall \ a, b \in R$

Any homomorphism of a ring R into itself is called an endomorphism and a bijective endomorphism is called an automorphism.

Example(4.52):

i). $f:\mathbb{Z}\to\mathbb{Z}$ by $f(r)=[r]$

ii). (not homomorphism) $f:\mathbb{Z}\to\mathbb{Z}\ by\ f(x)=-x.$

$$Then\ \ f(m+n)=\ -(m+n)=-m-n=f(m)+f(n).$$

Now$f(2\cdot 3)=-(2\cdot 3)\neq(-2)(-3)=f(2)f(3).$

4.19.1. (Kernel): (i) $\ker f=\{x\in R: f(x)=\ 0_s\}.kerf$is an ideal of $R.$ (ii) f is one – one if only if $kerf\ =\{0_R\}.$

1st , 2nd, 3rd isomorphism theorem also holds for ring homomorphism.

Example(4.53): Find all homomorphism from the ring $\mathbb{Z}\ onto\ \mathbb{Z}.$

Answer: Only one which is identity homomorphism.

4.19.2. (Maximal ideal): A proper ideal I of a ring $R\neq\{0\}$is called a maximal ideal of R if I is not contained in any other proper ideal of R i.e. for any ideal $J\ of\ R,\ I\subseteq R\ \Rightarrow either\ I=J\ or\ J=R.$

Example(4.54).

i). $3\mathbb{Z}$ is maximal ideal $m\mathbb{Z}$. But $6\mathbb{Z}$ is not maximal is $\mathbb{Z}$. Since $6\mathbb{Z}\subset 3\mathbb{Z}\subset\mathbb{Z}$. In general $p\mathbb{Z}$ for any prime P, is a maximum ideal in $\mathbb{Z}$.

ii). Consider $\mathbb{Z}_6$. In this ring {0}, {0, 2, 4}, {0, 3} and $\mathbb{Z}_6$. $\{0,2,4\}\ and\ \{0,3\}$are maximal ideal in $\mathbb{Z}_6$.

iii). Let F be a field. Since {0} and F are only two ideals of F,{0} in the only maximal ideal of F.

4.19.3. Theorem: Let R be a commutative ring with identity $I\neq 0$. Then R is a field $\Leftrightarrow$ {0} is a maximal ideal of R.

4.19.4. Theorem: Let R be a commutative ring with identity, $I\neq 0$. Then an ideal $M\ of\ R$ is maximal $\Leftrightarrow R/M$ is a field.

4.19.5. (Prime ideal): Let R be a ring such that $R\neq\{0\}$.A proper ideal $P\ of\ R$ is called a prime ideal, if for any ideal $A,B\ in\ R, AB\subseteq P\ \Rightarrow A\subseteq P\ or\ B\subseteq P.$

4.19.6. Theorem: Let R be a ring with $R\neq\{0\}$ and P be a proper ideal of R such that for any $a,b\in R,\ \ ab\in P\ \Rightarrow a\in P\ or\ b\in P$.Then P is a prime ideal of R.

Example(4.55):$P\mathbb{Z}$ of $\mathbb{Z}$. Let $a,b\in R$ such that $ab\in P\mathbb{Z}\Rightarrow P(ab)\Rightarrow$ $either\ P|a\ or\ P|b\ as\ P\ is\ prime.$

4.19.7.(Theorem). Let R be a commutative ring with identity. Then every maximal ideal if R is prime.

4.19.8. Theorem: Let R be a commutative ring with identity, $I\neq 0$. A proper ideal $P\ of\ R$ is prime ideal $\Leftrightarrow R|P\ is\ an\ integral\ domain(ID).$

Note: $P\mathbb{Z}, P$ is prime, are both prime and maximal ideal in $\mathbb{Z}$.

4.19.9. Theorem:

i). In a Boolean ring B with identity, every prime ideal is a maximal ideal. ⇒prime ideal ⇔ maximal ideal.

ii). Let R be ring with identity.Then every proper ideal of R is contained in a maximal ideal of R.

iii). Let R be a ring with identity, $I \neq 0$. Then$R$ has a maximal ideal.

Example(4.55):

Find all prime and maximal ideal of $\mathbb{Z}_8$.

Answer: (i) Ideals of $\mathbb{Z}_8$are $\{0\}, \{0, a\}, \{0,2,4,6\}, \mathbb{Z}_8 \Rightarrow \{0,2,4,6\}$ is the only maximal ideal. By the theorem(4.19.9) it is also prime ideal. Now, $\{0\}$ is not prime, since$4 \times 2 = 0\ but\ 2,4, \notin \{0\}$. $\{0,4\}$ is not prime as $2 \times 2 = 4\ but\ 2 \notin \{0,4\}$.

(ii) In the ring $\mathbb{Z}[i]$, the subset $I = \{a + ib \in \mathbb{Z}[1] : a, b\ are\ the\ both\ muliples\ of\ 3\}$ is a maximal ideal of $\mathbb{Z}[i]$.

(iii) $\mathbb{Z}[i]/I$ is a field of 9 elements.

4.20. Polynomial Rings:

Definition: Let R be a commutative ring. The set of polynomials $R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \ldots\ldots\ldots + a_1 x + a_0 = a_i \in R, n > 0\}$ is called the ring of polynomials over R in the indeterminate x.

4.20.1. Theorem: If D is and integral domain (ID), then $D[x]$ is an integral domain (ID).

4.20.2. Theorem(Division Algorithm): Let F be a field and let $f(x), g(x), \in F(x)$ with $g(x) \neq 0$. Then

∃unique polynomials $q(x) and\ r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x), r(x) = 0\ or\ \deg r(x) < \deg g(x)$.

4.20.3. Corollary –I (Remainder Theorem): Let F be a field, $a \in F$ and $f(x) \in F[x]$.Then$f(a)$ is the remainder in the division of $f(x)\ by\ x - a$.

4.20.4. Corollary – II (Factor Theorem): Let F be a field, $a \in F\ and\ f(x) \in F[x]$. Then a is a zero of $f(x) \Leftrightarrow x - a$ is a factor of $f(x)$.

4.20.5. Corollary – III : A polynomial of degree n has at most n zeros counting multiplicity.

4.20.6. Theorem(PID): Let Fbe a field. Then $F[x]$ is a PID. So any ideal $I\ inF[x], I = \langle f(x) \rangle$ where $f(x)$ is a non-zero minimum degree polynomial in I.

Example(4.56): Let $\phi : \mathbb{R}[x] \to \mathbb{C}$ be defined by $\phi[f(x)] = f(i)\ \forall\ f(x) \in \mathbb{R}[x]$. Then ϕ is a homomorphism and $x^2 + 1 \in ker\phi\ and\ x^2 + 1$ is the minimum degree polynomial in $ker\phi$. Thus $ker\phi = \langle x^2 + 1 \rangle$ By 1st isomorphism theorem $\mathbb{R}[x] | \langle x^2 + 1 \rangle \simeq \mathbb{C}$.

4.20.7. (Irreducible, Reducible Polynomial): Let D be an integral domain. A polynomial $f(x)$ form $D[x]$ that is neither zero nor unit in $D[x]$ is said to be irreducible order D, if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$ with $g(x), h(x) \in D[x]$ then either $g(x)$ *or* $h(x)$ is a unit in $D[x]$.

A non- zero, non-unit element of $D[x]$ that is not irreducible over D is called reducible over D.

Example(4.57):

i). $x^2 - 2$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$.

ii). $2x^2 + 4$ is irreducible over $\mathbb{Q}$ and $\mathbb{R}$ but reducible over $\mathbb{C}$.

iii). The polynomial $x^2 + 1$ i.e. irreducible over $\mathbb{Z}_3$ but reducible over $\mathbb{Z}_5$ (Hint. in $\mathbb{Z}_3, x^2 + 1$ has no zero but in $\mathbb{Z}_5$, $x^2 + 1 = x^2 + 1 + (-5) = x^2 - 4 = (x-2)(x+2) = (x - 2 + 5)(x+2) = (x+3)(x+2)$).

4.20.8. Theorem: Let F be a field and $f(x) \in F[x]$ with $degf(x) = 2$ *or* 3.Then$f(x)$ is reducible over $F \Leftrightarrow f(x) has\ a\ zero\ in\ F$.

4.20.9. (Content of polynomial, Primitive polynomial): The content of a non-zero polynomial$a_n x^n + a_{n-1}x^{n-1} + \dots\dots\dots + a_1 x + a_0$ where $a_i \in \mathbb{Z}$, is the gcd of $a_{0,}a_1, \dots\dots\dots a_n$. A primitive polynomial is an element of $\mathbb{Z}[x]$ with content 1.

4.20.10. Lemma(Gauss): The product of two primitive polynomials is primitive.

4.20.11. Theorem: Let $f(x) \in \mathbb{Z}[x]$. If f(x) id reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

Example(4.58):

$$f(x) = 6x^2 + x - 2 = \left(3x - \frac{3}{2}\right)\left(2x + \frac{4}{3}\right)$$

$$\Rightarrow 2 \cdot 3\, f(x) = 2\left(3x - \frac{3}{2}\right) 3\left(2x + \frac{4}{3}\right) = 2 \cdot 3(2x-1)(3x+2)$$

$$\Rightarrow f(x) = (2x-1)(3x+2).$$

4.20.12. Theorem(Mod P Irreducible Test): Let P be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) \geq 1$. Let $f^2(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficient of $f(x)$moduls P. If $f^2(x)$ is irreducible over $\mathbb{Z}_p$ and $degf^2(x) = degf(x), then\ f(x)$ is irreducible over $\mathbb{Q}$.

Example (4.59): Let $f(x)21x^3 - 3x^2 + 2x + 9$. Then over Z_2. Thus $f(x)$ is irreducible over $\mathbb{Q}$ *and hence over* $\mathbb{Z}$.

4.20.13.Theorem(Eisenstein Criterion): Let $f(x) = \{a_n x^n + a_{n-1}x^{n-1} + \dots\dots\dots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there is a prime P such that $P \nmid a_n, P|a_{n-1}, \dots\dots, P|a_0$ *and* $P^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

4.20.14. Corollary: For any prime P, the P^th cyclotomic polynomial

$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots\dots\dots + x + 1$is irreducible over $\mathbb{Q}$.

4.20.15. Theorem: Let F be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x] \Leftrightarrow p(x)$is irreducible polynomial over F.

4.20.16. Corollary – I : Let F be a field and $p(x)$ an irreducible polynomial over F. Then $F[x]|\langle p(x)\rangle$ is a field.

4.20.17. Corollary – II : Let F be a field and let $p(x), a(x), b(x) \in F[x]$. If $p(x)$ is irreducible over F and $p(x)|a(x)b(x),\ then\ p(x)|a(x)\ or\ p(x)|b(x)$.

4.20.18. Theorem: $Z[x]$ is a unique factorization domain(UFD) i.e. $f(x) \in \mathbb{Z}[x]$.

$$f(x) = b_1b_2 \dots \dots . . b_s p_1(x) \dots \dots \dots \dots \dots . p_m(x) = c_1c_2 \dots \dots . . c_t q_1(x) \dots \dots \dots \dots \dots . q_n(x)$$

where$b's adn\ c's$ are irreducible polynomial of degree 0 and the $p(x)'s, q(x)'s$ are irreducible polynomial of positive degree. Then $s = t,\ m = n\ and\ b_i = \pm c_i,\ p_i(x) = \pm q_i(x)$.

4.21. Divisibility in Integral Domain(ID):

Elements a, b of an integral domain D are called associates if $a = ub$ where $b, c \in D\ with\ a = bc, then\ b\ or\ c$ is unit. A non-zero element $a \in D$ is called prime if a is not unit and $a|bc \Rightarrow a|b\ or\ a|c$.

4.21.2. **Theorem**(Prime ⇒ Irreducible in ID):

In an integral domain(ID), every prime is an irreducible. Converse is not true.

Example(4.61):

$1 + \sqrt{-5}, 1 - \sqrt{-5},\ 3, 2, 3 \pm \sqrt{-5},\ \ 2 \pm 3\sqrt{-5},\ 3 \pm 2\sqrt{-5},\ 1 \pm 2\sqrt{-5},\ 1 \pm 3\sqrt{-5}$are irreducible in $\mathbb{Z}[\sqrt{-5}]$ but they are not prime in $\mathbb{Z}[\sqrt{-5}]$.

Let $1 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5})$

$$\Rightarrow (1 + \sqrt{-5)(1 - \sqrt{-5}}) = (a + b\sqrt{-5})(a - b\sqrt{-5})(c + d\sqrt{-5})(c - d\sqrt{-5})$$

$$\Rightarrow 1 + 5 = (a^2 + 5b^2)(c^2 + 5d^2)$$

$$\Rightarrow 2 \times 3 = (a^2 + 5b^2)(c^2 + 5d^2) = 6 \times 1\ \Rightarrow 6 = a^2 + 5b^2, \quad 1 = c^2 + 5d^2$$

$\Rightarrow 2 = a^2 + 5b^2, \qquad 3 = c^2 + 5d^2\ (There\ is\ no\ a, b, c, d \in \mathbb{Z})$

$\Rightarrow a = \pm 1, b = \pm 1 \qquad \Rightarrow c = \pm 1, d = 0$

$\Rightarrow c + d\sqrt{-5}\ \ is\ unit. .$

4.21.4. (Unique Factorization Domain (UFD)).

An integral domain D is a unique factorization domain if –

(i) Every non-zero and non- unit element of D can be written as a product of irreducible of D.

(ii) The factorization into irreducible is unique up to associates and the order in which the factors appear.

4.21.5. Theorem: Every principal ideal domain (PID) is a unique factorization domain (UFD).

Converse is not true. Since $\mathbb{Z}[x]$ is unique factorization domain (UFD) but is not PID.

4.21.6. Corollary: Let F be a field. Then $F[x]$ is a unique factorization domain (UFD).

4.21.7. Definition (Euclidean Domain): An integral domain D is called a Euclidean domain (ED) if ∃ function N form the non-zero elements of D to the non-negative integers such that-

(i) $N(a) \leq N(ab)\ \forall\ non - zero\ a, b \in D$

(ii) If $a, b \in D, b \neq 0, then\ \exists\ q, r \in D\ such\ that\ a = bq + r\ where\ r = 0\ or\ N(r) < N(b).$

Example (4.62.):

i). The ring $\mathbb{Z}$ is a Euclidean Domain(ED) with $N(a) = |a|$.

ii). Let F be a field. Then F[x] is a Euclidean Domain with $N(f(x)) = degf(x) \Rightarrow$ $F[x] is$ Euclidean Domain, Principal Ideal Domain, Unique Factorization Domain, Integral Domain.

iii). The ring of Gaussian integers $\mathbb{Z}[i] = \{a + ib = a, b \in \mathbb{Z}\}$ is Euclidean Domain with $N(a + ib) = a^2 + b^2$.

iv). $\mathbb{Z}[\sqrt{n}]$ is Euclidean Domain only for $n = -1, -2, 2, 3$

v). In Principal Ideal Domain(PID), if $\langle a \rangle\ and\ \langle b \rangle\ two\ ideal\ \langle a, b \rangle = \langle a \rangle + \langle b \rangle = \langle d \rangle$

$$\langle a \rangle \cap \langle b \rangle = \langle l \rangle\ where\ d = \gcd(a, b), l = lcm(a, b)$$

vi). If $N(a)$ is prime is D then a is irreducible.

$$F \subset ED \subset PID \subset UFD \subset FDC \subset ID \subset R$$

	ID	FD	UFD	PID	ED	F
	$\mathbb{Q}$	√	√	√	√	√
	$\mathbb{R}$	√	√	√	√	√
	$\mathbb{Z}$	√	√	√	√	×
$F[x], Field$	$\mathbb{Q}[x]$	√	√	√	√	×
	$\mathbb{R}[x]$	√	√	√	√	×
	$\mathbb{Z}\left[\frac{1+i\sqrt{7}}{2}\right]$	√	√	√	×	×
	$\mathbb{Z}[x]$	√	√	×	×	×
	$\mathbb{Z}[i\sqrt{5}$	√	×	×	×	×
Ring	R	×	×	×	×	×

4.22. (Extension Field): A field E is and extension field of a field $F\ if\ F \subseteq E$ and the operation of F are those of E restricted to F.

Example: $\mathbb{R}$ is a extension field of $\mathbb{Q}$.

Theorem (Fundamental Theorem of Field): Let F be a field and $f(x)$ a non-constant polynomial in $F[x]$. Then there exist an extension field E of F in which $f(x)$ has a zero.

Example(4.63): Let $f(x) = x^2 + 1 \in \mathbb{Q}[x].$ $Then\ in\ E = \mathbb{Q}[x]|\langle x^2+1\rangle$, we have

$$f(x + \langle x^2+1\rangle) = (x + \langle x^2+1\rangle)^2 + 1 = x^2 + \langle x^2+1\rangle + 1$$

$$= x^2 + 1 + \langle x^2+1\rangle = 0 + \langle x^2+1\rangle = \langle x^2+1\rangle$$

$$\Rightarrow f\ has\ zero\ in\ E = \mathbb{Q}[x]/\langle x^2+1\rangle$$

Since, in $G|H,\ (a+H)(b+H) = ab + H\ \ and\ (a+H)+(b+H) = (a+b)+H$

Note : H is the '0' element and 1+H is the '1' element in $G|H$.

Example(4.64): Let $(x) = x^5 + 2x^2 + 2x + 2 \in \mathbb{Z}_3[x]$. Then its irreducible factorization over $\mathbb{Z}_3[x]$ is $(x^1+1)(x^3+2x+2)$.So, we may take its extension field as $E = \mathbb{Z}_3[x]/\langle x^2+1\rangle = \{a + bx + \langle x^2+1\rangle : a, b \in \mathbb{Z}_3\}$ with 9 elements or $\mathbb{Z}_3[x]/\langle x^3+2x+1\rangle$ with 27 elements.

Note: (i) Construct field with 8, 9, 27 etc.

(ii) Let $\deg f(x) = n\ and\ f(x)$ is irreducible in $\mathbb{Z}_p[x]$, the order of the field $\mathbb{Z}_p[x]/\langle f(x)\rangle\ \ is\ p^n$.

4.22.1. (Splitting Field): Let E be an extension field of F and let $f(x) \in F[x]$. We say that $f(x)$ splits in $E\ if\ f(x)$ can be factored as a product of linear factors in $E[x]$. We call E a splitting field for $f(x)$ over $F\ if\ f(x)$ splits in E but no proper subfield of E.

Example (4.65). Consider the polynomial $f(x) = x^2 + 1 \in \mathbb{Q}[x]$.

Since $x^2 + 1 = (x+i)(x_i), i = \sqrt{-1}$. We see that f(x) splits in $\mathbb{C}$, but a splitting field over $\mathbb{Q}\ is\ \mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$

A splitting field for $x^2 + 1 \in \mathbb{R}[x]\ \ is\ \mathbb{C}$. Similarly $x^2 - 2 \in \mathbb{Q}[x]$ splitting in $\mathbb{R}$ but its splitting field is $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}\ : a, b \in \mathbb{Q}\}$.

4.22.2. Theorem (Existence of Splitting Fields) : Let F be a field and let $f(x)$ be a non-constant elements of $F[x]$. Then $\exists$ a splitting field E for $f(x)$ over F.

Example (4.66):

i. Let G be a simple group of order 60. Then $G \simeq A_5$ and it has a subgroup of order 12.

ii. Let $|G| = 2p\ (2 < p - prime)$. Then G is either cyclic or dihedral (D_p)

Note :

(a) $Z(D_n) = \begin{cases} \{e\},\ n\ odd \\ \left\{e, a^{\frac{n}{2}}\right\},\ n\ even \end{cases}$

(b) conjugate classes in $D_{2n+1}\ are\ \{e\}, \{b, ba, \ldots\ldots, ba^{2n}\}, \{a^r, a^{-r}\}, 1 \le r \le n.$

iii. Conjugate classes in

$D_{2n}\ are\ \{e\}, \{b, ba^2, ba^4, \ldots\ldots ba^{2n}\}, \{ba, ba^3, ba^5, \ldots\ldots ba^{2n-1}\}, \{a^r, a^{-r}\},$

$(1 \le r \le n)\ and\ \{a^n\}$

Example (4.67):

A. Dihedral group of degree 4 (D_4) :

$$D_4 = \langle a, b\rangle, a, b \text{ are generators with } O(a) = 4, O(b) = 2.$$
$$D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\ (= ba)\} \Rightarrow |D_4| = 2 \times 4 = 8$$

1). Subgroups (Total number of subgroups is 1 and order 2 $subgroup = 5$ & $order\ 4 = 3$).

$$H_0 = \{e\}, H_1 = \{e, a^2\}, H_2 = \{e, b\}, H_3 = \{e, ab\}, H_4 = \{e, a^2b\}, H_5 = \{e, a^3b\}$$

$$T = D_4, T_1 = \{e, a, a^2, a^3\}, T_2 = \{e, a^2, b, a^2b\}, T_3 = \{e, ab, a^2, a^3b\}$$

2). $H_5$is normal in T_3 and T_3 is normal in D_4, but H_5 is not normal inD_4.

3). $Z(D_4) = \{e, a^2\} = H_1(w)I_{nn}(D_4) \simeq D_4/Z(D_4)$

B. Quaternion group Q_4: (generator are a, b)

$$Q_4 = \{e, b, a^2, a^3, b, ab, a^2b, a^3b(= ba)\} \text{ with } O(a) = 4 = O(b), a^2 = b^2$$

1). Subgroup (Number of subgroup=4+2):

$$H_0 = \{e\}, H_1 = \{e, a^2\}, H_2 = \{e, a, a^2, a^3\}, H_3 = \{e, ab, a^2, a^3b\},$$
$$H_4 = \{e, b, a^2, a^2b\}, H_5 = Q_8$$

Note :$Q_8 = \langle A, B\rangle \text{ where } A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, O(A) = 4 = O(B) and$

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = B^2, A^3B = \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix} = BA$$

2). $D_4 \not\simeq Q_4$

3). Upto isomorphism there exists only two non-commutative groups of order 8 (eg. Q_4, D_4

- $|Aut(Z_n)| = \phi(n)\&\ Aut\ (\mathbb{Z}_n) \simeq U_n$
- (i) Normal subgroup in S_3 are $\{e\}, A_3, S_3$

$K_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$
$= \{e, a, b, ab\}$

(ii) Normal subgroup in S_4 are $\{e\}, K_4, A_4, S_4 (Note\ K_4\ is\ normal\ in\ A_4)$

$$and\ \frac{S_4}{K_4} \simeq S_3$$

(iii) Normal subgroup S_5 are$\{e\}, A_5,\ S_5\ (Note\ A_5\ is\ simple.$