COUNCILE OF SCIENTIFIC & INDUSTRIAL RESEARCH

Mathematical Science Code: 04

Unit – 2 :

Syllabus

Sub Unit – 2 : Abstract Algebra

SL NO.	TOPICS
1	2.1 Set 2.1.1. Set 2.1.2. Power Set 2.1.3. Ordered Pair
2	2.2. Cartesian Product 2.2.1. Cartesian Product
3	2.3 Relations 2. 3.1. Relations 2. 3.2. Composition 2. 3.4. Equivalence Relation 2. 3.5. Anti Symmetric 2. 3.6. Partially Order Set or Poset 2. 3.7. Linearly Ordered Set or Chain
4	2.4 Functions 2. 4.1. Definition, Identity Mapping, Constant Mapping 2. 4.4. Theorem 2. 4.7. Theorem 2. 4.8. Theorem

5	**2.5 Integers** **2. 5.1. Division Algorithm, General Statement** **2. 5.2. Prime to each other** **2. 5.3. Linear Diophantine Equation** **2. 5.4. Perfect Number** **2. 5.5. Prime Number** **2. 5.6. Fundamental Theorem of Arithmetic** **2. 5.7. Congruence** **2. 5.8. Primitive Roots** **2. 5.9. Divisibility Test** **2. 5.10. Chinese Remainder Theorem** **2. 5.11. Polynomial Congruence** **2.5.12. Linear congruence** **2. 5.13. Phi function / Euler's Phi function** **2. 5.14. Fermat's Theorem** **2. 5.15. Euler's Theorem** **2. 5.16. Wilson's Theorem** **5.17. Greatest integer function**
6	**2.6 Permutations and Combinations** **2. 6.1. Definition of Permutation** **2. 6.2. Definition of Combination** **2.6.3. Pigeonhole Principle**
7	**2.7 Binary Operation** **2. 7.1. Definition** **2. 7.2. Multiplication Table** **2. 7.3. Theorem** **2. 7.4. Semi group** **2. 7.5. Monoid** **7.6. Quasi group**

8	**2.8 Groups** **2. 8.2. Abelian (Commutative)** **2. 8.3. Non commutative** **2. 8.4. Theorem** **2. 8.9. Order** **2. 8.21. Order and length**
9	**2.9 Sub group** **2. 9.2. Theorem** **2. 9.3. Corollary** **2.9.5. Theorem** **2. 9.6. Definition** **2.9.7. Theorem** **2. 9.10. Centre of G**
10	**2.10 Cyclic Group** **2. 10.4. Theorem** **2. 10.6. Theorem**
11	**2.11 Co-set and Lagrange's Theorem** **2. 10.6. Theorem** **2. 11.4. Index of subgroup** **2. 11.5. Lagrange's Theorem** **2. 11.11. Fermat Theorem** **2. 11.13. Corollary**
12	**2.12 Normal Subgroup and Quotient Groups** **2. 12.1. Definition** **2. 12.2. Limit Superior and Lint Inferior** **2. 12.3. Theorem** **2. 12.4. Theorem (Quotient group or factor group)** **2. 12.5. Results**

Abstract Algebra

2.1. Set:

2.1.1. 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 belong to a set i.e. there should be no ambiguity what so ever regarding the membership of such collection of a set.

Example (2.1) : 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.

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

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

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

2.1.3. 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, $(x, y) = \{\{x\}, \{x, y\}\} \neq \{\{y\}, \{x, y\}\} = (x, y), \text{where } x \neq y$

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

2.2. Cartesian Product:

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

(i) Assume $X \times \emptyset = \emptyset = \emptyset \times X \text{ for any set } X.$

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

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

2.3. Relations:

2.3.1. Relations: A binary relation or simply a relation ρ 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$(\boldsymbol{\rho^{-1}})$**:** $(\rho^{-1}) = \{(b, a) : (a, b) \in \rho\}, \ (\rho^{-1})^{-1} = \rho$

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

2.3.3. 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 $a, b, c \in A, whenever\ (a, b) \in \rho\ wher\ (b, c) \in \rho\ \Rightarrow (a, c) \in \rho$

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

2.3.5. 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 (2.2):

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

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

2.3.6. 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 (2.3): $(\mathbb{R}, \leq), (P(X),\ \subseteq)$.

2.3.7. 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 (2.4): $(\mathbb{R}, \leq)$ 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 (2.5): 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 $2^{\frac{n^2-n}{2}}$

2.4. Functions:

2.4.1. 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 (2.6): 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 2^{nd} 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.

2.4.2. 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

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

2.4.4. (Theorem): Suppose that $f: A \rightarrow B \text{ and } g: B \rightarrow C$. 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.

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

2.4.6. (Theorem): For any finite set A if $f: A \rightarrow A \text{ is injective}$, then f is bijective.

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

2.4.7. Definition: Consider a function $f: A \rightarrow B$ then f is called

- **(i).** Left invertible, if $\exists\, g: B \rightarrow A \text{ such that } g \circ f = i_A \text{ and } g$ is called left inverse of f.
- **(ii).** Right invertible if $\exists\, h: B \rightarrow A$ 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 (2.7): $f : \mathbb{N} \rightarrow \mathbb{N},\ f(n) = n + 1\ \forall\, n \in \mathbb{N}$ and $g: \mathbb{N} \rightarrow \mathbb{N},\ g(1) = 1$ 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 $f \circ g(1) = f\big(g(1)\big) = f(1) = 2 \ \Rightarrow g \text{ is not right inverse of } f.$

2.4.8. (Theorem): Let $f: A \rightarrow B$ 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.

2.5. Integers

2.5.1. Division Algorithm: Given integers $a \text{ and } b$ with $b > 0$, there exist unique integers $q \text{ and } r$ such that $a = bq + r \text{ where } 0 \leq r < b$.

Note: q is called quotient and r is called remainder.

General Statement: Given integers $a \ and \ b$, with $|b| \neq 0$, there exist unique integers $q \ and \ r$ such that $a = bq + r, \ \ 0 \leq r < |b|$.

(i) $a|b \ and \ b|a \ \Leftrightarrow a = \pm b$

(ii) $a|b \ \ and \ a|c \ \Rightarrow a|(bx + cy) \ for \ any \ x, y \in \mathbb{Z}$.

(iii) The square of an odd integers is of the form $8k + 1$ where $k \in \mathbb{Z}$.

(iv) Let $d = \gcd(a, b)$Then

(I) $d|a \ and \ d|b$

(II) if $c|a \ \ and \ \ c|b \ \ then \ d|c$

(III) $\exists$ integers u, v such that $d = au + bv$.

Example (2.8):

$\gcd(475, 120) = 5$

Now,

$$\left.\begin{array}{l} 475 = 120 \times 3 + 115 \\ 120 = 115 \times 1 + 1 \end{array}\right\} \Rightarrow 5 = 120 + 115(-1) = 120 + (-1)[475 - 120 \times 3]$$

$= (-1) \ 475 + \ \ 4 \times 120$

Note: The $gcd(a, b)$ is the least positive value of $ax + by$ where $x, y \in \mathbb{Z}$.

2.5.2. Definition (Prime to each other): Two integers $a \ and \ b$ are said to be prime to each other if a, b not both zero and $gcd(a, b) = 1$.

(i) If $a|bc \ and$ $\gcd(a, b) = 1.$ $Then \ a|c$.

(ii) If $ap = bq \ and \ a$ is prime to b the $a|q \ \ and \ b|p$

(iii) If $a|c \ and \ b|c \ \ with$ $\gcd(a, b) = 1, then \ ab|c$

(iv) If $a \ is \ prime \ to \ b$ and $a \ is \ prime \ to \ c$ then $a \ is \ prime \ to \ bc$.

(v) If $a \ is \ prime \ to \ b$, then (I) $a + b$ is prime to ab

(II) a^2 is prime to b.

(III) a^2 is prime to b^2.

(vi) If $d = \gcd(a, b)\,, then \ d^2 = \gcd(a^2, b^2)$

(vii) Euclidean Algorithm: If $a = bq + r \ \ then$ $\gcd(a, b) = \gcd(b, r)$

(viii) If a, b are two integers different from zero, then $lcm(a, b) \times \gcd(a, b) = |ab|$.

2.5.3. Linear Diophantine Equation:

If a, b, c are integers and a, b are not both zero, the equation $ax + by = c$ has an integral solution $\Leftrightarrow d = \gcd(a, b)$ divided c. If (x_0, y_0) be any particular solution of the equation, then all integral solutions are given by $(x_0 + \frac{b}{d}t, \ y_0 - \frac{a}{d}t)$ for different integers t.

Example (2.9):

Find general and the positive integral solution of $9x + 7y = 200$.

$\gcd(9,7) = 1\ divided\ 200$

Now,

$$\left.\begin{array}{l} 9 = 7 \times 1 + 2 \\ 7 = 2 \times 3 + 1 \end{array}\right\} \Rightarrow 1 = 7 - 2 \times 3 = 7 - 3(9-7) = (-3)9 + 4 \times 7$$

$\Rightarrow (-600)9 + (800) \times 7 = 200$

$\therefore x_0 = -600, y_0 = 800$

$\therefore x = -600 + 7t, y = 800 - 9t, \quad t = 0, \pm 1, \pm 2\ldots\ldots.$

For positive integral solutions $x = -600 + 7t > 0 \Rightarrow t > \frac{600}{7}$

and $y = 800 - 97 > 0 \Rightarrow t < \frac{800}{9}$

$\therefore t = 86, 87, 88$ so, it has three positive integral solutions.

We denote $\gcd(a,b) = (a,b)$ and $lcm(a,b) = [a,b]$. If a, b, c be positive integers then –

(i) $(a,[b,c]) = [(a,b),(a,c)]$

(ii) $[a,(b,c)] = ([a,b],[a,c])$

(iii) The sum of all positive divisors of a positive integer n. If $n = {p_1}^{\alpha_1}, {p_2}^{\alpha_2}\ldots\ldots\ldots {p_k}^{\alpha_k}$ then

$S(n) = (1 + p_1 + {p_1}^2 + \ldots\ldots + {p_1}^{\alpha_1})\ldots\ldots\ldots(1 + p_k + \ldots\ldots + {p_k}^{\alpha_k})$

$= \frac{{p_1}^{\alpha_1+1}-1}{p_1-1} \cdot \frac{{p_2}^{\alpha_2+1}-1}{p_2-1}\ldots\ldots\frac{{p_k}^{\alpha_k+1}-1}{p_k-1}$

$= Sum\ of\ all\ positive\ divisors\ of\ n.$

Example (2.10):

$S(48) = \dot{S}(2^4 \cdot 3) = \frac{2^5-1}{2-1} \times \frac{3^2-1}{3-1} = 31 \times 4 = 124$

Note: (I) $d(mn) = d(m)d(n), \gcd(m,n) = 1$

(II) $S(mn) = S(m)S(n); \gcd(m,n) = 1$

2.5.4. Definition (Perfect Number): n is perfect if $S(n) = 2n$.

Example (2.11): $Since, S(6) = S(2 \cdot 3) = \frac{2^2-1}{2-1} \times \frac{3^2-1}{3-1} = 3 \times 4 = 12 = 2 \times 6$

6 is perfect.

- The product of all positive divisors of a positive integer n is $p(n) = n^{\frac{d(n)}{2}}$.

Example (2.12): $p(6) = 6^{\frac{4}{2}} = 6^2 = 36 = 1 \cdot 2 \cdot 3 \cdot 6$

- Find the least positive integer having m number of positive divisors. Let n be the such number. $m = d_1, d_2 \dots \dots d_k$ $with$ $2 \le d_1 \le d_2 \dots \dots \le d_k$

$\therefore n = 2^{d_k - 1} 3^{(d_{k-1}-1)} 5^{(d_{k-2}-1)} \dots \dots \dots p_k{}^{d_1 - 1}$ where p_k is the $k-th$ prime.

Example (2.13):

Find the least positive integer having 24 number of positive divisors.

$24 = 2 \times 3 \times 4$ $\therefore n = 2^3 \cdot 3^2 \cdot 5^1 = 360$

2.5.5. Prime Number

Definition:

(I) An integer $p > 1$ is said to be a prime number or simple a prime, if its only positive divisors are 1 and p.

(II) $p > 1$ is prime $\Leftrightarrow p|ab \Rightarrow either\ p|a\ or\ p|b$.

(i) For $n > 3$ the integers $n, n+2, n+4$ cannot be all primes.

(Hints: Any integer n is of the forms $3k, 3k+1, 3k+2$. If

$n = 3k$ $then\ n\ is\ not\ prime.$

$n = 3k + 1$ $then\ n + 2 = 3(k+1)$ $and\ n+2\ is\ not\ prime.$

$n = 3k + 2$ $then\ n+4 = 3(k+2)$ $and\ n+4\ is\ not\ prime.$)

(ii) p is a positive integer and $p, 2p+1$ and $4p+1$ are primes. Find p.

(Hints: $p = 3k,\ 3k+1,\ 3k+2$. For $p = 3k+1,\ 2p+1 = 2(3k+1)$ not prime and $p = 3k+2, 4p+1 = 3(4k+1)$ is not prime. Then only possibility is $p = 3k \Rightarrow k = 1$ $and\ hence\ p = 3$.)

(iii) If p and $p^2 + 8$ are both primes, then $p = 3$

(iv) If $p \ge q \ge 5$ and p, q are both primes, then $24|(p^2 - q^2)$

(Hints: Either $p, q = 3k+1, 3k+2$ or $p, q = 4k+1, 4k+3$ $forms$)

(v) If $2^n - 1$ is prime, then n is prime.

[Hints: if $n = pq$ $then$ $2^n - n = 2^{pq} - 1 = (2^p - 1)\left(2^{p(q-1)} + 2^{p(q-2)} + \dots \dots \dots + 2^p + 1\right)$]

(vi) if $2^n + 1$ is prime, then $n = 2^k$, k $positive\ integer$.

2.5.6. Fundamental Theorem of Arithmetic: Any integer $n(>1)$ is of the form

$n = p_1^{\alpha_1}, p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$ where p_i are distinct primes with $p_1 < p_2 < \ldots\ldots\ldots < p_k$ and exponents α_i's are positive.

The number of positive divisors of a positive integer n.

$n = p_1^{\alpha_1}, p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$. Then number of positive divisors of n is $(\alpha_1 + 1) \ldots\ldots (\alpha_k + 1)$

$\therefore d(n) = (\alpha_1 + 1), (\alpha_2 + 1) \ldots\ldots (\alpha_k + 1)$

Example (2.14): $d(48) = d(2^4 \cdot 3) = (4+1)(1+1) = 10$

Note – I: $d(n)$ is odd $\Leftrightarrow n$ is a perfect square.

Note – II: Square free divisors of $n = p_1^{\alpha_1}, p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$ is 2^k.

(Hints: Here $0 \leq \alpha_i \leq 1 \Rightarrow P(X), X = \{p_1, \ldots\ldots\ldots, p_k\}$ and so $|P(X)| = 2^k$)

Example (2.15):

(i) $n = 23146123 = 23 \times (1000)^2 + 146\,(1000) + 123$ is divisible by $7, 11, 13$.

Since, $123 - 146 + 23 = 0$ is divisible by $7, 11, 13$.

(ii) Find least positive remainder in 3^{36} (mod 77).

Ans: $3^4 \equiv 4 (mod\ 77) \Rightarrow 3^{12} \equiv 4^3 (mod\ 77) \equiv -13\ (mod\ 77) - a$

$\Rightarrow 3^{24} \equiv 169\ (mod\ 77) \equiv 15\ (mod\ 77) - b$

$\therefore (a \times b) \Rightarrow 3^{36} \equiv 15 \times (-13) (mod\ 77) \equiv 36 (mod\ 77)$.

(iii) Find the remainder when $1! + 2! + \ldots\ldots\ldots + 100!$ is divisible by 15.

Ans: Since, $5! \equiv 0\ (mod\ 15) \Rightarrow (5+n)! \equiv 0 (mod 15)$ for any $n(\geq 0)$ integer

$\therefore 1! + 2! + \ldots\ldots\ldots + 100! \equiv (1! + 2! + 3! + 4!)(mod\ 15) \equiv 33\ (mod\ 15) \equiv 3(mod 15)$

(iv) Prove that $3 \cdot 4^{n+1} \equiv 3\ (mod\ 9)$ for all positive integers n .

Ans:

$3 \cdot 4^{n+1} = 12 \cdot 4^n = (9+3)4^n = 9 \cdot 4^n + 3 \cdot 4^n$

$3 \cdot 4^n = 12 \cdot 4^{n-1} = (9+3)4^{n-1} = 9 \cdot 4^{n-1} + 3 \cdot 4^{n-1}$

$3 \cdot 4^2 = \qquad\qquad\qquad = 9 \cdot 4 + 3 \cdot 4$

$3 \cdot 4 = \ldots\ldots\ldots\ldots \ldots\ldots\ldots\ldots\ldots\ldots = 9 + 3$

$\therefore\ 3 \cdot 4^{n+1} = 9\,(1 + 4 + \ldots\ldots\ldots + 4^n) + 3$

$\Rightarrow 3 \cdot 4^{n+1} \equiv 3\ (mod\ 9)$

2.5.7. Congruence: Let m be a fixed positive integer. Two integers a and b are said to be congruent modulo m if $a - b$ is divisible by m. This is expressed as $a \equiv b(mod\ m)$.

2.5.8. Definition (Primitive Roots): A number m is called a primitive root modulo n if and only if every integer a such that $\gcd(a, n) = 1$, $\exists$ an integer K such that $m \equiv a(mod\ n)$. K is called the index of a to the base $m\ modulo\ n$.

Example (2.16): 2 is a primitive root mod 5, as every integer a relatively prime to 5, $\exists$ an integer K such that $2^k \equiv a\ (mod\ n)$. All the integers relatively prime to 5 are 1, 2, 3, 4 and each of these satisfies the equation $2^k \equiv a\ (mod\ 5)$.

Properties of congruence:

(i) $a \equiv a\ (mod\ m)$.

(ii) $a \equiv b\ (mod\ m) \Rightarrow b \equiv a\ (mod\ m)$

(iii) $a \equiv b\ (mod\ m), b \equiv c(mod\ m)\ then\ a \equiv c\ (mod\ m)$.

(iv) $a \equiv b(mod\ m)$ then for any integer c, $a + c \equiv b + c(mod\ m)$

$$ac \equiv bc\ (mod\ m)$$

(v) If $a \equiv b\ (mod\ m)\ and\ c \equiv d\ (mod\ m)\ \ then\ a + c \equiv b + d(mod\ m)$

$$ac \equiv bd\ (mod\ m)$$

(vi) If $a \equiv b\ (mod\ m)\ \ and\ \ d|m, d > 0, then\ a \equiv b\ (mod\ d)$.

(vii) If $a \equiv b\ (mod\ m)\ \ and\ a^n \equiv b^n(mod\ m)$ for all positive integers n.

Converse is not true e.g., $9^2 \equiv 7^2(mod\ 8)\ but\ 9 \not\equiv 7\ (mod\ 8)$

(viii) If $ax \equiv ay\ (mod\ m) and\ a$ is prime to m then $x = y\ (mod\ m)$

Note: $3 \cdot 2 \equiv 3 \cdot 4\ (mod\ 6)\ but\ 2 \not\equiv 4\ (mod\ 6)\ \ as\ \gcd(3,6) = 2 \neq 1$

(ix) If $d = \gcd(a, m)\ then\ ax \equiv ay\ (mod\ m) \Leftrightarrow x = y\ \left(mod\ \frac{m}{d}\right)$

$4 \cdot 7 \equiv 4 \cdot 10\ (mod\ 6) \Rightarrow 7 \equiv 10\ \left(mod\ \frac{6}{2}\right)$

(x) $x \equiv y\ (mod\ m_i)\ for\ i = 1, 2, \ldots\ldots, k \Leftrightarrow x \equiv y\ (mod\ m)\ where$

$m = lcm(m_1, m_2, \ldots\ldots, m_k)$.

(xi) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots\ldots + a_0$ be a polynomial with integral coefficient a_i, if $a \equiv b\ (mod\ m)\ \ then\ f(a) \equiv f(b)(mod\ m)$.

2.5.9. Divisibility Test:

Let $n = a_m 10^m + a_{m-1}10^{m-1} + \ldots.. + a_2 10^2 + a_1 10 + a_0$. Where $a_k \in \mathbb{Z}$ and $0 \le a_k \le 9 k = 0, 1, 2, \ldots \ldots . m$ be the decimal representation of a positive integer n.

Let $S = a_0 + a_1 + \ldots \ldots + a_m$ and $T = a_0 - a_1 + \ldots \ldots + (-1)^m a_m$. Then

(i) n is divisible by 2 $\Leftrightarrow$ a_0 is divisible by 2

(Hints:$10 \equiv 1(mod\ 2) \Rightarrow f(10) \equiv f(0)(mod\ 2)$

(ii) n is divisible by 9 $\Leftrightarrow$ S is divisible by 9

(Hints: $10 \equiv 1(mod\ 9) \Rightarrow f(10) \equiv f(1)(mod\ 9)$

(iii) n is divisible by 11 $\Leftrightarrow$ T is divisible by 11

(Hints: $10 \equiv -1(mod\ 11) \Rightarrow f(10) \equiv f(-1)(mod\ 11)$.

Example (2.17):

35078571 is divisible by 9 since $3 + 5 + 0 + 7 + 8 + 5 + 7 + 1 (= 36)$ is divisible by 9 and it is also divisible by 11 as $1 - 7 + 5 - 8 + 7 - 0 + 5 - 3 (= 0)$ is divisible by 11.

Let $n = a_m(1000)^m + a_{m-1}(1000)^{m-1} + \ldots \ldots + a_1(1000) + a_0$ where $a_k \in \mathbb{Z}$ and $0 \le a_k \le 999, k = 0, 1, \ldots., m$ be the representation of a positive integer n.

Let $T = a_0 - a_1 + \ldots \ldots + (-1)^m a_m$. Then –

(i) n is divisible by 7 $\Leftrightarrow$ T is divisible by 7

(ii) n is divisible by 13 $\Leftrightarrow$ T is divisible by 13

(iii) n is divisible by 11 $\Leftrightarrow$ T is divisible by 11

2.5.10. Chinese Remainder Theorem: Let $m_1, m_2, \ldots \ldots, m_k$ be positive integers such that $\gcd(m_i, m_j) = 1$ for $i \ne j$ *and* $m = m_1, m_2, \ldots \ldots, m_k$ and $c_1, c_2, \ldots \ldots, c_k$ be any integers. Then the system of linear congruence, $x \equiv c_1(mod\ m_1)$, $x \equiv c_2(mod\ m_2), \ldots \ldots, x \equiv c_k(mod\ k)$ has a simultaneous solution which is unique modulo m. [i.e., if x_0 be a solution then $x \equiv x_0(mod\ m)$ is also a solution]

Method:

$m = m_1, m_2, \ldots \ldots, m_k$, $M_i = \frac{m}{m_i}$, $i = 1, 2, \ldots \ldots, k$

$\gcd(M_i, m_i) = 1\ for\ \ i = 1, 2, \ldots \ldots, k$

$\Rightarrow M_i\, x \equiv 1\ (mod\ m_i)\ \ has\ unique\ solution\ \ x_i, i = 1,2, \ldots \ldots, k$

$\therefore$ Solution of the system is $x_0 = c_1 M_1\, x_1 + c_2 M_2 x_2 + \ldots \ldots . + c_k M_k\, x_k$

All solutions are $x \equiv x_0(mod\ m)$

Examples (2.18):

Find four consecutive integers divisible by 3, 4, 5, 7 respectively.

Let $x, x+1, x+2, x+3$ be the four consecutive integers.

Then $x \equiv 0\ (mod\ 3),\ x+1 \equiv 0\ (\ mod\ 4), x+2 \equiv\ 0\ (\ mod\ 5), x+3 \equiv 0\ (mod\ 7)$

i.e., $x \equiv 0\ (mod\ 3)\ , x \equiv 3\ (mod\ 4), x\ \equiv 3\ (mod\ 5)\ x\ \equiv 4\ (mod\ 7)$.

Here, $m = 3 \times 4 \times 5 \times 7 = 420$, $M_1 = \frac{m}{3} = 140$

$M_2 = \frac{m}{4} = 105$

$M_3 = \frac{m}{5} = 84$

$M_4 = \frac{m}{7}$

Since, $\gcd(3, M_1) = \gcd(3, 140) = 1$ then $M_1\ x = 1\ (mod\ 3)$ has unique solution $x_1 = 2$

$M_2\ x = 1\ (mod\ 4) i.e., 105\ x \equiv 1\ (mod\ 4)$ has unique solution $x_2 = 1$

$M_3\ x = 1\ (mod\ 5) i.e., 84\ x \equiv 1\ (mod\ 5)$ has unique solution $x_3 = 4$

$M_4\ x = 1\ (mod\ 7) i.e., 60\ x \equiv 1\ (mod\ 7)$ has unique solution $x_4 = 2$

$\therefore x_0 = \sum_{i=1}^{4} c_i M_i\ x_i = 0 \cdot 140 \cdot 2 + 3 \cdot 105 \cdot 1 + 3 \cdot 84 \cdot 1 + 4 \cdot 60 \cdot 2 = 1803$

$\therefore x\ \equiv\ 1803\ (mod\ 420)\ i.e., x\ \equiv 123\ (mod\ 420)$

$i.e., x = 123 + 420\ t\ ,\ \ t = 0, \pm 1, \pm 2, \ldots\ldots$

2.5.11. Definition (Polynomial Congruence):

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_0\ (x \geq 1)$ be a polynomial with integer co – efficient $a_0, a_1, \ldots\ldots, a_m$ with $a_0 \not\equiv 0 (mod\ m)$.

Then $f(x) \equiv 0 (mod\ m)$ is said to be a polynomial congruence $(mod\ m)$ of degree n.

If $\exists$ an integer x_0 such that $f(x) \equiv 0\ (mod\ m)$, then x_0 is said to be a solution of the congruence. If x_1 be such that $x_1\ \equiv\ x_0 (mod\ m)$. Then

$f(x_1) \equiv\ f(x_0)(mod\ m)\ \equiv 0 (mod\ m), \Rightarrow\ x_1$ is another solution.

Two solutions x_1 and x_2 of $f(x)\ \equiv 0 (mod\ m)$ are said to be distinct if $x_1 \not\equiv x_2\ (mod\ m)$.

Example (2.19):

(i) $x^2\ \equiv 1\ (mod\ 8) \rightarrow (i) x_0 = 1$ is a solution so $x\ \equiv x_0 (mod\ 8)$.

i.e., $x\ \equiv 1\ (mod\ 5)\ \ or,\ x =\ 8k + 1,\ k$ being integers are also solution. Also see that $x_1 = 3,\ x_2 = 5\ , x_3 = 7$ are also solution and $x_0\ , x_1\ , x_2, x_3$ are distinct $\Rightarrow$ The congruence may have more solutions than its degree.

(ii) $x^2\ \equiv 3\ (mod\ 5)$ has no solution.

2.5.12. Definition (Linear congruence): A polynomial congruence of degree 1 is said to be a linear congruence. It is of the form $ax \equiv b \ (mod\ m)$ where $a \not\equiv 0\ (mod\ m), m > 1$.

Results:

(I) If $\gcd(a, m) = 1,\ then\ ax \equiv b\ (mod\ m)$ has unique solution.

(II) If $\gcd(a, m) = d, then\ ax \equiv b\ (mod\ m)$ has no solution if d does not devide b and if d divides b, then $ax \equiv b\ (mod\ m)$ has d distinct (incongruent) solutions $(mod\ m)$ which are $x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots\ldots\ldots\ldots, x_0 + \frac{(d-1)m}{d}\ \ (mod\ m)$

Examples (2.20):

(i) $5x\ \equiv 3\ (mod\ 11),\ \ \gcd(5, 11) = 1\ \ divides\ 3$ it has unique solution.

$11 = 5 \times 2 + 1\ \Rightarrow 1 = 11 + 5\ (-2)\ \Rightarrow 3 = 11 \times 3\ \ 5\ (-6)$

$\therefore\ x_0 = -6$

$\therefore$ All solutions are $x \equiv -6\ (mod\ 11) \equiv 5\ (mod\ 11)$.

(ii) $15x\ \equiv 9\ (mod\ 18) \ldots . (*) \gcd(15, 18) = 3$ divides 9. So, it has 3 incongruent solutions.

$18 = 15 \times 1 + 3 \Rightarrow 9 = 15(-3) + 18 \times 3$

$\therefore\ \ x_0 = -3\ (mod\ 18)$

$\therefore$ Therefore, distinct solutions are $-3, -3 + \frac{18}{3}, -3 + 2 \times \frac{18}{3} (mod\ 18)$

i.e., $-3, 3, 9\ (mod\ 18)$.

Another Method:

$(*)$ is equivalent to $5x\ \equiv 3\ (mod\ 6)$ has unique solution as $\gcd(5,6) = 1$ and

$1 = 6 + 5(-1) \Rightarrow 3 = 6 \times 3 + 5\ (-3)\ \Rightarrow\ x_0 = -3$

(iii) Let $m_1, m_2, \ldots\ldots., m_k$ be positive integers and $a_1, a_2, \ldots\ldots., a_k$ be any integers. Then the system of linear congruences

$x \equiv\ a_1(mod\ m_1),\ x \equiv\ a_2(mod\ m_2), \ldots\ldots, x \equiv\ a_k(mod\ m_k)$

will have a simultaneous solution $\Leftrightarrow \gcd(m_i,\ m_j), (i \neq j)$ divides $(a_i - a_j)$ and if this condition be satisfied the solution is unique modulo $lcm(m_1, m_2, \ldots\ldots., m_k)$

Example (2.21): Solve the system of linear congruence

$x \equiv 11\ (mod\ 15), x\ \equiv 6\ (mod\ 35) \ldots\ldots\ldots\ldots. (i)$

Since, $\gcd(15, 35) = 5$ divides $(11 - 6) = 5$ so the system has a solution.

(i) is equivalent to $x\ \equiv 11(mod\ 3), x \equiv 6\ (mod\ 5), x\ \equiv 6\ (mod\ 7)$

Again, since $x\ \equiv 11(mod\ 5) \equiv 6\ (mod\ 5)$. So, the given system is equivalent to

$x\ \equiv 11(mod\ 3), x \equiv 6\ (mod\ 5), x\ \equiv 6\ (mod\ 7) \ldots\ldots\ldots\ldots. (ii)$

$i.e., x \equiv 2\ (mod\ 3), x\ \equiv 1\ (\ mod\ 5)\ , x\ \equiv 6\ (mod\ 7)$

Solve (ii) by previous method

$x = 2 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 1 + 6 \cdot 15 \cdot 1 = 251$

$\therefore x \equiv 251\ (mod\ 105) \equiv 41\ (mod\ 105)$

2.5.13. Definition (Phi function / Euler's Phi function): The function ϕ, called phi function, is defined for all positive integers by $\phi(1) = 1$ and for $x > 1, \phi(x) =$ the number of positive integers less than n and prime to x .

Properties of Phi function:

(i) $\phi(m_1, m_2, \ldots\ldots, m_k) = \phi(m)_1 \phi(m_2) \ldots\ldots \phi(m_k)$ where $\gcd(m_i, m_j) = 1, (i \neq j)$,

(ii) $\phi(p^k) = p^k \left(1 - \frac{1}{p}\right)$

(iii) $\phi(n) = \phi({p_1}^{\alpha_1}, {p_2}^{\alpha_2}, \ldots \ldots {p_k}^{\alpha_k}) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots\ldots \left(1 - \frac{1}{p_k}\right)$

(iv) If $n > 1$ the sum of all positive integers less than n and prime to n is $\frac{n}{2}\phi(n)$.

(v) For any positive integer $n, n = \sum_{d/n} \phi(d)$, where the summation extends over all positive divisors $d\ of\ n$.

(vi) If $n > 2$ the $\phi(n)$ is an even integer.

(vii) If n is odd integer, then $\phi(2n) = \phi(n)$ $(Hints: \phi(2n) = \phi(2)\phi(n) = \phi(n)$

(viii) If n is even integer, then $\phi(2n) = 2\,\phi(n)$.

(ix) $\phi(n^2) = n\phi(n)$ for any positive integer n.

(x) $\phi(n) = \frac{n}{2} \Leftrightarrow n = 2^k$

(xi) $\phi(m\,n) = \phi(m)\phi(n)\frac{\alpha}{\phi(d)}, d = \gcd(m, n)$

(xii) $\phi(m\,n) = \phi\ (\gcd(m, n)) \cdot \phi\ (lcm\ (m, n))$

2.5.14. Fermat's Theorem:

If P be a prime and $P \times a$, then $a^{P-1} \equiv 1\ (mod\ P) \Rightarrow a^{P^2 - P} = 1\ (mod\ P^2)$

2.5.15. Euler's Theorem: If n be a positive integer and $\frac{n}{a}$, then $a^{\phi(n)} \equiv 1\ (mod\ n)$.

(Note: If $n = P\ it\ is\ Fermat's\ theorem.$)

2.5.16. Wilson's Theorem: If P be a positive then $(P-1)! + 1 \equiv 0\ (mod\ P)$. The converse is also true.

Examples (2.22):

(i) Find the least positive variance in $2^{41}(mod\ 23)$

$\gcd(2,23)=1 \quad \therefore 2^{\phi(23)} \equiv 1\ (mod\ 23)$

$\Rightarrow 2^{22} \equiv 1\ (mod\ 23)$

$\Rightarrow\ 2^{49} \equiv 1\ (mod\ 23) \equiv 24\ (mod\ 23)$

$\Rightarrow\ 2^{41}\cdot 8 \equiv 3\cdot 8\ (mod\ 23)$

$\Rightarrow 2^{41} \equiv 3\ (mod\ 23)(\because \gcd(8,23)=1)$

(ii) If ϕ be $\ prime\ > 2$, then $1^p + 2^p + \cdots + (p-1)^p \equiv 0\ (mod\ p)$

By Fermat's theorem,

$1^p \equiv 1(mod\ p),\ 2^p \equiv 2\ (mod\ p), \ldots, (p-1)^p \equiv (p-1)(mod\ p)$

$1^p + 2^p + \cdots + (p-1)^p \equiv (1+2+\cdots+p-1)(mod\ p)\ \equiv \frac{p(p-1)}{2}(mod\ p)$

$\equiv 0\ (mod\ p) \quad (\because p-1\ is\ even)$

(iii) Find unit digit, in 3^{100} by Euler's theorem, $3^{\phi(10)} \equiv 1\ (mod\ 10)\ \ as \gcd(3,10)=1$

$\Rightarrow 3^4\ \equiv (mod\ 10)$

$\Rightarrow 3^{100}\ \equiv 1^{25}(mod\ 10)\ \equiv 1\ (mod\ 10)$

(iv) Show that $4(29)! + 5!$ is divisible by 31.

Since, 31 is prime, by Wilson's theorem,

$30! + 1\ \equiv 0\ (mod\ 31)$

$or,\ 30\cdot 20! + 1\ \equiv 0\ (mod\ 31)$

$or,\ (31-1)29! + 1\ \equiv 0\ (mod\ 31)$

$or,\ -29\,! + 1 \equiv 0\ \ (mod\ 31)$

$or, 29! - 1\ \equiv 0\ (mod\ 31)$

$or,\ 4\cdot 29! - 4\ \equiv 0\ (mod\ 31)$

$or,\ 4\cdot 29! + 5! \equiv (5! + 4)(mod\ 31)$

$or,\ 4\cdot 29! + 5! \equiv 124\ (mod\ 31) \equiv 0\ (mod\ 31)$

(v) If $2n+1$ is prime prove that $(n!)^2 \equiv (-1)^{n+1}\left(mod\ (2n+1)\right)$

By Wilson's theorem $(2n)! \equiv -1\ \left(mod\ (2n+1)\right)$

Now, $(2n)!\ \equiv n!\,(n+1+(n+2)\ldots\ldots(2n)$ and

$n+1\ \equiv\ -n\left(mod\ (2n+1)\right)$

$n+2\ \equiv\ -(n-1)\left(mod\ (2n+1)\right)$

.

.

.

.

$2n\ \equiv\ -1\ \left(mod\ (2n+1)\right)$

$\therefore (n+1)(n+2)\ldots\ldots 2n \equiv (-1)^n\, n!\left(mod\ (2n+1)\right)$

$\therefore (2n)! \equiv (-1)^n (n!)^2\left(mod\ (2n+2)\right)$

$or, (n!)\ \equiv (-1)^n (2n)!\left(mod\ (2n+1)\right)$

$\equiv (-1)^n(-1)\left(mod\ (2n+1)\right)$

$\equiv\ (-1)^{n+1}\left(mod\ (2n+1)\right)$

2.5.17. Definition (Greatest integer function):

$[x]$ is the greatest integer not greater than x.

Example (2.23): $[0.3] = 0, [3] = 3, [n] = 3$

Properties:

(I) $[a+b] \geq [a]+[b]\ \forall\ a,b \in \mathbb{R}\ \Rightarrow [a_1+a_2+\cdots+a_n] \geq [a_1]+[a_2]+\cdots+[a_n]$

(II) $[a]+[-a] = \begin{cases} 0, & if\ a\ is\ an\ integer. \\ -1, & Otherwise \end{cases}$

(III) $[a]+\left[a+\frac{1}{2}\right] = [2a]\ \ \forall\ a \in \mathbb{R}.$

(IV) f a is positive real number then $\left[\frac{a}{2}\right]+\left[\frac{a+1}{2}\right] = [a]$

2.6. Permutations and Combinations:

2.6.1. Definition (Permutation):

Given a certain number of things each of different arrangement that can be made out of them, taking some of them or all of them at a time, is called a permutation.

2.6.2. Definition (Combination): Given a certain number of things, each of the different groups or selections that can be formed out of them, by taking some of them or all of them at a time (ignoring the order of choice of the things in each group) is called a combination.

2.6.3. Pigeonhole Principle: Suppose that $n+1$ (or more) objects are put into n boxes. Then some box contains at least two objects.

Inclusion and Exclusion Principle: The inclusion-exclusion principle is a counting technique which generalizes the familiar method of obtaining the number of elements in the union of n number of finite sets. Mathematically,

$S = \left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n}|A_i| - \sum_{1\le i<j\le n}\left|A_i \cap A_j\right| +$

$\sum_{1\le i<j<k\le n}\left|A_i \cap A_j \cap A_k\right| - \ldots\ldots\ldots + (-1)^{n-1}|A_1 \cap A_2 \cap \ldots\ldots \cap A_n|$

4.6.4. The number of permutations of n different things, taken r at a time $(0 < r \le n)$ is

$^{n}P_r = \frac{n!}{(n-r)!}$

Cor: $n = r,$ the number of permutations of n different things taken all together is

$^{n}P_r = \frac{n!}{(n-r)!} = \frac{n!}{0!} = n!$

$^{n}P_r = {}^{n-1}P_r + r \cdot {}^{n-1}P_{r-1}$

Note – I: The number of permutations of n different things taken r at a time in which one particular thing is never occurs is given by $^{n-1}P_r$.

Note – II: The number of permutations of n different tings taken r at a time, in which one particular thing is bound to occur is given by $r \cdot {}^{n-1}P_{r-1}$

2.6.5. The number of permutations of $n = p_1 + p_2 + \cdots + p_k$things not all different is given by $\frac{n!}{p_1!p_2!\ldots p_k!}$

Example (2.24): The number of different ways the words of KOLKATA can be arranged is

$\frac{7!}{2!2!} = 1260\ (A = 2, K = 2)$

2.6.6. The number of permutations of n different things, taking r at a time, when each thing can be replaced once, twice, ……… up to r times, in any arrangement is n^r(i.e., r position can be filled by n thing with replacement).

Example (2.25):

How many numbers of two digits can be formed with the digits $1, 2, 3, 4$ when the digits may be replaced?

Ans: $4^2 = 16$

2.6.7. The number of permutations of n different things taken r at a time in which k particular things never occur is $^{n-k}P_r$ $where\ n - k \ge r.$

2.6.8. The number of permutations of n different things taken r at a times in which k particular things always occur is $^{n-k}P_{r-k}$ $where\ \ k \le r \le n.$

2.6.9. The number of permutations of n different things taken r at a time in which k particular things are placed in k given places

(i) in a definite order is ${}^{n-k}P_{r-k}$

(ii) in any order is $k!\ {}^{n-k}P_{-k}$

Example (2.26):

(i) How many numbers lying between 100 and 10,000 can be formed by 1, 2, 3, 4, 5?

Numbers must be either 3 digits of 4 digits

$\therefore\ {}^{5}P_{3} + {}^{5}P_{4} = 180$

(ii) How many odd number of six significant digits can be formed with the digits 0, 1, 4, 5, 6, 7 when no digits are repeated?

						1

…………5!………..

0						1

…………4!…………..

Ans. $3(5! - 4!) = 3 \times 96 = 288$

(iii) In how many ways 10 different examination papers be arranged so that

(a) The best and the worst always come together? (Answer: $2!\ 9!$)

(b) The best and the worst never come together?

(Answer: $10! - 2!\ 9!$)

(iv) In how many ways can the letters of the word 'BALLOON)' be arranged, so that the three vowels must not come together?

Total number of permutations $= \frac{7!}{2!2!} = 1260$ ($0 = 2, L = 2$).

Let $A, 0, 0$ treat as single digits, so three vowels come together is $\frac{3!}{2!} \times \frac{5!}{2!} = 180$ $\left(\because 0 = 2\ in \frac{A,o,o}{X^*}\ \ and\ X^*BLLN = 5\ and\ L = 2\right)$

$\therefore$ Result $1260 - 180 = 1080$

(v) Find the number of ways in which the letters of the word INTERMIDIATE can be arranged taken all at a time so that vowels are not all together?

$\frac{|2!}{3!2!2!} = Total\ permutations \quad (I = 3, T = 2, E = 2)$

Vowels together $\frac{7!}{2!} \times \frac{6!}{3!2!}$ $(take\ AEEIII = singel \frac{6!}{3!2!}\ and\ total\ number\ 7\ and\ T = 2 = \frac{7!}{2!}$

$\therefore$ Result $\left(\frac{|2!}{3!2!2!} - \frac{7!}{2!} \times \frac{6!}{3!\,2!}\right) = 19807200.$

(vi) Find the number of ways of arranging the letters AAAAABBBCCCDEEE in a row, so that the C's are separated from one another.

Total letters = 15 and 3 C's.

$\therefore$ remaining letters $= 12.$

i.e., $\frac{|2!}{5!2!2!}(A = 5, B = 3, E = 2)$

In between and two extremes there 13 places for the 12 letters and in these places 3 c's can be inserts in $\frac{13p_3}{3!}$ ways.

Hence the result $= \frac{|2!}{5!2!2!} \times \frac{13p_3}{3!}$

2.7. Binary Operation:

2.7.1. Definition: Let A be a nonempty set. A binary operation $* \ on\ A$ is a function from $A \times A \to A$.

Example (2.27): $(\mathbb{Z}, +), (\mathbb{N}, +), (\mathbb{R}, \cdot), (\mathbb{R}, +)$ not binary operation $(\mathbb{N}, -)$ since 1 – 2 = –1$\not\subset \mathbb{N}$.

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

$$M \equiv \begin{array}{c|ccc} * & 1 & \omega & \omega^2 \\ \hline 1 & 1 & \omega & \omega^2 \\ \omega & \omega & \omega^2 & 1 \\ \omega^2 & \omega^2 & 1 & \omega \end{array}$$

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

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

Example (2.28):

(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) $(\mathbb{Z},*), with\ a * b = a.$

2.7.4. (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 (2.29): $(\mathbb{Z}, -)$.

2.7.5. (Monoid): Semi group with identity.

Example (2.30): $(\mathbb{N}, +)$ is a semi group but not monoid and $(\mathbb{N} \cup \{0\}, +)$ is monoid.

2.7.6. (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 $a * x = \ b\ and\ y * a = b$ has a unique solution in G.

Example (2.31):

(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 (2.32): 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 $= 2^{\frac{n^2+n}{2}} = number\ of\ symmetric\ realtion.$

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

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

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

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

Example (2.33):

(i). $(\mathbb{Z}_n, +) = \{\bar{0}, \bar{1}, \dots \dots \dots, \overline{n-1}, +\}, \forall\ \bar{a}, b \in \mathbb{Z}_n,\ a + \ = a + b$ 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). $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}\, b : a\ .\ b \in \mathbb{Q}\}\ Then(\mathbb{Q}[\sqrt{2}], +)\ and\ (\ \mathbb{Q}[\sqrt{2}]|\{\bar{0}\},\ \cdot)$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 $G = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0\}$ and $*$ is the matrix multiplication. Then $GL(2, \mathbb{R})$ is a $SL(2, \mathbb{R}) = \left(\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1\right\}, *\right)$

2.8.4. (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 $x\ and\ y.$

2.8.5. (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.

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

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

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

2.8.7. (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 $S\ for\ x\ and\ y.$

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

$*$ Finite is necessary.

Example (2.34): $(\mathbb{Z}\{0\},\ \cdot)$ is a semi group and satisfies cancellation laws but inverse of an element $1 \neq a \in \mathbb{Z}\{0\}$ does not exist.

2.8.9. 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.

2.8.10. (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 (2.35): 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.

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

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

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

2.8.14. 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 (2.17): $(S_3, 0)$, S_n symmetric group and $|S_n| = n!$

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

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

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

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

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

2.8.19. (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 $length \geq 2$.

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

Example (2.36):

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 6 & 3 & 7 & 4 & 2 & 1 \end{pmatrix} = (1 \quad 8)(2 \quad 5 \quad 7)(3 \quad 6 \quad 4)$$

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

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

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

2.8.22. (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 $O(\sigma_i) = n_i, i = 1,2, \ldots \ldots, k.\ Then\ O(\sigma) = lcm(n_1, n_1 \ldots \ldots, n_k)$

Example (2.37):

(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.

2.9. 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 (2.38): $(E,+)\ of\ (\mathbb{Z},+)\ where\ E = \{2x : x \in \mathbb{Z}\}$.

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

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

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

2.9.4. (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 (2.39): Consider $G = S_3\ and\ H = \{e, (2,3)\}\ and\ K = \{e, (1,2)\}$

Then H, K are two subgroup of S_3. Now, $H \cup K = \{e, (1 \quad 2), (2 \quad 3)\}$ is not a group. Since

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

2.9.5. (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 $\frac{n!}{r \times (n-r)!}$

2.9.6. 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* $(1 \quad 3)(1 \quad 2) = (1 \quad 2 \quad 3) \in H_k$

2.9.7. (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.

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

2.9.9. (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 $T_n = \{r_n : r \in \mathbb{Z}\}, n \in \mathbb{N}_0$

2.10. (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 (2.40):

(i). $G = \{1, -1, i, -i\}, G = < i > = < -i >$

(ii). $(\mathbb{Z}, +) = (< 1 >, +)$

(iii). $(\{2n : n \in \mathbb{Z}\}, +) = (< 2 >, +)$

(iv). $(\mathbb{Z}, +) = \{[1], +\}$

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

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

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

2.10.4. (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* $G \Leftrightarrow \gcd(n, k) = 1$

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

2.10.6. (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 ∃ 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) G has only two generators.

2.11. 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 H in 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.

- $aH \neq Ha$ always.

Example (2.41): $H = \{e, (1\quad 2)\}$ 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.$(2\quad 3)H \neq H(2\quad 3)$

2.11.1. (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 $aH \cap bH = \phi\ or\ aH = bH\ (iii*) Either\ Ha \cap Hb = \phi\ or\ Ha = Hb$

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

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

2.11.3. (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 H in G.

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

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

2.11.10. (Corollary):

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

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

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

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

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

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

Converse of Lagrange's Theorem not true:

Example (2.41) 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.

2.12. Normal Subgroups and Quotient Groups:

2.12.1. 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.

2.12.2. 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). $gHg^{-1} = H \quad \forall\ g \in G$

2.12.3. 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 of 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.

2.12.4. 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.

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

2.13. Homomorphisms of Groups:

2.13.1. 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 (2.42):

(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: $f : G\lfloor(2, \mathbb{R}) \to \mathbb{R}^*$by $f(A) = detA\ \ \ \forall\, A \in G\lfloor(2, \mathbb{R}).$

Note: $\left|G\lfloor(n, F_p)\right| =\ (p^n - p^0)(p^n - p^1) \ldots\ldots\ldots\ (p^n - p^{n-1})\ and\ \left|S\lfloor(n, F_p)\right| = \frac{|G\lfloor(n,F_p)|}{p-1}$

2.13.2. (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). $f(a^n) = f(a)^n\ \ \forall\ a \in G\ and\ \forall\ \ x \in \mathbb{Z}.$

2.13.3. (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 $f(H) = \{f(h) : h \in H\}\ in\ subgroup\ o\ f\ \ G_1.$

(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 (2.43): (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 $\mathbb{Z}_3$.

2.13.4. (Kernel): Let $f : G \to G_1$be a homomorphism. The Kernel of f is defined by $Ker\ f = \{x \in G : f(x) = e_1\}$.

2.13.5. (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) $\Leftrightarrow\ kerf = \{e\}$.

2.13.6. (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 $i_b\ G > \langle a \rangle, then\ G_1 = \langle f(a) \rangle$.

2.13.7. (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 ∃ an isomorphism $f : G \to G_1$. In this case we write $G \simeq G_1$.

Example (2.44):

(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). $I : G \to G\ by\ I(x) = x\ \forall\ x \in G$.

2.13.8. (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 (2.45): 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 (2.46): $\mathbb{Z}_4$ cyclic and k_4 is non-cyclic.

IV. Two groups of infinite order and commutative may not be isomorphic.

Example (2.47): $(\mathbb{Z}, +)$ cyclic and $(\mathbb{Q}, +)$ non cyclic.

V. Two groups of infinite order, non-cyclic and commutative may not be isomorphic.

Example (2.48): $(\mathbb{R}^*, \cdot)$ has number of element of order 4 but $(\mathbb{C}^*, \cdot)$ has i of order 4.

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

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

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

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

Example (2.49):

(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 $f(m) = nm = f_n(m) \Rightarrow f \equiv f_n, n = 1, \pm 1, \pm 2, \ldots \ldots$

(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. δ 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.

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

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

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

Example (2.50):

(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). $U(m) = U(n_1) \oplus\ U(n_2) \oplus \ldots\ldots\ldots \oplus U(n_k)\ where\ m =\ n_1, n_2, \ldots.\ ..n_k$ $and\ \ gc\,d(n_i, n_j) = 1, i \neq j$.

(v). Consider S_3, its normal sub groups are $\{e\}, S_3, A_3$. Hence all homomorphic images of S_3 are $S_3|S_3,\quad S_3|\{e\} = S_3,\ S_3|A_3 = \mathbb{Z}_2$.

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

2.13.16. 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 (2.51):

- 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 $\mathbb{Z}|n\mathbb{Z} \simeq \mathbb{Z}n, n = 0,1,2, \ldots..$

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.

2.14. Direct Product of Groups:

Theorem: Let G and G be two groups. Then the set $G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1 \; and \; g_2 \in G_2\}$
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). $G_1 \times G_2 = H_1H_2 = H_2H_1, \; H_1 \cap H_2 = \{(e_1, e_2)\}$

2.14.1. Definition (Direct Product of groups):

The group $(G_1 \times G_2, *)$ of the above theorem is called the direct products of the groups$G_1 and \; G_2$ $(or \; external \; direct \; product \; of \; the \; groups \; G_1 and \; G_2)$.

2.14.2. 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) $hk = kh \; \forall \; h \in H \; and \; k \in K$

Example (2.52): $k_4 = \{e, a, b, ab\}, H_1 = \{e, a\}, H_2 = \{e, b\}, -$

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

2.14.3. (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). $H \cap k = \{e\}$.

2.14.4. (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). $G|H \simeq K \; and \; G|K \simeq H$

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

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

2.14.7. (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 (2.53): 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 and H_m take direct product to $\mathbb{Z}_r$. This $G \simeq H \times \mathbb{Z}_r\ and\ |G| = n$.

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

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

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

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 $G = \cup_{i=1}^{k} cl(a_i)$.

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

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

Example (2.54): $S_3, cl(e) = \{e\}, cl(1\quad 2) = \{(1\quad 2), (1\quad 3), (2\quad 3)\}$

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

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

2.14.9. 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 $\mathbb{Z}(G) \subseteq C(a)$.

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

2.14.11. (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.

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

2.14.13. Theorem (Cauchy): Let G be a finite group and $p\big||G|$. 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.

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

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

2.14.14. (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.

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

2.14.16. 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 $p - subgroup$.

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

2.14.18. 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 $k_p + 1\ (k \geq 0)\ and\ n_p\big||G|$.

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

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 (2.55):

(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 of order 7 and G has Sylow 7 – subgroup H. Now, $n_7 = 7k + 1\ (k \geq 0) and\ n_7 | 14 \Rightarrow n_7 = 1.$ 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 $p^n (p - prime)\ and\ n \in \mathbb{Z}, n \geq 1$. 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.

2.15. Simple Groups:

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

2.15.2. Theorem: A commutative group G is simple ⇔ $G \simeq \mathbb{Z}_p$ 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. ∴ 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.

2.16. Rings:

2.16.1. 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 (2.56):

(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 $(f \circ g)(x) = f\big(g(x)\big) \ \forall \ f, g \in R$ *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.

2.16.2. 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) $(a + b)^2 = a^2 + ab + ba + b^2$

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

2.16.4. (**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 (2.57): See example (viii) of (4.56) .

2.16.5. 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.

2.16.6. (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 (2.58):

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

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

2.16.7. (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.

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

2.16.9. (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 (2.59):

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

2.16.10. (Cancellation Law): A ring R is said to satisfy left (right) cancellation property if $\forall\ \ a, b, c \in R,\ \ a \neq 0\ \ and\ \ ab = ac\ [represent\ \ ba = ca]\ \Rightarrow b = c$

2.16.11. 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.

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

Examples (2.60):

- **(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 $(0, b) \cdot (a, 0) = (0,0)$.

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

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

2.16.15. (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 (2.61):$R = \{\left(\frac{\alpha}{\beta}, \frac{\beta}{\alpha}\right) \in M_2(\mathbb{C}): \bar{\alpha}, \bar{\beta}\ are\ conjugate\ of\ \alpha, \beta$

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

Examples (2.62): $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$

2.16.17. Theorem: Any field is an integral domain.

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

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

2.16.20. (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 (2.63)

(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.

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

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

2.17. 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 (2.64.):

(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) Let R_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 $\mathbb{C}$.

2.17.1. 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 $a, b \in S \Rightarrow a - b, ab \in S$.

2.17.2. 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 $\mathbb{Z}$.

2.17.3. (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*.

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

2.17.5. (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 (2.65):

(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. $A = \{\alpha \in \mathbb{C} :\ a_0 + a_1\alpha + a_2\alpha^2 \ldots\ldots\ldots\ldots + a_n\alpha^n = 0, a_i \in \mathbb{Q},\ n \in \mathbb{N}_0\}$

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

2.17.6. 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. $ab^{-1} \in S\ \forall\, a \in S, b \in S\ |\{0\}$.

2.17.7. Theorem: Let $\{S_\alpha : \alpha \in \wedge\}$ be a collection of subfield of a field F. Then $S = \bigcap_{\alpha \in \wedge} S_\alpha$ 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 $\mathbb{R}$.

2.18. (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 (2.66):

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.

2.18.1. Theorem: Let $\{I_\alpha\ : \alpha \in \wedge\}$ be a collection of left [right ideal] of a ring R.

Then $I = \bigcap_{\alpha \in \wedge} I_\alpha$ 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* $\mathbb{Z}$ ($As\ 2\mathbb{Z} \cup 3\mathbb{Z}\ is\ a\ subring\ of\ \mathbb{Z}.$).

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

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

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

2.18.3. 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 $I \cup J$.

2.18.4. 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 –

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

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

2.18.6. (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 (2.67):

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

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

Example (4.68): (i) $\mathbb{Z}_p$ (ii) $M_2(\mathbb{R})$ (iii) Any field.

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

2.20. (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 (2.69): 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.

2.20.1. 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.

2.21. (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 (2.70):

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

2.21.1. (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 (2.71): Find all homomorphism from the ring $\mathbb{Z}\ onto\ \mathbb{Z}.$

Answer: Only one which is identity homomorphism.

2.21.2. (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 (2.72):

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 $F.$

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

2.21.4. 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.

2.21.5. (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 $A, B\ in\ R, AB \subseteq P\ \ \Rightarrow A \subseteq P\ or\ B \subseteq P.$

2.21.6. 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 (2.73): $P\mathbb{Z}$ of $\mathbb{Z}$. Let $a, b \in R$ such that $ab \in P\mathbb{Z} \Rightarrow P(ab) \Rightarrow$
$either\ P|a\ or\ P|b\ as\ P\ is\ prime.$

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

2.21.8. 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 $\mathbb{Z}$.

2.21.9. Theorem:

i). In a Boolean ring B with identity, every prime ideal is a maximal ideal. $\Rightarrow$ prime ideal $\Leftrightarrow$ 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 (2.74):

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 (2.19.9) 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.

2.22. 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.

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

2.22.2. Theorem (Division Algorithm): Let F be a field and let $f(x), g(x), \in F(x)$ with $g(x) \neq 0$. Then $\exists$ unique polynomials $q(x) and \ r(x)$ in $F[x]$ such that

$f(x) = g(x)q(x) + r(x), r(x) = 0 \ or \deg r(x) < \deg g(x)$.

2.22.3. 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 $f(x) \ by \ \ x - a$.

2.22.4. 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 $f(x)$.

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

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

Example (2.75): 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 $\mathbb{R}[x] | \langle x^2 + 1 \rangle \simeq \mathbb{C}$.

2.22.7. (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 (2.76):

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 $\mathbb{Z}_5$, $x^2 + 1 = x^2 + 1 + (-5) = x^2 - 4 = (x - 2)(x + 2) = (x - 2 + 5)(x + 2) = (x + 3)(x + 2)$).

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

2.22.9. (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.

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

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

Example (2.77):

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

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

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

2.22.12. 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 $f(x)$ modulo P. If $f^2(x)$ is irreducible over $\mathbb{Z}_p$ and $deg\ f^2(x) = deg\ f(x), then\ f(x)$ is irreducible over $\mathbb{Q}$.

Example (2.78): Let $f(x)21x^3 - 3x^2 + 2x + 9$. Then over Z_2. Thus $f(x)$ is irreducible over $\mathbb{Q}$ *and hence over* $\mathbb{Z}$.

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

Example (4.79): $3x^5 + 15\,x^4 - 20\,x^3 + 10\,x + 20 \in \mathbb{Z}(x), p = 5$. $f(x)$ is irreducible over $\mathbb{Q}$.

2.22.14. Corollary: For any prime P, *the* P^{th} cyclotomic polynomial

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

2.22.15. 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.

2.22.16. 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.

2.22.17. 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* $p(x)|b(x)$.

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

$f(x) = b_1 b_2 \ldots\ldots\ldots b_s p_1(x) \ldots\ldots\ldots\ldots\ldots\ldots p_m(x) = c_1 c_2 \ldots\ldots\ldots c_t q_1(x) \ldots\ldots\ldots\ldots\ldots\ldots q_n(x)$

where $b'sadn\ c's$ 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* $b_i = \pm\, c_i,\ p_i(x) = \pm\, q_i(x)$.

2.23. 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* $a|c$.

2.23.1. Theorem (Prime ⇒ Irreducible in ID):

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

Example (2.80):

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

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

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

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

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

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

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

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

2.23.2. (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.

2.23.3. 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.

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

2.23.5. Definition (Euclidean Domain): An integral domain D is called a Euclidean domain (ED) if $\exists$ 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 (2.81.):

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 $N\big(f(x)\big) = degf(x) \Rightarrow F[x]$ 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	×	×	×	×	×

2.24. (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 $\mathbb{Q}$.

2.24.1. 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 (2.82): 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 (2.83): 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.

2.24.2. (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 (2.84): 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 $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

2.24.3. 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 (2.85):

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 $\{e\}, \{b, ba, \dots\dots, ba^{2n}\}, \{a^r, a^{-r}\}, 1 \le r \le n$.

iii. Conjugate classes in

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

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

Example (2.86):

A. Dihedral group of degree 4 (D_4) :

$D_4 = \langle a, b\rangle, a, b$ 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 in D_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)

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

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

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

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 $\{e\}, A_5, S_5$ ($Note\ A_5\ is\ simple.$

Example (2.87):

2.24.4. Some results on Finite Fields:

1. For each prime p and each positive integer n there is, upto isomorphism, a unique finite field of order P^n. This is denboted by $GF(P^n)$, in honor of Galois, and call it the Galois field of order P^n.
2. **Structure of finite fields:** As a group under addition $GF(P^n)$ is isomorphic to $Z_P \oplus Z_P \oplus \ldots.. \oplus Z_P$ (n times). As a group under multiplication, the set of non-zero elements of $GF(P^n)$ is isomorphic to Z_{P^n-1} (and is, therefore, cyclic).
3. $[GF(P^n): GF(P)] = n$.
4. **Subfields of a Finite field:** For each divisor m of $n, GF(P^n)$ has unique subfield of order P^m. Moreover, these are the only subfields of $GF(P^n)$.
5. If m divides n, then $[F(P^n): GF(P^m)] = \frac{n}{m}$.

Note: Let K be a finite extension field of the field E and E be a finite extension field of the field F. Then K is a finite extension field of F and $[K:F] = [K:E] \times [E:F]$

Example (2.88): $[Q(\sqrt{2},\sqrt{3}):Q] = [Q(\sqrt{2},\sqrt{3}):Q(\sqrt{3})] \times [Q(\sqrt{3}):Q] = 2 \times 2 = 4$

2.25. Galois Theory

2.25.1. Definition (Automorphism, Galois Group, Fixed Field of H)

Let E be an extension field of the field F. An automorphism of E is a ring isomorphism from E ontu E. The Galois group of E over $F, Gal(E/F)$, is the set of all automorphisms od E that take every element of F to itself. If H is subgroup of $Gal(E/F)$, the set

$E_H = \{x \in E: \phi(x) = x \; \forall \; \phi \in H\}$ is called the fixed field of H.

Example (2.89):

Let us consider the extension field $Q(\sqrt{2})$ of Q. Since $Q(\sqrt{2}) = \{a + b\sqrt{2}: a, b \in \mathbb{Q}\}$

Any automorphism of a field containing Q mum act as the identity an Q. An automorphism ϕ of $Q(\sqrt{2})$ is completely determined by $\phi(\sqrt{2})$.

Therefore, $2 = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = \left(\phi(\sqrt{2})\right)^2$

$$\Rightarrow \phi(\sqrt{2}) = \pm\sqrt{2}$$

This shows that the group $Gal\left(\phi(\sqrt{2})/\mathbb{Q}\right)$ has two elements, the identity mapping and the mapping that sends $a + b\sqrt{2}$ to $a - b\sqrt{2}$

2.25.2. Fundamental Theorem of Galois Theory

Let F be a field of characteristic 0 or a finite field. If E be the splitting field over F for some polynomial in $F[x]$, then the mapping from the set of subfields of $Gal(E/F)$ given by $G \to Gal(E/G)$ is a one-one correspondence. Also, for any subfield G of E containing F,

- **i.** $[E:G] = |Gal(E/G)|$ and $[G:F] = |Gal(E/F)|/|Gal(E/G)|$ that is the index of $Gal(E/G)$ in $Gal(E/F)$ equal to the degree of G over F.
- **ii.** If G is the splitting field of some polynomial in $F[x]$, then $Gal(E/G)$ is a normal subgroup of $Gal(E/F)$ and $Gal(E/F)$ is isomorphic to $Gal(E/F)/Gal(E/G)$.
- **iii.** $G = E\, Gal(E/G)$ that is the fixed field of $Gal(E/G)$ is G.
- **iv.** If H is a subgroup of $Gal(E/F)$, then $H = Gal(E/E_H)$ is the automorphism group of e fixing E_H is H.

2.25.3. Definition (Solvable by Radicals)

Let f be a filed and $f(x) = F[x]$. We say that $f(x)$ is solvable by radicals over F if $f(x)$ splits in some extension $F(a_1, a_2, \ldots, a_n)$ of F and $\exists$ positive integers $m_1, m_2, \ldots, m_n$ such that $a_1{}^{m_1} \in F \text{ and } a_i{}^{m_i} \in F\ (a_1, a_2, \ldots, a_{i-1})$ for $i = 2,3,4, \ldots, n$.

Example (2.90):

Let $\alpha = \cos\left(\frac{2\pi}{8}\right) + i \sin\left(\frac{2\pi}{8}\right) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$

Thus $x^8 - 3$ splits in $Q\left(\alpha, \sqrt[\delta]{3}\right), \alpha^8 \in \mathbb{Q}$ and $\left(\sqrt[\delta]{3}\right)^8 \in \mathbb{Q}\ CQ(\alpha)$. Hence, $x^8 - 3$ is solvable by radicals over $\mathbb{Q}$. The zero of $x^8 - 3$ can be written as $\sqrt[\delta]{3}, \sqrt[\delta]{3}\alpha, \sqrt[\delta]{3}\alpha^2, \ldots, \sqrt[\delta]{3}\alpha^7$, the notion of solvable by radicals is best illustrated by writing them in the following form $\pm\sqrt[\delta]{3}$, $\pm\sqrt{-1}\sqrt[\delta]{3}$, $\pm\sqrt[\delta]{3}\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{-1}\sqrt{2}}{2}\right)$, $\pm\sqrt[\delta]{3}\left(\frac{\sqrt{2}}{2} - \frac{\sqrt{-1}\sqrt{2}}{2}\right)$

2.25.4. Definition (Solvable Group)

We say that a group G is solvable if G has a series of subgroups

$\{e\} = H_0 C H_1\ C H_2\ C \ldots . . C H_K = G$

Where for each $0 \leq i < k, H_i$ is normal in H_{i+1} and $\frac{H_{i+1}}{H_i}$ is abelian.

2.25.5. Splitting field of $x^n - a$

Let F be a field of characteristic 0 and let $a \epsilon F$. If E is the splitting field of $x^n - a$ over F, then the Galois group $Gal(E/F)$ is solvable.

i. **Theorem:** A factor group of a solvable group is solvable.

ii. **Theorem:** Let N be a normal subgroup of a group G. If both N and G/N are solvable, then G is solvable.

Theorem: Let F be a field of characteristic O and let $f(x) \in F[x]$. Also, let $f(x)$ splits in $F(a_1, a_2, \ldots, a_n)$, where $a_1^{n_1} \in F$ and $a_1^{ni} \in F(a_1, a_2, \ldots, a_{i-1})$ for $f(x)$ over F in $F(a_1, a_2, \ldots, a_K)$ the