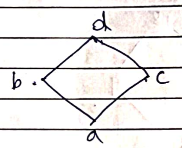
## * Chain – Antichain

A chain is a subset where every part of element is comparable.

Antichain → Not comparable.




Chain → a–b, b–d, c–d, ~~a–c~~, a–c, a–b–d, a–c–d

Anti chain – b–c

An antichain on the other is a subset where no two elements are comparable.

## Mathematical Induction

It is a mathematically proven technique.

1) Basis of Induction
2) Induction step
3) Inducting Hypothesis.

1) Basic of Induction – In basic step given eqⁿ is proved by substituting the basic value of numbers, minimum value of n.

2) In this step given eqⁿ is assumed to be true for k of n

3) In this step given eqⁿ is proved for n = k+1

Q. Prove that $1+2+3+\cdots n = \frac{n(n+1)}{2}$, $n \geq 1$ using MI.

→ Let E be $1+2+3+\cdots n = \frac{n(n+1)}{2}$

Step 1: for $n=1$ we have

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

∴ E is true for $n=1$.

Step 2: Assume that E is true for $n=k$

$$1+2+3+\cdots k \Rightarrow \boxed{k = \frac{k(k+1)}{2}} \quad (1)$$

Step 3: Induction hypothesis

i.e. $1+2+3\cdots k+k+1 = \frac{(k+1)(k+1+1)}{2}$

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

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

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

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

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

Page No.:
Date:

Q. Proof that $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$, $n \geq 1$

→ 1) Basis step-

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

∴ E is true for $n = 1$

2) Assume that E is true for $n = k$

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6} \quad \text{— (I)}$$

3) For $n = k+1$

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

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

$$LHS = 1^2 + 2^2 + \cdots + k^2 + (k+1)^2$$

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

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

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

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

Page No.:
Date:

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

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

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

$$= \frac{(k+1)(k+2)(2k+3)}{6} = RHS.$$

12
7
4 3

Q. Show that $n^4 - 4n^2$ is divisible by 3 for $n \geq 2$ by Induction.

→ Step 1: For $n = 2$ we have.

$2^4 - 4 \times 2^2$, $16 - 16 = 0$; divisible by 3.

Step 3: Assume $n^4 - 4n^2$ is divisible by 3 for $n = k$

∴ $k^4 - 4k^2 = 3x$

∴ $k^4 = 3x + 4k^2$

Step 3: Consider $n^4 - 4n^2$ for $n = k+1$

i.e

$$(k+1)^4 - 4(k+1)^2$$

$$= (k+1)^2((k+1)^2 - 4)$$

$$= (k^2 + 2k + 1)(k^2 + 2k - 3)$$

$$= k^4 + 2k^3 - 3k^2 + 2k^3 + 4k^2 - 6k + k^2 + 2k - 3$$

$$= k^4 + 4k^3 + 2k^2 - 4k - 3$$

$$= 3x + 4k^2 + 4k^3 + 2k^2 - 4k - 3$$

$= 3x + 4k^3 - 4k + 6k^2 \cancel{\quad} - 3$

$= 4k(k^2 - 1) + 6k^2 + 3x - 3$

$= 4k(k+1)(k-1) + 6k^2 + 3x - 5$

$= 4(3y) + 6k^2 + 3x - 3$

$\because (k-1)(k)(k+1)$ is product of 3 consecutive no. which is divisible by 3

~~Ik it~~ Bring in form of multiple in these type of sums

Assume that ~~k~~ $(k-1)\,k\,(k+1) = 3y$

$= 3.(4y + 2k^2 + x - 1)$

Multiplied with 3 so its divisible.

$\therefore (k+1)^4 - 4(k+1)^2$ is divisible by 3.

Q. $8^n - 3^n$ is multiple of 5.

Step 1: $n = 1$

$8^1 - 3^1 = 5$

Step 2: $n = k$

$8^k - 3^k = 5x$ —— (II) $\Rightarrow 8^k = 5x + 3^k$

Step 3: $n = k+1$

$8^{k+1} - 3^{k+1}$

$= 8^k \cdot 8 - 3^k \cdot 3$

$= \cancel{8^k} \; 8 \cdot [5x + 3^k] - 3^k \cdot 3$

Inference Theory ✕

NESO

$= 40x + 8 \cdot 3^k - 3 \cdot 3^k$

~~$= 40x + 5 \cdot 3^k$~~ $= 40x + 3^k(8-3)$

~~$= 5[8k + 3^k]$~~ $= 5(8x + 3^k)$

$\therefore$ It is a multiple of 5

So, $8^{k+1} - 3^{k+1}$ is divisible by 5.

## * Elements in POSET -

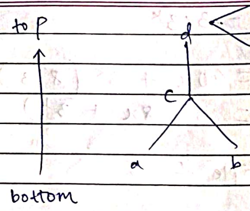
i) Maximal elements - If in a POSET any element is not related to any other element then its called maximal element.

ii) Minimal element - If in a POSET no element is related to any element then it is called minimal element.

iii) Maximum element - It is ~~the~~ a maximal and every element is related to it.

iv) Minimum element - It is minimal and is related to every element in the POSET

Imp Q. in exam.




Maximal — high → one or more

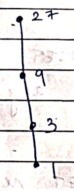
Maximum → Null or only one (greatest)

— low

Minimal — low → Minimal - one or more

Minimum → Minimum - Null or only one (least)

Q. Determine whether the POSET represented by Hasse dig. have greatest, least, maximal, minimal element.



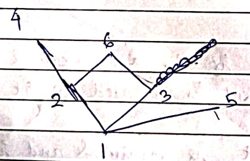

Minimal = 1

Maximal = 27

Maximum = 27

Minimum = 1

Maximum } if elements NULL
Minimum } (not greater than 1)

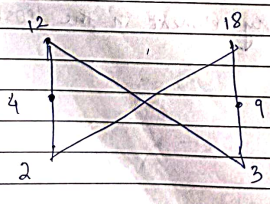



Minimal = 1

Maximal = 4, 6, 5

Maximum = NULL

Minimum = 1

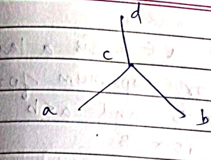



Minimal = 2, 3

Minimum = NULL

Maximal = 12, 18

Maximum = NULL

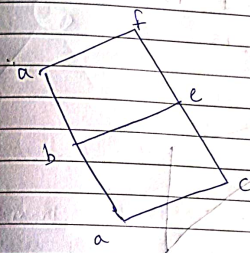



Minimal = a, b

Minimum = NULL

~~Minimal~~ Maximal = d

Maximum = d

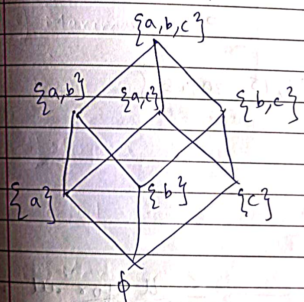



Minimum = a

Minimal = a

Maximum = f

Maximal = f




Minimal = $\phi$

Minimum = $\phi$

Maximal = {a, b, c}

Maximum = {a, b, c}

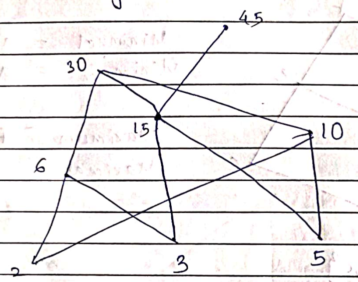
Let B be the subset of poset A

1) Upperbound — An element u belongs to A is called an upper bound of B; If u succeds every element of B where B is POSET

$x \leq u$ for all $x \in B$

Page No.:
Date:

ii) **Least upper bound** - An element $a \in A$ is a least upperbound or supremum for B if a is an upperbound for B and $a < b$ where b is any upperbound for B.




Set A = {2, 3, 5, 6, 10, 15, 30, 45}.

Subset B = {2, 3}

UB, LUB

$2 \rightarrow \underline{6}, 10, \underline{30}$ —— $\leq u$ for all $x \in B$

$3 \rightarrow \underline{6}, 15, \underline{30}, 45$

UB - 6, 30

LUB - 6 (It is the first element we reach for UB)

That's it for POSET

Page No.:
Date:

Let B be the subset of poset B.

**Lowerbound** - An element $l \in A$ is called a lower bound of B if $l$ preceds every element of B.

$l \leq x$ for all $x \in B$

**Greatest Lower Bound** - An element $a \in A$ is greatest lower bound for B if A is lower bound for B and $B < a$ where b is any lower bound for B

Set A = {1, 3, 5, 6, 10, 15, 30, 45}

Subset B = {30, 45}

30 - 6, ~~15~~, 10, 2, ~~3~~, ~~5~~

45 - ~~15~~, ~~3~~, ~~5~~ $\leq u$ for all $x \in B$

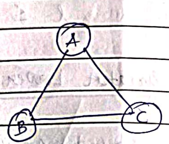
LB = 15, 3, 5

GLB = 15. (greater of all LB)

Page No.:
Date:

Graph – A graph is defined as anordered pair of set of vertices and set of edges.

$G = (V, E)$




Types of Graph

i) Undirected graph – An ~~unin~~ undirected graph has edges that don't point in any direction ~~So, relations~~ meaning relationships between vertices are bidirectional.

ii) Directed graph – A directed graph has an edge with arrows showing relationship btwn vertices is one-way.

iii) Complete graph – A complete graph is the one in which every pair of ~~distict~~ distinct vertices is connected by an edge.

Graph Representation

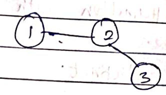
i) Adjacency Matrix –
ii) Adjacency list

Xtra problem Q. > Javapoint, geek for geeks.

Page No.:
Date:

| | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 0 | 1 | 0 |
| 2 | 1 | 0 | 1 |
| 3 | 0 | 1 | 0 |

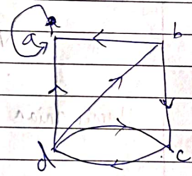
Adjacency Matrix.




Adjacency List

1 : [2]
2 : [1,3]
3 : [2]

Degree of a Vertex. –
In Degree, Outdegree, Total degree (sum of first two)



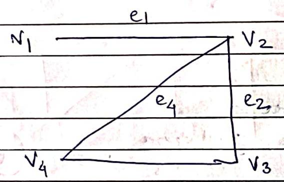

| Vertex | in | out | Total |
|---|---|---|---|
| a | 3 | 1 | 4 |
| b | 1 | 2 | 3 |
| c | 2 | 1 | 3 |
| d | 1 | 3 | 4 |

Hamilton Path – Path must contain all vertices of the graph but the end points can be distinct.

Hamilton circuit – A circuit in a graph That contains that contains all the vertex exactly once except the start and end vertex. (start and end same)

Hamitonian graph – (Which is both Hamiltonian path and circuit)

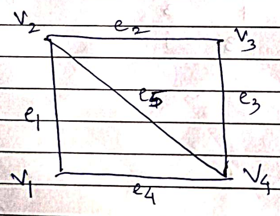
eg;




→ Not a graph

Hamiltonian Path → $V_1 - V_2 - V_3 - V_4$

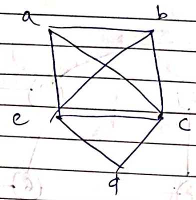
eg;




Hamiltonian Path → $V_1 - V_2 - V_3 - V_4$

Hamiltonian circuit → $V_1 - V_2 - V_3 - V_4 - V_1$

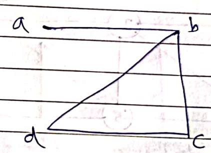
eg;




Hamiltonian Path → a-b-c-d-e.

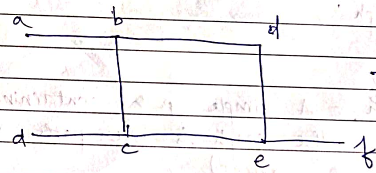
Circuit → a-b-c-d-e-a

eg;



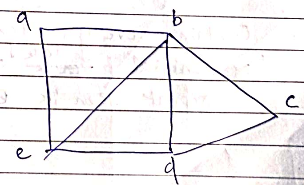

→ It's a path not circuit

eg;




→ Not a path ~~not a circuit~~

eg;



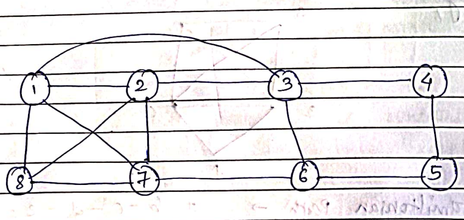

H. Path → a-b-c-d-e

H. Circuit → a-b-c-d-e-a

∴ It is also H. graph

Page No.:
Date:

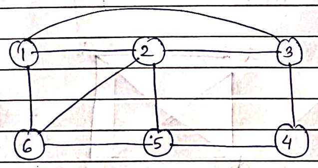
eg;




In exam show all paths.

H path as well as H. circuit hence H. graph.

eg;




If Q. comes then write defi and ~~as~~ then answer.

Is H. graph.

(Talking about edge not vertex)

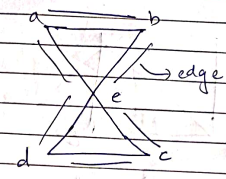
Euler path - A simple path containing all edges of the graph is Euler path. (Edge must not repeat)

Euler circuit - Contains every edge of the graph (~~Eg~~ Initial ~~vertex~~ node and end ~~vertex~~ node repeat then its Euler circuit)

If it's circuit then it's also a path.

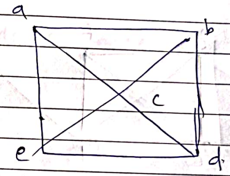
Page No.:
Date:

eg;




Euler path → a - b - e - c - d
Euler circuit → a - b - e - c - d - a

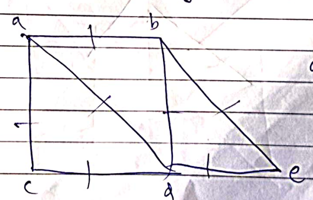
eg;




Not Euler path and not euler circuit.

IMP

eg; { A graph ~~has~~ has only Euler circuit iff every vertex has even degree.
A graph has Euler path and not Euler circuit iff it has exactly two vertex with odd degree



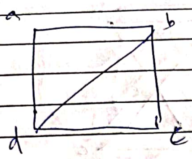

adcadeb

acdebdab

For circuit
Start node = End node.

Euler path - ~~abde~~ ~~abc~~
adcabe d b.

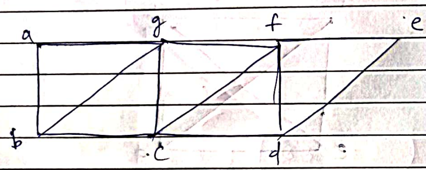
eg;




E· path = b d c b a d

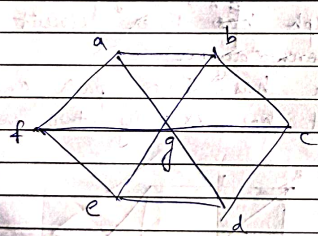
E· circuit X

eg;




E· path - bag fed feg b cd.

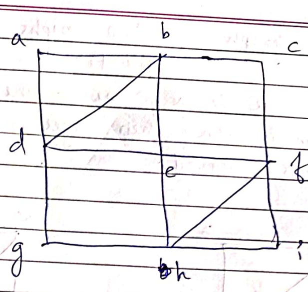
eg;




Not E·path
Not E· circuit

Euler → Edge
Hamilton → Vertex

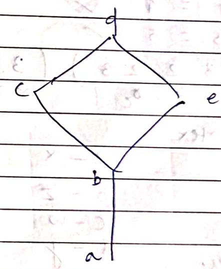
eg;




Is E· circuit ~~tele~~ hence also path

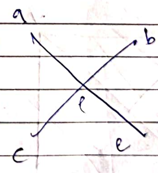
d abdebc fe hi fh gd

eg;



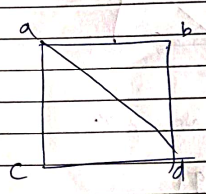

E·P ✓
E·C ✓
∴ E·G ✓

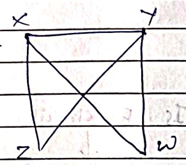
eg;




E·P X
E·C X
E·G X

**Isomorphic graph** - Two graphs G and G' are said to be isomorphic to each other if there is a one to one correspondence. i.e bijection between their edges such that the incidence relationship is preserved.




i) Vertex = 4 = 4 ✓

ii) Edges = 5 = 5 ✓

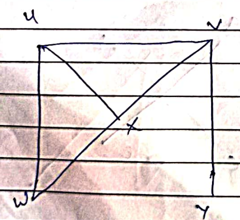
iii) Degree = $\begin{pmatrix} 3 & 2 & 2 & 3 \\ a & b & c & d \end{pmatrix}$ $\begin{pmatrix} 3 & 3 & 2 & 2 \\ x & y & z & w \end{pmatrix}$

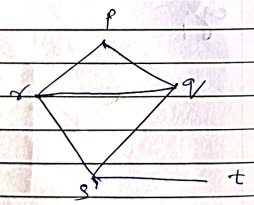
iv) Mapping vertex

a — x
b — z } Have edges
c — w
d — y } don't have edges.

v) Validate edges.

eg;




i) Edges = 6 = 6

ii) Vertex = 5 = 5

iii) Degree = $\begin{matrix} 3 & 3 & 2 & 3 & 1 \\ u & v & w & x & y \end{matrix}$ $\quad \begin{matrix} 2 & 3 & 3 & 3 & 1 \\ p & q & r & s & t \end{matrix}$

iv) Mapping

y — t
w — p
v — s
u — q
x — r

Validate edges.

**Biprite graph** -

Page No.:
Date:

## Counting Principle

Counting principle is used in counting problems like combination, probability or chances in calculation.

Sum Rule and Product Rule are used to decompose difficult counting problems into simple problems.

If a sequence of task $t_1, t_2, t_3, \dots t_n$ can be arranged in $w_1, w_2, w_3 \dots w_n$ ways but in the condition; no task can be performed simultaneous then the number of ways to do this problem is –

$$w_1 + w_2 + w_3 + \dots + w_n$$

## Sum Rule –

$$\begin{array}{ccccc} T_1 & \dots & T_2 & \dots & T_n \\ | & & | & & | \\ w_1 & & w_2 & & w_n \end{array}$$

Not at same time.

$$w_1 + w_2 + w_3 \dots w_n.$$

eg; Distribute bags to IT or CMPN department.
To students in IT or CMPN
100 150

$= 100 + 150 = 250$ ways.

Page No.:
Date:

## Rule of Product

If a sequence of task $t_1, t_2, t_3 \dots t_n$ can be done in $w_1, w_2 \dots w_n$ ways respectively and every task arrives after the occurence of previous task then there are ~~$w_1 \cdot t_1, t$~~ ~~$t_1 \cdot w_1, t_2 \cdot w_2, \dots$~~ ~~$t_n w_n$ ways to perform the task.~~
$w_1 \times w_2 \times \dots w_n$ ways to perform the task.

eg; How many different license plates are there that contain 3 english letters.

→

$$\underset{26}{\_\_} \quad \underset{26}{\_\_} \quad \underset{26}{\_\_} \Rightarrow 26 \times 26 \times 26 \text{ ways.}$$

## Pigeon Hole Principle

If $n+1$ or more objects are placed into $n$ boxes. then there is at least one box containing two or more objects.

Q. If 6 colours are used to paint 37 houses. Show that atleast 7 of them will have the same colours.

→

Mod $\frac{37}{6} = 6 \rightarrow$ Quotient
$1 \rightarrow$ Remainder $\Rightarrow$ 1 house has same color

Q. Find the minimum no. of teachers in the college to ensure that 4 of them are born in a same month.

(pigeon)

$k + 1 = 4$

$k = 3$

pigeon holes $\rightarrow n = 12$

$kn = 36 + 1 = 37$

Page No.:
Date:

Q. A box contains 10 blue balls, 20 red balls, 18 green balls, 15 yellow balls and 25 white balls. How many balls we must choose to ensure that we have 12 balls of same color.

$n \to$ pigeon ~~holes~~ holes
$n+1 \to$ pigeons

$n = 5 \to$ 5 different colors

$k+1 = 12$
$k = 11$

$kn+1 = 11 \times 5 + 1 = 56$

Q. If 8 persons are chosen from any grp. show that at least two of them will have the same birthday.

Since there are 8 persons which are more than pigeon holes (7 days) two of them will have same bday.

Q. If 7 colours are used to paint 50 bicycles. Show that at least 8 will be of same color.

→ Mod.

Q. What is the least no. of person in a grp such that name of atleast two of them so that name of each of them will start with same alphabet.

→ 27. (26 alphabets so, 27 person)

# Algebraic Structure

Page No.:
Date:

Algebraic structures with Binary Operation - Semigroup, Monoid, group, Subgroup, Abelian group

Algeb
Coding Theory
Binary Information
Error Correction

Two

Sets
N: Natural Nos.
Z: Integer "
R: Real "
Q: Rational "
C: Complex Nos.

(1) Binary Operations

$G \times G \xrightarrow{\text{belongs to}} G$ Operation (+)

$a, b \in G$ $(a+b) \in G$

Two elements belong to a set and its operation result also belongs to the same set then this concept is called closure.

eg; $\underline{Z}$
3, 5

$3 + 5 = 8$
$8 \in Z$ ∴ It is a closure.

$(Z, +) \to$ Is algebraic structure if its closure

set, operation

Given an algebraic structure it will follow closure property'
i) Associative
ii) Commutative
iii) Identity
iv) Inverse
and depending on these property it is a semigroup, moniod, group or albelian group.

Closure Property -

$a * b \in G$ of $\forall$ ab, $\in G$ is unique.

eg; $Z = \{\infty \ldots -2, -1, 0, 1, 2, \ldots \infty\}$

$(-3, -2) \in Z$
$(-3) + (-2) = -5 \in Z$

$\therefore$ Z is said to be close with respect to $(+)$

$-, *$ } Binary op

/ - Not ~~op~~ binary operation.

Algebraic Structures - A non empty set together with or more than one binary operation is called algebraic structure.

eg; $Z = \{-\infty, \ldots -1, 0, 1, \ldots \infty\}$

$(\underbrace{Z}_{\text{set}}, \underbrace{+, \cdot}_{\text{Binary operation}})$

Laws and properties of binary operations

I) Associative - A binary operation on a set S is said to be associative iff

$a * (b * c) = (a * b) * c$ for all $a, b, c \in S$

eg; Let algebraic structure $(Z, +)$
$Z = \{\infty, \ldots -2, -1, 0, 1, 2, \ldots \infty\}$
Let $-3, -2, 4 \in Z$
$\therefore (-3 + (-2)) + 4 = -3 + ((-2) + 4)$

$-1 = -1$

The ~~asso~~ algebraic ~~representation~~ structure $(Z, +)$ where the binary operation $+$ on set Z holds associative property.

ii) Commutative property - A binary operation on the element of a set is commutative iff

$\boxed{a * b = b * a \quad \forall \; a, b \in S}$

eg; Let algebraic structure $(Z, +)$

$Z = \{-\infty, \ldots -2, -1, 0, 1, 2, \ldots \infty\}$

$-7, 6 \in Z$
$-7 + 6 = 6 + (-7)$
$-1 = -1$
$\therefore$ The algebraic structure $(Z, +)$ where binary operation of addition on Z is commutative.
Also, $(Z, \cdot)$, ~~(Z, -)~~

$*$ → Binary operation
$\cdot$ → into (Multiply)

Page No.:
Date:

iii) Identity element: – An identity element in a set S is called an identity element w.r.t binary operation $*$ iff

$$\underbrace{a * e}_{\text{Right Identity element}} = \underbrace{e * a}_{\text{Left Identity element}} = a$$

Identity element

eg, $Z = \{-\infty, \ldots -2, -1, 0, 1, 2 \ldots \infty\}$

$$\underbrace{-5 + 0 = -5 + 0}_{\text{Identity element}} = -5$$

0 is identity element w.r.t binary operation addition.

$(Z, \cdot)$ → Identity element is 1

iv) Inverse Element – If identity element is present then and only inverse element is present. Consider the set S having identity element 'e' w.r.t binary operation $*$.
If corresponding to each element a, such that $a \in S$ there exist an element b such that $\exists B \in S$ then

$$\boxed{a \times b = b \times a = e}$$

Then b is said to be inverse of a
$a^{-1} = b$

Page No.:
Date:

given a set a binary operation is defined on that set then this property is called closure property.

1) Closure property → Algebraic structure (groupoid)
Z and $*$ → $(Z, *)$
↓
2) Associative property → Semigroup.
↓
3) Identity element → Monoid.
↓
4) Inverse element → Group
↓
5) Cumutative property → ~~Abe~~ Abelian group

Group – Let $(G, *)$ be an algebraic structure where $*$ be a binary operation then $(G, *)$ is called a group under this operation if closure property, associative property, identity and inverse property are satisfied.

eg; Let $(R, +)$ be the algebraic structure. Comment whether it is a group or not.

Check for closure
If algebraic structure is given then its closure.

1) Associative : $(3+10)+2 = 3+(10+2)$
$15 = 15$
$15 \in R$

2) Identity element –

Identity element

$15 + 0 = 0 + 15$ $(e = 0)$
$15 = 15$

In exam write law no terms.

3) Inverse element :

~~2 + (-2) = 0~~

$$2 + (-2) = 0 = (-2) + 2$$

$\to e$

$\therefore (R, +)$ is group.

Q2. Prove that 4th root of unity $1, -1, i, -i$ is a form of multiplicative group.

| $\times$ | $1$ | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ |

$\therefore$ It is a group

Since all elements belong to G so G is close w.r.t. binary operation.

$1 \times (i \times (-i)) = (1 \times i) \times (-i)$

$= 1 \times 1 \qquad = i \times -i$

$= 1 \qquad = 1$ Associative ✓

$e = 1$ $\therefore$ It is a multiplication grp.

Q. Prepare a ~~multiplication~~ composition table for multiplication on the element in set A

$A = \{1, \omega, \omega^2\}$ where $\omega$ is the cube root of unity. Show that algebraic structure $(A, \times)$ is Abelian group. ($\times$ → Multiplication)

| $\times$ | $1$ | $\omega$ | $\omega^2$ |
|---|---|---|---|
| $1$ | $1$ | $\omega$ | $\omega^2$ |
| $\omega$ | $\omega$ | $\omega^2$ | $1$ |
| $\omega^2$ | $\omega^2$ | $1$ | $\omega$ |

$\because \omega^3 = 1$

It is a closure.

For Associative Property –

Now,

$$\omega \times (1 \times \omega^2) = (\omega \times 1) \times \omega^2$$

$$\therefore \omega \times \omega^2 = \omega \times \omega^2$$

$$\omega^3 = \omega^3$$

$$1 = 1$$

For identity, $e = 1$

It is an abel

For inverse, $(1, 1), (\omega, \omega^2), (\omega^2, \omega)$ → It is equal to value of e.

$1^{-1} = 1, \quad \omega^{-1} = \omega^2 \quad \omega^{-2} = \omega$

$a \times b = b \times a$

Cumutative

$1 \times w = w \times 1$

$\therefore w = w$

It is abelian group.

Q. Determine the set together with Binary operation is semigroup or not.

$Z^+$, where $a * b = \max(a,b)$

$a, b \in Z^+$

$\rightarrow$

$100, 200 \in Z^+$

$\underset{\substack{\downarrow \\ \text{Max}}}{100 * 200} = 200 \in Z^+$

Closure ✓

∴ It is monoid

$(50 * 100) * 500 = 50 * (100 * 500)$

$100 * 500 = 50 * 500$

$500 = 500$.

Here $e = 1$.

$-i$

$-i \times i \times -i$

$-1 \times -i = i$

Ring –

An algebraic system $(R, +, \cdot)$ is called ring if

i) $(R,+)$ is abelian ii) $(R, \cdot)$ is semigroup i.e

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $a, b, c \in R$

Various types of ring also there.

iii) Operative must be distributive over the operation. $\pm$ is satisfied.

i.e $a \cdot (b + c) = a \cdot b + b \cdot c$ $\forall a, b, c \in R$.

Cyclic group – Show that the multiplicative group $G = \{1, -1, i, -i\}$ is a cyclic group.

We have,

$1^1 = 1$

$\boxed{1^2 = 1 \times 1 = 1}$

$\Rightarrow O(1) = 1$

Order of 1

$-1^1 = -1$ and $-1^2 = 1$

$\Rightarrow O(-1) = 2$

For $i$,

$i^1 = i$

$i^2 = -1$

$i^3 = -i$

$i^4 = 1$

After next element the sequence gets repeated. $O(i) = 4$

Here generative element (element on which operation performed).

$-i^1 = -i$

$-i^2 = 1$

$-i^3 = i$

$-i^4 = -1$

$O(-i) = 4$.

eg;

$G = \{1, \omega, \omega^2\}$

$1 = 1$ $\qquad O(\omega^2) = 3$

$1^2 = 1$ $\qquad O(\omega) = 3$

$\qquad O(1) = 1$

eg; $(G, +_6)$ → Modulus 6.

$G = \{0, 1, 2, 3, 4, 5\}$

% 8

~~$1^1 = 1$~~

~~$1^2 = 1 +_6 1 = 2$~~

$1^1 = 1$

$1^2 = 1 +_6 1 = 2$ $\quad$ ( 2 % 6

$1^3 = 1 +_6 1 +_6 1 +_6 = 3$

$1^4 = 4$

$1^5 = 5$

$1^6 = 0$

$O(1) = 6.$

## Lattice –

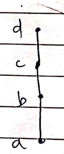
Poset
↓
Subset
$\begin{cases} \text{LUB} & \text{— Join — Join semi lattice} \\ \text{GUB} & \text{— Meet — Meet semilattice.} \end{cases}$

Let A, B ∈ Lattice L then ~~LUB – S~~

LUB (a, b) $\qquad \underset{\text{disjunction.}}{\vee} \qquad \underset{\text{union}}{\cup} \qquad$ supremum.

Consider the

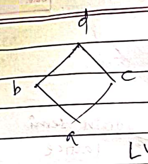
In a poset if join exist for every pair of elements then it is called join semilattice.

d
c
b
a


LUB

| + ∨ ∪ | a | b | c | d |
|---|---|---|---|---|
| a | a | b | c | d |
| b | b | b | c | d |
| c | c | c | c | d |
| d | d | d | d | d |

If table filled then it is join semilattice.




LUB.

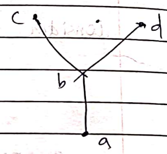
| V | a | b | c | d |
|---|---|---|---|---|
| a | a | b | c | d |
| b | b | b | d | d |
| c | c | d | c | d |
| d | d | d | d | d |

It is a joined semi lattice.

Q. If two element at tops then its not joined semi lattice.

| V | a | b | c | d |
|---|---|---|---|---|
| a | | | | |
| b | | | | |
| c | | | | |
| d | | | | |

LUB



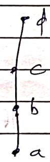

It is not joined semi lattice.

## Meet Semi Lattice – ∧, ∩, ·, *

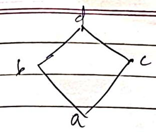
Q.

| ∧ | a | b | c | d |
|---|---|---|---|---|
| a | a | a | a | a |
| b | a | b | b | b |
| c | a | b | c | c |
| d | a | b | c | d |

GLB




Q.




GLB

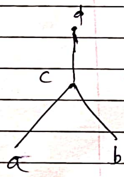
| ∧ | a | b | c | d |
|---|---|---|---|---|
| a | a | a | a | a |
| b | a | b | a | b |
| c | a | a | c | c |
| d | a | b | c | d |

It is meet semi lattice

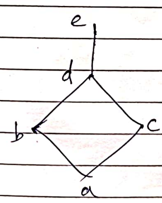
Q Any diagram that has two element at bottom will not be a meet semi lattice.

| | a | b | c | d |
|---|---|---|---|---|
| a | | | | |
| b | | | | |
| c | | | | |
| d | | | | |

GLB




$x \vee y = \text{LUB}\{x, y\}$
$x \wedge y = \text{GLB}\{x, y\}$




| V | a | b | c | d | e |
|---|---|---|---|---|---|
| a | a | b | c | d | e |
| b | b | b | d | d | e |
| c | c | b | c | d | e |
| d | d | d | d | d | e |
| e | e | e | e | e | e |

LUB

It is Join Semi Lattice.

eg;