Date ___/___/___
Page No. ___

Representation of Sets
⇒ Roaster or Tabular
⇒ Rule or Set builder

Set
Finite
Infinite
Singleton
Subset
Universal
Disjoint
Null

Operation on set
⇒ Union '∪'
⇒ Intersection '∩'
⇒ Complement 'A^c / A'' = U - A
⇒ Relative Complement (A - B)
↳ Relative complement of B wrt A
⇒ Symmetric Difference A Δ B or A ⊕ B = (A - B) ∪ (B - A)

e.g. A = {-3, 0, 1, 2} B = {1, 2, 3, 4}
A ⊕ B = {-3, 0, 3, 4}

Algebra of Sets

⇒ Idempotent law
A ∩ A = A
A ∪ A = A

Date...../...../.....
Page No.....

⇒ **Associative law**

$(A \cup B) \cup C = A \cup (B \cup C)$

$(A \cap B) \cap C = A \cap (B \cap C)$

⇒ **Commutative law**

$A \cup B = B \cup A$

$A \cap B = B \cap A$

⇒ **Distributive law**

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

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

⇒ **Identity**

$A \cup \phi = A$

$A \cup A \cup = U$

$A \cap \phi = \phi$

$A \cap U = A$

⇒ **Involution law**

$(A')' = A$

⇒ **Complement law**

$A \cup A' = U$

$A \cap A' = \phi$

⇒ **D' Morgan's law**

$(A \cup B)' = A' \cap B'$

$(A \cap B)' = A' \cup B'$

Swapan Kumar Sarkar

Date...../...../.....
Page No.....

$(A \cup B)' = A' \cap B'$

L.H.S: $(A \cup B)'$

Let $x \in (A \cup B)'$

$x \in U - (A \cup B)$

$\Rightarrow x \in U \ \& \ x \notin A \cup B$

$\Rightarrow x \in U \ \& \ (x \notin A \ \& \ x \notin B)$

$\Rightarrow (x \in U \ \& \ x \notin A) \ \& \ (x \in U \ \& \ x \notin B)$

$\Rightarrow x \in U - A \ \& \ x \in U - B$

$\Rightarrow x \in A' \ \& \ x \in B'$

$\Rightarrow x \in A' \cap B'$

$(A \cup B)' \subseteq A' \cap B'$ - ① & $(A \cup B)' \supseteq A' \cap B'$ - ②

From ① & ②

$(A \cup B)' = A' \cap B'$

$(A \cap B)' = A' \cup B'$

L.H.S. $(A \cap B)'$

Let $x \in (A \cap B)'$

$\Rightarrow x \in U - (A \cap B)$

$\Rightarrow x \in U \ \& \ x \notin A \cap B.$

$\Rightarrow x \in U \ \& \ (x \notin A \ \text{or} \ x \notin B)$

$\Rightarrow (x \in U \ \& \ x \notin A) \ \text{or} \ (x \in U \ \& \ x \notin B)$

$\Rightarrow x \in U - A \ \text{or} \ x \in U - B$

$\Rightarrow x \in A' \ \text{or} \ x \in B'$

$\Rightarrow x \in A' \cup B'$

$(A \cap B)' \subseteq A' \cup B'$ - ① & $(A \cup B)' \supseteq A' \cup B'$ - ②

From ① & ②

$(A \cap B)' = A' \cup B'$

Date...../...../.....
Page No.....

Cardinal No: OR Cardinality ($|A|$ / $n(A)$)

Properties of Cardinal no.

* $|A \cup B| = |A| + |B| - |A \cap B|$

* $|A - B| = |A| - |A \cap B|$

* $|B - A| = |B| - |B \cap A|$

* $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$

Power set $|P(A)| = 2^{|A|}$

Theorem :- If $A \subseteq B$ then $P(A) \subseteq P(B)$

Countable set

* Finite & infinite set with one-one correspondance with natural numbers

e.g. $Z = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$
↳ countable

$\aleph_0$ (Aleph not)

$|N| = |Z| = |Q| = \aleph_0$

* $\aleph_0 + \aleph_0 = \aleph_0$
* $\aleph_0 \times \aleph_0 = \aleph_0$

$|A| = \aleph_0$ $\quad |P(A)| = 2^{\aleph_0} = C$ (Canters No)
(Uncountable)

Theorem:- Union of countable families of countable sets is countable

Proof:- Let $\{A_1, A_2, A_3, \ldots A_n\}$ be countable family of countable sets

$A_1 = \{a_{11}, a_{12}, a_{13}, \ldots\}$

$A_2 = \{a_{21}, a_{22}, a_{23}, \ldots\}$

$A_3 = \{a_{31}, a_{32}, a_{33}, \ldots\}$

$\ldots\ldots\ldots\ldots\ldots$

$A_n = \{a_{n1}, a_{n2}, a_{n3} \ldots\}$

then $\bigcup_{i=1}^{n} A_i$ can be found in following way

$A_1 = a_{11}, a_{12}, a_{13}, \ldots$

$A_2 = a_{21}, a_{22}, a_{23}, \ldots$

$A_3 = a_{31}, a_{32}, a_{33}, \ldots$

$A_4 = a_{41}, a_{42}, a_{43}, \ldots$

list the elements

a_{11}

a_{21} a_{12}

a_{31} a_{22} a_{13}

a_{41} a_{32} a_{23} a_{14}

$\ldots\ldots\ldots\ldots$

a_{n1} $a_{(n-1)2}$ $a_{(n-2)3}$ $a_{(n-3)4}$

It is clear that a_{ij} is the jth element of $(i+j-1)$th row. Thus all the ele. have been counted. Thus $\bigcup_{i=1}^{n} A_i$ is countable.

Theorem :- Show N×N is countable

Proof :- (1,1) , (1,2) , (1,3) . . .
(2,1) , (2,2) , (2,3) . . .
(3,1) , (3,2) , (3,3) . . .
(4,1) , (4,2) , (4,3) . .
. . . .

List the elements (1,1)
(2,1) , (1,2)
(3,1) , (2,2) , (1,3)
(4,1) , (3,2) , (2,3) , (1,4)

Or it is clear that a_{ij} is the jth ele of row. Thus all ele have been counted.
Thus $\bigcup_{i=1}^{n} A_i$ is countable

If A & B are countable the A×B is countable

Relation

$R \subseteq A \times B = \{(a_1,b_1), (a_2,b_2), (a_3,b_3) \ldots (a_n,b_n)\}$
$\phi \subset R$ (void)
$A \times B \subseteq R$ (universal)

Total no of relation $= 2^{mn}$
$|A| = m \quad |B| = n$
$|A \times B| = mn$

Date...../...../.....
Page No.....

Types of Relation

1. Inverse Relation

R be a relation from A to B.
R^{-1} be a relation from B to A
i.e. $R^{-1} = \{(b,a) \ldots, (a,b) \in R\}$
or, $x R y \Rightarrow y R^{-1} x$

Eg $A = \{2, 3, 5\}$ $B = \{6, 8, 10\}$
$\forall (x,y) \in A$ or B, $(x,y) \in R \Leftrightarrow x$ divide y
R & $R^{-1} = ?$

$2R6$, $2R8$, $2R10$, $3R6$, $5R10$
$R = \{(2,6), (2,8), (2,10), (3,6), (5,10)\}$
$R^{-1} = \{(6,2), (8,2), (10,2), (6,3), (10,5)\}$

Domain (R) = Range (R^{-1}) = $\{2, 3, 5\}$
Domain (R^{-1}) = Range (R) = $\{6, 8, 10\}$

2. Identity Relation

$I_A = \{(x,x) : x \in A\}$

Eg $A = \{1, 2, 3\}$
$I_A = \{(1,1), (2,2), (3,3)\}$

3. Reflexive Relation

$(a,a) \in R$ i.e. aRa $\forall$ $a \in A$.

4. Irreflexive

$(a,a) \notin R$ i.e. $a \not R a \quad \forall a \in A$.

5. Symmetry

$(a,b) \in R \Rightarrow (b,a) \in R$

i.e. $a R b \Rightarrow b R a \quad \forall a, b \in A$

6. Asymmetric

$(a,b) \in R \Rightarrow (b,a) \in R$

i.e. $a R b \Rightarrow b \not R a \quad \forall (a,b) \in A$.

7. Antisymmetric

$(a,b) \in R$ & $(b,a) \in R$

$\Rightarrow a = b$.

i.e. $a R b$ & $b R a \Rightarrow a = b \quad \forall (a,b) \in A$

Transitive

$a R b$ & $b R c \Rightarrow a R c$

$\forall a, b, c \in A$

2 Equivalence Relation

If R is relation in Z defined by

$R = \{(x,y) : x, y \in Z ; (x-y)$ divisible by $6\}$

Reflexive : $x R x \Rightarrow x - x$ is divisible by 6

Symmetric : $x R y \Rightarrow x - y$ is divisible by 6

$\Rightarrow -(y-x)$ is divisible by 6.

$\Rightarrow y R x$

Transitive: $x-y$ divisible by 6
$\Rightarrow y-x$ divisible by 6.
$x-z$ divisible by 6

Note:

(1) R is reflexive $\Rightarrow R^{-1}$ is reflexive
(2) R is symmetric $\Leftrightarrow R^{-1}$ is symmetric
(3) R is antisymmetric $\Leftrightarrow R \cap R^{-1} \subseteq I$
(4) R & S are reflexive $\Rightarrow R \cup S$ & $R \cap S$ are also reflexive.
(5) R & S are symmetric $\Rightarrow R \cup S$ & $R \cap S$ are also symmetric
(6) R & S are transitive $\Rightarrow R \cap S$ is transitive
(7) R & S are equivalence $\Rightarrow R \cap S$ is equivalence
(8) R is equivalence $\Rightarrow R^{-1}$ is equivalence

Partial Order Rel:

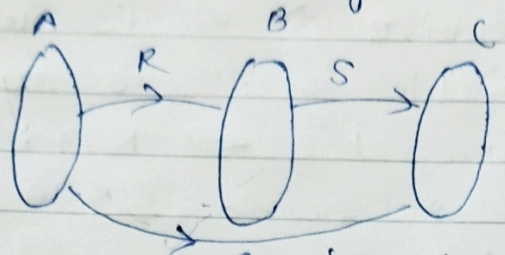
A relation R on set S. is partial order if
reflexive : aRa ; $\forall a \in S$
Antisymmetric : aRb & $bRa \Rightarrow a=b$ $\forall a,b \in S$
Transitive : aRb & $bRc \Rightarrow aRb$ $\forall a,b,c \in S$

A set S together with partial order R
i.e. (S,R) is partial order

'$\geq$' relation is partial order on Z
Reflexive $a \geq a$
Antisymmetric : $a \geq b$ & $b \geq a \Rightarrow a=b$
Transitive : $a \geq b$ & $b \geq c \Rightarrow a \geq c$
(Z,R)

Composite Relation

If A, B & C are non empty sets & R be a relation from A to B & S be a relation from B to C then composite relation of R & S is relation from A to C



$SOR = \{(a,c) : a \in A, c \in C\}$

Ex $A = \{1,2,3\}$; $B(p,q,r)$, $C = \{x,y,z\}$

$R = \{(1,p), (1,q), (2,q), (3,q)\}$

$S = \{(p,y); (q,y); (r,z)\}$

~~$ROS = \{(1,y); (1,x); \}$~~

$SOR = \{(1,y), (1,x); (2,x), (3,x)\}$

Function

- One-one (Injective) $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
- Many-one → ~~co-domain~~ ~~A के कोई~~ $x_1 \neq x_2 \Rightarrow f(x_1) = f(x_2)$
- Onto (Surjective)
- Into → co-domain का कोई ele. बच जाए.

jective ←

Composition of Function

Let $f: A \to B$ & $g: B \to C$

Composition of f & g $gof: A \to C$ defines as

$gof(x) = g[f(x)]$ $\forall x \in A$

Qu $A = \{1, 2, 3\}$; $B = \{a, b\}$; $C = \{r, s\}$

$f: A \to B$ as $f(1) = a$; $f(2) = a$, $f(3) = b$.

$g: B \to C$ as $g(a) = s$; $g(b) = r$

$gof \quad A \to C$

$g(f(x)) = g(f(1)) = g(a) = s.$

$g(f(2)) = g(a) = s$

$g(f(3)) = g(b) = r$

Property

⇒ Associative : $f \circ (g \circ h) = (f \circ g) \circ h$

$A \to B \quad B \to C \quad C \to D$

$f: A \to B \quad g: B \to C \quad h: C \to D$

$gof : A \to C$ & $hog : B \to D$

Hence : $h \circ (gof) : A \to D$

& $(hog) \circ f : A \to D$

Dom. of $[h \circ (gof)]$ = dom. $[(hog) \circ f]$

let $x \in A$; $y \in B$, $z \in C$

i.e. $f(x) = y$ & $g(y) = z$

then

$[(h \circ g) \circ f](x) = h(z)$ — ①

$[h \circ (g \circ f)](x) = h(z)$ — ②

From ① & ②

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

Theorem:

Let $f: A \to B$ & $g: B \to C$

(a) If f and g are injection then gof is injection

(b) If f & g are surjection then gof is surjection

PROOF:-

(a) Let $a_1, a_2 \in A$.

We have $(gof)a_1 = (gof)a_2$

$\Rightarrow g[f(a_1)] = g[f(a_2)]$

$f(a_1) = f(a_2)$ [g is injection]

$a_1 = a_2$ [f is injection]

Thus, gof is injection

b) Let $c \in C$, then we can find $a \in A$ s.t. $(gof)(a) = c$

g is onto $C \Rightarrow b \in B$ s.t $g(b) = c$

then since f is onto B, there exist $a \in A$ s.t $f(a) = b$

Thus $(gof)(a) = g[f(a)] = g(b) = c$.

Inverse

Let $f: A \to B$ then $g: B \to A$ if $gof = I_A$ & $fog = I_B$

Q Show that $f(x) = x^3$ & $g(x) = \sqrt[3]{x}$ $\forall x \in R$ are inverse to each other

$$fog(x) = f[g(x)] = f[\sqrt[3]{x}] = x = Ix$$
$$gof(x) = g[f(x)] = g[x^3] = x = Ix$$

Theorem:

$f : A \to B$ is one-one & onto then $f^{-1} : B \to A$ is one-one & onto

Proof:

Given :- $f : A \to B$ is one-one & onto

Let $a_1, a_2 \in A$ & $b_1, b_2 \in B$

so $b_1 = f(a_1)$, $b_2 = f(a_2)$

& $a_1 = f^{-1}(b_1)$; $a_2 = f^{-1}(b_2)$.

f is one-one $f(a_1) = f(a_2) \Leftrightarrow a_1 = a_2$

$b_1 = b_2 \Leftrightarrow f^{-1}(b_1) = f^{-1}(b_2)$

i.e. $f^{-1}(b_1) = f^{-1}(b_2) \Rightarrow b_1 = b_2$

$\therefore f^{-1}$ is one-one

f is onto :-

all element at B is associated with unique ele. at A.

i.e.

For any $a \in A$ is pre image of $b \in B$

where $b = f(a) \Rightarrow a = f^{-1}(b)$

i.e. for $b_1 \in B$ f^{-1}

So f^{-1} is onto

Date...../...../.....
Page No.....

Principle of Mathematical Induction

1) $S(n)$ is true for $n = 1$ i.e. $S(1)$ is true
2) $S(k)$ is true $\Rightarrow$ $S(k+1)$ is true

Qu $1 + 2 + 3 \ldots + n = \frac{n(n+1)}{2} \in N$

For $n = 1$

$S(1) = \frac{1(1+1)}{2} = 1$

For $n = k$

$S(k) = \frac{k(k+1)}{2}$

For $n = k+1$, we have to prove

$S(k+1) = \frac{(k+1)(k+2)}{2}$

$\Rightarrow$ $1 + 2 + 3 + \ldots k + (k+1) = \frac{k(k+1)}{2} + k + 1$

$= (k+1)\left[\frac{k}{2} + 1\right]$

$= \frac{(k+1)(k+2)}{2}$

Q $1^2 + 2^2 + 3^2 + \ldots n^2 = \frac{1}{6} n(n+1)(2n+1)$

For $n = 1$

$$S(1) = \frac{1}{6}(2)(3)$$

$$= 1$$

For $n = k$

$$S(k) = \frac{k}{6}(k+1)(2k+1)$$

For $n = k+1$

$$1^2 + 2^2 + 3^2 + \ldots k^2 + (k+1)^2 = \frac{k}{6}(k+1)(2k+1) + (k+1)^2$$

$$= (k+1)\left[\frac{k(2k+1)}{6} + k+1\right]$$

$$= (k+1)\left[\frac{2k(2k+1) + 6k + 6}{6}\right]$$

$$= \frac{1}{6}(k+1)\left[2k^2 + k + 6\right]$$

$$=$$

$$= (k+1)\left[\frac{k(2k+1)}{6} + k+1\right]$$

$$= (k+1)\left[\frac{2k^2 + k + 6k + 6}{6}\right]$$

$$= \frac{(k+1)}{6}\left[2k^2 + 7k + 6\right]$$

$$= \frac{(k+1)}{6}\left[2k^2 + 4k + 3k + 6\right]$$

$$= \frac{(k+1)}{6}\left[2k(k+2) + 3(k+2)\right] = \frac{(k+1)}{6}\left[(k+2)(2k+3)\right]$$

Date...../...../.....
Page No.....

Prove by mathematical induction
$6^{n+2} + 7^{2n+1}$ is divisible by 43 $\forall n \in Z$

Proof :

For $n=1$

$6^{1+2} + 7^{2+1} = 6^3 + 7^3$

$= 559$

which is divisible by 43.

For $n=k$

$6^{k+2} + 7^{2k+1}$ is divisible by 43

$\Rightarrow 6^{k+2} + 7^{2k+1} = 43m$, $\forall m \in Z$

For $n=k+1$

$6^{k+3} + 7^{2k+3}$

$= 6^{k+2+1} + 7^{2k+1+2}$

$= 6^{k+2} \cdot 6 + 7^{2k+1} 7^2$

$= 6 \cdot 6^{k+2} + 7^{2k+1} (43+6)$

$= 6 \left[6^{k+2} + 7^{2k+1} \right] + 43 \cdot 7^{2k+1}$

$= 6 \cdot 43m + 43 \cdot 7^{2k+1}$

$= 43 \left[6m + 7^{2k+1} \right]$

UNIT - 2

Date...../...../.....
Page No.....

1- Algebraic Structure

Let G be a non-empty set & * be the binary operation, then the ordered pair (G, *) is c/a algebraic structure

Group :- An algebraic structure (G, *) where G → non empty set and * is binary operation, then algebraic structure is called group if satisfy following property

1) Closure property :- $\forall\ a, b \in G,\ a * b \in G$

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

3) Existance of Identity :- $\forall\ a \in G,\ \exists\ e \in G$
s.t. $a * e = e * a = a$

4) Existence of inverse :- $\forall\ a \in G\ \exists\ a' \in G$ s.t.
$a * a' = a' * a = e$

G SM Grp abelian

Groupoid :- $(G, *)$ is groupoid if
Closure $\forall a, b \in G$, $a * b \in G$

Semigroup :- $(G, *)$ is semigroup if
1) Closure $\forall a, b \in G$, $a * b \in G$
2) Associative $\forall a, b, c \in G$
$a * (b * c) = (a * b) * c$

Monoid :- $(G, *)$ is monoid if
1) Closure $\forall a, b \in G$, $a * b \in G$
2) Associative $\forall a, b, c \in G$
$a * (b * c) = (a * b) * c$
3) Existance of identity
$\forall a \in G \quad \exists e \in G$ s.t
$a * e = e * a = a$

Abelian / commutative Grp :-
1) Closure
2) Associative
3) Existance of identity
4) Existance of inverse
5) Commutative $\forall a, b \in G$
$a * b = b * c$

$(Z, +)$
Closure ✓
Associative ✓
Existance of identity ✓
Existence of inverse ✓
Comm ✓

Date ..../..../.....
Page No. .....

§ $(Z, \cdot) \rightarrow$ Monoid.

§ $(C, +) \rightarrow$ Abelian

Closure :- $(a_1 + ib_1) + (a_2 + ib_2)$ ⟶

Associative :-

§ $(Z^-, \cdot)$

Addition modulo m $(+_m)$

$G_1 = \{1, 2, 3, \ldots m-1\}$

Q. ~~Show~~ check the set $\{1,2,3,4,5\}$ is group or what under addition & multiplication modulo 6.

$+_6$	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

$\times_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Not a group.

Q $\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$

Is multiplicative grp?

⇒ **Properties of grps :-**

Theorem :- Cancellation law

If $(G, *)$ is grp & $a, b, c \in G$ then

① $a * b = a * c \Rightarrow b = c$ (Left cancellation law)

② $b * a = c * a \Rightarrow b = c$ (Right cancellation law)

Proof :-

$\because a \in G \quad \exists\ a^{-1} \in G$

$a * b = a * c$

$\Rightarrow a^{-1} * (a * b) = a^{-1} * (a * c)$

$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$

$\Rightarrow e * b = e * c$

$\Rightarrow b = c$

(2) $\because a \in G \quad \exists\ a^{-1} \in G$

$b * a = c * a$

$(b * a) * a^{-1} = (c * a) * a^{-1}$

$b * (a * a^{-1}) = c * (a * a^{-1})$

$b * e = c * e$

$b = c$

Theorem :- Left identity = Right identity

i.e.

$e * a = a * e = a$

Proof :-

If a^{-1} is inverse of a then

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

$= e * e$

$= e = a^{-1} * a$

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

$a * e = a$ — ① [By L.C.L]

Similarly $e * a = a$ — ② [By R.C.L]

From ① & ②

$a * e = e * a = a$

Theorem :- Left inverse = Right inverse.

i.e. $a^{-1} * a = a * a^{-1} = e$

Proof :-

$$a^{-1} * (a * a^{-1}) = (a^{-1} * a) * a^{-1} \quad \text{(Ass.)}$$
$$= e * a^{-1} \quad \text{(Identity)}$$
$$= a^{-1} * e \quad \text{[Identity]}$$

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

$\Rightarrow a * a^{-1} = e$ —— ① [By L.C.L]

Similarly, $a^{-1} * a = e$ —— ② [By R.C.L.]

From eqn ① & ②

$a * a^{-1} = a^{-1} * a = e$

Theorem :- In a grp $(G, *)$

① $a * x = b$ has unique soln $x = a^{-1} * b$

② $y * a = b$ has unique soln $y = b * a^{-1}$

Proof :- Let $a * x = b$ has soln $x \& x'$

then $a * x = b \;\&\; a * x' = b$

$\Rightarrow a * x = a * x'$

$\Rightarrow \boxed{x = x'}$ [L.C.L]

$\therefore$ $a * x = b$ has unique soln

$a * x = a * (a^{-1} * b)$ (Given)

$= (a * a^{-1}) * b$ (Ass.)

$= e * b$ (identity)

$= b$

$\Rightarrow x = a^{-1} * b$ satisfy the eqn

(2) Let $y * a = b$ has unique soln. y & y' then

$y * a = b$ & $y' * a = b$

$\Rightarrow y * a = y' * a$

$\Rightarrow y = y'$ [By R.C.L]

$\therefore y * a = b$ has unique soln

$y * a = y * (y^{-1} * b)$

$= (y * y^{-1}) * b$

$= e * b$

$= b.$

Theorem: (1) $(a^{-1})^{-1} = a$

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

Proof: Let e be identity in G.

We have $a * a^{-1} = e$ [$\forall a \in G \; \exists a^{-1} \in G$

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

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

$a = (a^{-1})^{-1}$ [R.C.L]

② $a * b \in G$ (Closure)

$\Rightarrow (a*b)^{-1} * (a*b) = e$ [Inverse] ①

$\forall\ a, b \in G \ \exists\ a^{-1}, b^{-1} \in G$

$\therefore (b^{-1} * a^{-1}) * (a * b)$

$= b^{-1} * (a^{-1} * a) * b$

$= b^{-1} * e * b$

$= b^{-1} * b$

$= e$ —— ②

From ① & ②

$(a*b)^{-1} * (a*b) = (b^{-1} * a^{-1}) * (a*b)$

$(a*b)^{-1} = b^{-1} * a^{-1}$

(Rev)

Order of grp :-

Order of element :- $g \in G_r$ is the smallest positive integer n such that $g^n = e$ if no such integer exist then g has infinite order, denoted by $o(g)$

Ex:- Let $G_r = \{1, -1, i, -i\}$ be multiplicative grp. Find order of each element.

The multiplicative identity is 1

$o(1) = 1^1 = 1$

$(-1)^2 = 1 \Rightarrow o(-1) = 2$

$(i)^4 = 1 \Rightarrow o(i) = 4$

$(-i)^4 = 1 \Rightarrow o(-i) = 4$

Date...../...../.....
Page No.....

Subgrp :- Let $(G, *)$ be a grp & H is subset of G s.t. $(H, *)$ itself is a grp then $(H, *)$ is subgrp of $(G, *)$

Normal subgrps :- A subgrp H of a grp G is said to be normal if for every $x \in G$ and for every $h \in H$, $xhx^{-1} \in H$

Coset :- $\forall\ a \in (G, +)$ & $h \in (H, +)$
$(a+H)$ is left coset of G w.r.t. addition
$(h+a)$ is right . . . . . .

$a \in (G, \cdot)$ & $h \in (H, \cdot)$
ah is left coset w.r.t multiplication
ha is right . . . . . .

Theorem :- A subgrp H of grp G is normal iff $xHx^{-1} = H\ \forall\ x \in G$

Soln

Let $xHx^{-1} = H\ \forall x \in G$
$xHx^{-1} \subseteq H\ \forall x \in G$
$\Rightarrow$ H is normal subgrp of G

Conversely, H is normal subgrp of G, then
$xHx^{-1} \subseteq H\ \forall\ x \in G$ — (1)

Then $x \in G$, $x^{-1} \in G$
$x^{-1} H (x^{-1})^{-1} \in H\ \forall\ x \in G$
$x^{-1} H x \in H\ \forall\ x \in G$
$x (x^{-1} H x) x^{-1} \subseteq xHx^{-1}\ \forall\ x \in G$

$\Rightarrow H \subseteq xHx^{-1}$ — ②

From ① & ②

$H = xHx^{-1}$

⇒ **Theorem :-** A subgp H of gp G is normal if left coset of H in G is right coset of H in G

i.e. H is normal subgp of G

$\Leftrightarrow xH = Hx \quad \forall x \in G$

Proof :-

Let H be normal sub gp of G

then $xHx^{-1} = H$

$\Rightarrow (xHx^{-1})x = Hx$

$\Rightarrow xH = Hx$

⇒ left coset = right coset

Conversely

Let $xH = Hx \quad \forall x \in G$

then

$xHx^{-1} = Hxx^{-1}$

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

Date...../...../.....
Page No.....

Q. Let $(\{a,b\}, *)$ be semigrp where $a * a = b$
show $a * b = b * a$

Proof: $a * b = a * (a * a)$
$= (a * a) * a$
$= b * a$

(2) $b * b = b$

Qu Let G be a grp with binary operation multiplication & H be a subgrp.
Let $a \in G$ then
$Ha = \{ ha : h \in H \}$
is right coset of H in G generated by a
$aH = \{ ah : h \in H \}$ is left coset of H on G generated by a

Of operation is addition

$H + a = \{ h + a : h \in H \}$ is right coset
& $a + H = \{ a + h : h \in H \}$ is left coset