Set theory :

(1) Group theory :

Note :

- $N = \{1, 2, 3 \dots\}$
- $W = \{0, 1, 2, \dots\} = \{0\} \cup N$
- $Z = \{0, \pm 1, \pm 2, \dots\}$
- $Q = \{p/q \mid q \neq 0 \text{ and } p, q \text{ doesn't have any common factor other than } 1\}$
- $Q' = \{\sqrt{2}, \sqrt{3}, 2+\sqrt{3}, 2\sqrt{3} \dots\}$
- $R = Q \cup Q'$
- Q_0 = Non zero rational nums ; R_0 = Non zero real nums ; Z_0 = non zero integers
- Q^+ = +ve Rational nums ; R^+ = +ve real nums ; Z^+ = +ve integers.

(i) Binary operation : (BO)

Let 'G' be non-empty set. An operation $*$ is called Binary operation on 'G' if

$\forall a, b \in G \quad a * b \in G$

Note :

- If $*$ is a BO on G then 'G' is said to be satisfying closure property wrt '$*$'.
- If G is closed wrt '$*$' then $(G, *)$ is called **Quassi group**

Ex:- $a * b = a^b \quad \forall a, b \in N$

$\forall a, b \in N \quad a^b \in N$

$a * b \in N$

'$*$' is a B.O

$(N, *)$ is a quassi group

Ex:- $a * b = a^b \quad \forall a, b \in Q$

$\forall a, b \in Q \quad a^b \notin Q$ If $a = 2, b = 1/2$.

$a^b = 2^{1/2} = \sqrt{2} \in Q'$

$\therefore *$ is not B.O

$(Q, *)$ is not quassi group

$(Q, \cdot)$ is not satisfying closure property

(ii) Associative property :

- Let 'G' be an non-empty set with '$*$' is a B.O on G.
- $\forall a, b, c \in G$ if $(a * b) * c = a * (b * c)$ then '$*$' is associative on 'G'
- 'G' is said to be satisfying Associative property wrt '$*$'
- $(G, *)$ is called **semi group**

Ex:- $a * b = a^b \quad \forall a, b \in N$.

$*$ is a B.O.

LHS : $(a * b) * c$

$(a^b) * c$

$(a^b)^c = a^{bc}$

RHS : $a * (b * c)$

$a * (b^c)$

a^{b^c}

LHS $\neq$ RHS.

$(N, *)$ is not Semi Group but Quasi group.

Ex:- $a * b = \frac{ab}{3} \quad \forall a, b \in Q$

$*$ is a B.O

LHS : $(a * b) * c$

$\left(\frac{ab}{3}\right) * c$

$\frac{abc}{9}$

RHS : $a * (b * c)$

$a * \left(\frac{bc}{3}\right)$

$\frac{abc}{9}$

LHS = RHS

$\therefore (N, *)$ is semi group.

Scanned by CamScanner

(III) Identity property :

- Let 'G' be a non Empty set with '$*$' is a B.O on G.
- $\forall a \in G$, $\exists e \in G$ such that $\boxed{a*e = e*a = a}$ then e is called Identity Element in 'G'.

Note :

- $\forall a \in G$, $\exists e \in G$ such that $\boxed{a*e = a}$ then 'e' is right Identity in 'G'
- $\forall a \in G$, $\exists e \in G$ such that $\boxed{e*a = a}$ then 'e' is left Identity in 'G'.
- If left Identity and right Identity (Exists) and they are (Equal) then we can say that Identity Exists in G

Note : Let G be a non-Empty set and satisfies
(I) Closure property
(II) Associative property
(III) Identity property
} then $(G, *)$ is called monoid / loop

Ex:- $a*b = \frac{ab}{3}$ $\forall a, b \in Q$
$*$ is a B.O
Let e be Identity in Q
$a*e = e*a = a$

$a*e = a$	$e*a = a$
$\frac{ae}{3} = a$	$\frac{ea}{3} = a$
$\boxed{e = 3} \in Q$	$\boxed{e = 3} \in Q$
left Identity / right Identity	left Identity / right Identity

$=$

Identity Element

$\therefore (Q, *)$ is monoid

Ex:- $a*b = a^b$ $\forall a, b \in N$
$*$ is a B.O
Let e be Identity in Q
$a*e = e*a = a$

$a*e = a$	$e*a = a$
$a^e = a^1$	$e^a = a$
$\boxed{e = 1} \in N$	$e = a^{\forall a}$, $\forall a \notin N$
left Identity / right Identity	right Identity / left Identity doesn't Exist

$(N, *)$ is not monoid.

Take care about domain
Imp.

(IV) Inverse property :

- Let G be a non Empty set with '$*$' is a B.O on G
- $\forall a \in G$, $\exists b \in G$ such that $\boxed{a*b = b*a = e}$ where e is Identity in G then 'b' is called Inverse and it is denoted by $b = a^{-1}$

Note : Let G be a non Empty set with '$*$' is a operation on G. If G satisfies
(I) Closure property
(II) Associative property
(III) Identity property
(IV) Inverse property
} then $(G, *)$ is said to be a Group.

Ex:- $a*b = \frac{ab}{3}$ $\forall a, b \in Q$
$*$ is a B.O
3 is Identity Element then
$a*b = b*a = e$

$a*b = 3$
$\frac{ab}{3} = 3$
$b = \frac{9}{a} \notin Q$ if $a = 0$
a^{-1} doesn't Exist
$(Q, *)$ is not Group

Ex:- $a*b = \frac{ab}{3}$ $\forall a, b \in Q_0$
$*$ is a B.O
3 is Identity Element then
$a*b = b*a = 3$

$a*b = 3$
$\frac{ab}{3} = 3$
$b = \frac{9}{a} \in Q_0$

$b*a = 3$
$\frac{ba}{3} = 3$
$b = \frac{9}{a} \in Q_0$

a^{-1} exists.
$(Q_0, *)$ is Group

Find 7^{-1}
$a = 7$
Inverse $(b) = \frac{9}{a}$
$\therefore 7^{-1} = \frac{9}{7}$

Scanned by CamScanner

(V) Commutative property :

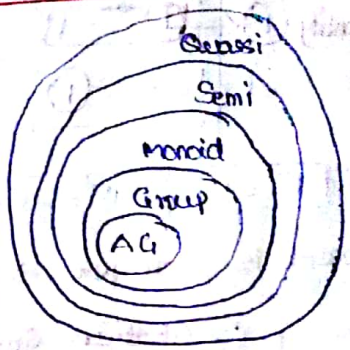
- If '*' is a B.O on G and
- $\forall a,b \in G$, if $a*b = b*a$ then '*' is Commutative on G

Note :

If '*' is a B.O and a group which satisfies commutative property is called Abelian Group

Points to remember

	Closure	Associative	Identity	Inverse	Commutative
Quassi	✓				
semi	✓	✓			
Moroid	✓	✓	✓		
Group	✓	✓	✓	✓	
Abelian Group	✓	✓	✓	✓	✓



Ex:- the set of all rational nums forms Abelian Group under ~~multiplication~~ Addn

(i) Closure : $a \in Q, b \in Q, a+b \in Q$ ✓

(ii) Assoc : $(a+b)+c = a+(b+c)$

(iii) Identity : $a+e = a$, $e = 0 \in Q$ | $e+a = a$, $e = 0 \in Q$

(iv) Inverse : $a+b = 0$, $b = -a \in Q$

(v) Comm : $a+b = b+a$

$\therefore (Q, +)$ is Abelian Group

Ex:- The set of all rational nums forms Abelian group under multiplication

(i) Closure : $a \in Q, b \in Q \Rightarrow ab \in Q$ ✓

(ii) Assoc : $(ab)c = a(bc)$

(iii) Identity : $ae = a$, $e = 1 \in Q$ | $ea = a$, $e = 1 \in Q$

(iv) Inverse : $ab = 1$, $b = \frac{1}{a} \notin Q$ if $a \neq 0$

$\therefore (Q, *)$ is not Abelian Group

Order of Group : $o(G)$

- Num of Elements in a group is called order of the group

Note :

If $o(G)$ is Finite $\Rightarrow$ G is called Finite group
$o(G)$ is Infinite $\Rightarrow$ G is called Infinite group

Examples of finite group :

Group of order 1 :

Ex:- $G = \{1\}$ wrt $\cdot$

(i) Closure : $\forall a,b \in G$, $a \cdot b \in G$

(ii) Assoc : $(a \cdot b) \cdot c = a(b \cdot c)$

(iii) Identity : $a \cdot e = ea = a$, $e = 1 \in G$

(iv) Inverse : $ab = ba = e$, $ab = 1$, $b = 1 \in G$

(v) Comm : $ab = ba$

$\therefore$ Abelian Group

Ex:- $G = \{1\}$ wrt $+$

(i) Closure $\forall a,b \in G$, $a+b$, $1+1 = 2 \notin G$ ✗

Not Quassi group

$\Rightarrow$ ∵ lenghty procedure

↓sol

Composition table

Note :

- Every Group of order 1 is Abelian Group
- In a Group of order 1 it contains only Identity Element and that Element has self Inverse

Scanned by CamScanner

Composition table method.

Group of order 2 :

$G = \{1, -1\}$ wrt $\cdot$

Composition table

$\cdot$	1	-1
1	1	-1
-1	-1	1

Similar

Identity (1)

$\in G \Rightarrow$ Quasi

$1^{-1} = 1$ $\quad (-1)^{-1} = -1$ — Inverse.

Matrix is Transpose $\Rightarrow$ Commutative

$\therefore$ Abellian Group

Note :

- Every Group of order 2 is Abellian group
- In a group if every element has its own Inverse then it must be Abellian and converse need not be true.

Group of order 3 : $G = \{1, \omega, \omega^2\}$ wrt $\cdot$ $\omega^3 = 1$

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Identity (1)

$\in G \Rightarrow$ Quasi

Transpose

$1^{-1} = 1$; $\omega^{-1} = \omega^2$; $(\omega^2)^{-1} = \omega$

$\therefore$ Abellian Group.

Note :

Every Group of order 3 is Abellian Group

Points to remember :

Group order	Example	Remarks
1	$G = \{1\}$ wrt $\cdot$ $G = \{1\}$ wrt $\div$	- Group of order 1 is always Abellian - It Contains only identity element and that Element has self Inverse.
2	$G = \{-1, 1\}$ wrt $\cdot$	- Group of order 2 is abellian group - In a Group if every element has its own Inverse then it must be Abellian group and Converse need not be true
3	$G = \{1, \omega, \omega^2\}$ wrt $\cdot$ $\{\omega^3 = 1\}$	- Group of order 3 is Abellian group
4.	$G = \{1, -1, i, -i\}$ wrt $\cdot$ $(i^2 = -1)$	- Group of order 4 is Abellian Group.
5.	$G = \{1, \omega, \omega^2, \omega^3, \omega^4\}$ wrt $\cdot$ $(\omega^5 = 1)$	- Group of order 5 is Abellian group
6.	$G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ wrt fncomposition $(\circ)$ $f_1(z) = z$, $f_2(z) = \frac{1}{z}$, $f_3(z) = 1 - z$ $f_4(z) = \frac{z}{z-1}$, $f_5(z) = \frac{1}{1-z}$, $f_6(z) = \frac{z-1}{z}$	- Every Group of order 6 need not be Abellian group
7	$G = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6\}$ wrt $\cdot$ $\{\omega^7 = 1\}$	- Every Group of order 7 is Abellian group
8	$G = \{\pm i, \pm j, \pm k, \pm 1\}$ wrt $\cdot$ $i^2 = j^2 = k^2 = -1$, $i \cdot j = -j \cdot i = k$ $j \cdot k = -k \cdot j = i$ $k \cdot i = -i \cdot k = j$ and so on	- Group of order 8 is not Abellian group and it is Quaternion group

Scanned by CamScanner

Note:
If $G = \{1, \omega, \omega^2 \dots \omega^{p-1}\}$ where $\omega^p = 1$ (p → prime) then
$1 \Rightarrow$ identity.
$(\omega^r)^{-1} = \omega^{p-r}$ and $(1)^{-1} = 1$

Note:
Every group of prime order is always Abelian Group

Infinite group

- $(\mathbb{Z}, +)$ is an infinite abelian group
- $(\mathbb{Q}, +)$
- $(\mathbb{R}, +)$
- $(\mathbb{Z}_0, \cdot)$
- $(\mathbb{Q}_0, \cdot)$
- $(\mathbb{R}_0, \cdot)$

Order of an element:

Def1: Let $(G, \cdot)$ be a group if there exist a least +ve integer 'n' such that $a^n = e$ where e is identity in G then $O(a) = n$

Def2: Let $(G, +)$ be a group if there exist a least +ve integer 'n' such that $na = e$ where e is identity in G then $O(a) = n$

Ex:- $G = \{1, \omega, \omega^2, \omega^3, \omega^4\}$ $(\omega^5 = 1)$ wrt $\cdot$
here $e = 1$ $\quad O(G) = 5$

$O(1)$	$O(\omega)$	$O(\omega^2)$	$O(\omega^3)$	$O(\omega^4)$
$(1)^n = 1$	$(\omega)^n = 1$	$(\omega^2)^n = 1$	$(\omega^3)^n = 1$	$(\omega^4)^n = 1$
$n = 1, 2 \dots$	$n = 5, 10 \dots$	$n = 5, 10 \dots$	$n = 5, 10 \dots$	$n = 5, 10 \dots$
$\therefore O(1) = 1$	$O(\omega) = 5$	$O(\omega^2) = 5$	$O(\omega^3) = 5$	$O(\omega^4) = 5$

Note:
In a Group
- $O(e) = 1$
- $O(a^{-1}) = O(a)$
- $O(a)$ divides $O(G)$ ie (order of element divides order of Group)

Note:
- $O(a) > 1$ if $a \neq e$
- $G = \{1, \omega, \omega^2 \dots \omega^{p-1}\}$ and $\omega^p = 1$ then where p is prime
  $O(1) = 1$
  $O(\omega) = O(\omega^2) = \dots = O(\omega^{p-1}) = p$

Note:
If $O(a) = n$ and $a^m = e$ iff n divides m (n → least +ve int such that $a^n = e$)

Addition modulo m:

Let $a, b \in \mathbb{Z}$
$a +_m b = r$ where 'r' is non-negative remainder which is obtained when (a+b) divided with 'm'

Ex:- $3 +_4 4 = 1$ | Ex:- $19 +_3 (-20) = 2$ | Ex:- $19 +_3 (-22) = 0$ ← $19 - 22 = -3$; $-3 + 3 = 0$

Multiplication modulo m:

Let $a, b \in \mathbb{Z}$
$a \times_m b = r$ where 'r' is non-negative remainder which is obtained when ab divided with m

Ex:- $3 \times_5 4 = 12 \bmod 5 \to 2$ | $3 \times_5 -4 = -12 \bmod 5 = 3$

Scanned by CamScanner

Imp model : $G = \{0,1,2\}_{+3}$

Method 1

$+_3$	0	1	2
Id (0)	0	1	2
1	1	2	0
2	2	0	1

$\in G$

Method 2: $O(G) = 3$ prime → Abelian

$0^{-1} = 0 \quad 1^{-1} = 2 \quad 2^{-1} = 1$

Transpose → notation

Note:
- In a group 'G' Identity Element is always unique
- In a group 'G' Every Element has unique Inverse

Note:
$Z_m = \{0,1,2 \cdots m-1\}_{+m}$ is always Abelian group of order m with
Identity → 0
$r^{-1} = m - r \; ; r > 0$

Note:
$Z_p = \{1, 2, 3 \cdots p-1\}_{\times p}$ where p is prime then $(Z_p, \times_p)$ is always Abelian group with order p-1
(mul modulo p)

Sub Group:

Let $(G, *)$ be a group and $H \neq \phi$, $H \subseteq G$
$(H, *)$ is said to be subgroup of G iff $(H, *)$ is a group

Note: Num of possible sub groups = $2^{O(G)} - 1$

Ex:- $G = \{1, \omega, \omega^2\}$ wrt $\cdot$ Find num. of sub groups.

$H_1 = \{1\} \Rightarrow (H_1, \cdot)$ is sub group

$H_2 = \{\omega\} \Rightarrow$

	ω
ω	$\omega^2 \notin H_2$

×

$H_3 = \{\omega^2\} \Rightarrow$

	ω^2
ω^2	$\omega \notin H_3$

×

$H_4 \Rightarrow \{1, \omega\} \Rightarrow$

	1	ω
1	1	ω
ω	ω	$\omega^2 \notin H_4$

×

$H_5 \Rightarrow \{1, \omega^2\} \Rightarrow$

	1	ω^2
1	1	ω^2
ω^2	ω^2	$\omega \notin H_5$

×

$H_6 \Rightarrow \{\omega, \omega^2\} \Rightarrow$

	ω	ω^2
ω	ω^2	$1 \notin H_6$
ω^2	1	ω

×

$H_7 \Rightarrow \{1, \omega, \omega^2\} \Rightarrow (H_7, \cdot)$ is subGroup

Num of sub groups = 2.

reduced ⟹

Note:
Sub Group Always Contains Identity Element

$H_1 \{1\} \Rightarrow (H_1, \cdot)$ is sub group

$H_2 \{1, \omega\} \Rightarrow$ ×

$H_3 \{1, \omega^2\} \Rightarrow$ ×

$H_4 \{1, \omega, \omega^2\} \Rightarrow$ ✓ $(H_4, \cdot)$ is sub Group.

∴ Num of sub groups = 2

Legranges theorem:

Let $(G, *)$ be a Finite group, if $(H, *)$ is a subgroup of G then 'O(H) divides O(G)'

Ex:- $G = \{1, \omega, \omega^2\} \Rightarrow O(G) = 3$.

$H_1 = \{1\}$ ∴ $O(H) = 1 \Rightarrow$ 1 divides 3

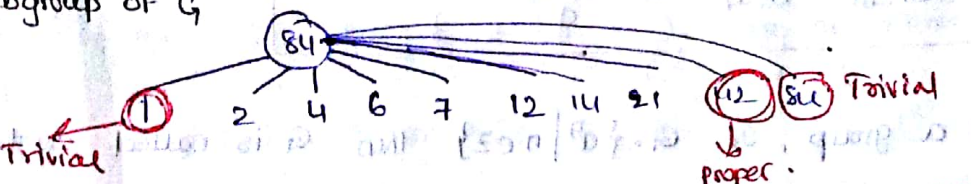
$H_2 = \{1, \omega, \omega^2\}$ ∴ $O(H) = 3 \Rightarrow$ 3 divides 3

Note:
Converse of legranges theorem need not be true ie If O(H) divides O(G) then H need not be subgraph of G

Scanned by CamScanner

Note:
If $(G, *)$ be a group then
$H_1 = \{e\}$, $H_2 = G$ are Improper or Trivial subgroups of G and rest of them are Proper or non-trivial subgroups of G

Ex:- Let G be a finite group of 84 elements. The size of the largest possible Proper subgroup of G



Note:
If $N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \cdots \times p_n^{\alpha_n}$ where $p_i \to$ distinct primes. then.
$\alpha_i \in N$

- $\tau(n)$ = Num of +ve divisors of n
  $= (1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_n)$
- If $O(G) = n$ then num of distinct ordered subgroups are $\tau(n)$

Properties of subgroups:

- H is a subgroup of $(G, \cdot)$ iff (i) $ab \in H$ $\forall a,b \in H$; (ii) $a^{-1} \in H$ $\forall a \in H$
- H is a subgroup of $(G, +)$ iff (i) $a+b \in H$ $\forall a,b \in H$; (ii) $a^{-1} \in H$ $\forall a \in H$
- H is a subgroup of $(G, \cdot)$ iff (i) $ab^{-1} \in H$ $\forall a, b \in H$
- H is a subgroup of $(G, +)$ iff (i) $a-b \in H$ $\forall a,b \in H$

Imp If H and K are subgroups then $H \cap K$ is also subgroup of G
Imp If H and K are subgroup of G then $H \cup K$ need not be subgroup of G
Imp If H and K are subgroup of G then $H \cup K$ is subgroup of G only if H is subset of K or K is subset of H
If $H \subseteq K$ then $H \cup K = K \to$ subgroup
If $K \subseteq H$ then $H \cup K = H \to$ subgroup.

Imp Ex:- Find order of every element $G = \{0,1,2,3,4,5\}$ +6
Identity = 0
$O(0) = 1$
$O(1) = O(5)$ $n \cdot 1 = 0 \Rightarrow n \cdot 1 \bmod 6 = 0$. $n = 6$
$O(1) = O(5) = 6$
$O(3)$: $3 \cdot n = 0 \Rightarrow 3n \bmod 6 = 0$. $n = 2$
$O(2) = O(4)$ $n \cdot 2 = 0 \Rightarrow 2n \bmod 6 = 0$. $n = 3$
$O(2) = O(4) = 3$
$\therefore O(0) = 1, O(1) = 6, O(2) = 3, O(3) = 2, O(4) = 3, O(5) = 6$.

Scanned by CamScanner

Note:

$\mathbb{Z}_m$ ie $\{0,1,2,\ldots m-1\}_{+m}$ is always a Abelian group

Identity = 0

$r^{-1} = m - r$

Order of any element $O(a) = \frac{\text{Lcm}(a,m)}{a}$

Ex:- Find $O(16)$ in $\mathbb{Z}_{30}$

$\mathbb{Z}_{30} = \{0,1,\ldots 29\}_{+30}$

$O(16) = \frac{\text{Lcm}(16,30)}{16}$ $\quad 2\overline{)16,30}$ $\quad 8,15$

$= \frac{2\times 8\times 15}{16} \Rightarrow 15$

Cyclic group:

- Let $(G,\cdot)$ be a group, If $G = \{a^n \mid n \in \mathbb{Z}\}$ then G is called cyclic group generated by a
- Let $(G,+)$ be a group, If $G = \{na \mid n \in \mathbb{Z}\}$ then G is called cyclic group generated by a

Here a is called Generator denoted by $G = \langle a \rangle$

Ex:- $G = \{1, \omega, \omega^2\}$ wrt $\cdot$ is cyclic?

$1^n = 1$ ✓	$\omega^n = 1$; $n=3$	$(\omega^2)^n = 1$; $n=3$
$1^n \neq \omega$	$\omega^n = \omega$; $n=1$	$(\omega^2)^n = \omega$; $n=2$
$1^n \neq \omega^2$	$\omega^n = \omega^2$; $n=3$	$(\omega^2)^n = \omega^2$; $n=1$
$G \neq \langle 1 \rangle$	$G = \langle \omega \rangle$	$G = \langle \omega^2 \rangle$

$\therefore \omega, \omega^2$ are generators

$\therefore G$ is cyclic

Properties of cyclic group:

1. If $O(G) > 1$ then $G \neq \langle e \rangle$
2. If G is a cyclic group and $G = \langle a \rangle$ then $G = \langle a^{-1} \rangle$
3. If G is a cyclic group of order 'n' then total num of generators in G is $\phi(n)$ Eulers totient fn

Finding $\phi(n)$:

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$; $p_i \to$ prime, $\alpha_i \in N$

$$\phi(n) = \frac{n(p_1-1)(p_2-1)\cdots(p_n-1)}{p_1 p_2 p_3 \cdots p_n}$$

Apps of Eulers totient fn

- Num of +ve Integers which are less than n and co-prime
- RSA Algorithm
- Num of generators in cyclic group

Note: $G = \{\pm 1, \pm i, \pm j, \pm k\}$ is not cyclic so they have no generators.

Note:

- Every cyclic group is abelian but every abelian need not be cyclic
- In an abelian group, every element has its own inverse.
- Every Group of prime order is abelian and cyclic
- Every group of prime order has 'p-1' generators
- Every subgroup of cyclic group is cyclic
- Every subgroup of abelian group need not be abelian

Scanned by CamScanner

SET THEORY

Sets :

- well defined collection of unordered objects is called sets.

Equal Sets :

- Two sets A and B are said to be equal if they contains same elements.

$|A| = |B|$

Subset :

- Let A, B are two sets. If every element of A is also an element in B then A is subset to B.

Subset : $A \subseteq B$ ie $A = B$ or $A \subset B$

Proper subset : $A \subset B$ ie $A \subset B$

Powerset : set of all possible subsets of A

Note : If $|A| = n$ then

Num of elements $|P(S)| = {}^nC_0 + {}^nC_1 + {}^nC_2 + \cdots + {}^nC_n \Rightarrow 2^n$

Ex:- $A = \{1, 2, \{1,2\}, \{3\}\}$

(i) $2 \in A \Rightarrow$ ✓

(ii) $\{2\} \in A \Rightarrow$ ✗

(iii) $\{2\} \subseteq A \Rightarrow$ ✓ (✗ ✓)

(iv) $\{1,2\} \in A \Rightarrow$ ✓

(v) $\{\{1,2\}\} \subseteq A \Rightarrow$ ✓

(vi) $\{\{3\}\} \in A \Rightarrow$ ✗

(vii) $\{3\} \in A \Rightarrow$ ✓

(viii) $\{3\} \subseteq A \Rightarrow$ ✗

Note :

$A \Delta B = (A - B) \cup (B - A)$

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

$n(A - B) = n(A) - n(A \cap B)$

$n(A \cup B) = n(A) + n(B) - n(A \cap B)$

Disjoint sets : $A \cap B = \phi$

Multisets : Multisets are unordered collection of elements where an element can occur as a member more than once.

Ex:- $A = \{a, a, b, b, b, c, c, c, c, d\}$

$A = \{2 \cdot a, 3 \cdot b, 4 \cdot c, 1 \cdot d\}$

Algebraic Multiplicity

Imp

- Union of the multisets P and Q is also a multiset where the multiplicity of an element is the max of its multiplicities of P and Q
- Intersection of the multisets P and Q is also a multiset where the multiplicity of an element is the min of its multiplicities of P and Q
- Ex:- $A = \{3 \cdot a, 2 \cdot b, 1 \cdot c\}$, $B = \{2 \cdot a, 3 \cdot b, 4 \cdot d\}$ then

  $A \cup B = \{3 \cdot a, 3 \cdot b, 1 \cdot c, 4 \cdot d\}$

  $A \cap B = \{2 \cdot a, 2 \cdot b\}$

  $A - B = \{1 \cdot a, 1 \cdot c\}$ (b not considered)

  $A + B = \{5 \cdot a, 5 \cdot b, 1 \cdot c, 4 \cdot d\}$

Cartesian product :

Let A, B are two finite sets, the cartesian product of A, B is denoted by $A \times B$

$A \times B = \{(m, n) \mid m \in A, n \in B\}$

Scanned by CamScanner

Properties of cartesian product:

- $A \times B \neq B \times A$
- If $A \times B = B \times A$ then
  $A = B$ (or) $A = \phi$ (or) $B = \phi$
- If $|A| = m$, $|B| = n$, $|C| = p$ then $|A \times B| = mn$
  $|A \times B \times C| = mnp$
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$
- $|A| = n$ then $|A \times A| = n^2$

Relations:

Let A, B are two finite sets, A subset R of $A \times B$ is called a relation from A to B.

Note: $|A| = m, |B| = n$

$|A \times B| = mn$

$|P(A \times B)| = 2^{mn} \Rightarrow$ Total possible relns

- If a relation defined from A to A then it is called Binary relation on A.
- If $|A| = n$ then num of binary relns is 2^{n^2}

Ex:- $A = \{1, 2, 3\}$ $B = \{p, q\}$

$|A| = 3$ $|B| = 2$

Num of reln's $= 2^{3 \cdot 2} = 64$

$A \times B$

(1,p) 0/1	(1,q) 0/1
(2,p) 0	(2,q) 0/1
(3,p) 0/1	(3,q) 0/1

(i) Num of reln's which doesn't contain (2,p)

$\Rightarrow 2^5 \cdot 1 \Rightarrow 32$

(ii) Num of reln's which contain atleast 3 elements

$\rightarrow {}^6C_3 + {}^6C_4 + {}^6C_5 + {}^6C_6 \Rightarrow$

Note:

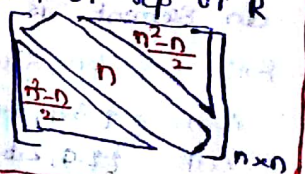
- If R is a binary relation on set A such that $R = \{(a, a) / \forall a \in A\}$ then R is called Diagonal relation on A. It is denoted by Δ_a

  $\therefore \Delta_a = \{(a, a) / \forall a \in A\}$
- If $|A| = n$ and R is a binary reln on A then in matrix form of rep of R

  (i) Num of diagonal elements $= n$

  (ii) Num of non-diagonal elements $= n^2 - n$

  (iii) Num of elements which are above/below the diagonal $= \frac{n^2 - n}{2}$



Types of relation

(1) Reflexive relation:

Let R be a Binary reln on A such that $xRx \ \forall x \in A$ then R is called reflexive relation

Ex:- $A = \{1, 2, 3\}$

$R_1 = \{(1,1)(2,2)(3,3)\}$ ✓

$R_2 = \{(1,1)(2,2)\}$ × (3,3) not avail

$R_3 = \{(1,1)(2,2)(2,3)(3,3)\}$ ✓

Scanned by CamScanner

Note:
- Smallest reflexive relation $\Rightarrow (\Delta_A)$ $\Rightarrow$ min num of Elements $= n$
- largest reflexive relation $(A \times A)$ $\Rightarrow$ max num of Elements $= n^2$
- If $|A| = n$ then num of reflexive relations on set A is 2^{n^2-n}
- Num of reln's which are not reflexive $= 2^{n^2} - \left[2^{n^2-n}\right]$.

(2) Irreflexive relation:

- Let R be a binary relation on A such $\boxed{xRx,\ \forall x \in A}$ then R is Irreflexive reln.

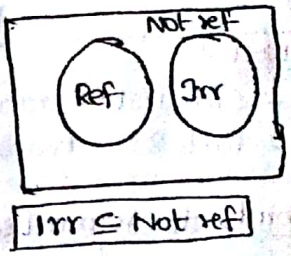
Ex:- $A = \{1,2,3\}$

$R_1 = \phi$ $\Rightarrow$ Irr, Not ref

$R_2 = \{(1,2)(2,1)\}$ $\Rightarrow$ Irr, Not ref

$R_3 = \{(1,2)(1,3)(2,1)(2,3)(3,1)(3,2)\}$ $\Rightarrow$ Irr, Not ref

$R_4 = \{(1,1)(2,1)\}$ $\Rightarrow$ Not Irr, Not ref



Irr $\subseteq$ Not ref

Note:
- smallest Irreflexive relation $\Rightarrow \phi$ $\Rightarrow$ min num of Elements $= 0$
- largest Irreflexive relation $\Rightarrow (A \times A) - \Delta_a$ $\Rightarrow$ max num of Element $= n^2 - n$
- If $|A| = n$ the num of Irreflexive relations on A 2^{n^2-n}
- Num of reln's which are not Irreflexive $= 2^{n^2} - \left[2^{n^2-n}\right]$

(3) Symmetric relation:

- If $\boxed{xRy \text{ then } yRx,\ \forall x,y \in A}$ then R is called symmetric relation

Ex:- $A = \{1,2,3\}$

$R_1 = \phi$ ✓

$R_2 = \{(1,2)(2,1)\}$ ✓

$R_3 = \{(1,2)(2,1)(1,1)(1,3)(3,1)(2,3)(3,2)(3,3)(2,2)\}$ ✓

$R_4 = \{(1,2)(2,1)(3,1)\}$ ✗ (Asym)

Note:
- Smallest sym reln $= \phi$ $\Rightarrow$ min num of Element $= 0$
- largest sym reln $= A \times A$ $\Rightarrow$ max num of Element $= n^2$
- If $|A| = n$ then num of sym relns on A $= 2^n \cdot 2^{\frac{n^2-n}{2}} = 2^{\frac{n(n+1)}{2}}$

Note: If xRy and yRx then R is Asymmetric reln

(4) Antisymmetric relation:

- If $\boxed{xRy \text{ and } yRx \text{ then } x=y \quad \forall x,y \in A}$ then R is Asymmetric relation

Ex:- $A = \{1,2,3\}$

$R_1 = \phi$ ✓

$R_2 = \{(1,2)(1,3)(2,3)\}$ ✓

$R_3 = \{(1,1)(3,2)(2,3)\}$ ✓

$R_4 = \{(1,2)(2,1)(1,3)\}$ ✗

Note:
- Smallest Anti sym reln $= \phi$ $\Rightarrow$ min num of Elements $= 0$
- largest Anti sym reln $=$ depends upon the reln.
  ie If $|A| = n$ then num of Elements in largest Anti sym reln is $\frac{n^2-n}{2} + n = \frac{n^2+n}{2}$
- If $|A| = n$ then num of Anti symmetric relns $= 2^n \cdot 3^{n^2+n/2}$.

Note: The difference b/w Antisym and Asym is, In Asym diagonal Elements are always absent but in Antisym the diagonal elements may present or absent

Scanned by CamScanner

te:

f $|A|=n$ then total num of Asym rels on $A = 1 * 3^{\frac{n^2-n}{2}}$

) Transtive ~~Closure~~ Relation:

OR xRy, yRz such that $xRz \quad \forall x,y,z \in A$ then R is called Transtive relation on A

If xRy and yRz but $x \not R z$ then R is transtive

:- $A = \{1,2,3\}$

$R_1 = \phi$ ✓

$R_2 = \{(1,2)(2,1)(1,1)\}$ × bcoz $(2,2) \times$

$R_3 = \{(1,1)(2,2)(3,3)\}$ ✓

$R_4 = \{(1,1)(2,2)(3,3)(2,1)(1,2)(3,1)(1,3)(2,3)(3,2)\}$ ✓

lote:

- smallest transtive rel = ϕ ⇒ min num of elements = 0
- largest transtive rel = $A \times A$ ⇒ max num of elements = n^2

ints to remember:

reln	Def.	Smallest reln	largest reln	min Elements	max Elements	Num of rel's
reflexive	$xRx \quad \forall x \in A$	Δ_a	$A \times A$	n	n^2	2^{n^2-n}
Irreflexive	$x \not R x, \forall x \in A$	ϕ	$(A \times A) - \Delta_a$	0	n^2-n	2^{n^2-n}
Symmetric	If xRy then $yRx, \forall x,y \in A$	ϕ	$A \times A$	0	n^2	$2^{\frac{n(n+1)}{2}}$
Antisymmetric	If xRy and yRx then $x=y$	ϕ	depends upon rel	0	$\frac{n^2+n}{2}$	$2^n \cdot 3^{\frac{n^2-n}{2}}$
Asymmetric	If xRy then $y \not R x, \forall x,y \in A$	ϕ	depends upon rel	0	n^2-1	$1 \cdot 3^{\frac{n^2-n}{2}}$
Transtive	xRy, yRz then $xRz, \forall x,y,z \in A$	ϕ	$A \times A$	0	n^2	—

Point to remember → we can find $\{U, -\}$

Every Asym rel is Irreflexive

Num of rels	∩	Ref	Irr	Sym	Anti	Asym
2^{n^2-n}	Ref		0	$2^{\frac{n^2-n}{2}}$	$3^{\frac{n^2-n}{2}}$	0
2^{n^2-n}	Irr			$2^{\frac{n^2-n}{2}}$	$3^{\frac{n^2-n}{2}}$	$3^{\frac{n^2-n}{2}}$
$2^n \cdot 2^{\frac{n^2-n}{2}}$	Sym				2^n	$1(\phi)$
$2^n \cdot 3^{\frac{n^2-n}{2}}$	Anti					$3^{\frac{n^2-n}{2}}$

Shortcut:

A → set Relation R

$M_R = [\quad]$

(i) Ref → 1 1 1

(ii) Irr → 0 0 ... 0

(iii) Sym → $M_R^T = M_R$ ⇒ 1/0 mirror 1/0

(iv) Anti → 1/0/0 mirror 1/0/0

(v) Asym → 1 0 ... 0 / 0/1/0 ... 0

Transtive Closure: (R^*)

The smallest transtive rel which contains the given rel is called Transtive closure

Ex:- $A = \{a,b,c\}$ $R = \{(a,b)(b,c)\} \Rightarrow R^* = \{(a,b)(b,c)(a,c)\}$

Reflexive closure: $(R^{\#})$

Let R be a rel on A, A smallest reflexive rel which contains 'R' is called Reflexive closure

Ex:- $A = \{a,b,c\}$ $R = \{(a,b)(b,c)\} \Rightarrow R^{\#} = \{(a,b)(b,c)(a,a)(b,b)(c,c)\}$

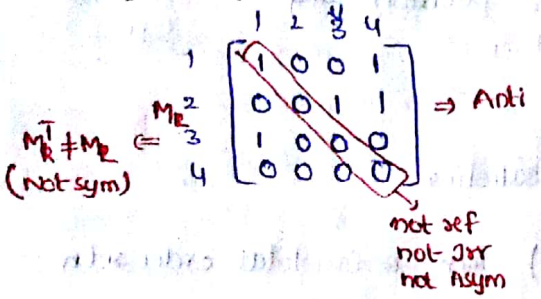
Scanned by CamScanner

Symmetric Closure : (R^+)

- A smallest sym reln which contains given relation 'R' is called Symmetric Closure

Ex:- $A=\{a,b,c\}$ $R=\{(a,b)(b,c)\}$ $R^+=\{(a,b)(b,c)(c,b)(b,a)\}$

Ex:- $A=\{1,2,3,4\}$ $R=\{(1,1)(2,3)(1,4)(2,4)(3,1)\}$



Equivalence relation :

Let R be a binary relation on A, If R satisfies (i) Reflexive (ii) symmetric (iii) Transtive then R is called Equivalence relation.

Note :

~~Let R be~~

Smallest Equivalence reln = Δ_A

Largest Equivalente reln = $A \times A$

If $|A|=n$ then num of Equivalence reln on A is B_n (Bell number)

$B_1 = 1$	$B_3 = 5$	$B_5 = 52$
$B_2 = 2$	$B_4 = 15$	$B_6 = 203$

Note :

$\cup / \cap$	Ref (R_2)	Irr	Sym	Anti	Asym	Trans	Equi
Ref (R_1)	Ref/Ref						
Irr		IR/IR					
Sym			sym/sym				
Anti				Not/Anti			
Asym					Not/Asym		
Trans						Not/Tr	
Equi							Not/Equi

Equivalence class :

Let A be a finite set, 'R' is an Equivalence reln on A

Equivalence class of x is denoted by [x] and

$$[x] = \{ y \mid y \in A \text{ and } xRy \} \quad \forall x \in A$$

Note :

If $A_1, A_2 \cdots A_n$ are n subsets of A such that (i) $i \neq j$; $A_i \cap A_j = \phi$ (ii) $\bigcup_{i=1}^{n} A_i = A$ then

$P\{A_1, A_2 \cdots A_n\}$ is called partition set

Ex:- $A=\{1,2,3,4,5\}$

$R=\{(1,1)(2,2)(3,3)(4,4)(5,5)(1,3)(3,1)(2,5)(5,2)\}$

$\Rightarrow [1]=\{1,3\}$; $[2]=\{2,5\}$; $[3]=\{3,1\}$; $[4]=\{4\}$

$[5]=\{2,5\}$

$\therefore [1]=[3]$ & $[2]=[5]$

$\therefore P=\{[1],[2],[5]\}$

(i) $[1] \cup [2] \cup [5] = A$

(ii) $[1] \cap [2] = \phi$

$[1] \cap [5] = \phi$

$[2] \cap [5] = \phi$

Scanned by CamScanner

Partial order relation :

Let R be a binary relⁿ on set A and If R satisfies
(i) Reflexive
(ii) Antisymmetric
(iii) Transtive then R is called partial order relation and [A ; R] is called poset

Total order relation :

Let R be a binary relⁿ on set A and If R satisfies.
(i) partial order
(ii) Comparability ($\forall a,b \in A$ then $a \not\equiv b$ or $b \not\equiv a$) then R is total order relⁿ

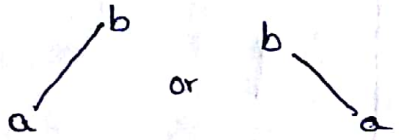
Quassi order relation :

Let R be a binary relⁿ on set A and If R satisfies.
(i) Irreflexive
(ii) Transtive then R is called quassi order relⁿ

Note :
A quassi order relation is always antisymmetric

Hasse diagram :

- The digraph of partial order relation is called Hasse diagram
- Each vertex is represented by •
- No need to exhibit self loops (No self-loops)
- If aRb then we have to show edge from a to b in upward direction



(Transtive relns are Implicit)

- If aRb and bRC then no need to exhibit an edge from a to C.

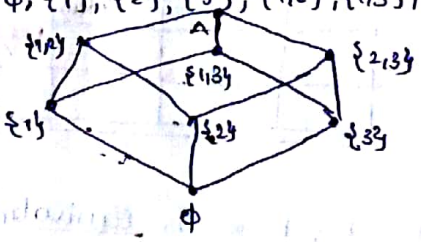
Ex:- (i) $[D_8 ; /]$

Sol : R{(1,2) (1,4) (1,8) (2,4) (2,8) (4,8)

Num of Edges = 3

Ex:- A = {1,2,3} draw $(P(S), \subseteq)$ → |A| = 3 ⇒ cube, |A| = 2 ⇒ square

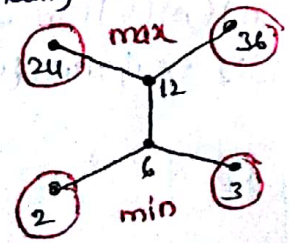
P(S) = { ϕ, {1}, {2}, {3}, {1,2}, {1,3}, {2,3}, A }



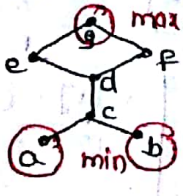
Elements of poset :

[finding MAX, MIN, Greatest, Smallest Elements in poset]

Ex:-



No Greatest
No lowest



No smallest
lowest

Greatest	lowest
aRg	gRa
bRg	gRb
cRg	gRc
dRg	gRd
eRg	gRe
fRg	gRf

Note :
- In a poset max and min elements always exist
- Greatest and smallest may or may not exist, if they exist then they are unique

Scanned by CamScanner

Lower bound : (LB)

Let p be a poset with ordering $\leq$

Assume $A \subseteq P$

x is called lower bound of A iff

$\forall y \in A, x \leq y, (x \in P)$

↓

x is predecessor to all the elements of A

Upper bound : (UB)

Let p be a poset with ordering $\leq$

Assume $A \subseteq P$

x is called upperbound of A iff

$\forall y \in A, x \geq y \Rightarrow y \leq x \quad (x \in P)$

↓

x is a successor to all elements of A

Greatest lower bound (GLB)

- Greatest (Lower bound)
- Let p be a poset with ordering $\leq$

  Assume L is lowerbound of A

  x is called GLB of A iff

$\forall y \in L \quad x \geq y \Rightarrow y \leq x \quad (x \in P)$

↓

Greatest in LB

Lowest Upper bound (LUB)

- Lowest (Upper bound)
- Let p be a poset with ordering $\leq$

  Assume U is UB of A

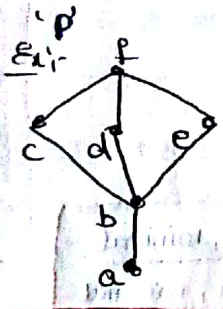
  x is called LUB of A iff

$\forall y \in U \quad x \leq y \quad x \in P$

↓

lowest in UB

Ex:- P



⇒

Lower bound	Upperbound	GLB	LUB
- LB(c,d) = {b,a}	- UB(c,d) = f	- GLB(c,d) = b	- LUB(c,d) = f
- LB(P) = a (least)	- UB(P) = f (Greatest)	- GLB(P) = a	- LUB(P) = f
- LB(d) = d,b,a	- UB(d) = d,f	- GLB(d) = d	- LUB(d) = d
- LB(f,b,c,d) = b,a	- UB(f,b,c,d) = f	- GLB(f,b,c,d) = b	- LUB(f,b,c,d) = f

Note :

- GLB / LUB of single element is itself

Lattice :

Let $(P, \leq)$ be a poset

$(P, \leq)$ is a lattice iff every 2 elements of P contains both LUB (Join ∨) and GLB (meet ∧)

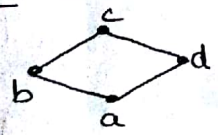
(or)

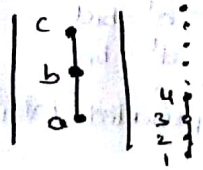
$\forall x, y \in P, \; x \vee y$, $x \wedge y$ Exists

Shortcut : Join → future, meet → past

Common Elements ↗

Ex:- For lattice





Not Lattice ← Open (No meet), Cross (No meet, No Join), disconnected

No meet (a,e)

No meet (a,d) | No join (a,d)

disconnected.

Always prefer to identify not lattice in gate

Types of lattices

- Chain – totally ordered
- Finite
- Infinite
- Bounded
- Complimented
- Distributive
- Boolean.

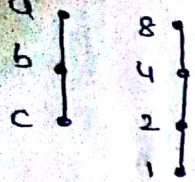
2mp

(P.T.O)

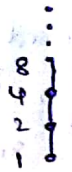
Scanned by CamScanner

① Chain lattice :

- Linearly / Totally ordered

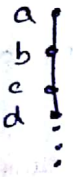


*) $(N, \leq)$ – For Entire lattice Join not Exists



⇒ Semi meet lattice

*) $(N, \geq)$ – For Entire lattice meet not Exists



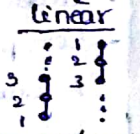
⇒ Semi join lattice

② Finite lattice :

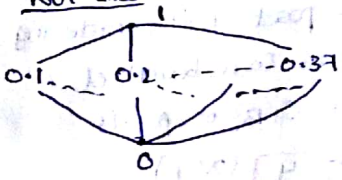
- lattice with finite num of elements

③ Infinite lattice.

Linear



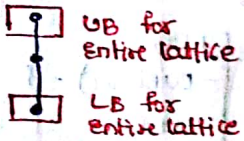
Not linear



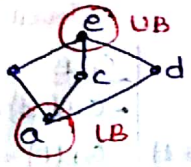
④ Bounded lattice :

- A lattice which has both lowerbound and upperbound for Entire lattice

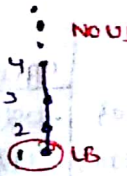
Ex:-



Bounded ✓



Bounded ✓



Not Bounded but lattice.

Note :
- If LB Exist for Entire Bounded lattice It is also called as GLB, least, minimal
- If UB Exist for Entire Bounded lattice. It is also called as LUB, Greatest, maximal

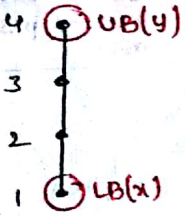
⑤ Complimented lattice :

Def : It is a bounded lattice with 'x' as LB and 'y' as UB if a and b are compliment to each other then

$a \vee b = y$ (Join)
$a \wedge b = x$ (meet)

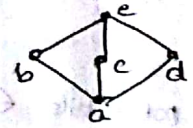
⇒ There Exist a compliment for every Element in the lattice such lattice is called Complemented lattice

Ex:-



$1^c = 4$
$4^c = 1$
2^c = No comp but join & meet Exists
3^c = No Comp but join & meet Exists.

Not Complimented lattice



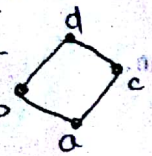
$a' = e$
$e' = a$
$b' = c, d$
$c' = b, d$
$d' = b, c$

∴ Complemented lattice

⑥ Distributive lattice :

Def : In a bounded lattice, if Compliment Exist then it must be unique

Ex:-

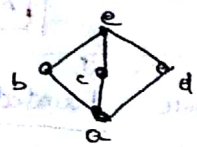


$a' = d$
$d' = a$
$b' = c$
$c' = b$

$1' = 4$
$4' = 1$
$2' = \times$
$3' = \times$

Bounded
Not Complemented

These might be a Chance It is distributive bcoz (0 or 1's comp)



$a' = e$
$e' = a$
$b' = c, d$
$c' = d, b$
$d' = b, c$

Not distributive

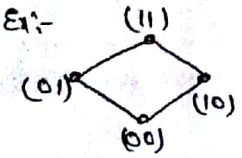
Scanned by CamScanner

Boolean lattice:

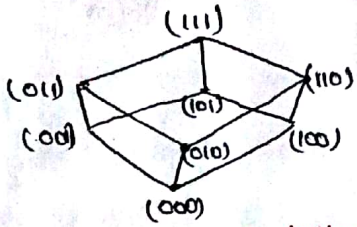
$(B, \vee, \wedge, ', 1, 0)$ is boolean Algebra.

- It is Complemented and distributive ie Every Element has Exactly one Comp

Ex:-



2 var Boolean lattice



3 var Boolean lattice

Functions:

Imp

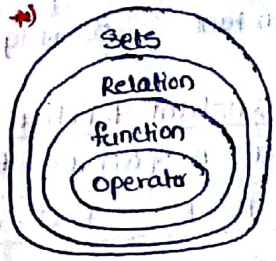
{ _ , _ } set : $A = \{1,2\}$

{ (,) (,) ... } Relation : $R \subseteq A \times B$ where $A = \{1,2\}$ $B = \{a,b,c\}$

{ (_,_) ... } Function : $F : A \to B$

Every Element of domain

{ (,), c, ... } operation : $O : G \times G \to G$



Def: Let $f: A \to B$ [f is a fn from A to B] where A and B are non-Empty sets then

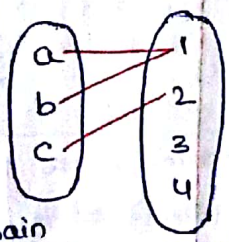
(i) $f \subseteq A \times B$

(ii) $\forall a \in A \ \exists b \in B$ such that $f(a) = b$

(for every Element of domain there Exist Codomain Element as an Image)

(iii) Every Element has unique Image.

Ex:- $f: A \to B$



Domain $= \{a,b,c\}$

Co-domain $\{1,2,3,4\}$

Range $= \{1,2\}$

$\therefore f = \{(a,1)(b,1)(c,2)\}$ such that

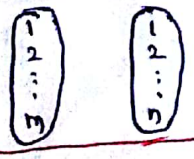
$f(a) = 1 \quad f(b) = 1 \quad f(c) = 2$

$\forall a \in A \ \underbrace{\exists b \in B}_{\text{unique}}$.

$\therefore$ f is function.

Note:

- Size of function $(|f|)$ = Num of $\underset{\text{(or) } |\text{domain}|}{\text{pairs}}$ in f
- Num of possible fns from A to B; If $|A| = m$ & $|B| = n$



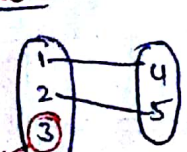
$\Rightarrow n^m \Rightarrow (\text{Codomain})^{\text{domain}}$

Note:

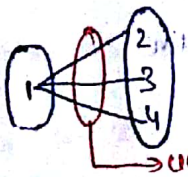
Num of relns which are not fns = Num of relns − Num of fns.

$$\text{Not fns} = 2^{|A||B|} - |B|^{A}$$

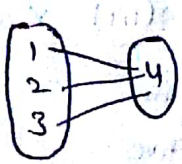
Note:



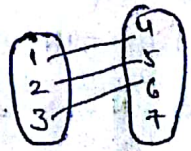
No mapping
Not fn
but reln



unique mapping
Not fn
but reln

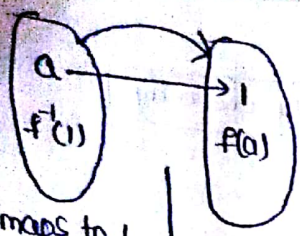


fn ✓



fn ✓

Scanned by CamScanner



a maps to 1
Image of a is 1
$f(a) = 1$

Pre Image of 1 is a
$f^{-1}(1) = a$.

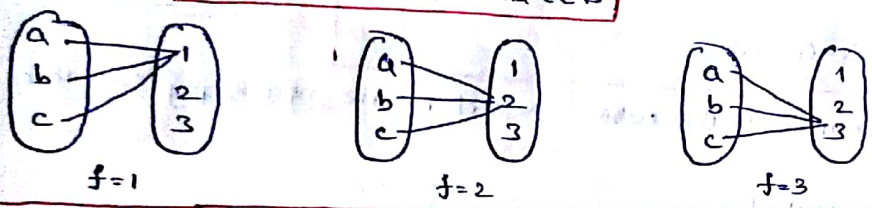
Types of functions :

Constant | Identity | Injective (one-one) | Surjective (onto) | Bijective (Invertible) (1-1 + onto) | Composition

① Constant function :

Let $A = \{a, b, c\}$ $B = \{1, 2, 3\}$

$f : A \to B$ $\quad f(x) = c \quad \forall x \in A$ and $c \in B$



$f = 1$ $\quad f = 2$ $\quad f = 3$

Note : Num of possible Constant functions = |Codomain|

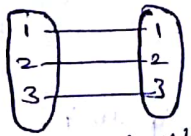
② Identity function :

$f : A \to A$ $\quad f(a) = a \quad \forall a \in A$

Note :
Num of possible Identity fns = 1

$A = \{1, 2, 3\}$

Id :



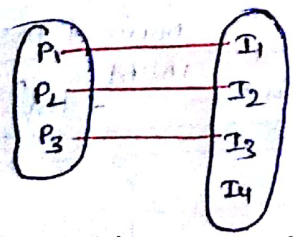
I_R : $\{(1,1)(2,2)(3,3)\}$

Matrix $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Graph :

③ Injective function (one-one)

Def 1 : $f : A \to B$ and
$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$



Def 2 : If $f(x_1) = f(x_2)$ then
$x_1 = x_2$.
⇓
used to solve problems.

Ex :- $f(x) = x^2$ $\quad f : \mathbb{Z} \to \mathbb{Z} \Rightarrow (-1,1)\ (1,1)$ ✗ Not Injective

$f(x) = x^2$ $\quad f : \mathbb{Z} \to \mathbb{N} \Rightarrow (-1,1)\ (1,1)$ ✗ Not Injective

$f(x) = x^2$ $\quad f : \mathbb{N} \to \mathbb{Z} \Rightarrow$ Injective

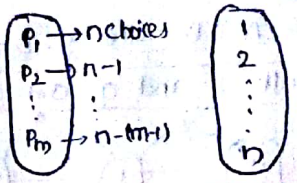
$f(x) = x^2$ $\quad f : \mathbb{N} \to \mathbb{N} \Rightarrow$ Injective

Scanned by CamScanner

Note :

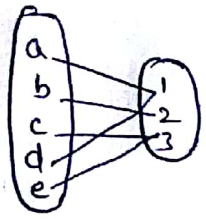
Num of injective fns $= n*(n-1)*(n-2)\ldots(n-(m-1))$

$= {}^{n}P_{m}$



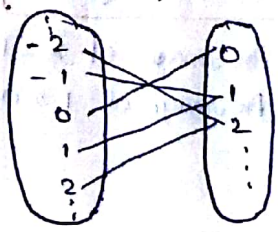
④ Surjective functions (onto)

Def : $\forall b \in B \ \exists a \in A$ such that $f(a) = b$.



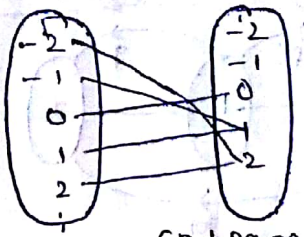
Codomain = range

Ex:- $f(x) = |x|$, $f: Z \to N$



Onto ✓ (CD = Range)
One-one ✗

Ex:- $f(x) = |x|$ $f: Z \to Z$



CD ≠ Range
onto ✗
one-one ✗

Note : $f: A \to B$

Num of possible onto functions : $\sum_{i=0}^{|B|-1} \left[(-1)^i \, {}^{|B|}C_i \, (|B|-i)^{|A|} \right]$

Ex:- $f: A \to B$ $A = \{a,b,c,d\}$ $B = \{1,2,3\}$ Num of onto fns ?

Sol) $|A| = 4$, $|B| = 3$

Num of fns $= |B|^{|A|} \to 3^4 \to 81$

Num of onto = Num of fns − Num of non-onto fns

Non-onto fns : ${}^{3}C_1 \cdot 2^4 - {}^{3}C_2 (1)^4 + {}^{3}C_3 (0)^4$

: 45

∴ Num of onto = 81 − 45 → 36.

⑤ Bijective function :

Def 1 : It is injective and surjective.

Def 2 : f is invertible

Def 3 : f and f^{-1} are functions

Note :

Applicable to finite sets

Injective : $|A| \le |B|$

Surjective : $|A| \ge |B|$

Bijective : $|A| = |B|$

Note : $|A| = n$ $|B| = n$; $f: A \to B$

Num of Bijective fns = $n!$

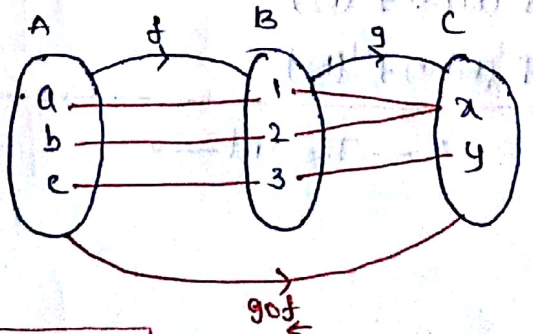
⑥ Composition of fns :

$f: A \to B$.

$g: B \to C$

$gof: A \to C$

← Right to left Association.



Note :

fog and gof need not be same always

Note : Composition opern is Associative

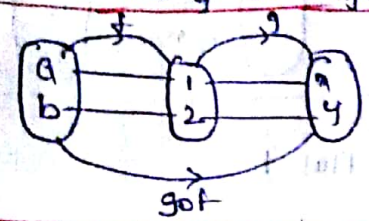
$fo(goh) = (fog)oh$

Scanned by CamScanner

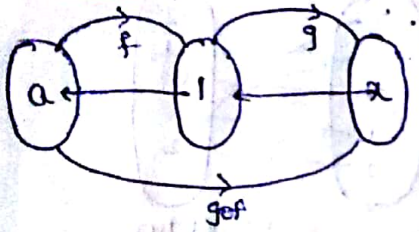
Theorems:

Let $f: A \to B$ and $g: B \to C$ then

① If both f and g are injective, gof is also injective

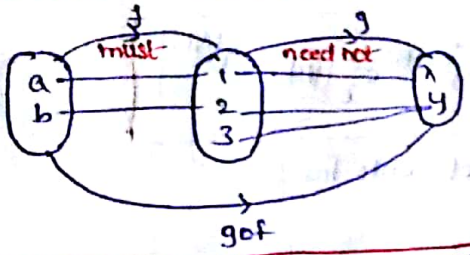


② If f and g are surjective then gof is also surjective

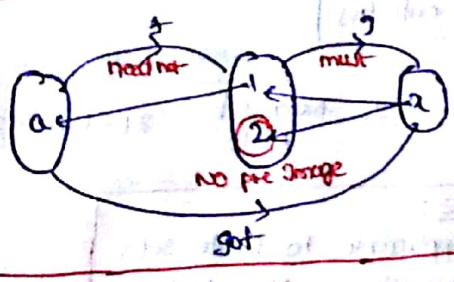


Pre Image of $x = 1$
Pre Image of $1 = a$.

③ If gof is injective then f must be injective [g need not be injective]



④ If gof is surjective then g must be surjective [f need not be surjective]



Note: $g \circ f$
↓ Injective depends here
↓ Surjective depends here

Note:
Let $f: A \to B$ and A_1 and A_2 are subsets of A, B_1 and B_2 are subsets of B

(i) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
(ii) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$
(iii) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$
(iv) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$
(v) $f \circ f^{-1} = I_A$
(vi) $f^{-1} \circ f = I_B$

× — The end — ×

Scanned by CamScanner