Unit VI

6 Algebraic Structures

6.1 : Algebraic Structure

Q.1 Define binary operation. ☞[SPPU : Dec.-05]

Ans. : Binary operation : I) Let A be any non empty set. A function $f : A \times A \to A$ is called the binary operation on the set A.

'$*$' is a binary operation on the set A iff $a * b \in A \ \forall \ a, b \in A$ and $a * b$ is unique.

II) An n-ary operation on a set $A \neq \phi$,
is a function $f : A \times A \times \ldots \times A$ (n times) $\to A$ i.e. $f : A^n \to A$

The n-ary operation is defined for each n-tuple $(a_1, a_2, \ldots a_n) \in A$ for $a_2 \in A$

If n = 1 then f is called unary operation

If n = 2 then f is called binary operation

If n = 3 then f is called ternary operation

Examples

1) A function $f : \Re \to \Re$ such that $f(x) = x \ ; \ \forall x \in \Re$ then f is a unary operation.
2) A function $f : \Re \times \Re \to R$ such that $f(x, y) = x + y$ then f is a binary operation.
3) A function $f : Z \times Z \times Z \to Z$ such that $f(x, y, z) = x + y + z$. then f is a ternary operation.

Properties of binary operations

I) Commutative property

A binary operation '$*$' on A is said to be commutative if $a * b = b * a$, for all $a, b \in A$. e.g. $x + y = y + x$ and $x \times y = y \times x$ for all $x, y \in \Re$

∴ '+' and '×' are commutative binary operations on $\Re$

But '–' is not commutative on $\Re$

II) Associative property :

A binary operation '*' on set A is said to be associative if
$a*(b*c) = (a*b)*c$; $\forall$ a, b, c $\in$ A

e.g. '+' and '×' are associative on the set of real numbers '–' is not associative on $\Re$

III) Idempotent

A binary operation '*' on set A is said to be idempotent if $a*a = a$; for all $a \in A$

e.g.

1) 1 is idempotent element in $\Re$ w.r.t. binary operation 'X'.

2) 0 is idempotent element in $\Re$ w.r.t. '+'.

3) 1 is not idempotent element in $\Re$ w.r.t. '+'.

Q.2 For each of the following, determine whether * is a binary operation.

i) R is the set of real numbers and $a * b$ = ab

ii) z^+ is the set of positive integers and $a * b$ = a/b.

iii) On z^+ where $a * b$ = a – b. iv) On R, where $a * b$ = min {a, b}

v) On R, where $a * b = a \times |b|$ vi) On z, where $a * b = a^b$.

Ans. : i) Yes, since $f : R^2 \rightarrow R$ defined as f(a, b) = ab is a function, with $ab \in R$

ii) No, since $(a,b) \in z^+ \times z^+$ does not imply that $a*b = a/b \in z$

$(1, 2) \in z^+ \times z^+$, but $1/2 \notin z^+$

iii) No, since $(1, 2) \in z^+ \times z^+$ but

iv) Yes, since, * is a function with min {a, b} $\in$ R

v) Yes, since * is a function with $a \times |b| \in R$

vi) No, since $2*(-1) = 2^{-1} = \frac{1}{2} \notin z$

Q.3 Determine whether or not following operations on the set of integers Z are associative. i) Division ii) Exponentiation

☞[SPPU : Dec.-05, Marks 3]

Ans. : i) Division on the set of integers is not associative as

$(a/b)/c \neq a/(b/c)$

ii) Exponentiation on the set of integers is not associative as

$(a^b)^c \neq a^{(b^c)}$

Q.4 Consider the binary operation * defined on the set A = {a, b, c, d} by the following table.

*	A	b	c	d
a	a	c	b	d
b	d	a	b	c
c	c	d	a	a
d	d	b	a	c

Find i) $c*d$ **and** $d*c$ **ii)** $b*d$ **and** $d*b$
iii) $a*(b*c)$ **and** $(a*b)*c$ **iv) Is * commutative, associative ?**

Ans. :

i) $c*d = a$ $\quad d*c = a$

ii) $b*d = c$ $\quad d*b = b$

iii) $b*c = b$ $\quad a*(b*c) = a*b = c$

$a*b = c$ $\quad$ Hence $(a*b)*c = c*c = a$

iv) * is not commutative, since $b*d \neq d*b$

* is also not associative, since $a*(b*c) \neq (a*b)*c$

Q.5 Define groupoid, semigroup, monoid with examples.

[SPPU : Dec.-06, 13]

Ans. : 1. Groupoid : A non empty set k with binary operation '*' is called groupoid if the binary operation '*' satisfies $\forall a, b \in G, a*b \in G$
In other words, every algebraic structure is groupoid.

e.g. $(\Re, +)$, $(\Re, -)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \times)$ are groupoids.

2. Semigroup : A non empty set G with binary operation '*' is called a semigroup if it satisfies the following properties.

$a*(b*c) = (a*b)*c$; $\forall a, b, c \in G$

i.e. '*' is associative in G

A semigroup is said to be commutative if $*$ is commutative.

e.g. i) $(\Re, +)$, $(N, +)$, $(Z, +)$ are commutative semigroups.

ii) $(\Re, \times)$, $(Z, \times)$ are commutative semigroups.

iii) $(Z, -)$ is not a semigroup as '–' is not associative.

3. Monoid

Let G be a non empty set and $*$ be a binary operation on G. $(G, *)$ is called monoid if.

i) Associative property : $a*(b*c) = (a*b)*c$; $\forall a, b, c \in G$

ii) Existence of identity : $\exists$ an element $e \in G$ such that $e*a = a*e = a$; $\forall a \in G$

The element 'e' is called the identity element.

e.g. 1) $(\Re, +)$ is a monoid as $a+b \in \Re$, $\forall a, b \in \Re$

i.e. $(\Re, +)$ is closed

and $a + (b + c) = (a + b) + c$

and $0 + a = a + 0 = a$, $\forall a \in \Re$

0 is the identity element in $\Re$ w.r.t. '+'.

Example 1 : $(C, +)$, $(C, \times)$, $(Z, +)$, $(Z, \times)$, $(Q, +)$ are monoids.

Example 2 : $(N, \times)$ is a monoid but $(N, +)$ is not monoid as $0 \notin N$

Q.6 Show that the algebraic system (A, +) is a monoid, where A is the set of integers and '+' is a binary operation giving addition of two integers. ☞**[SPPU : Dec.-06, Marks 4]**

Ans. : Let A be the set of all integers and '+' defined on A.

i) Closure property : $a+b \in A$; $\forall a, b, \in A$ as a + b is an integer.

ii) Associative property :

$a + (b + c) = (a + b) + c$; $\forall a, b, c \in A$

iii) Existence of identity element :

For any $a \in A$, $\exists\ 0 \in A$ such that

$a + 0 = 0 + a = a$

Therefore (A, +) is a monoid.

6.2 : Group and Abelian Group

Q.7 Define group and abelian group.

☞[SPPU : Dec.-08,09,10,12, May-14, Marks 4]

Ans. : Let G be a non empty set equipped with a binary operation '$*$'. $(G, *)$ is called a group if it satisfies the following postulates or axioms.

i) Associativity : $a*(b*c) = (a*b)*c$; $\forall$ a, b, c $\in$ G

ii) Existence of the identity : For any $a \in G$, $\exists\ e \in G$

s.t. $a*e = e*a = a$;

An element e is called the identity element in $(G, *)$

iii) Existence of the inverse :

For all $a \in G$, $\exists\ b \in G$ such that

$$a*b = b*a = e$$

Then b is called the inverse of a in $(G, *)$

$\therefore$ $b = a^{-1}$

Abelian Group or Commutative Group :

A group $(G, *)$ is called an Abelian group if

$$a*b = b*a \quad ; \quad \forall\ a, b \in G.$$

i.e. $*$ is commutative in $(G, *)$

Q.8 Explain properties of group with proof.

☞[SPPU : Dec.10, Marks 2]

Ans. : I) The identity element in a group is unique.

Proof : Suppose e_1 and e_2 are two identity elements in group G.

We have, $e_1 e_2 = e_1$; if e_2 is identity element in G.

and $e_1 e_2 = e_2$; If e_1 is identity element in G.

$\Rightarrow$ $e_1 e_2 = e_1 = e_2$. Hence the identity element in group G is unique.

II) The inverse of each element in group G is unique.

☞[SPPU : Dec.-10, Marks 4]

Let a be any element of a group G and let e be identity element in group G.

Suppose b and c are two inverses of a in G.

$\therefore$ $ba = ab = e$ and $ac = ca = e$

We have, $b = be = b(ac)$

$b = (ba)\, c$

$b = ec$

$b = c$

Hence, the inverse of each element is unique.

III)The inverse of an inverse of the element is the original element. i.e. If the inverse of a is a^{-1} then $(a^{-1})^{-1} = a$.

Proof : Let $e \in G$ be the identity element of the group G.

Let $a \in G$.

We have, $a^{-1}a = e$

$[(a^{-1})^{-1}(a^{-1}]a = (a^{-1})^{-1} e$ ... (Multiplying by $(a^{-1})^{-1}$)

$[(a^{-1})^{-1}(a^{-1}]\, a = (a^{-1})^{-1}$ ... ($\because$ Associativity of e identity)

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

$\Rightarrow \quad a = (a^{-1})^{-1}$ Hence, the proof

IV)Prove that the inverse of the product of two elements of a group G is the product of the inverses taken in reverse order. i.e. $(ab)^{-1} = b^{-1} a^{-1}$, $\forall$ a ; b $\in$ G.

Proof : Let a^{-1} and b^{-1} be the inverses of a and b in a group G respectively. Let e be the identity in G. Then $a^{-1}\, a = a\, a^{-1} = e$ and $b^{-1}\, b = b^{-1}\, b = e$

Consider, $(ab)(b^{-1}\, a^{-1}) = a(bb^{-1})\, a^{-1}$ ($\because$ Associativity)

$= a(e)\, a^{-1}$ ($\because bb^{-1} = e$)

$= (ae)\, a^{-1} = aa^{-1} = e$ ... (1)

Similarly, $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}\, a)\, b = b^{-1}(e)\, b$

$= b^{-1}\, b = e$ ... (2)

From equation (1) and equation (2), $(ab)(b^{-1}a^{-1}) = (b^{-1}\, a^{-1})(ab)$

$b^{-1}\, a^{-1}$ is the inverse of ab

$(ab)^{-1} = b^{-1}\, a^{-1}$

V) Prove that the cancellation laws hold in a group.i.e. If a, b, c $\in$ G then ab = ac $\Rightarrow$ b = c and ba = ca $\Rightarrow$ b = c.

Proof : Let a be any element in G and e be the identity element of a group G.

Now we have, [illegible]ac

Permultiplying by a^{-1} we get,

$a^{-1}(ab) = a^{-1}(ac)$

$(a^{-1}a)\,b = (a^{-1}a)\,c$ ... ($\because$ Associativity)

$eb = ec$ ... ($\because aa^{-1} = e$)

$b = c$

Similarly, $ba = ca$

$\Rightarrow \quad (ba)\,a^{-1} = (ca)\,a^{-1} \Rightarrow be = ce$

$\Rightarrow \quad b = c$ Hence, the proof

VI) If a, b are any elements of a group G then equation ax = b and ya = b have unique solutions in G.

Proof : Let $a \in G$

$\therefore \exists\ a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$

$a, a^{-1} \in G$ and $b \in G \Rightarrow a^{-1}b \in G$.

Now substituting $a^{-1}b$ for x in the L.H.S. given equation, we get,

$ax = a(a^{-1}b) = (aa^{-1})\,b = eb = b$

Thus, $x = a^{-1}b$ is the solution of $ax = b$

Let us suppose that x_1 and x_2 are two solutions of $ax = b$.

$\therefore \quad ax_1 = b$ and $ax_2 = b$

$\Rightarrow \quad b = ax_1 = ax_2 \Rightarrow x_1 = x_2$

Hence solution is unique.

Similarly prove for $ya = b$.

Q.9 If set Q_1 of all rational numbers other than 1 with $a * b = a + b - ab$. Show that (G, *) is a group. ☞ **[SPPU : Dec.-09, Marks 4]**

Ans. : We have, $a * b = a + b - ab$, $\forall\ a, b \in G$.

(i) Closure property : Let $a, b \in Q_1$, $a \neq 1$, $b \neq 1$ $\therefore ab \neq 1$.

$\therefore \quad a * b = a + b - ab \neq 1$ and $a * b \in Q_1$

Q_1 is closed w.r.t. *

(ii) Associativity : Let $a, b, c \in Q_1$.

$(a * b) * c = (a + b - ab) * c = (a + b - ab + c - (a + b - ab)\,c$

$= a + b - ab + c - ac - bc - abc$ ... (1)

$a * (b * c) = a * (b + c - bc) = a + b + c - bc$

$= a(b + c - bc) = a + b + c - bc - ab - ac + abc$ ...(2)

∴ From equation (1) and equation (2)

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

∴ * is associative

iii) **Existence of the identity :** Let e be the identity element in Q_1

$$a * e = a$$

$$\Rightarrow \quad a + e = ae = a$$

$$\Rightarrow \quad e - ae = 0$$

$$\Rightarrow \quad e(1 - a) = 0 \qquad \text{(But } a \neq 1\text{)}$$

$$\Rightarrow \quad e = 0$$

∴ 0 is the identity element.

iv) **Existence of the inverse :** Let $a \in Q_1$, $a \neq 1$.

Suppose $b \in Q$, is the inverse of a.

$$\therefore \quad a * b = e$$

$$\Rightarrow \quad a + b - ab = 0$$

$$\Rightarrow \quad a + b(1 - a) = 0$$

$$b(1 - a) = -a$$

$$\Rightarrow \quad b = \frac{-a}{1-a} = \frac{a}{a-1} \neq 1 \text{ and } b \in Q_1.$$

∴ The inverse exist for all a in Q_1.

Thus, $(Q_1, *)$ is a group.

Q.10 If S = {(a, b) | a ≠ 0, a, b, ∈ ℜ and (a, b) * (c, d) = (ac, bc + d) then show that G is a group but not abelian group w.r.t.*

Ans. : (i) Closure property : Let (a, b) (c, d) ∈ S ; a ≠ 0 ; c ≠ 0

∴ ac ≠ 0.

(a, b) * (c, d) = (ac, bc + d) ∈ S

(ii) Associativity : Let (a, b), (c, d) and (e, f) ∈ S

Consider

$[(a, b) * (c, d)] * (e, f) = [ac, bc + d) * (e, f) = ([ac]\ e, [bc + d]\ e + f)$

$= (ace, bce + de + f)$ ... (Q.10.1)

and $(a, b) * [(c, d) * (e, f)] = (a, b) * [ce, de + f] = [ace, b(ce) + de + f]$

$= (ace, bce + de + f)$ ... (Q.10.2)

From equation (Q.10.1) and equation (Q.10.2) * is associative operation.

(iii) Existence of the identity : Let $(a, b) \in S$ and $(x, y) \in S$, $x \neq 0$

Consider, $(a, b) * (x, y) = (a, b)$

$$(ax, bx + y) = (a, b)$$

$\Rightarrow$ $ax = a$ and $bx + y = b$

$\Rightarrow$ $x = 1$ and $b + y = b$

$\Rightarrow$ $y = 0$

Similarly, $(x, y) * (a, b) = (a, b)$

$(1, 0)$ is the identity element in S.

(iv) Existence of the inverse : Let (a, b) and $(c, d) \in S$.

$(a, b) * (c, d) = (1, 0)$

$(ac, bc + d) = (1, 0)$

$\Rightarrow$ $ac = 1$

and $bc + d = 0$

$\therefore$ $c = \frac{1}{a}$

and $d = -bc = -\frac{b}{a}$ and $c \neq 0$

Thus $\left(\frac{1}{a}, -\frac{b}{a}\right)$ is the inverse of (a, b) in S.

Thus $(S, *)$ is a group.

Consider, $(a, b) * (c, d) = (ac, bc + d)$

and $(c, d) * (a, b) = (ca, da + b)$

$\Rightarrow$ $(a, b) * (c, d) \neq (c, d) * (a, b)$

Thus, $(S, *)$ is not an abelian group.

Q.11 If $G = \left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} \middle/ x \text{ is non zero real number} \right\}$. **Show that G is an abelian group w.r.t. matrix multiplication.**

Ans. : (i) Closure property :

Let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$ and $B = \begin{bmatrix} y & y \\ y & y \end{bmatrix} \in G$

then $AB = \begin{bmatrix} x & x \\ x & x \end{bmatrix}\begin{bmatrix} y & y \\ y & y \end{bmatrix} = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \in G$

(ii) Associativity : We know that any matrix multiplication is associative.

(iii) Existence of the identity : Let $E = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$ such that

$AE = A \Rightarrow$

$$\begin{bmatrix} x & x \\ x & x \end{bmatrix}\begin{bmatrix} e & e \\ e & e \end{bmatrix} = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$$

$$\Rightarrow \quad \begin{bmatrix} 2xe & 2xe \\ 2xe & 2xe \end{bmatrix} = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$$

$$\Rightarrow \quad 2xe = e$$

$$\Rightarrow \quad 2x = 1$$

$$\Rightarrow \quad x = \frac{1}{2}$$

$$\therefore \quad E = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \text{ is the identity element of G.}$$

(iv) Existence of the inverse : Let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \in G$ and

$B = \begin{bmatrix} y & y \\ y & y \end{bmatrix} \in G$ such that $AB = E$

$$\Rightarrow \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

$$\Rightarrow \quad 2xy = \frac{1}{2}$$

$$\Rightarrow \quad xy = \frac{1}{4}$$

$$\Rightarrow \quad y = \frac{1}{4x}$$

$$A^{-1} = \begin{bmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{bmatrix}$$

(v) Commutative property :

We have, $AB = BA = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \in G$

Thus G is an abelian group w.r.t. matrix multiplication.

Q.12 Let G be the set of all non-zero real numbers and let $a * b = \frac{ab}{2}$. Show that (G, *) is an abelian group.

☞[SPPU : Dec.-08, Marks]

Ans. : (i) Closure property : Let $a, b \in G$.

$$a * b = \frac{ab}{2} \in G \text{ as } ab \neq 0$$

(ii) Associativity : Let $a, b, c \in G$

Consider $a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a(bc)}{4} = \frac{abc}{4}$

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{(ab)c}{4} = \frac{abc}{4}$$

$\Rightarrow$ * is associative in G.

(iii) Existence of the identity : Let $a \in G$ and $\exists$ e such that

$$a * e = \frac{ae}{2} = a$$

$$\Rightarrow \quad ae = 2a$$

$$\Rightarrow \quad e = 2$$

$\therefore$ 2 is the identity element in G.

(iv) Existence of the inverse : Let $a \in G$ and $b \in G$ such that $a * b = e = 2$

$$\Rightarrow \quad \frac{ab}{2} = 2$$

$$\Rightarrow \quad ab = 4$$

$$\Rightarrow \qquad b = \frac{4}{a}$$

$\therefore$ The inverse of a is $\frac{4}{a}$, $\forall\ a \in G$.

(v) Commutativity : Let $a, b \in G$

$$a * b = \frac{ab}{2}$$

and $$b * a = \frac{ba}{2} = \frac{ab}{2}$$

$\Rightarrow$ * is commutative

Thus, (G, *) is an abelian group.

Q.13 Show that the set $G = \{1, w, w^2\}$ where w is the cube root of unity is a group with respect to multiplication.

☞[SPPU : Dec.-12, Marks 6]

Ans. : Consider the following composition table of G.

	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

(i) Closure property : From table all elements belong to G.

$\therefore$ G is closed w.r.t. multiplication.

(ii) Associativity : As all elements of G are complex numbers and multiplication of complex numbers is associative.

$\therefore$ (G, x) is associative.

(iii) Existence of the identity : From the composition table

$$1\ (1) = 1\ ,\ 1\ (w) = 1\ ,\ 1\ (w^2) = w^2$$

$\therefore$ 1 is multiplicative identity in G.

(iv) Existence of the inverse : From table, the inverses of 1, w, w^2 are 1, w^2, w respectively. Thus (G, x) is a group.

Q.14 Let (A, *) be a group. Show that (A, *) is abelian group iff $a^2 * b^2 = (a * b)^2$

☞[SPPU ; Dec.-12, Marks 4]

Ans. : Let (A, *) be an abelian group.

$$a * b = b * a$$

Consider, $a^2 * b^2 = (a * a) * (b * b)$

$= a * (a * b) * b$ (* is associative)

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

$a^2 * b^2 = (a * b)^2$

Conversely suppose

$$a^2 * b^2 = (a * b)^2 \quad \text{(Q.14.1)}$$

L.H.S. $= a^2 * b^2 = (a * a) * (b * b) = a * (a * b) * b$

R.H.S. $= (a * b)^2 = (a * b) * (a * b) = a * (b * a) * b$

Equation (1) $\Rightarrow$

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

By cancellation laws,

$$a * b = b * a$$

$\Rightarrow$ (A, *) is an abelian group.

Q.15 Show that the set of all idempotents in a commutative monoid S is a submonoid of S.

[SPPU : Dec.-12, Marks 4]

Ans. : We know that an element $x \in S$ is called an idempotent if $x * x = x$.

Let T be the set of all idempotents in S.

i) For any $x, y \in T$, Consider

$(x * y) * (x * y) = ((x * y) * x) * y = (y * (x * x)) * y = (y * x) * y$

$= (x * y) * y = x * (y * y) = x * y$

$\therefore x * y \in T$ for all $x, y \in T$

T is closed w.r.t. '*'

ii) Associativity, Let $x, y, z \in T \subseteq S$

$\therefore \quad x * (y * z) = (x * y) * z$ in T

* is associative in T

iii) Existence of the identity :

Let e be the identity element in S

As $e * e = e \quad \therefore \quad e \in T$

$\therefore$ e is the identity element in T.

$\therefore$ T is a monoid

Thus T is a submonoid of S.

Q.16 Prove that the set $\mathbb{Z}$ of all integers with binary operation $*$ defined by $a * b = a + b + 1$ such that $\forall\ a, b \in \mathbb{Z}$ is an abelian group : **☞[SPPU : May-14, Marks 4]**

Ans. : We have $a * b = a + b + 1 \quad , \quad \forall\ a, b \in \mathbb{Z}$

i) Closure property

For $a, b \in \mathbb{Z} \Rightarrow a + b + 1 \in \mathbb{Z} \Rightarrow a * b \in \mathbb{Z}$

$\therefore$ $\mathbb{Z}$ is closed w.r.t. $*$

ii) Associative : Let $a, b, c \in \mathbb{Z}$

$$(a * b) * c = (a + b + 1) * c$$
$$= a + b + 1 + c + 1 = a + b + c + 2 \quad \ldots (Q.16.1)$$

and $$a * (b * c) = a * (b + c + 1)$$
$$= a + b + c + 1 + 1 = a + b + c + 2 \quad \ldots (Q.16.2)$$

From equation (Q.16.1) and equation (Q.16.2) $(a * b) * c = a * (b * c)$

$\therefore$ $*$ is associative in $\mathbb{Z}$

iii) Existence of the identity :

Let e be the identity in $\mathbb{Z}$

$\therefore$ For any $a \in \mathbb{Z}$, $a * e = e * a = a$

$$\Rightarrow a + e + 1 = a$$
$$\Rightarrow e + 1 = a$$
$$\Rightarrow e = -1 \text{ is the identity element in } \mathbb{Z}$$

iv) Existence of the inverse :

Let $a \in \mathbb{Z}$. Suppose $b \in \mathbb{Z}$ is the inverse of a in $\mathbb{Z}$

$\therefore$ $$a * b = e$$
$$a + b + 1 = -1$$
$$a + b = -2$$
$$b = -a - 2 \in \mathbb{Z}$$

$\therefore$ The inverse exists for all $a \in \mathbb{Z}$

Thus $(\mathbb{Z}, *)$ is a group.

Now consider $a * b = a + b + 1$ $(\because a + b = b + a)$

$= b + a + 1 = b * a \quad , \quad \forall\, a, b \in \mathbb{Z}$

$\therefore$ * is commutative in $\mathbb{Z}$

$\therefore$ $(\mathbb{Z}, *)$ is an abelian group.

Q.17 Define modulo m. ☞[SPPU : Dec.-11, May-08]

Ans. : I) Let and b are any integers and m is a fixed positive integer then the addition modulo m denoted by $a +_m b$ and defined as $a +_m b = r$; $0 \le r \le m$

Where r is the least non negative remainder when a + b is divided by m.

e.g. $5 +_3 9 = 2$ as $5 + 9 = 14$ and $14 = 3 \times 4 + 2$

$15 +_5 25 = 0$ as $15 + 25 = 40$ and $40 = 5 \times 8 + 0$

II) Let a and b be any integers and m is a fixed positive integer. Then the multiplication modulo m is denoted by $a \times_m b$ and defined as

$$a \times_m b = r \; ; \; 0 \le r \le m$$

Where r is the least non negative remainder when a × b is divided by m.

e.g. $3 \times_4 5 = 3$ as $3 \times 5 = 15$ and $15 = 4 \times 3 + 3$

$9 \times_6 4 = 0$ as $9 \times 4 = 36$ and $36 = 6 \times 6 + 0$

III) If a and be are any two integers such that a – b is divisible by a fixed positive integer m, is called "a congruent to b modulo m".

It is denoted by $a \equiv b \pmod m$

Q.18 Show that $(z_6, +)$ is an abelian group. ☞[SPPU : May-08]

Ans. : Let z_6 be the set of residue classes modulo6.

$\therefore$ $z_6 = \{[0], [1], [2], [3], [4], [5]\}$

Or $z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

Consider the following table

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\boxed{\bar{0}}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\boxed{\bar{0}}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\boxed{\bar{0}}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\boxed{\bar{0}}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\boxed{\bar{0}}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\boxed{\bar{0}}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

i) Closure Property : Every element of a table belongs to z_6

i.e. $\bar{a} + \bar{b} \in z_6 \quad \forall\ \bar{a}, \bar{b} \in z_6$

$\therefore$ + is closed in z_6

ii) Associativity : By table, for any $\bar{a}, \bar{b}, \bar{c} \in z_6$

$$\bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c}$$

$\therefore$ '+' is associative in z_6

iii) Existence of the Identity : By observing the first row and the first column,

For any $\bar{a} \in z_6, \exists\ \bar{0} \in z_6$ such that

$$\bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a}$$

$\therefore$ $\bar{0}$ is the identity element in z_6.

iv) Existence of the Inverse

From table, identify the identity elements

As $\bar{0} + \bar{0} = \bar{0}$, $\bar{0}$ is the inverse of $\bar{0}$

As $\bar{1} + \bar{5} = \bar{5} + \bar{1} = \bar{0}$, $\bar{1}$ is the inverse of $\bar{5}$ and $\bar{5}$ is the inverse of $\bar{1}$

As $\bar{2} + \bar{4} = \bar{4} + \bar{2} = \bar{0}$, $\bar{2}$ is the inverse of $\bar{4}$ and $\bar{4}$ is the inverse of $\bar{2}$

As $\bar{3} + \bar{3} = \bar{0}$, $\bar{3}$ is the inverse of $\bar{3}$

$\therefore$ Every element of z_6 has inverse in z_6.

v) Commutative Property

From table, For all $\bar{a}, \bar{b} \in z_6$

$$\bar{a} + \bar{b} = \bar{b} + \bar{a}$$

$\therefore$ '+' is commutative in z_6.

Hence $(z_6, +)$ is an abelian group.

Q.19 Let z = {0, 1, 2, 3, 4, ... (n – 1)} and '◊' be a binary operation such that $a \diamond b$ = remainder of abelian when divided by n. Construct a table for n = 4,
Is $(z_4, \diamond)$ is groupoid, monoid, semigroup and abelian group ?

☞ **[SPPU : Dec.-11]**

Ans. : We have $z_4 = \{0, 1, 2, 3\}$

Table of z_4 is

$\Diamond$	0	1	2	3
0	[0]	0	0	0
1	0	1	2	3
2	0	2	[0]	2
3	0	3	2	1

i) From table, for any a, b $\in z_4$, $a \Diamond b \in z_4$

$\therefore$ $(z_4, \Diamond)$ is a groupoid and $\Diamond$ is a binary operation in z_4 i.e. $\Diamond$ is closed in z_4.

ii) Semigroup : By table for any a, b, c, $\in z_4$

$$a \Diamond (b \Diamond c) = (a \Diamond b) \Diamond c$$

$\therefore$ $\Diamond$ is associative in z_4

OR Let $a \Diamond b = r$ and $b \Diamond c = t$

$\therefore$ $ab = 4p + r$ and $bc = 4l + t$

$\therefore$ $(a \Diamond b) \Diamond c = r \Diamond c = s$ where $rc = 4q + s$

$a \Diamond (b \Diamond c) = a \Diamond t = k$ where $at = 4m + k$

Prove that $s = k$

$$a(bc) = 4al + at = 4al + 4m + k \quad \ldots (Q.19.1)$$

$$(ab)c = (4p + r)c = 4pc + rc = 4pc + 4q + s \quad \ldots (Q.19.2)$$

Equations (Q.19.1) and equation (Q.19.2) are equal

$$\Rightarrow 4al + 4m + k = 4pc + 4q + s$$

$$\Rightarrow k = s$$

Hence $(a \Diamond b) \Diamond c = a \Diamond (b \Diamond c)$

Thus $(z_4, \Diamond)$ is a semigroup

iii) Monoid

By observing the first row and the first column of table

For any $a \in z_4$, $\exists$ $0 \in z_4$ such that

$$a + 0 = 0 + a = a$$

$\therefore$ 0 is the identity element in z_4

Thus from (i), (ii) and (iii), $(z_4, +)$ is a monoid.

iv) Existence of the inverse

From table, identify the identity elements.

x is the inverse of 3 in z_4

$\therefore$ $x \lozenge 3 = 0$ and $x \lozenge 3 = 4$ if $3x = 4m + r$

$\therefore$ $3x - 4m = 0$

$\Rightarrow$ $3x = 4m$

$\Rightarrow$ $x = \frac{4m}{3}$ which is an integer

For $m = 1, 2,$ x is not an integer

For $m = 3,$ $x = 4$ which is an integer

But $x = 4 \notin z_4$

Thus 3 does not have inverse in z_4

$\therefore$ $(z_4, \lozenge)$ is not a group

Hence $(z_4, \lozenge)$ is not an abelian group.

Q.20 Define permutation group.

Ans. : I) Let $S = \{1, 2, 3, ..., n\}$ be a finite set with n distinct elements. If $f : S \to S$ is a bijective function then f is called a permutation of degree n.

Let $f(a_1) = b_1, \quad f(a_2) = b_2, \quad f(a_3) = b_3, \quad .... \; f(a_n) = b_4$

Then the permutation is denoted by

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & .... & a_n \\ b_1 & b_2 & b_3 & .... & b_n \end{pmatrix} \begin{matrix} \\ \to \text{ Elements in Domain} \\ \to \text{ Elements in Co-domain} \end{matrix}$$

II) The permutation corresponding to the identity function is called the identity permutation

$$I = \begin{pmatrix} a_1 & a_2 & a_3 & .... & a_n \\ b_1 & b_2 & b_3 & .... & b_n \end{pmatrix}$$

III) If $f_1 = \begin{pmatrix} a_1 & a_2 & a_3 & .... & a_n \\ b_1 & b_2 & b_3 & .... & b_n \end{pmatrix}$ and $f_2 = \begin{pmatrix} b_1 & b_2 & b_3 & .... & b_n \\ c_1 & c_2 & c_3 & .... & c_n \end{pmatrix}$

Then the product of two permutations is given by

$$f_1 f_2 = \begin{pmatrix} a_1 & a_2 & a_3 & .... & a_n \\ c_1 & c_2 & c_3 & .... & c_n \end{pmatrix}$$

(To write product use $a_1 \to b_1 \to c_1 \Rightarrow a_1 \to c_1$ and so on)

6.3 : Subgroup

Q.21 Define complexes and subgroups.

Ans. : 1) Complex of a group : Let $(G, *)$ be a group. Any non empty subset of a group G is called a complex of the group.

e.g. $H_1 = \{1, 2, 3, 4, 5\}$, $H_2 = \{1, 2, 3, ...\}$, $H_3 = \mathbb{Z}$

are complexes of a group $(\Re, +)$

2. Subgroup

Let $(G, *)$ be a group. A non empty subset H of a group G, is said to be subgroup of G if $(H, *)$ itself is a group.

Examples

1) $(\mathbb{Z}, +)$ is a subgroup of $(\Re, +)$
2) $(\Re, +)$ is a subgroup of $(\mathbb{C}, +)$
3) $(N, +)$ is not a subgroup of $(\mathbb{Z}, +)$
4) $(\Re_0, \cdot)$ is a subgroup of $(\mathbb{C}_0, \cdot)$
5) $(\{1\}, \cdot)$ is a subgroup of $(Q_0, \cdot)$, $(\Re_0, \cdot)$, $(\mathbb{C}, \cdot)$
6) $(\Re, +)$ is a subgroup of $(\Re, +)$

Note :

1) $\{e\}$ and $\{G\}$ are subgroups of group G : These subgroups are called improper subgroups.
2) Subgroups which are not improper are called proper subgroups.

Q.22 Explain properties of subgroup with proof.

Ans. : Theorem I) : Prove that the identity of a subgroup is the same as that of the group.

Let H be a subgroup of the group G.

Let e and e' be the identities of G and H respectively.

Now, $a \in H \Rightarrow e' a = a$

also $a \in H \Rightarrow a \in G \Rightarrow ea = a$ ... [$\because$ e' is identity of H]

[$\because$ e is identity of G]

$$e'a = ea$$

$\therefore$ in G we have,

$\Rightarrow$ $e' = e$ ... [by right cancellation law in G]

Theorem II) : Prove that the inverse of any element of a subgroup is the same as the inverse of the same regarded as an element of the group.

Let H be a subgroup of the group G.

Let e be the identity of G as well as of H.

Let $a \in H$, suppose b is the inverse of a in H and c is the inverse of a in G. Then we have,

$$ba = e$$

and $$ca = e$$

$\therefore$ in G we have, $ba = ca \Rightarrow b = c$

Theorem III) : Prove that the order of any element of a subgroup is the same as the order of the element regarded as a member of the group.

Let H be a subgroup of the group G.

Let $a \in H$, But $a \in G$ and $a^n = e$ in G.

$a^n = e$ in H also. Hence the proof.

Theorem IV) : A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup is that $a \in H$, b

$H \Rightarrow ab^{-1} \in H$ where b^{-1} is the inverse of b in G.

Suppose H is a subgroup of G.

Let $a \in H$, $b \in H$. Now each element of H must possess inverse because H itself is a group.

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

Further H must be closed with respect to multiplication i.e. the composition in G.

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

(i) The condition is sufficient. Now it is given that $a \in H$,

$b \in H \Rightarrow ab^{-1} \in H$. We have to prove that H is a subgroup of G.

(ii) Existence of identity :

We have $a \in H$, $a \in H \Rightarrow aa^{-1} \in H$ ... By given condition

$$\Rightarrow e \in H$$

Thus the identity e is an element of H.

(iii) Existence of inverse :

Let a be any element of H. Then by the given condition, we have,

$e \in H, a \in H \Rightarrow ea^{-1} \in H \Rightarrow a^{-1} \in H.$

Thus each element of H possesses inverse.

(iv) Closure property : Let $a, b \in H$. Then as shown above

$b \in H \Rightarrow b^{-1} \in H$. Therefore applying the given condition we have,

$a \in H, b^{-1} \in H \Rightarrow a (b^{-1})^{-1} \in H \Rightarrow ab \in H.$

(v) Associativity : The elements of H are also the elements of G. The composition in G is associative. Therefore, it must also be associative in H.

Hence H itself is a group for the composition in G. Therefore, H is a subgroup of G.

Theorem V) : If H_1 and H_2 are two subgroups of a group G, then $H_1 \cap H_2$ is also a subgroup of G.

Let H_1 and H_2 be any two subgroups of G. Then $H_1 \cap H_2 \neq \phi$ Since at least the identity element e is common to both H_1 and H_2.

In order to prove that $H_1 \cap H_2$ is a subgroup it is sufficient to prove that

$a \in H_1 \cap H_2, b \in H_1 \cap H_2 \Rightarrow ab^{-1} H_1 \cap H_2$

Now, $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$

$a \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$

But H_1, H_2 are subgroups.

$\therefore$ $a \in H_1, b \in H_1, \Rightarrow ab^{-1} \in H_1$

$a \in H_2, b \in H_2 \Rightarrow ab^{-1} \in H_2$

Finally $ab^{-1} \in H_1$, $ab^{-1} \in H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Thus, we have shown that, $a \in H_1 \cap H_2$, $b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Hence $H_1 \cap H_2$ is a subgroup of G.

Theorem VI) : Show that the union of two subgroups is a subgroup if and only if one is contained in the other.

Suppose H_1 and H_2 are two subgroups of a group G.

Let $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Then $H_1 \cup H_2 = H_2$ or H_1.

But H_1, H_2 are subgroups and therefore, $H_1 \cup H_2$ is also a subgroup. Conversly suppose $H_1 \cup H2$ is a subgroup. To prove that $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Let us assume that H_1 is not a subset of H_2 and H_2 is also not a subset of H_1.

Now H_1 is not a subset of $H_2 \Rightarrow \exists\ a \in H_1$ and $a \notin H_2$ ... (Q.22.1)

and H_2 is not a subset of $H_1 \Rightarrow \exists\ b \in H_2$ and $B \notin H_1$ ... (Q.22.2)

From equation (Q.22.1) and (Q.22.2).

We have, $a \in H_1 \cup H_2$ and $b \in H_1 \cup H_2$

Since $H_1 \cup H_2$ is a subgroup, therefore $ab = c$ (say) is also an element of $H_1 \cup H_2$.

But $ab = c \in H_1 \cup H_2 \Rightarrow ab = c \in H_1$ or H_2

Suppose $ab = c \in H_1$

Then $b = a^{-1} c \in H_1$,

... [$\because H_1$ is a subgroup. $\therefore a \in H_1 \Rightarrow a^{-1} \in H_1$]

But from (2), we have $b \in H_1$. Thus we get the contradiction.

Again suppose $ab = c \in H_2$

Then, $a = cb^{-1} \in H_2$

... [$\because H_2$ is a subgroup, therefore $b \in H_2, \Rightarrow b^{-1} \in H_2$]

But from (1), we have $a \notin H_2$. Thus here also we get a contradiction.

Hence either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Q.23 Is union of two subgroups is a subgroup? If not, give example.

Ans. : The union of two subgroups is not necessarily a subgroup.

Let $H_1 = \{...., -4, -2, 0, 2, 4, 6, ...\}$

$H_2 = \{...., -6, -3, 0, 3, 6, ...\}$ are subgroup of $(\mathbb{Z}, +)$

Now $H_1 \cup H_2 = \{-6, -4, -3, -2, 0, 2, 3, 4, 6, ...\}$

$2, 3 \in H_1 \cup H_2$ but $2 + 3 = 5 \notin H_1 \cup H_2$

$\therefore$ + is not binary operation on $H_1 \cup H_2$

$\Rightarrow$. $H_1 \cup H_2$ is not a subgroup of G.

Q.24 Define cosets with example.

Ans. : Let $(G, *)$ be a group and H be any subgroup of G.

Let $a \in G$ be any element, then the set

$H*a = \{h*a\}/\forall h \in H\}$ is called a right coset of H in G.

and $a*H = \{a*h/\forall h \in H\}$ is called a left coset of H in G.

Note :

1) $H*a$ and $a*H$ are subsets of G.

2) If $(G, *)$ is an abelian group then $H*a = a*H$ in G.

e.g. 1) Let $(\mathbb{Z}, +)$ is a group and

$H = \{...., -10, -5, 0, 5, 10, ...\}$ is a subgroup of $G = \mathbb{Z}$

$\therefore$ For $1 \in \mathbb{Z}$, $H+1 = \{...., -9, -4, 1, 6, 11, ...\}$

$3 \in \mathbb{Z}$, $H+3 = \{...., -7, -2, 3, 8, 13, ...\}$

$5 \in \mathbb{Z}$, $H+5 = \{...., -5, 0, 5, 10, ...\} = H$

are right cosets of H in G.

Q.25 Order of an element of a group.

Ans. : Let $(G, \cdot)$ be a group. The smallest positive integer is called the order of an element $a \in G$ if

$a^n = e$(identity element in G)

If is denoted by $o(a) = n$.

If no such positive number exists, then we say that a is of infinite order or zero order.

Note :

1) For the order of the group is the number of distinct elements in G.

2) The order of the identity element is 1 i.e. $o(e) = 1$

3) In a group G, $o(a) = o(a^{-1})$; $\forall a \in G$

4) In a group G, $o(a) \leq o(G)$

Q.26 Define cyclic group.

Ans. : A group G is called a cyclic group if $\exists$ at least one element $a \in G$ such that every element $x \in G$ can be written as $x = a^m$ where m is some integer.

The element a is called the generator of G and denoted by $G = \langle a \rangle$

Example 1 : Four fourth roots of unity form a cyclic group with respect to multiplication.

$$G = \{1, -1, i, -i\}$$

We have $(i)^1 = i, \quad (i)^2 = -1, \quad (i)^3 = -i, \quad (i)^4 = 1$

$\therefore$ i is the generator of $G \Rightarrow G$ is a cyclic group.

Moreover, $(-i)^1 = -i, \quad (-i)^2 = -1, (-i)^3 = i, \quad (-i)^4 = 1$

$\therefore$ $-i$ is also generator of G

$\therefore$ $$G = \langle i \rangle = \langle -i \rangle$$

Q.27 Define normal subgroups.

Ans. : A subgroup H of a group $(G, *)$ is said to be a normal subgroup of G if for all $g \in G$ and for all $h \in H$

$g*h*g^{-1} \in H$ (We may write $g\,h\,g^{-1} \in H$)

Every group G possesses at least two normal subgroups namely {e} and G. These groups are called improper normal subgroups.

Simple Group : A group G is said to be simple group if it has only two normal subgroups, {e} and G.

Notes :

1) Every subgroup of an abelian group is normal.

2) The intersection of normal subgroups is a normal subgroup.

Q.28 Define quotient groups. ☞**[SPPU : Dec.-14. 15, May-15]**

Ans. : Let $(G, *)$ be a group and N be a normal subgroup of G. Let G/N be the collection of all cosets of N in G.

$$G/N = \{N*a / a \in G\}$$

$(G/N, *)$ is called the quotient group or factor group.

Q.29 Prove that $(G/N, *)$ is a group. ☞**[SPPU : Dec.-15, May-15]**

Ans. : Let $(G, *)$ be a group and N is the normal subgroup at G

$\therefore$ $$G/N = \{N*a / \forall a \in G\}$$

Theorem :

1) Closure Property : Let $a, b \in G, \therefore N*a, N*b \in G/N$

$(N*a)*(N*b) = N*(a*N)*b$ ($\because$ N is normal)

$= N*(N*a)*b = (N*N)*(a*b)$

$= N*c$ ($\because N*N = N$ and $a*b = c \in G$)

$\therefore (N*a)*(N*b) \in G/N$

$\therefore$ G/N is closed w.r.t. *

2) Associativity : Let a, b, c $\in$ G

and N*a, N*b and N*c $\in$ G/N

$\therefore (N*a)*[(N*b)*(N*c)] = N*a*[N*(b*c)]$ by (1)

$= N*a*(b*c)$ by (1)

$= N*(a*b)*c)$ (* is associative in G)

$= (N*(a*b))*(N*c) = [(N*a)*(N*b)]*(N*c)$

$= [(N*a)*(N*b)]*(N*c)$

Thus * is associative in G/N

3) Existence of the identity :

We have $N = N*e \in G/N$ and for any $N*a \in G/N$

$(N*a)*(N*e) = N*(a*e)$ (by (1))

$= N*a$

$\therefore N*e = N$ is the identity element in G/N.

4) Existence of the inverse : Let $a \in G$, $N*a \in G/N$

$\therefore \exists\ a^{-1} \in G$ and $N*a^{-1} \in G/N$ such that

$$(N*a)*(N*a^{-1}) = N*(a*a^{-1}) = N*e = N$$

Hence $N*a^{-1}$ is the inverse of N*a in G/N

Thus (G/N, *) is a group, known as quotient group.

Q.30 Prove lagranges theorem : The order of each subgroup of a finite group is a divisor of the order of the group.

Ans. : Let G be a group of finite order n. Let H be a subgroup of G and let O (H) = m. Suppose $h_1, h_2 \ldots h_m$ are the m members of H.

Let $a \in G$. Then Ha is a right coset of H in G and we have

$$Ha = \{h_1a, h_2a, \ldots\ldots, h_m a\}$$

Ha has m distinct members, since $h_i a = h_j a \Rightarrow h_i = h_j$.

Therefore each right coset of H in G has m distinct members. Any two distinct right cosets of H in G are disjoint i.e. they have no element in common. Since G is a finite group, the number of distinct right cosets of H in G will be finite, say equal to K. The union of these K distinct right cosets of H in G is equal to G.

Thus, if $Ha_1, Ha_2, \ldots Ha_k$ are the K distinct right cosets of H in G, then

$$G = Ha_1 \cup Ha_2 \cup \ldots\ldots\ldots \cup Ha_k$$

$\Rightarrow$ The number of elements in G = The number of elements in Ha_1 + The number of elements in Ha_2 + ... + The number of elements in Ha_k

... [$\because$ two distinct right cosets are mutually disjoint]

$$\Rightarrow \quad O(G) = Km \Rightarrow n = Km$$

$$\Rightarrow \quad K = \frac{n}{m} \Rightarrow m \text{ is a divisor of } n$$

$\Rightarrow$ O (H) is a divisor of O (G).

Q.31 Prove the order of every element of a finite group is a divisor of the order of the group.

Ans. : Suppose G is a finite group of order n.

Let $a \in G$ and O (a) = m. Prove that m is a divisor of n.

Let H = { ..... , $a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3$, ...} be the subset of G consisting of all integral powers of a.

We know that H is a subgroup of G.

We have to show that H contains only m distinct elements and that they are a, a, $a^2, a^3, \ldots\ldots, a^m = e\ a^o$

Let $1 \le r \le m$, $1 \le s \le m$, and $r > s$.

then $a^r = a^s \Rightarrow a^r a^{-s} = a^s a^{-s} \Rightarrow a^{r-s} \Rightarrow a^0 \Rightarrow a^{r-s} = e$

Thus there exists a positive integer r – s less than m such that $a^{r-s} = e$.

m is the least positive integer such that $a^m = e$.

$\therefore \quad a^r \neq a^s$

$\therefore$ a, $a^2, a^3, \ldots\ldots, a^m = a^0 = e$ are all distinct elements of H.

Now suppose at is any element of H where t is any integer.

By division algorithm,

We have, $t = mp + q$ ... [p and q are some integers, $0 \le q < m$]

We have, $a^t = a^{mp+q} = a^{mp} a^q = \left(a^m\right)^p a^q = a^q \quad \ldots (0 \le q < m)$

$\therefore$ a^q is one of the m element a, $a^2, \ldots\ldots, a^m = a^0$

Hence, H has only m distinct elements. Thus order of H is m.

By Lagrange's theorem m is a divisor of n.

Q.32 Prove that if G is a finite group of order n and $a \in G$, then $a^n = e$.

Ans. : In a finite group, the order of each element is finite.
Let O (a) = m. The subset H of G consisting of all integral powers of a is a subgroup of G and the order of H is m.
By Lagrange's theorem, m is a divisor of n.

Let $k = \frac{n}{m}$ then $n = mk$

Now, $a^n = a^{mk} = (a^m)^k = e^k$ ... $O(a) = m \Rightarrow am = e$

$= e$

6.4 : Cyclic Group

Q.33 Prove that every cyclic group is an abelian group.

☞ **[SPPU : Dec.-14, Marks 3]**

Ans. : Let G = {a} be a cyclic group generated by a.

Let x, y be any two elements of G. Then there exist integers r and s such that $x = a^1$, $y = a^s$.

Now, $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$

Thus, we have, $xy = yx \ \forall \ x, y \in G$.

Therefore G is abelian.

Q.34 Prove that If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Let G = {a} be a cyclic group generated by a.

Let a^1 be any element of G, where r is some integer.

as $a^r = (a^{-1})^{-r}$

$\therefore$ $-r$ is also some integer.

$\therefore$ Each element of G, is generated by a^{-1}

Thus, a^{-1} is also a generator of G.

Q.35 Prove that every group of order 3 is cyclic.

OR Prove that every group of prime order is cyclic.

Ans. : Suppose G is a finite group whose order is a prime number P, then to prove that G is a cyclic group. As an integer P is said to be a prime number if $P \neq 0$, $P \neq \pm 1$, and if the only divisors of P are $\pm 1, \pm P$.

$\because$ G is a group of prime order, therefore G must contain at least 2 elements.

As 2 is the least positive prime integer.

There must exist an element $a \in G$ such that $a \neq t$, the identity element e.

Since a is not the identity element, therefore O (a) is definitely ≥ 2.

Let O (a) = m, If H is the cyclic subgroup of G generated by a then

$$O(H) = O(a) = m.$$

By Lagrange's theorem m must be divisor of P.

But P is prime and $m \geq 2$. Hence m = P

$\therefore$ H = G. Since H is cyclic. Therefore G is cyclic and a is a generator of G.

Q.36 Prove that every subgroup of a cyclic group is cyclic.

Ans. : Suppose G = {a} is a cyclic group generated by a. If H = G or {e}, then obviously H is cyclic. So let H be a proper subgroup of G. The elements of H are integral powers of a. If $a^s \in H$, then the inverse of a^s.

i.e. $a^{-s} \in H$.

$\therefore$ H contains elements which are positive as well as negative integral powers of a.

Let m be the least positive integer such that $a^m \in H$.

Then we shall prove that $H = \{a^m\}$

i.e. H is cyclic and is generated by a^m.

Let a^1 be any arbitrary element H.

By division algorithm,

there exist integers q and r such that $t = mq + r$, $0 \leq r < m$.

Now, $a^m \in H \Rightarrow (a^m)^q \in H$ ... by closure property

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

Also, $a^t \in H$ $a^{-mq} \in H \Rightarrow a^t\, q^{-mq} \in H \Rightarrow a^{t-mq} \in H \Rightarrow a^r \in H$.

Now m is the least positive integer such that $a^m \in H$ and $0 \leq r < m$.

Therefore r must be equal to 0. Hence t = mq.

$\therefore$ $a^t = a^{mq} = (a^m)^q$

Thus every element $a^t \in H$ is of the form $(a^m)\, q$.

Therefore H is cyclic and a^m is a generator of H.

Q.37 Define the subgroup of a group. Let (G, 0) be a group. Let H = {a | a ∈ G and aob = boa for all b in G}. Show that H is normal subgroup of G.

Ans. : Let (G, x) be a group. A non empty subset H of a group G is said to be a subgroup of G if (H, *) itself is a group.

Given that, $H = \{a \mid a \in G \text{ and } a \circ b = b \circ a ; \forall b \in G\}$

Let $a, b \in H \Rightarrow a \circ x = x \circ a$ and $b \circ x = x \circ b$, $\forall x \in G$.

$$\Rightarrow (b \circ x)^{-1} = (x \circ b)^{-1}$$

$$\Rightarrow x^{-1} \circ b^{-1} = b^{-1} \circ x^{1} \quad \ldots (Q.37.1)$$

$$\Rightarrow b^{-1} \in H.$$

Now, $(a \circ b^{-1}) \circ x = a \circ (b^{-1} \circ x)$ [∵ o is associative]

$= a \circ (x \circ b^{-1})$ [∵ use (1) or $b^{-1} \in H$]

$= (a \circ x) \circ b^{-1}$ [∵ $a \in H$]

$= (x \circ a) \circ b^{-1} = x \circ (a \circ b^{-1})$

$\Rightarrow \quad a \circ b^{-1} \in H$

Therefore H is a subgroup of group G.

Let $h \in H$ and $g \in G$ and any x in G.

Consider,

$(g \circ h \circ g^{-1}) \circ x = (g \circ g^{-1} \circ h) \circ x$ [∵ $h \in H$]

$= (e \circ h) \circ x = h \circ x = x \circ h$ (∵ $h \in H$)

$= x \circ (h \circ g \circ g^{-1}) = x \circ (g \circ h \circ g^{-1})$ (∵ $h \in H$)

$\Rightarrow g \circ h \circ g^{-1} \in H$ for any $g \in G$

∴ H is a normal subgroup of G.

Q.38 Show that the four permutations I, (a b), (c d), (a b) (c d) on four symbols a, b, c, d form a finite abelian group with respect to the multiplication.

Ans. : Let

$$f_1 = I = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$$

$$f_2 = (a\ b) = \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}$$

$$f_3 = (c\ d) = \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}$$

$$f_4 = (a\ b)\ (c\ d) = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$$

Let $G = \{f_1, f_2, f_3, f_4\}$

Consider the multiplication table

X	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

(i) **Closure property :** All elements of table belong to G. (G, x) is closed w.r.t. x.

(ii) **Multiplication** of permutations is associative.

(iii) $f_1 = I$ is the identity element in G.

(iv) In G, $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$ and $f_4^{-1} = f_4$

(v) Multiplication table is symmetric about main diagonal $\therefore$ (G, x) is commutative.

Hence (G, x) is an ablein group of order 4.

6.5 : Homomorphism and Isomorphism

Q.39 Define homomorphism of groups with properties.

[SPPU : Dec.-15, 14, 12, 11, May-15]

Ans. : Let $(G_1, *)$ and (G_2, o) be two groups. A function

$f : (G_1, *) \rightarrow (G_2, o)$ is said to be homomorphism.

If $f(a * b) = f(a)\ o\ f(b)$ for all $a, b \in G_1$.

i.e. $a * b$ in $G_1 \rightarrow f(a)\ o\ f(b)$ in G_2

A homomorphism from G to itself is called as endomorphism.

Properties of group homomorphism.

Let $f : G_1 \rightarrow G_2$ be group homomorphism and $((G_1, *)$ and $(G_2 * o)$ are groups then

i) $f(e_1) = (e_2)$

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

Proof : 1) Let $a \in G_1$ and $f(a) \in G_1$ and e_2 is the identity element in G_2.

$\therefore \quad f(a) o e_2 = f(a) = f(a * e_1)$

$f(a) o e_2 = f(a) o f(e_1)$

$\Rightarrow f(e_1) = e_2$

2) Let $a \in G_1$ then $a^{-1} \in G$

and $e_2 = f(e_1) = f(a * a^{-1})$ (f is homomorphism)

$e_2 = f(a) o f(a^{-1})$

$\Rightarrow \quad f(a^{-1}) = [f(a)]^{-1}$

Q.40 Define isomorphism of groups.

[SPPU : Dec.-13, 12, 11, 10, May-08, 10]

Ans. : Let $(G_1, *)$ and (G_2, o) be two groups. A function

$f : (G_1, *) \rightarrow (G_2, o)$ is said to be isomorphism.

If i) f is a homomorphism from $G_1 \rightarrow G_2$, ii) f is bijective function.

If $f : G_1 \rightarrow G_2$ is an isomorphism of groups then G_1 and G_2 are called as isomorphic groups and denoted by $G_1 \cong G_2$.

An isomorphism from G to itself is called as automorphism of group G.

Q.41 Let G be a group with identity e show that a function $f : G \rightarrow G$ defined by $f(a) \forall = e, a \in G$ is a homomorphism (Endomorphism).

[SPPU : May-08, 10, Marks 3]

Ans. : We have $f : G \rightarrow G$ and $f(a) = e, \forall a \in G$.

Let $a, b \in G \Rightarrow f(a), f(b) \in G$

$\therefore \quad f(a * b) = e$ (as $a * b \in G$)

$= e * e = f(a) * f(b)$

$\therefore$ f is a homomorphism.

Q.42 Explain homomorphism and antomorphism of groups with examples.

[SPPU : Dec.-11, 12, 13, Marks 3]

Ans. : Refer Q.39 and Q.40 for definition.

e.g. 1) The homomorphism $f : (\mathbb{Z}, +), (\mathbb{Z}, +)$ such that

$f(n) = -n$ is an antomorphism of group.

2) The homomorphism $f : (R_o, o) \to (R_o, o)$ such that

$f(x) = x; \ \forall x \in \Re_o$ is an antomorphism of groups.

Q.43 Let $\Re$ be the additive group of real numbers and $\Re +$ be the multiplicative group of positive real numbers. Prove that the mapping $f : (R, +) \to (\Re_+, X)$ defined by $f(x) = e^x, \forall x \in \Re$ is an isomorphism of $\Re$ onto $\Re_+$ ☞[SPPU : Dec.-10, Marks 4]

Ans. : If x is any real number, then e^x is always positive real number and e^x is unique. Therefore, $f : \Re \to R_+$ is a function such that $f(x) = e^x$.

Let $x_1, x_2 \in \Re$ then $f(x_1) = f(x_2)$

$\Rightarrow \quad e^{x1} = e^{x2} \Rightarrow x_1 = x_2$

$\therefore$ f is one to one mapping.

For any $y \in \Re_+$ then $\log y \in \Re$ such that

$f(\log y) = e^{\log y} = y$

$\therefore$ f is onto.

Now for any $x_1, x_2 \in \Re$

Consider, $f(x_1 + x_2) = e^{x1+x2} = e^{x1 \times x2} = f(x_1) \times f(x_2)$

$\therefore$ f preserves compositions in $\Re$ and $\Re+$

$\therefore$ f is an isomorphism of $\Re$ onto $\Re+$.

Hence $\Re \cong \Re_+$

6.6 : Rings

Q.44 Define rings, integral domains and fields.

☞[SPPU : Dec.-08, 10, 11, 12, 13, 14, May-14]

Ans. : 1. Rings ☞ SPPU : Dec.-13, May-14

Let R be a non empty set equipped with two binary operations called addition and multiplication and denoted by '+' and '' respectively.

An algebraic structure (R,+, ·) is called a ring if it satisfies following axioms.

1) (R, +) is an abelian group i.e.

i) **Closure property :** for $a, b \in R, a + b \in R$

ii) **Associativity :** for a, b, c $\in$ R, $a + (b + c) = (a + b) + c$

iii) **Existence of the identity :** For any $a \in R$, $\exists\ o \in R$ s.t., $a + 0 = 0 + a = a$.

$\therefore$ 0 is called as the additive identity element of ring.

iv) **Existence of the inverse :** for each $a \in R$, $\exists\ -a \in R$

Such that $a + (-a) = -a + a = 0$

$-a$ is called the additive inverse of a

v) **Commutative property :** For a, $b \in R$

$a + b = b + a$

2) (R, $\cdot$) is semigroup i.e.

i) **Closure property :** $\forall a, b \in R, a \cdot b \in R$

ii) **Associativity :** for a, b, c $\in$ R,

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3) Multiplication distributes over addition $\forall a, b, c \in R$

i) $a \cdot (b + c) = a \cdot b + a \cdot c$ (Right distributive law)

ii) $(a + b) \cdot c = a \cdot c + b \cdot c$ (Left distributive law)

2. Commutative Ring : A ring (R, +, $\cdot$) is said to be commutative ring if $\forall\ b \in R$, $a \cdot b = b \cdot a$

3. Ring with Unity : A ring (R, +, $\cdot$) is said to be ring with unity if $\forall\ a \in R$, $\exists$, $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$.

Examples :

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

2) ($2\mathbb{Z}$, +, $\cdot$) is a commutative ring without unity where $2\mathbb{Z}$ = set of even integers.

3) The set of $n \times n$ matrices over real numbers with respect to usual matrix addition and multiplication is a non commutative ring with unity.

4. Properties of a Ring : If (R, +, $\cdot$) is a ring with identity 0 and unit element 1 then following are true for all a, b, c $\in$ R.

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

ii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

iii) $(-a)\cdot(-b) = a\cdot b$

iv) Unit element is unique

5. Subring : Let $(R, +, \cdot)$ be a ring. A non empty subset S of R is said to be subring of R if $(S,+, \cdot)$ is a ring. e.g. $(\mathbb{Z},+, \cdot)$ is a subring of $(\Re +, \cdot)$.

6. Zero Divisors : Let $(R, +, \cdot)$ be a commutative ring. An element $a \neq 0$ in R is said to be zero divisor if $\exists\ b \neq 0$ in R such that $a\cdot b = 0$.
A ring $(R, +, \cdot)$ is said to be without zero divisors.

if $a\cdot b = 0 \Rightarrow a = 0$ or $b = 0$, $\forall\ a, b \in R$.

e.g. 1) $\overline{2}$ is a zero divisor in $(\mathbb{Z}_4, +, \cdot)$ as $\overline{2}\cdot\overline{2} = \overline{4} = 0$

2) $(M_{2\times2}\ \Re), +, \cdot 1)$ is a ring with zero divisors.

as $$A\cdot B = \begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}\cdot\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix} = 0$$ but $A \neq 0$ and $B \neq 0$

3) $(\mathbb{Z}, +, \cdot)$ is a ring without zero divisors i.e. $a\cdot b = 0 \Rightarrow a = 0$ or $b = 0$.

7. Integral Domain ☞**[SPPU : Dec.-13, 11, 10, May-14]**

A commutative ring with zero divisors is called an integral domain.

e.g. 1) $(\Re, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are integral domains.

2) $(\mathbb{Z}_4, +, \cdot)$ is a ring with zero divisors

$\therefore$ It is not integral domain.

8. Field ☞**[SPPU : Dec.-13, 12, 11, 10, May-14]**

A commutative ring with unity in which every non zero element possesses their mulplicative inverse, is called as field.

A field is an integral domain.

e.g. 1) $(\Re, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(Q, +, \cdot)$ are fields.

2) $(\mathbb{Z}, +, \cdot)$ is integral domain but not field.

9. Ring Homomorphism

Let $(R, +, *)$ and $(S, +', \xi*')$ be two rings.

A function $\phi : R \to S$ is called a ring homomorphism

If for any $a, b \in R$

i) $\phi(a+b) = \phi(a)+\phi(b)$

ii) $\phi(a * b) = \phi(a) *' \phi(b)$

If ϕ is bijective then it is called as a ring isomorphism.

The kernal of ring homomorphism is defined as the set $\{a \in R / \phi(x) = 0'\}$.

It is denoted by ker (ϕ) or ker ϕ

Q.45 Let $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} : a, b \in z \right\}$ **f is the mapping that takes** $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ **to a – b.**

i) Show that f is a homomorphism. ii) Find Kernel of f.

☞[SPPU : Dec.-08]

Ans. : i) $f = \left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} + \begin{bmatrix} c & d \\ d & c \end{bmatrix} \right) = f\left(\begin{bmatrix} a+c & b+d \\ b+d & a+c \end{bmatrix} \right) = (a+c)-(b+d)$

$= (a-b)+(c-d) = f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) + f\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix} \right)$

Also $f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) \cdot \left(\begin{bmatrix} c & d \\ d & c \end{bmatrix} \right) = f \begin{bmatrix} ac+bd & ad+bc \\ bc+ad & bd+ac \end{bmatrix} = (ac+bd)-(ad+bc)$

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

$= f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) \cdot f\left(\begin{bmatrix} c & d \\ d & c \end{bmatrix} \right)$

ii) Ker $f = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} : a-b=0 \right\}$ i.e. $\left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} ; a \in z \right\}$

Q.46 Show that $S = \{a+b\sqrt{2}; a, b \in z\}$ **for the operations +, × is an integral domain but not a field.** ☞[SPPU : Dec.-14]

Ans. : We have,

$(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2}$

$(a+b\sqrt{2})+(c+d\sqrt{2} = (ac+2bd)+(bc+ad)\sqrt{2}$

Clearly S is commutative ring with unit element 1.

We have to prove S is an integral domain.

Let $(a+b\sqrt{2})(c+d\sqrt{2}) = 0$

$$ac + 2bd = 0 \quad \ldots (Q.46.1)$$

$\therefore$

$$bc + ad = 0 \quad \ldots (Q.46.2)$$

and

Suppose $a = 0$; then $bd = bc = 0$

either $b = 0$ or both $d = c = 0$

Hence, if $a = 0$, $a + b\sqrt{2} = 0$

or $c + d\sqrt{2} = 0$

Assume $a \neq 0$. Multiplying equation (Q.46.1) by d

we have, $acd + 2bd^2 = 0 \quad \ldots (Q.46.3)$

From equation (Q.46.2)

$$ad = -bc$$

Hence substituting this value in equation (Q.46.3)

We have, $-bc^2 + 2bd^2 = 0$

$\Rightarrow b(2d^2 - c^2) = 0$

$\therefore b = 0$ or $c^2 = 2d^2$, i.e. $c = \sqrt{2}\, d$

Since c is an integer, $c^2 = 2d^2$ is true only if $c = d = 0$

Hence if $c^2 \neq 2d^2$, $b = 0$. But $b = 0$ implies $a = 0$

Hence, in any case either $a + b\sqrt{2} = 0$ or $c + d\sqrt{2} = 0$

Hence, S is an integral domain.

To show that S is not a field consider the element $2+\sqrt{2}$. It's multiplicative inverse does not exit in S, for $\left(2+\sqrt{2}\right)\left(c+d\sqrt{2}\right) = 1$

$$\Rightarrow \quad 2c + 2d = 1 \Rightarrow c + d = \frac{1}{2}$$

Absurd, since $c, d \in z$.

Q.47 Let z_8 = {0, 1 ,2, 3, 4, 5, 6, 7 }. Let R is a relation under the operations addition modulo 7 and multiplication modulo 7. Does this system form a ring ? It is a commutative ring ? ☞**[SPPU : Dec.-11]**

Ans. : Consider the following tables,

Table 1 :

$\times_7$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	0
2	0	2	4	6	1	3	5	0
3	0	3	6	2	5	1	4	0
4	0	4	1	5	2	6	3	0
5	0	5	3	1	6	4	2	0
6	0	6	5	4	3	2	1	0
7	0	0	0	0	0	0	0	0

Table 2 :

$+_7$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	0
1	1	2	3	4	5	6	0	1
2	2	3	4	5	6	0	1	2
3	3	4	5	6	0	1	2	3
4	4	5	6	0	1	2	3	4
5	5	6	0	1	2	3	4	5
6	6	0	1	2	3	4	5	6
7	0	1	2	3	4	5	6	0

I) S.T. $(z_8, +_7)$ is an abelian group.

i) From table 2, all element are in z_8 $\therefore$ z_8 is closed w.r.t. $+_7$

ii) Associativity : for all a, b c $\in z_8$.

$a +_7 (b +_7 c) = (a +_7 b) +_7 c$

iii) By observing the first row of table 2. 0 is the additive identity in z_8.

6.7 : Group Codes

Q.48 Explain group code.

Ans. : Let S_n be the set of all binary words of length n. Let $\oplus$ be a binary operation on S_n such that for all x, y $\in S_n$ where

$x = (x_1, x_2 \ldots . x_n)$, $y = (y_1, y_2, \ldots y_n)$,

$x \oplus y = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots . . x_n \oplus y_n)$

Where the operation $\oplus$ denotes the addition modulo 2 on {0, 1} and is given by the following table.

$\oplus$	0	1
0	0	1
1	1	0

The algebraic structure $(S_n, \oplus)$ forms a group in which n tuple of 0's (0, 0, 0, ..., 0) is the identity and each element is its own inverse. In general, any code which is a group under the operation $\oplus$ is called a group code. Group code was first introduced by Hamming and it is very useful in binary encoding techniques.

e.g. if x = (1 0 1 0 1) and y = (0 1 1 0 0)

then $x \oplus y$ = (1 1 0 0 1)

Q.49 Define hamming distance. **[SPPU : Dec.-11, Dec.-15]**

Ans. : Let x be a word is S_n. The weight of x is denoted by w(x) and defined as

w(x) = Number of one's in x

e.g. w (0 0 1 0 1) = 2, w (0 0 0) = 0, w = (1 1 1 1) = 4

Let $x = (x_1, x_2, \ldots . x_n)$, $y = (y_1, y_2, \ldots . y_n)$ be any two elements in $(S_n, \oplus)$. The Hamming distance between x and y is denoted by d(x,y) and defined as

d (x, y) = The number of co-ordinates at which x_i and y_i are different.

e.g. If x = (1 0 1 1 0 1)

y = (0 1 1 1 1 0)

↓ ↓ ↓ ↓

different

$\therefore$ d (x, y) = 4, as x and y have first second, fifth, sixth positions different)

Now $x \oplus y = (1\ 1\ 0\ 0\ 1\ 1)$

$w(x \oplus y) = 4 = d(x, y)$

Thus for any $x, y \in S_n$, $d(x, y) = w(x \oplus y)$

Properties of Hamming Distance :

Let $x, y, z \in (S_n, \oplus)$ then

i) $d(x, y) \geq 0$

ii) $d(x, y) = 0$ iff $x = y$

iii) $d(x, y) = d(y, x)$

iv) $d(x, z) \leq d(x, y) + d(y, z)$

The minimum distance of a code is the minimum of all the distances between district pair of code words.

e.g. Let x (1 1 0 1 1 0), y = (0 0 1 1 1 1), z = (1 0 1 0 1 0)

$\therefore$ d (x, y) = 4, d (y, z) = 3, d (x, z) = 3

Out of 4, 3, 3, minimum is 3.

Therefore the minimum distance between the words x, y, z is 3

By using the weight and minimum distance, a combination of errors can be detected and corrected.

Q.50 Explain generation of codes by using parity checks.

Ans. : In 1950, Hamming developed the first complete error detecting and error correcting encoding procedure. This procedure has been frequently used in computer systems.

Hamming constructed the codes, called Hamming codes by introducing redundant digit called parity digits. In a message, that is n digits long, m digits ($m < n$) are used to represent the information part of the message and the remaining $k = n - m$ digits are used for the detection and correction of errors. These K digits are called parity checks.

Hamming single error detecting codes can be described as follows.

i) The actual message is contained in the first (n–1) digits of a code word of length n and the last digit position is set to 0 or 1 so as to make the entire message contain an even numbers of 1's. Such an encoding procedure is called a even parity check.

ii) Odd parity check can be used by making the entire message containing an odd no. of 1's. e.g. In even parity check {00, 10, 11} becomes {000, 101, 110}. In odd parity check { 00, 01, 10, 11}

becomes {001, 010, 100, 111}

The code words of length n in which information is contained m digits ($m < n$) and remaining $k = n - m$ digits are parity checks, can be generated by using $k \times n$ matrix H. This matrix is called parity check matrix, where elements are from set {0, 1} A single error correcting code of length n generated by H with k parity check is given by

$$2^k \geq n + 1 = (k + m) + 1$$

$$\therefore \quad m \leq 2^k - k - 1$$

The number of code words generated by H is $2^m = 2^{n-k}$ and the code generated in this way called the Hamming code.

Theorem 1 : Let H be a parity check matrix which consists of k rows and n columns. Then the set of words $x = (x_1, x_2, x_3, \ldots x_n)$ which belongs to the following set.

$C = \{ x \mid xH^t = 0 \pmod 2\}$ is a group code under the operation $\oplus$ (addition modulo 2) where H^t = Transpose of matrix H.

Theorem 2 : The parity check matrix H generates a code word of weight q iff $\exists$ a set of columns of H such that their k - tuple sum is zero.

For the parity check matrix H of order $k \times n$.

Where n = Length of code word

k = Number of parity check bits

The information digits will be $m = n - k$. The number of code words generated is $2^m = 2^{n-k}$. Consider the following steps for the generation of code words.

Step 1 : Find the system of equations from $x \cdot H^t = 0$.

Step 2 : Find the values of parity check bits interms of information digits from the equations obtained in step 1.

Step 3 : Give values 0 or 1 to information digits and calculate the values of parity check bits according to step 2. The binary words obtained in this way will be the required code words generated by H.

To find the number of errors defected and corrected first find the columns of H whose sum (addition modulo 2) is zero. The number of theses columns is equal to the minimum weight of the code and which is equal to the minimum distance of the code.

Q.51 Find the minimum distance of an encoding function $e : B^2 \rightarrow B^5$ given as .
e (0 0) = 00000, e (0 1) = 1 0 0 1 1, e (1 0) = 0 1 1 1 0,
e (1 1) = 1 1 1 1 1. ☞[SPPU : Dec.-06]

Ans. :

d [e (0 0), e (0 1)] = 3 d [e (0 0), e (1 1)] = 5
d [e (0 0), e (0 1)] = 3 d [e (0 0), e (1 0)] = 3
d [e (0 1), e (1 0)] = 4 d [e (0 1), e (1 1)] = 2
d [e (1 0), e (1 1)] = 2

The minimum along all distances is 2.

Thus the minimum distance of an encoding is 2.

Q.52 What is Hamming function (distance) ? Find the distance between the code words of C = { (0 0 0 0), (0 1 0 1), (1 0 1 1), (0 1 1 1)} Rewrite the message by adding even parity check bit and parity check bit. ☞[SPPU : Dec.-11, Marks 5]

Solution : Please refer Q.50 for the definition. We have

d [e (0 0 0 0), e (0 1 0 1)] = 2 d [e (0 0 0 0), e (1 0 1 1)] = 3
d [e (0 0 0 0), e (0 1 1 1)] = 3 d [e (0 1 0 1), e (1 0 1 1)] = 3
d [e (0 1 0 1), e (0 1 1 1)] = 1 d [e (1 0 1 1), e (0 1 1 1)] = 2

Even parity check bit of c is

{(0 0 0 0 0), (0 1 0 1 0), (1 0 1 1 1), (0 1 1 1 1)}

Odd parity check bit of c is

{(0 0 0 0 1), (0 1 0 1 1), (1 0 1 1 0), (0 1 1 1 0)}

Q.53 Given the parity check matrix $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$ **find the minimum distance of code generated by H. How many errors can it detect and correct.** ☞[SPPU : Dec.-15, Marks 5]

Ans. : From the given matrix H, select minimum number of column whose sum is zero.

$\therefore$ Consider columns $h_1 = \begin{bmatrix}1\\0\\1\end{bmatrix}$, $h_2 = \begin{bmatrix}1\\1\\0\end{bmatrix}$, $h_3 = \begin{bmatrix}0\\1\\1\end{bmatrix}$

The sum of these columns

$$h_1 \oplus h_2 \oplus h_3 = \begin{bmatrix}0\\0\\0\end{bmatrix}$$

Hence the minimum weight of the code is 3 which is equal to its minimum distance.

We know that the code can detect all combinations of k or fever errors iff the minimum distance between any two code words is at least k +1.

Here minimum distance is $3 = k+1 \Rightarrow k = 2$.

$\therefore$ This code can detect 2 or less errors.

Also it can correct k errors if the minimum distance is 2k +1.

$\therefore \quad 2k + 1 = 3 \Rightarrow k = 1$

This code can correct only one error.

Therefore this is a single error correcting code.

Q.54 Find the number of code words generated by the parity check matrix H given by $H = \begin{bmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{bmatrix}$ **find all the code words generated.** **[SPPU : Dec.-12, Marks 5]**

Ans. : The parity check matrix is

$$H = \begin{bmatrix}1&1&0&1&0&0\\0&1&1&0&1&0\\1&0&1&0&0&1\end{bmatrix}_{3\times6}$$

H is of order 3×6. Hence the length of the code word is 6 in which last three digits are parity check bits. The information digits are

$$M = n - k = 6 - 3 = 3$$

$\therefore$ The matrix H will generate. $2^m = 8$ code words.

They are the solution of $x \cdot H^t = 0$.

$$[x_1\ x_2\ x_3\ x_4\ x_5, x_6] \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0\ \ 0\ \ 0]$$

$$\Rightarrow \begin{aligned} x_1 + x_2 + \quad + x_4 + \quad &= 0 \\ x_2 + x_3 + \quad + x_5 + \quad &= 0 \\ x_1 + \quad + x_3 + \quad + x_6 &= 0 \end{aligned}$$

$$x_4 = x_1 + x_2$$

$$\Rightarrow \begin{aligned} x_5 &= x_2 + x_3 \\ x_6 &= x_1 + \quad + x_3 \end{aligned}$$

By giving different combinations of 0 and 1 to x_1, x_2, x_3, we get the following code words.

x_1	x_2	x_3	x_4	x_5	x_6
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	1	1	0
0	1	1	1	0	1
1	0	0	1	0	1
1	0	1	1	1	0
1	1	0	0	1	1
1	1	1	0	0	0

Hence the code is

C { (0 0 0 0 0) (0 0 1 0 1 1) (0 1 0 1 1 0)
(0 1 1 1 0 1) (1 0 0 1 0 1)
(1 0 1 1 1 0) (1 1 0 0 1 1) (1 1 1 0 0 0)}

END...

SOLVED MODEL QUESTION PAPER (In Sem)
Discrete Mathematics
S.E. (IT) Semester - III [As Per 2019 Pattern]

Time : 1 Hour] **[Maximum Marks : 30**

N.B. : ***i) Attempt Q.1 or Q.2 and Q.3 or Q.4.***

ii) Neat diagrams must be drawn wherever necessary.

iii) Figures to the right side indicate full marks.

iv) Assume suitable data, if necessary.

Q.1 a) *Draw Venn diagram and prove the expression. Also write the dual of each of the given statements.*

i) $(A \cup B \cup C)^C = (A \cup C)^C \cap (A \cup B)^C$

ii) $(U \cap A) \cup (B \cap A) = A$ **(Refer Q.6 of Chapter - 1)** **[5]**

b) *Prove by mathematical induction for* $n \geq 1$.

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

(Refer Q.19 of Chapter - 1) **[5]**

c) *Let p denote the statement, "The material is interesting'. q denote the statement, "The exercises are challenging", and r denote the statement, "The course is enjoyable".*

Write the following statements in symbolic form :

i) The material is interesting and exercises are challenging.

ii) The material is interesting means the exercises are challenging and conversely.

iii) Either the material is interesting or the exercises are not challenging but not both.

iv) If the material is not interesting and exercises are not challenging, then the course is not enjoyable.

v) The material is uninteresting, the exercises are not challenging and the course is not enjoyable. **(Refer Q.33 of Chapter - 1)** **[5]**

OR

Q.2 a) *State and prove the principle of inclusion and exclusion for sets.* **(Refer Q.11 of Chapter - 1)** [5]

b) *Show that $n^4 - 4n^2$ is divisible by 3 for all $n \geq 2$.*
(Refer Q.25 of Chapter - 1) [5]

c) *Prove by truth table $p \rightarrow (Q \vee R) \equiv (P \rightarrow Q) \vee (P \rightarrow R)$.*
(Refer Q.40 of Chapter - 1) [5]

Q.3 a) *How many 4 digits numbers can be formed by using the digits 2, 4, 6, 8 when repetition of digits are allowed ?*
(Refer Q.12 of Chapter - 2) [5]

b) *A committee of 5 people is to be formed from a group of 4 men and 7 women. How many possible committees can be formed if at least 3 women are on the committee ?* **(Refer Q.25 of Chapter - 2)** [5]

c) *Three students A, B and C are swimming in the race A and B have same probability of winning and each each is twice as likely to win as C. Find the probability that :*
i) B wins ii) C wins iii) B or C wins **(Refer Q.60 of Chapter - 2)** [5]

OR

Q.4 a) *Determine the number of ways in which 5 software engineers and 6 electronics engineers can be sitted at a round table so that no two software engineers can sit together.* **(Refer Q.19 of Chapter - 2)** [5]

b) *A bag contains 3 red and 5 black balls and a 2^{nd} bag contains 6 red and 4 black balls. A ball is drawn from each bag. Find the probability that 1) one is red and other is black. 2) both are red 3) both are black.* **(Refer Q.48 of Chapter - 2)** [5]

c) *The contents of urns I, II, III are as follows respectively.*
I → 1 white, 2 black, 3 red balls
II → 2 white, 1 black, 1 red balls
III → 4 white, 5 black, 3 red balls
One urn is chosen at random and two balls are drawn. They happen to be white and red.
What is the probability that they come from urn I, II or III ?
(Refer Q.55 of Chapter - 2) [5]

JUNE - 2022 [END SEM] [5869]-281 | Solved Paper

Course 2019

Time : $2\frac{1}{2}$ Hours] **[Max. Marks : 70**

Instructions to the candidates :

1) Answer Q.1 or Q.2, Q.3 or Q.4, Q.5 or Q.6, Q.7 or Q.8.

2) Figures to the right indicate full marks.

3) Draw neat diagrams wherever necessary.

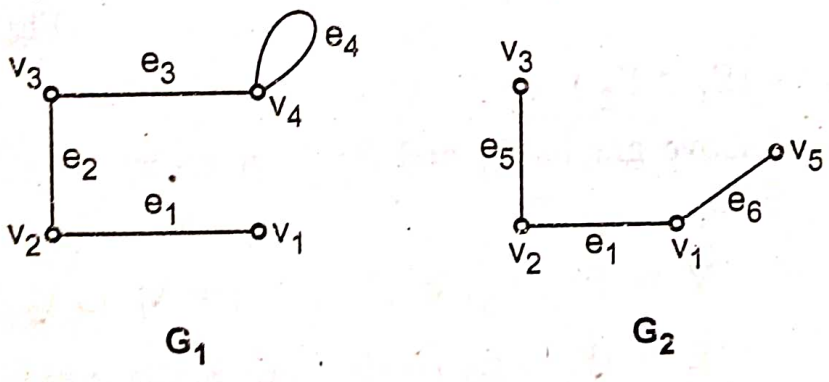
4) Use of scientific calculators is allowed.

5) Assume suitable data if necessary.

Q.1 a) *What are various operations on graph ? Explain it in detail ?* **[4]**

Ans. : A) Intersection of two graphs : The intersection of two graphs $G_1 (V_1, E_1)$ and $G_2 (V_2, E_2)$ is a graph G (V, E) whose vertex set is $V = V_1 \cap V_2$ and edge set is $E = E_1 \cap E_2$. The intersection of G_1 and G_2 is denoted by $G_1 \cap G_2$.

e.g.



G_1 G_2

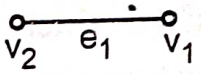
Fig. 1

$V_1 = \{v_1, v_2, v_3, v_4\}$ $V_2 = \{v_1, v_2, v_3, v_5\}$

$E_1 = \{e_1, e_2, e_3, e_4\}$ $E_2 = \{e_1, e_5, e_6\}$

Therefore $G = G_1 \cap G_2$ (v, E) where

$V = V_1 \cap V_2 = \{v_1, v_2, v_3\}$, $E = E_1 \cap E_2 = \{e_1\}$

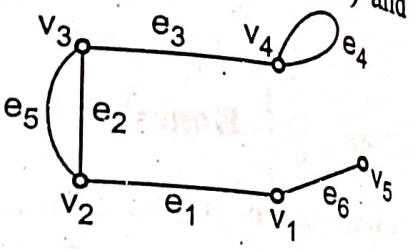


$G_1 \cap G_2$

Fig. 2

B) Union of two graphs : Let $G_1 (V_1, E_1)$, $G_2 (V_2, E_2)$ be two graphs. The union of G_1 and G_2 is denoted by $G_1 \cup G_2 = G (v, E)$ and it is a graph whose vertex set is $V = V_1 \cup V_2$ and Edge set is $E = E_1 \cup E_2$

Consider the graphs G_1 and G_2 as shown in above example :



$G_1 \cup G_2$

Fig. 3

The union of G_1 and G_2 is given by G (v, E)

where $V = V_1 \cup V_2 = \{v_1, v_2, v_3, v_4, v_5\}$

$V = V_1 \cup V_2 = \{e_1, e_2, e_3, e_4, e_5, e_6\}$

Note : Both graphs G_1 and G_2 are subgraphs of $G_1 \cup G_2$.

C) The ring sum of two graphs : The ring sum of two graphs $G_1 (V_1, E_1)$ and $G_2 (V_2, E_2)$ is denoted by $G = G_1 \oplus G_2$ (V, E) whose vertex set is $V = V_i \cup V_2$ and the edge set consists of those edges which are either in E_1 or in E_2 but not in both i.e.

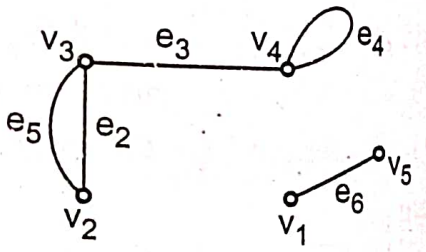


Fig. 4

$E = (E_1 \cup E_2) - (E_1 \cap E_2)$.

The ring sum of above graphs G_1 and G_2 is given by $G (V, E) = G_1 \oplus G_2$

$V = \{v_1, v_2, v_3, v_4, v_5\} = V_1 \cup V_2$

$E = (E_1 \cup E_2) - (E_1 \cap E_2) = \{e_2, e_3, e_4, e_5, e_6\}$

D) Sum of two graphs : The sum of two vertex disjoint graphs $G_1 (V_1, E_1)$ and $G_2 (V_2, E_2)$ is denoted by $G_1 + G_2 = G (V, E)$ is defined as the graph whose vertex set is $V (G_1 \cup G_2)$ and consisting of edges which are in G_1 or G_2 together with the edges obtained by joining each vertex of G_1 to each vertex of G_2. Thus $G_1 + G_2$ is nothing but the graph $G_1 \cup G_2$ in which each vertex of G_1 is joined to each vertex of G_2 by an edge.

e.g. If

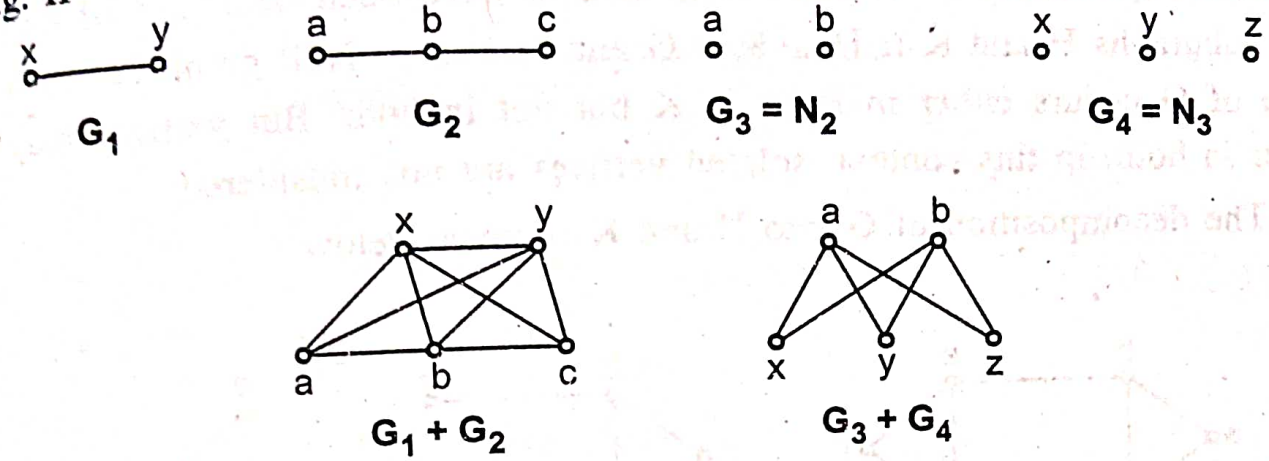


Fig. 5

Note : The sum $N_m + N_n$ of null graphs is nothing but the complete bipartite graph $K_{m, n}$.

E) Product of two graphs : Let $G_1 (V_1, E_1)$ and $G_2 (V_2, E_2)$ be two vertex disjoint graphs then the product of G_1 and G_2 is denoted by $G_1 \times G_2 = G (V, E)$ is a graph whose vertex set is $V = V_1 \times V_2$ and two edges (x_1, x_2) and (y_1, y_2) are adjacent if $x_1 = y_1$ and x_2 is adjacent to y_2 in G_2 or $x_2 = y_2$ and x_1 is adjacent to y_1 in G_1.

e.g. If

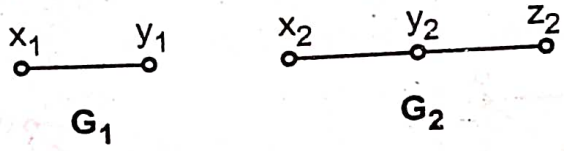


Fig. 6

Then $G_1 \times G_2$ is given below :

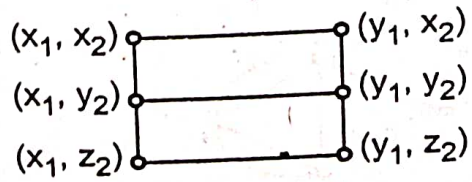


Fig. 7

F) Decomposition : A graph G is said to have been decomposed into two subgraphs H and K if $H \cup K = G$ and $H \cap K =$ Null graph i.e. each edge of G occurs either in H or in K but not in both. But vertices may occur in both. In this context isolated vertices are not considered.

e.g. The decomposition of G into H and K is given below :

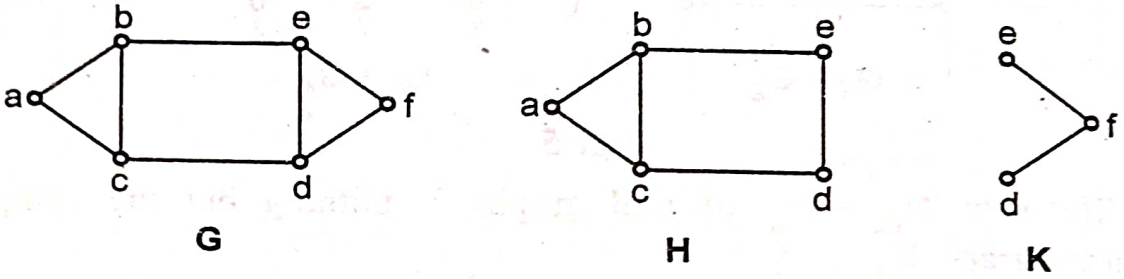


Fig. 8

G) Fusion of vertices : A pair of vertices a and b in a graph G are said to be fused if a and b are replaced by a single new vertex say c such that every edge that was incident on either a or b or both is incident on the new vertex c. The fusion of two vertices do not change the number of edges but reduced number of vertices by 1.

e.g.

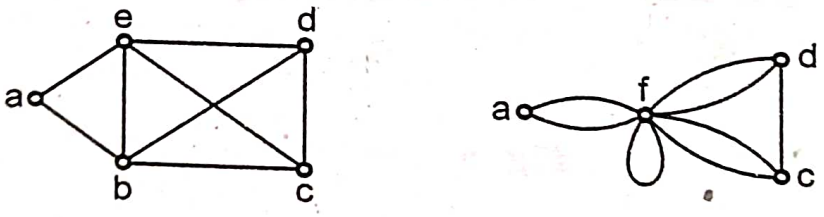


Fig. 9

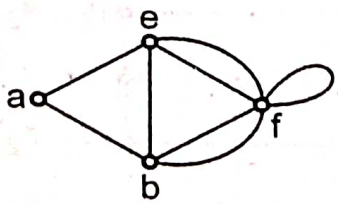
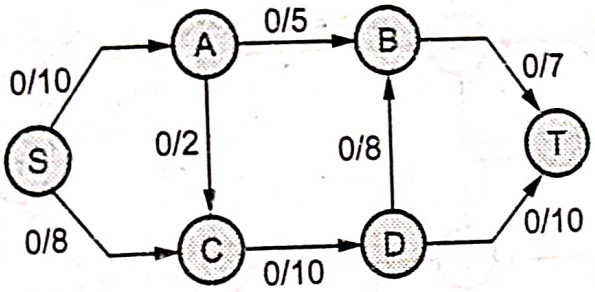


Fig. 10

b) *Find the maximum flow in the given network.* [8]

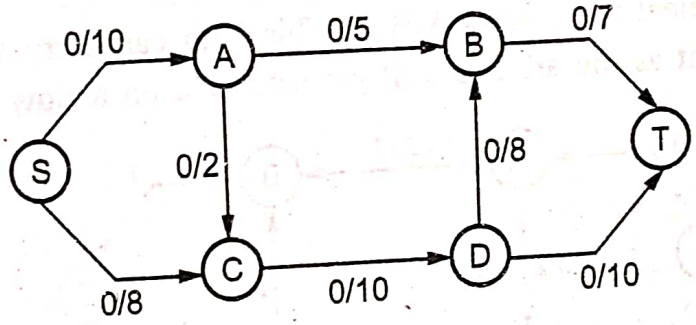
Network (G)



Flow = 0

Fig. 11

Ans. :

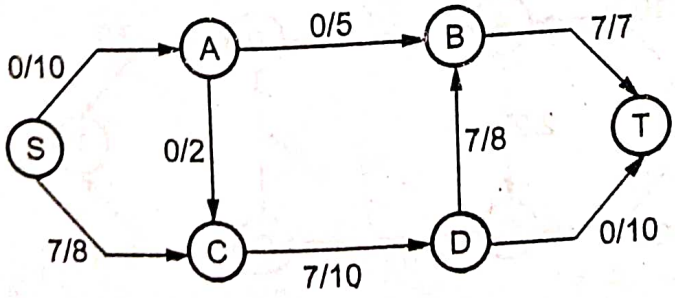


Flow = 0

Network (G)

Fig. 12

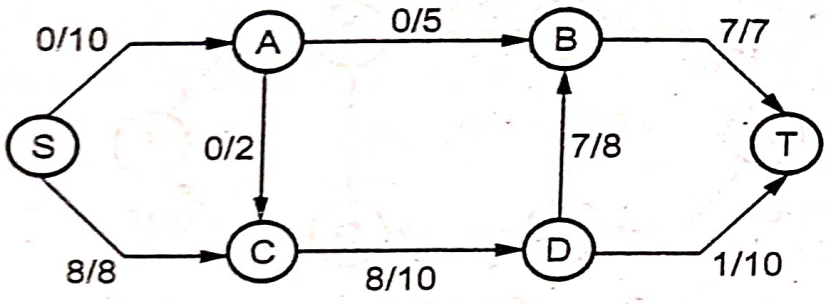
Step 1 : Select an arbitrary path S-C-D-B-T from the source vertex S to sink vertex T. This path can carry a flow of 7 units as the arc BT can carry a maximum of 7 units.



Flow = 0 + 7

Fig. 13

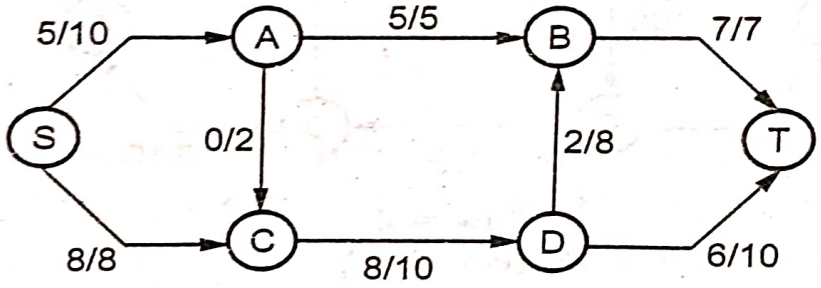
Step 2 : Now, select the path S-C-D-T. This path can carry a flow of 01 unit as the arc D.T will get saturated in a flow of 1 unit.



Flow = 0 + 1

Fig. 14

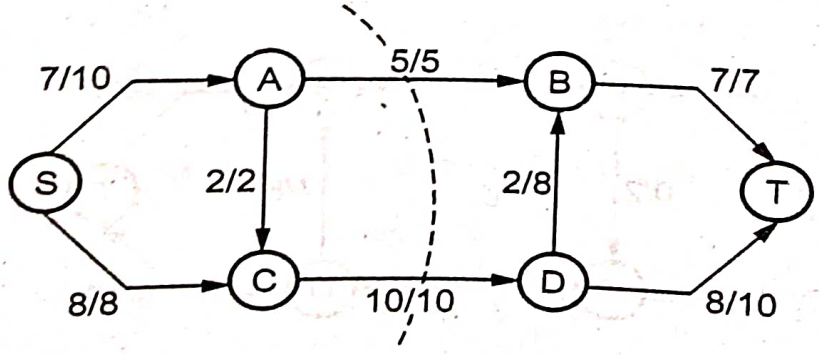
Step 3 : Now, select the path S-A-B-T. This path can carry an additional flow of unit 5 unit as the arc AB will get saturated on a flow of 5 unit.



Flow = 0 + 1

Fig. 15

Step 4 : Now, select the path S-A-C-D-T. This path can carry a flow of 2 units as the arc AC will get saturated on a flow of 2 units.



Flow = 0 + 5

Fig. 16

No more paths left, ∴ Maximum flow = 15

c) *Find the shortest path using Dijikstra's algorithm.* [6]

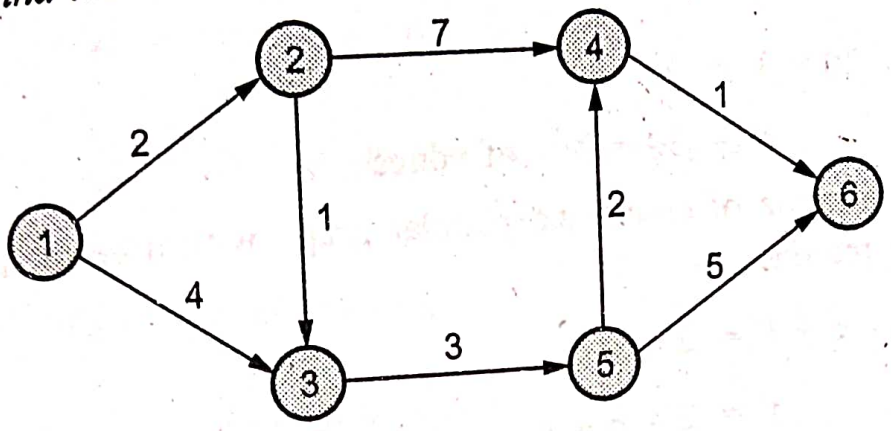


Fig. 17

Ans. : Step 1 : Select any arbitrary path of given network. Let 1 3 5 6 path selected 1 vertex is source and 6 vertex is sink. 35 arc can carry maximum of 3 units.

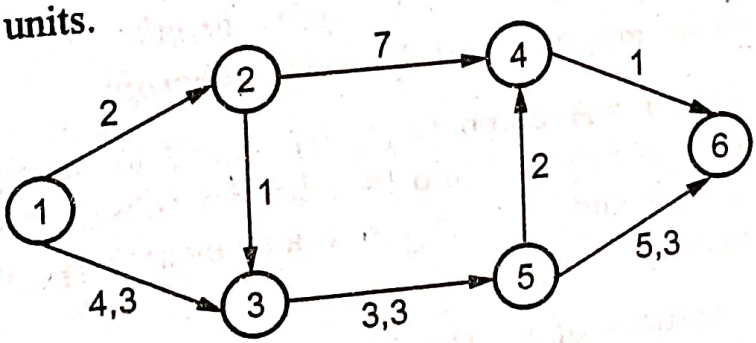


Fig. 18

Step 2 : Now select 1 2 4 6 path. This path can carry a flow of 2 units as the arc 12 will get saturated on a flow of 2 units.

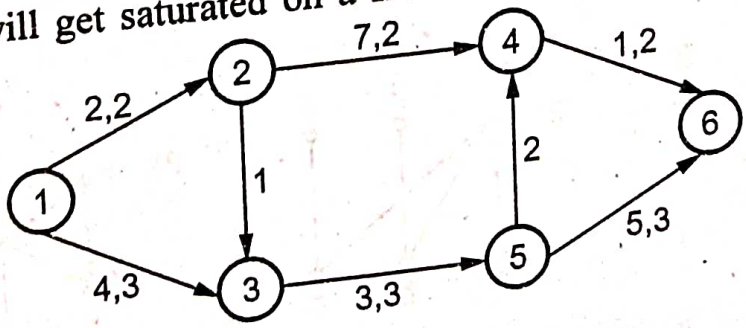


Fig. 19

OR

Q.2 a) *Let 'G' be a connected planar graph with 20 vertices and the degree of each vertex is 3. Find the number of edges and regions in the graph.* [6]

Ans. : Let G be a connected planar graph with n = 20 vertices.

i.e. D(v) = 3.

Using handshaking Lemma

$$\sum_{i=1}^{20} d(V_i) = 2e$$

$$\Rightarrow \quad 20 \times 3 = 2e$$

$$\Rightarrow \quad e = 30 = \text{No. of edges}$$

Using Euler's formula of connected plannar graph with n vertices, e edges and f faces or regions

$$n - e + f = 2$$

$$f = 2 - n + e$$

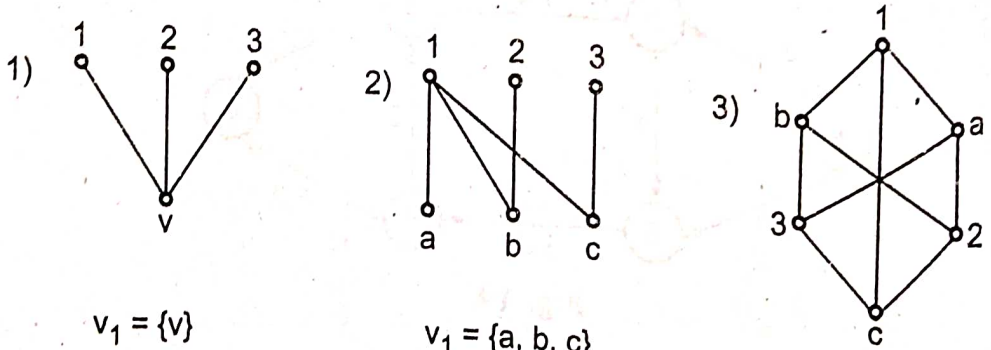
$$2 - 20 + 30 = 12$$

b) *Explain the following types of graphs with the help of examples : i) Bipartite graph ii) Complete graph iii) Regular graph iv) Spanning subgraph* [6]

Ans. : Bipartite graph : A graph G (v, E) is said to be bipartite graph if its vertex set can be partitioned into two disjoint subsets say v_1 and v_2 such that $v_1 \cup v_2 = v$ and $v_1 \cap v_2 = \phi$ and every edge of G joins a vertex of v_1 to a vertex of v_2.

In Bipartite graph, vertices of v_1 should not be adjacent. It is free from loops.

Following graphs are bipartite graphs



$v_1 = \{v\}$
$v_2 = \{1, 2, 3\}$

$v_1 = \{a, b, c\}$
$v_2 = \{1, 2, 3\}$

$v_1 = \{1, 2, 3\}$
$v_2 = \{a, b, c\}$

Fig. 20

Complete graph : A simple graph G in which every pair of distinct vertices are adjacent is called a complete graph. If G is a complete graph on n vertices then it is denoted by K_n.

In a complete graph, there is an edge between every pair of distinct vertices.

In graph K_n, every vertex is adjacent to remaining n–1 vertices so degree of each vertex is n – 1.

Thus K_n is a (n – 1) - regular graph.

K_n has exactly $\frac{n(n-1)}{2}$ edges.

Consider the following examples :

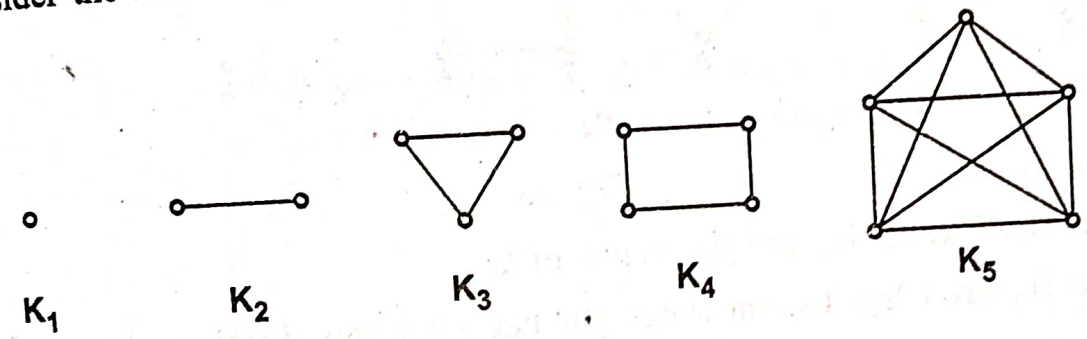


Fig. 21

Regular graph : A graph G is said to be r-regular graph if every vertex of G has degree r.

i) Regular graph of degree zero is called null graph.

ii) A regular graph of degree 3 is called cubic graph.

e.g.

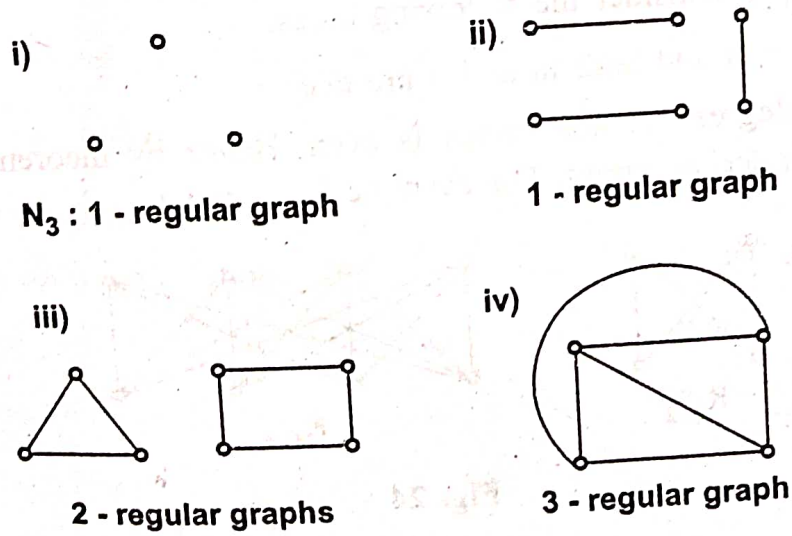


Fig. 22

Spanning subgp : Let G (V, E) be any graph. A subgraph H of a graph G is said to be spanning subgraph if V (G) = V (H).

Example : Let G be the following graph :

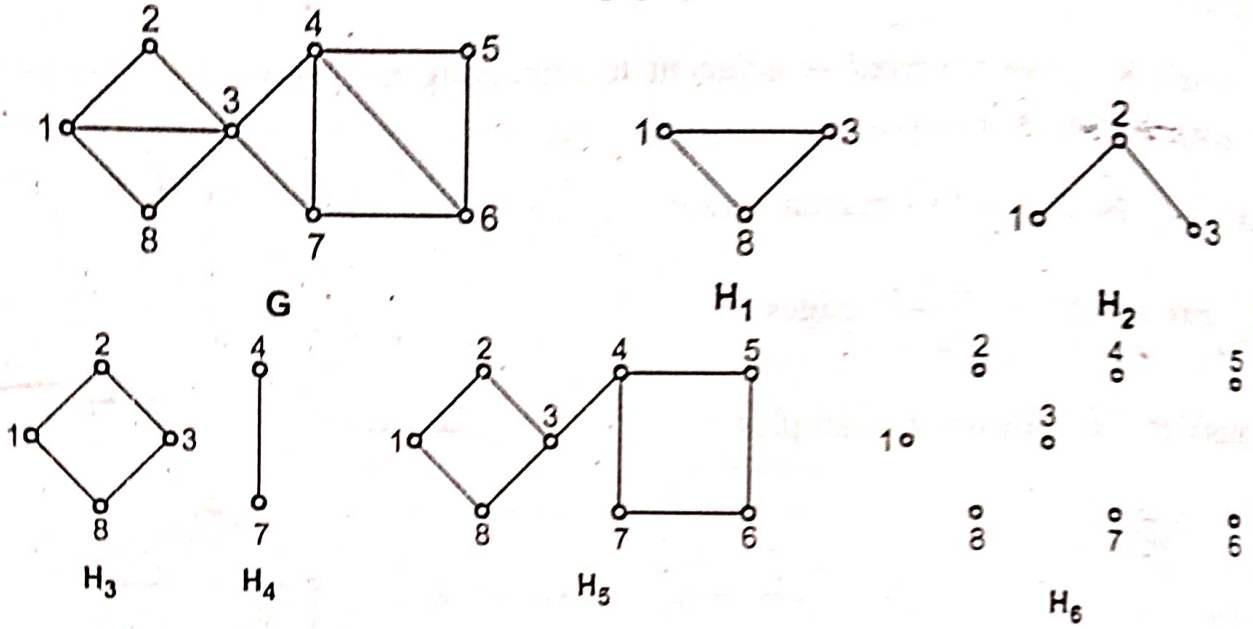


Fig. 23

Graphs H_1, H_2, ... H_6 are subgraphs of G.

H_1 and H_2 are edge disjoint subgraphs but not vertex disjoint subgraphs.

H_3 and H_4 are vertex disjoint subgraphs as well as edge disjoint subgraphs.

Subgraphs H_5 and H_6 are spanning subgraphs of G as V (H_5) = V (H_6) = V (G).

c) *Find under what conditions $K_{m,n}$ the complete bipartite graph will have an Eulerian circuit.* **[6]**

Ans. : In $K_{m, n}$ consider the following cases.

Case 1 : m = n and both m and n are even :

In this case, degree of each vertex is even, Hence by theorem 1, $K_{m, n}$ will have an Eulerian circuit. For example $K_{1, 2}$ and $K_{4, 4}$.

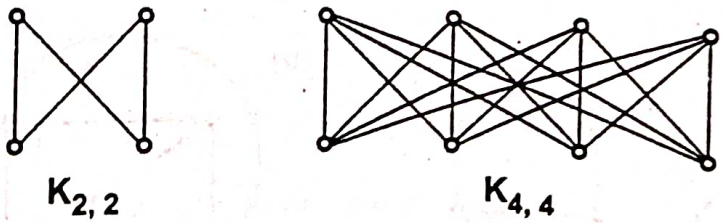
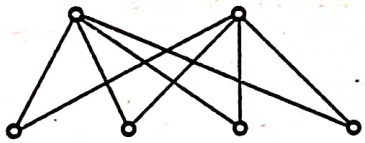


Fig. 24

Case 2 : If m = n and m, n are odd :

In this case degree of each vertex is odd. Hence Eulerian circuit will not exist.



$K_{2,4}$

Fig. 25

Case 3 : If $m \neq n$ but m and n are even :

In this case, degree of each vertex is even. So there exists an Eulerian circuit.

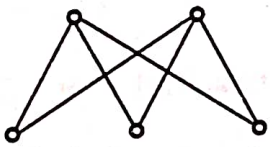


Fig. 26

Case 4 :

If $m \neq n$ and either m is odd or n is odd or both are odd : then graph will have vertices of odd degree. Hence Eulerian circuit does not exist. e.g. $K_2, 3$.

Q.3 a) *Suppose that the relation R on a set is represented by the matrix M_R. Is reflexive, symmetric and/or anti-symmetric ?* **[6]**

$$\begin{vmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{vmatrix}$$

Ans. : Let, A = {1,2,3} R be a relation defined on A. M_R is relation matrix.

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \end{array}$$

$$R = \{(1,1), (1,2), (2,1), (2,2), (2,3), (3,2), (3,3)\}$$

i) $\because$ (1,1), (2,2), (3,3) $\in$ R

So that R is reflexive.

ii) Here, R is symmetric because for all (a,b) $\in$ R there is aRb and bRa.

iii) Here, R is anti-symmetric because (a,b) $\in$ R (b,a) $\in$ R and a = b.

b) *Find the homogeneous solution for the recurrence relation* **[6]**

$A_n - 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ *with* $a_0 = 2,\ a_1 = 5,\ a_2 = 15$

Ans. : We have

$$a_n - 6\,a_{n-1} + 11\,a_{n-2} + 6\,a_{n-3} = 0 \qquad \ldots (1)$$

Step 1 : The characteristic equation is

$$\alpha^3 - 6\alpha^2 + 11\alpha - 6 = 0$$

$\alpha = 1$ is a trial root

$\therefore$ By synthetic division method

1	1	− 6	11	− 6
		1	− 5	6
	1	− 5	6	0

$$\therefore \quad (\alpha - 1)(\alpha^2 - 5\alpha + 6) = 0$$

$$(\alpha - 1)(\alpha - 2)(\alpha - 3) = 0$$

$\alpha = 1, 2, 3$ are real and distinct roots

$\therefore$ It's homogeneous solution is

$$a_n^{(h)} = A_1\,1^n + A_2\,2^n + A_3\,3^n \qquad \ldots (2)$$

Step 2 : But given that $a_0 = 2$, $a_1 = 5$, $a_2 = 15$

$\therefore$

$$a_0 = A_1 + A_2 + A_3 \Rightarrow 2 = A_1 + A_2 + A_3 \qquad \ldots(3)$$

$$a_1 = A_1 + 2\,A_2 + 3\,A_3 \Rightarrow 5 = A_1 + 2\,A_2 + 3\,A_3 \qquad \ldots(4)$$

$$a_2 = A_1 + 4\,A_2 + 9\,A_3 \Rightarrow 15 = A_1 + 4\,A_2 + 9\,A_3 \qquad \ldots(5)$$

Equation (4) + Equation (3) and equation (5) − Equation (3)

$\Rightarrow$

$$3 = A_2 + 2\,A_3 \qquad \ldots (6)$$

and

$$13 = 3\,A_2 + 8\,A_3 \qquad \ldots (7)$$

Equation (7) − 3 × Equation (6)

$$4 = 0 + 2\,A_3 \Rightarrow \boxed{A_3 = 2}$$

Equation (6) $\Rightarrow$ $A_2 = 3 - 2\,A_3 = 3 - 4 = -1$

Equation (3) $\Rightarrow$ $A_1 = 2 - A_2 - A_3 = 2 - (-1) - 2 = 1$

Hence $a_n^{(h)} = 1 + (-1)\,2^n + 2\,(3)^n$

c) *Let f(x) = x + 2, g(x) = x – 2, h(x) = 3x, for x ε R where R is the set of real numbers Find i) gof ii) fog iii) fof iv) hog v) gog.* [5]

Ans. :

i) $gof(x) = g[f(x)] = g[x + 2] = x + 2 - 2 = x$

ii) $fog(x) = f[g(x)] = f[x - 2] = x - 2 + 2 = x$

iii) $fof(x) = f[f(x)] = f[x + 2] = x + 2 + 2 = x + 4$

iv) $hog(x) = h[g(x)] = h[x - 2] = 3(x - 2) = 3x - 6$

v) $gog(x) = g[g(x)] = g[x - 2] = x - 2 - 2 = x - 4$

OR

Q.4 a) *Find relation matrix,* [6]

i) If A = {1,2, 3, 4, 5, 6} and a R b if a divides b for a, b ε A.

ii) R = {(a, b) /a < b} for a, b ε A.

Ans. : i) R = {(1, 2} (1, 3), (1, 4), (1, 5), (1, 6), (2, 4) (2, 6), (3, 6), (1, 1) (2, 2), (3, 3), (4, 4), (5, 5) (6, 6)}

$$\therefore \quad \text{Relation Matrix} = M_R = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{6\times6} \end{array}$$

i) We have $A = \{1, 2, 3, 4, 5, 6\}$

$R = \{(a, b)/a(b, \forall, a, b \in A)\}$

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

$(2, 4)\ (2, 5)\ (2, 6)\ (3, 4)\ (3, 5)\ (3, 6)$

$(4, 5)\ (4, 6)\ (5, 6)\}$

Relation matrix is M =

$$\begin{array}{c} \\ 1 \\ 2 \\ \\ \\ \\ \end{array}\begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}_{6\times 6} \end{array}$$

b) *Let A = {1, 2, 3, 4}, B = {a, b}, and R = {(1, a), (2, a), (3, a), (4, a)}, S = {(4, a), (4, b), (3, a), (3, b)}*
Find : i) A×B ii) ~R iii) ~S iv) ~R ∪ ~S **[6]**

Ans. : A = {1, 2, 3, 4} and B = {a, b}

R = {(1, a), (2, a), (3, a), (4, a)}

S = {(4, a), (4, b), (3, a), (3, b)}

i) $A \times B$ = {(1, a), (1, b), (2, a), (2, b), (3, a), (3, b), (4, a), (4, b)}

ii) ~R = (A × B) – R = {(1, b), (2, b), (3, b), (4, b)}

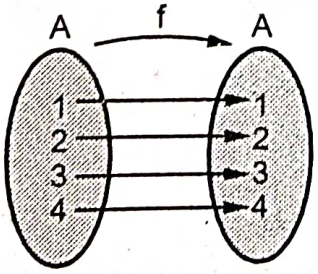
iii) ~S = (A × B) – S = {(1, a), (1, b), (2, a), (2, b)}

iv) ~R ∪ ~S = {(1, a), (1, b), (2, a), (2, b), (3, b), (4, b)}.

c) *Describe : i) Identity function ii) Composite function iii) Inverse function* **[5]**

Ans. : i) Identify function : Let A be any non empty set and function f : A → A is said to be the identity function if f(x) = x, ∀ x ∈ A.

e.g.



f : A → A is the identity function

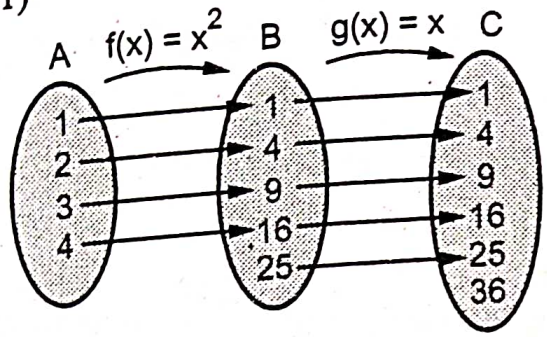
Fig. 27

ii) Composite function : Let f : A → B and g : B → C be two functions.

The composite function of f and g is denoted by gof and defined as gof : A → C is a function such that (gof) (a) = g[f(a)] ∀ a ∈ A.

Note : gof is defined only when the range of f is a subset of the domain of g.

e.g. 1)



Therefore gof : A ⟶ C

gof (1) = g[f(1)] = g(1) = 1
gof (2) = g[f(2)] = g(4) = 4
gof (3) = g[f(3)] = g(9) = 9
gof (4) = g[f(4)] = g(16) = 16

Fig. 28

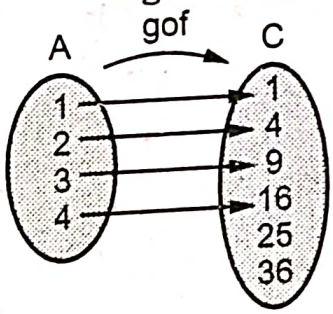


Fig. 29

iii) Inverse function : Let a function f : A → B be a bijective function then f^{-1} : B → A is called the inverse mapping of f and defined as $f(b)^{-1} = a$ iff f(a) = b

It is also known as **invertible mapping.**

Q.5 a) *Find the prime factorization of each of the following integer.* **[6]**

i) 6647 ii) 45500 iii) 10 !

Ans. : i) The prime factors are : 17 × 17 × 23 written in exponential form : $17^2 \times 23^1$

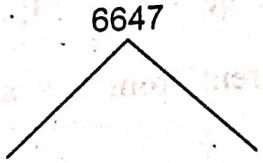


Fig. 30

ii) Prime factors of 45500 = 2, 2, 5, 5, 5, 7, 13 written in experimential form = $2^2 \times 5^3 \times 7 \times 13$

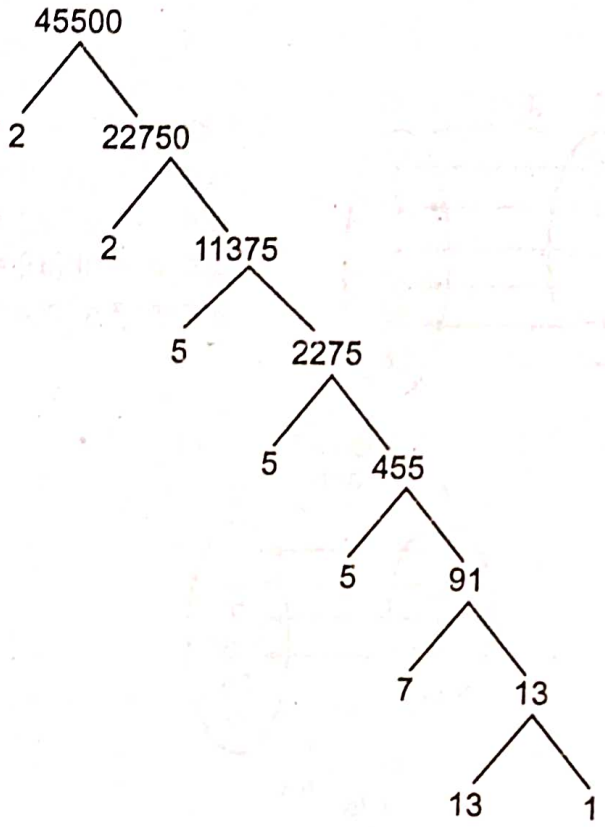


Fig. 31

iii) $10! = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$

$= 2^8 \times 3^4 \times 5^2 \times 7^1$

We can count the no. of factors of 10! which will be $(8+1) \times (4+1) \times (2+1) \times (1+1) = 270$

For each of the factor d of any number x, we can get x by multiplying d by $\frac{x}{d}$ where $\frac{x}{d}$ is another factor of x - 50, number of ways we can choose (a,b) such that a × b = 10! will be $\frac{270}{2} = 135$. In multiplication there is no need to consider a × b different from b × a, otherwise answer would be 270.

b) *Find integers p and q such that 51p + 36q = 3 using Extended Euclidian algorithm. Also find GCD.* **[6]**

Ans. : By Euclids Lemma, for integers a and b s.t a > b ... b and r s.t. $a = bq + r$ where $0 \leq r \leq b$

Take $a = 51$ and $b = 36$

$$\therefore \quad 51 = 36 \times 1 + 15 \qquad \ldots(1)$$

for 36 and 15 we have $36 = 15 \times 2 + 6$ ...(2)

$$15 = 6 \times 2 + 3 \qquad \ldots(3)$$

$$6 = 3 \times 2 + 0$$

The remainder has zero ∴ Our procedure stops here and by back substitution.

$$3 = 15 - 6 \times 2 \qquad \text{by equation (3)}$$

$$= 15 - (36 - 15 \times 2) \times 2 \qquad \text{by equation (2)}$$

$$= 15 - 36(2) + 15(4)$$

$$= 15(5) - 36(2) \qquad \text{by equation (1)}$$

$$= [51 - 36(1)]\ (5) - 36(2)$$

$$= 51(5) - 36(5) - 36(2)$$

$$3 = 51(5) - 36(7)$$

$$\therefore \quad 3 = 51p + 36(q)$$

$$\therefore \quad \boxed{p = 5} \text{ and } \boxed{q = -7}$$

and gcd of 51 and 36 = 3

c) *Find the values of the following using modular arithmetic.* **[6]**

i) 77 mod 9 *ii) 3110 mod 13*

Ans. : i) We first divide the dividend (77) by the divisor (9)

2nd multiply the whole part of the quotient in the previous step by the divisor (9).

Then, finally subtract answer in the 2nd step from the dividend (77) to get the answer.

$$\frac{77}{9} = 8.555556$$

$$8 \times 9 = 72$$

$$77 - 72 = 5$$

Thus the answer is 5.

ii) We first divide the dividend (3110) by the divisor (13)

2^{nd} we multiply the whole part of the quotient in the previous step by the divisor (13).

Then, finally subtract the answer in 2^{nd} step from the dividend (3110) to get the answer.

$$\frac{3110}{13} = 239.230769$$

$$239 \times 13 = 3107$$

$$3110 - 3107 = 3$$

Thus, the answer is 3.

OR

Q.6 a) *Solve the following using Fermat's Little theorem.* **[6]**

i) 7^{69} *mod 23* *ii)* 3^{101} *mod 13*

Ans. : i) $7^{69} = y \bmod 23$, here $n = 7$ and $p = 23$

By Fermat's Little theorem is,

$$n^{p-1} = 1 \bmod p$$

By substituting the values of a and p and rewrite the equation :

$$7^{(23-1)} = 1 \bmod 23$$

$$7^{(22)} = 1 \bmod 23$$

We can write 7^{69} as $(7^{22})^3 * 7^3$

Therefore,

$$7^{69} = y \bmod (23)$$

And can be written as

$$7^{69} = 7^{66} * 7^3$$

$$7^{69} = (7^{22})* 7^3 \bmod 23$$

$$7^{69} = (1)^3 * 7^3 \bmod 23$$

$$7^{69} = 343 \bmod 23$$

Therefore, the smallest positive residue y = 21.

ii) $$3^{101} = y \bmod 13$$

Here n = 3, P = 13 again by Fermat's Little theorem

$$n^{P-1} = 1 \bmod P$$

$$(3)^{(13-1)} = 1 \bmod 13$$

$$3^{(12)} = 1 \bmod 13$$

We can write 3^{101} as $(3^{12})^8 * 3^5$

Therefore, $3^{101} = y \bmod 13$

And can be written as : $3^{101} = 3^6 * 3^5$

$$3^{101} = (3^{12})^8 * 3^5 \bmod 13$$

$$3^{101} = (1)^8 * 3^5 \bmod 13$$

$$3^{101} = 243 \bmod 13$$

$$3^{101} = 9 \bmod 13$$

Therefore, the smallest positive residue y = 9.

b) *Find Euler Totient Function of the following numbers.* [6]

i) 75 ii) 5488 iii) 77

Ans. : i) $\phi(75)$, $n = 75 = 15 \times 5$

Here, n = 75, n is prime number

$$\phi(75) = \phi(15) * \phi(5)$$

$$= 14 * 4$$

$$= 56$$

ii) $\phi(5488)$

Here, $n = 5488 = 2^4 \times 7^3$

$$\phi(5488) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$$

$$= 5488 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{7}\right)$$

$$= 5488 \times \frac{1}{2} \times \frac{6}{7}$$

$$= 392$$

2	5488
2	2744
2	1372
2	686
7	343
7	49
7	7
	1

iii) $\phi(77)$

Here, $n = 77 = 11 \times 7$

$$\phi(77) = \phi(11) * \phi(7)$$

$$= 10 \times 6$$

$$= 60$$

c) *Compute GCD of the following using Euclidean algorithm.* [6]

i) GCD (831, 366)

ii) GCD (2222, 1234)

Ans. : i) GCD (831, 866)

$$831 = 366 * 2 + 99$$

$$366 = 99 * 3 + 69$$

$$99 = 69 * 1 + 30$$

$$69 = 30 * 2 + 9$$

$$30 = 9 * 3 + 3$$

$$9 = 3 * 3 + 0$$

Hence, gcd(831, 366) = 3

ii) GCD (2222, 1234)

$$2222 = 1234 * 1 + 988$$

$$1234 = 989 * 1 + 246$$

$$988 = 246 * 4 + 4$$

$$246 = 4 * 61 + 2$$

$$61 = 2 * 3 + 1$$

$$2 = 1 * 2 + 0$$

Hence, GCD (2222, 1234) = 0

Q.7 a) *Consider the (2, 6) encoding function e.e(00) = 100000,* [7]

e(10) = 101010

e(01) = 001110, e(11) = 101001

Find minimum distance of e.

How many errors will e detect ?

Ans. :

d (100000, 101010) = 2

d (100000, 001110) = 4

d (100000, 101001) = 2

d (101010, 001110) = 2

d (101010, 001110) = 2

d (001110, 101001) = 4

∴ Minimum distance of the code = Minimum of all the distance = 2

∴ Code can detect (2 – 1) or fewer errors.

b) *Let R = {0°, 60°, 120°, 180°, 240°, 300°} and * = binary operation, so that a * b is overall angular rotation corresponding to successive rotations by a and then by b. Show that (R,*) is a Group.* [6]

Ans. : Given that R = {0° = 360°, 60°, 120°, 180°, 240°, 300°}

Consider the following table.

*	0	60	120	180	240	300
0	0	60	120	180	240	300
60	60	120	180	240	300	0
120	120	180	240	300	0	60
180	180	240	300	0	60	120
240	240	300	0	60	120	240
300	300	0	60	120	180	240

From this table we get,

a) * is closed

i.e. For any a, b ∈ R, a * b ∈ R

b) * is associative

i.e. a * (b * c) = (a * b) * c

c) Existence of the identity

0° is the identity element in R.

d) Existence of the inverse

Element	0	60	120	180	240	300
Inverse	0	300	240	180	120	60

∴ (R, *) is a group.

c) *Prove that the following table on relation of elements of set G = {0, 1, 2, 3, 4, 5} multiplication mod 6 is not a group.* **[4]**

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	0
5	5	0	1	2	3	4

Ans. : $G = \{0, 1, 2, 3, 4, 5\} = Z_6 \pmod 6$

To check whether $G = Z_6$ is a group under multiplication, we have to check if it satisfies four conditions.

1) Closure 2) Associativity 3) Identity and 4) Inverse.

Closure : Multiplication is closed i.e. for any $a, b \in G$ we have $a \cdot b \in G$

Associativity - Modulo multiplication is associative, for any $a, b, c \in G$ we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c \pmod 6$

Identity : Take $e = 1 \in G$

∴ We have for any $a \in G$

$$a \cdot e = e \cdot a = a$$

Multiplication Inverse : For this condition we want a and b such that

$$a \cdot b = e = 1$$

But for $a = 0 \in G$ we can not find any $b \in G$ such that

$$0 \cdot b = 1$$

$\therefore$ Inverse property does not satisfies.

$\therefore$ G is not a group under multiplication.

OR

Q.8 a) *Determine whether description of * is a valid definition of a binary operation on the set.* **[6]**

*i) On R, a * b = ab (ordinary multiplication)*

*ii) On z^+, a * b = a / b*

*iii) On z, a * b = ab*

*iv) On z+, a * b = a – b*

*v) On z, a * b = 2a + b*

*vi) On R, a * b = ab/3*

Ans. :

i) Yes, since $f : R^2 \to R$ defined as f(a, b) = ab is a function, with $a\,b \in R$.

ii) No, since $(a,b) \in z^+ \times z^+$ does not imply that $a * b = a/b \in z$

$(1, 2) \in z^+ \times z^+$, but $1/2 \notin z^+$

iii) No, since $(1, 2) \in z^+ \times z^+$ but

iv) Yes, since, * is a function with $\min\{a, b\} \in R$

v) Yes, since * is a function with $a \times |b| \in R$

vi) No, since $2 * (-1) = 2^{-1} = \frac{1}{2} \notin z$

b) *S = {1, 2, 3, 6, 12} where a * b is defined as LCM (a, b). Determine whether it is an Abelian Group or not.* **[7]**

Ans. : $S = \{1, 2, 3, 6, 12\}$

$a * b = \text{LCM}(a, b)$

i) Take $a = 2, b = 3$

$a * b = 6$ since 6 is in set S.

Also 3 * 1, 2 * 1, 6 * 2, 3 * 2 all possibility in sets.

Hence closure axiom is true.

ii) $(a * b) * c$ = (LCM of $a * b) * c$

Let's Take $a = 2, b = 3, c = 6$

$$(a * b) * c = 6 * 6$$
$$= 6$$
$$a * (b * c) = a * (6)$$
$$= 2 * 6$$
$$= 6$$

Hence, associative axiom it true.

iii) $a * e$ = (LCM of a and e)

$$= 2 \times 1 = 2$$

$2 \times 1, 3 \times 1, 6 \times 1, 12 \times 1$ satisfying $a * e = e$.

so $e = 1$. Hence identity axiom is true.

iv) $a * a^{-1} = a^{-1} * a = e$ for inverse axiom.

For each element it is observed that no inverse element exist so it is not Abelian group. [4]

c) *Define ring.*

Ans. : Let R be a non empty set equipped with two binary operations called addition and multiplication and denoted by '+' and '·' respectively.

An algebraic structure (R,+, ·) is called a ring if it satisfies following axioms.

1) (R, +) is an abelian group i.e.

i) **Closure property :** for $a, b \in R$, $a + b \in R$

ii) **Associativity :** for a, b, c $\in$ R, $a + (b + c) = (a + b) + c$

iii) **Existence of the identity :** For any $a \in R$, $\exists$ o$\in$ R s.t., $a + 0 = 0 + a = a$.

$\therefore$ 0 is called as the additive identity element of ring.

iv) Existence of the inverse : For each $a \in R$, $\exists -a \in R$

Such that $a + (-a) = -a + a = 0$

$-a$ is called the additive inverse of a

v) Commutative property : For $a, b \in R$

$$a + b = b + a$$

2) $(R, \cdot)$ is semigroup i.e.

i) Closure property : $\forall a, b \in R, a \cdot b \in R$

ii) Associativity : for $a, b, c \in R$,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

3) Multiplication distributes over addition $\forall a, b, c \in R$

i) $a \cdot (b + c) = a \cdot b + a \cdot c$ (Right distributive law)

ii) $(a + b) \cdot c = a \cdot c + b \cdot c$ (Left distributive law)

END...