Ex prove that the fourth roots of unity $1, -1, i, -i$ form an abelian multiplicative group.

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

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

i) closure property :- Since all the entries in the table are the elements of G hence G is closed

ii) Associative law

$$a(bc) = (ab)c \text{ for all values of } a, b, c \text{ in } G$$

(iii) Commutative Law $ab = ba$ for all a, b in G

(iv) Identity element $1 \in G$ is identity element as $1 \cdot a = a \cdot 1 = a$ ~~It~~ can be seen from the first row and first column of the table.

(v) Inverse of ~~$1 = 1$, $-1 = -1$, $i = -i$, $-i = i$~~ $1 = 1$, $-1 = -1$, $i = -i$, $-i = i$

Ex Show that the matrices,

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

form a multiplicative abelian group.

Soln

Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $D = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

$G = \{A, B, C, D\}$

$$A \cdot A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0+1 & 0+0 \\ 0+0 & 0+1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = A$$

$$A \cdot B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1+0 & 0+0 \\ 0+0 & 0+1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = B$$

Similarly $AC = C$, $AD = D$, $BB = A$ etc.

X	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

(i) Closure property :- all the elements in table are the elements of G.

(ii) Associative law :-

$$(AB)C = A(BC)$$

(iii) Commutative law :-

$$A \cdot B = B \cdot A$$

(iv) Existence of Identity

$$AA = A, \quad AB = B, \quad AC = C, \quad AD = D$$

(v) Existence of Inverse

$$AA = A; \quad BB = A, \quad CC = A, \quad DD = A$$

hence $G = \{A, B, C, D\}$ is an abelian group

Ex Prove that the set $\{0, 1, 2, 3, 4\}$ is a finite abelian group of order 5 under addition modulo 5 as composition.

Sol :- To test the nature of the system $(G, +_5)$ where $G = \{0, 1, 2, 3, 4\}$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

~~2+4=1~~ from the table we can see that it follows all the five properties

i) closure ii) associative iii) Identity iv Inverse and commutative.

Ex Show that the set $\{1,2,3,4,5\}$ is not a group under addition and multiplication modulo 6.

Sol (i) Let $G = \{1,2,3,4,5\}$ the operation addition modulo 6 is denoted by $+_6$. We can operate $+_6$ on the element in G and prepare the composition table as -

$+_6$	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

Since all the entries in the composition table do not belong to G, in particular $0 \notin G$. Hence G is not closed w.r.t $+_6$ consequently $(G, +_6)$ is not a group.

(ii) The operation multiplication modulo 6 is denoted by $\times_6$.

$\times_6$	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

From the composition table, it is clear that all the entries in the composition table do not belong to G, In particular $0 \notin G$ Hence G is not closed w.r.t $\times_6$.

Consequently $(G, \times_6)$ is not a group.

General properties of a group.

1) The identity element is a group is unique.

Proof Let us suppose that $a \in G$ and, e, e' be the two identities in G.

$$e \in G \quad a \in G \Rightarrow ae = a \qquad \text{—(i)}$$

$$e' \in G \quad a \in G \Rightarrow ae' = a \qquad \text{—(ii)}$$

from (i) and (ii). we get

$$ae = ae' \Rightarrow e = e'$$

Hence the identity element of a group is unique.

2) The inverse of each element of a group is unique.

Proof Let $a \in G$ and $e \in G$

Let b and c be the two inverses of a in G.

$$a \in G \quad b \in G \Rightarrow ab = e \quad \text{(i)}$$

$$a \in G \quad c \in G \Rightarrow ac = e \quad \text{(ii)}$$

$$ab = ac$$

$$b = c$$

Hence inverse element in a group is unique.

From the composition table, it is clear that all the entries in the composition table do not belong to G, In particular $0 \notin G$ Hence G is not closed w.r.t $\times_6$.

Consequently $(G, \times_6)$ is not a group.

Algebric Structure (Mathematical Structure)

A non-empty set G equiped with some operations and some properties is called an algebric structure.

If $*$ is an operation on G then $(G, *)$ is an algebric structure. $(N, +)$, $(R; +, \times)$ are examples of algebric structure.

Group ⓘ– A group must follow these properties.

G_1: closure Property.

G_2: Associative Property.

G_3: Existence of Identity.

G_4: Existence of Inverse.

Abelian Group:- ⑤ A group G is said to be abelian group, if it satisfies the commutative property
G5: Commutative $a * b = b * a \ \forall a, b \in G$

Groupoid:- ① An algebric structure $(G, *)$ is said to be a groupoid, If it satisfies the closure property only.

Semi-group:- ② it satisfies the closure and associative properties.

Monoid ③- if it satisfies closure, associative and existence of Identity.

Scanned with CamScanner

Algebraic Structure

Binary operations:

Let A be a non-empty set, then a function $f: A \times A \to A$ is called a binary operation on A.

A function $g: A \to A$ is called unary operation on A and a function $h: A \times A \times A \to A$ is called ternary operation on A and in general, an n-ary operation is a function from $\underbrace{A \times A \times \cdots \times A}_{n \text{ factors}}$ A.

Properties of Binary operations

1. Associative law - An operation $*$ on a set A is said to be associative or to satisfy the associative law, if for any elements, a, b, c in A, ~~ab~~ we have

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

Ex Consider the set Z^+ of non-negative integers. Check whether the operation $*$ defined by

$$a*b = a^2+b \quad \forall\ a, b \in Z^+ \text{ is associative or not.}$$

Sol for $a, b, c \in Z^+$

$$(a*b)*c = (a^2+b)*c$$
$$= (a^2+b)^2+c = a^4+b^2+2a^2b+c$$

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

Thus $*$ is not an associative operation.

2. Commutative law :- A binary operation $*$ on the elements of the set is commutative or satisfies commutative property if and only if for any two elements a and $b \in A$

$$a * b = b * a$$

Ex Consider the operation $*$ defined on the set $\mathbb{Z}^+$ of non-negative integers as

$$a * b = a + b + 2 \text{ for } a, b \in \mathbb{Z}^+$$

Show that $*$ is commutative as well as associative.

Sol. $*$ is a commutative operation since.

$$a * b = a + b + 2 = b + a + 2 = b * a$$ (addition of integers is comm)

Now consider $a, b, c \in \mathbb{Z}^+$, then

$$(a * b) * c = (a + b + 2) * c$$

$$= (a + b + 2) + c + 2 = a + b + c + 4$$

and $$a * (b * c) = a * (b + c + 2)$$

$$= a + (b + c + 2) + 2 = a + b + c + 4$$

which shows that $*$ is an associative operation

Ex Consider the set N of Natural number. Define an operation $*$ on N as.

$$a * b = a^b \text{ for all } a, b \in N$$

Show that $*$ is neither commutative nor associative.

Solution :- $*$ is not commutative, since
$$2*3 = 2^3 = 8 \text{ and } 3*2 = 3^2 = 9$$
Also, $*$ is not associative since
$$(2*2)*3 = (2^2)*3 = (2^2)^3 = (4)^3 = 64$$
and $2*(2*3) = 2*(2^3) = 2*8 = 2^8 = 256$

Thus, $*$ is neither commutative nor associative.

3. Identity Element :-
An element 'e' in a set A is called an identity element with respect to the binary operation $*$ if, for any element 'a' in A.
$$a*e = e*a = a$$

4. Inverse element. Consider a set A having the identity element 'e' with respect to the binary operation $*$. If corresponding to each element $a \in A$ there exists an element $b \in A$ such that
$$a*b = b*a = e$$
then 'b' is said to be the inverse of 'a' and is usually denoted by a^{-1}.

Ex Consider the binary operation $*$ defined on the set $A = \{a, b, c\}$ by the following table -

*	a	b	c
a	b	c	b
b	a	b	c
c	c	a	b

Scanned with CamScanner

(a) Is $*$ a commutative operation?

(b) Compute $a*(b*c)$ and $(a*b)*c$

(c) Is $*$ an associative operation?

Solution :-

a) The operation $*$ is not commutative since $a*b=c$ and $b*a=a$

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

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

(c) $*$ is an associative operation since,

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

Cyclic group :-

A group $(G, *)$ is called cyclic if for $a \in G$, every element $x \in G$ is of the form a^n, where n is some integer. Symbolically, $G = \{a^n \mid n \in I\}$

The element a is then called a generator of G. We may occur more than one generator of a cyclic group. If G is a cyclic group generated by a then we write $G = \{a\}$ or $G = \{a\}$

Illustration :- The multiplicative group

$$G = \{1, -1, i, -i\} \text{ is cyclic.}$$

We can write $G = \{i, i^2, i^3, i^4\}$

Thus G is a cyclic group and generator this group is i. Also we can write

$$G = \{-i, (-i)^2, (-i)^3, (-i)^4\}$$

Thus $(-i)$ is also a generator of G.

Ex The multiplicative group of the three cube roots of unity. $\{w, w^2, w^3=1\}$ is a cyclic group of order 3. the generators of this group are w and w^2

Ex. The group $G=(\{0,1,2,3,4,5\},+_6)$ is cyclic group. Here the generators are 1 and 5 we can see that by composition table.

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

$1^1=1,\ 1^2=1+1=2,\ 1^3=1^2+1=3,\ 1^4=1^3+1=4$

$1^5=1^4+1=5,\ 1^6=1^5+1=0$

therefore $G=\{1,1^2,1^3,1^4,1^5,1^6=0\}$

$5^1=5,\ 5^2=5^1+5=4,\ 5^3=5^2+5=4+5=3,\ 5^4=3+5=2,$

$5^5=2+5=1,\ 5^6=1+5=0$

therefore $G=\{5,5^2,5^3,5^4,5^5,5^6=0\}$

hence 1 and 5 are the generators of the given group.

5.17.7 Cyclic Permutation

Let $S = \{a_1, a_2, a_3 \ldots a_n\}$ be finite set of n symbols. A permutation f defined on S is said to be cyclic permutation if f is defined such that

$$f(a_1) = a_2,\ f(a_2) = a_3,\ f(a_3) = a_4 \ldots f(a_{n-1})) = a_n \text{ and } f(a_n) = a_1.$$

Illustration: *Let* $S = \{1, 2, 3, 4\}$ *then* $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ *is cyclic permutation. It is written as* $f = (1\,2\,3\,4)$.

Illustration: *Let* $(1\,3\,4\,2\,6)$ *is cycle of length 5. Suppose it represents a permutation of degree 9 on a set S consisting of the elements* 1, 2, 3 ...9. *Then the permutation.*

$$f = \begin{pmatrix} 1 & 3 & 4 & 2 & 6 & 5 & 7 & 8 & 9 \\ 3 & 4 & 2 & 6 & 1 & 5 & 7 & 8 & 9 \end{pmatrix}$$

5.17.8 Transposition

A cycle of length 2 is called ***Transposition***

Remark: 1. Let $S=\{a_1, a_2, a_3 \dots a_n\}$ f, g, h be cyclic permutation on S. Then

(i) $(f o g)^{-1} = g^{-1} o f^{-1}$ (ii) $(f o g o h)^{-1} = h^{-1} o g^{-1} o h^{-1}$

2. If S_n is a permutation group on n symbols, then of the $n!$ permutation in S_n, $\frac{n!}{2}$ are even permutation and $\frac{n!}{2}$ are odd permutation.

3. The set of all even permutation of degree n form a group under the composition of permutations.

4. The group of even permutation is called ***Alternating Group***.

5. Every permutation may be expressed as the product of transposition in many ways.

6. If f is a cycle of length n, then f can be expressed as the product of $(n-1)$ transposition, even and odd permutation.

5.17.9 Even and Odd Permutation

A permutation f is said to be an even permutation if f can be expressed as the product of even number of transpositions. A permutation f is said to be an odd permutation if f can be expressed as the product of odd number of transposition.

Remark:

(i) An identity permutation is consider as an even permutation

(ii) A transposition is always odd

(iii) The product of two even permutation is even and also the product of two odd permutation is even.

(iv) The product of an even and an odd permutation is odd. Similarly the product of an odd permutation and an even permutation is odd.

5.17.10 Disjoint Cycle

Let $S=\{a_1, a_2, a_3, \dots a_n\}$. If f and g are two cycles on S such that they have no element common then f and g are said to be disjoint cycles.

Illustration: Let $S=\{1, 2, 3, 4, 5, 6\}$ if $f=(1\ 4\ 5)$ and $g=(2, 3, 6)$ Then f and g are disjoint cycle permutation on S.

Note:

1. The product of two disjoint cycles is commutative
2. Even permutation can be written as a product of disjoint cycles and transposition

Illustration: Let $f = (123)$ and $g = (45)$ be two permutations on 5 symbols 1, 2, 3, ...5. Then

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$$gf = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$$\therefore \qquad fg = gf$$

Illustration: Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 1 & 4 & 8 & 6 & 9 & 7 & 5 \end{pmatrix}$

be a permutation of degree 9 on the set (1, 2, 3..9)

We have $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 4 \\ 4 \end{pmatrix}\begin{pmatrix} 6 \\ 6 \end{pmatrix}\begin{pmatrix} 5 & 8 & 7 & 9 \\ 8 & 7 & 9 & 5 \end{pmatrix} \Rightarrow f = (1\ 2\ 3)(5\ 8\ 7\ 9)(4)(6)$

Example 49: *If* $S = (1, 2, 3, 4, 5, 6)$

Compute $(5\,6\,3)\,0(4\,1\,3\,5)$

Solution: We have $(5\ 6\ 3)\ 0\ (4\ 1\ 3\ 5) = \begin{pmatrix} 5 & 6 & 3 \\ 6 & 3 & 5 \end{pmatrix}\begin{pmatrix} 4 & 1 & 3 & 5 \\ 1 & 3 & 5 & 4 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 4 & 5 & 6 & 3 \\ 1 & 2 & 4 & 6 & 3 & 5 \end{pmatrix}\begin{pmatrix} 4 & 1 & 3 & 5 & 2 & 6 \\ 1 & 3 & 5 & 4 & 2 & 6 \end{pmatrix}$$

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

Example 50: *Express the following permutation as the product of disjoint cycles*

$$g = (1\ 3\ 2\ 5)\ (1\ 4\ 3)\ (2\ 5\ 1)$$

Solution: We have $g = (1\ 3\ 2\ 5)\ (1\ 4\ 3)\ (2\ 5\ 1)$

$$\Rightarrow g = \begin{pmatrix} 1 & 3 & 2 & 5 & 4 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 4 & 3 & 2 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}\begin{pmatrix} 2 & 5 & 1 & 3 & 4 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 3 & 2 & 5 & 4 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 3 & 5 & 4 \\ 5 & 4 & 3 \end{pmatrix} = (1\ 2)\ (3\ 5\ 4)$$

Example 51: *Show that* $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 3 & 1 & 8 & 5 & 6 & 2 & 4 \end{pmatrix}$ *is even*

Solution: We have $f = \begin{pmatrix} 1 & 7 & 2 & 3 \\ 7 & 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 4 & 8 \\ 8 & 4 \end{pmatrix}\begin{pmatrix} 5 \\ 5 \end{pmatrix}\begin{pmatrix} 6 \\ 6 \end{pmatrix}$ ✓

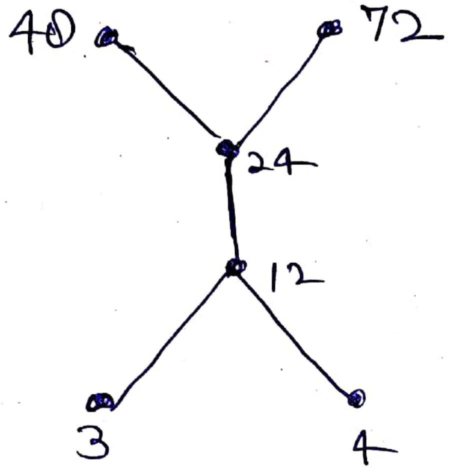
$\Rightarrow \qquad f = (1\ 7\ 2\ 3)\ (4\ 8)\ (5)\ (6)$

$\Rightarrow \qquad f = (1\ 7)(1\ 2)\ (1\ 3)\ (4\ 8)$

$\Rightarrow f$ is expressed as product of 4 transposition, therefore f is even permutation.

Ex ① Draw the Hasse diagram of $(A, \preceq)$ where $A = \{3, 4, 12, 24, 40, 72\}$ and relation $\preceq$ be such that $a \preceq b$ if a divides b.

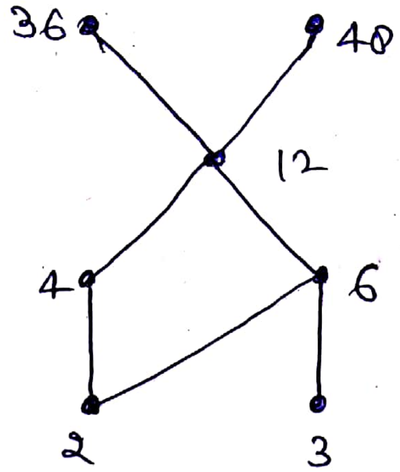
Sol



Ex ② Draw the Hasse diagram of the relation S defined as "divides" on set B where

$$B = \{2, 3, 4, 6, 12, 36, 40\}$$

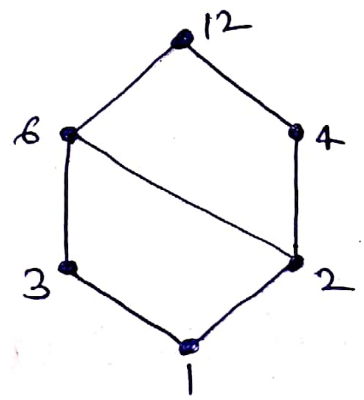
Sol



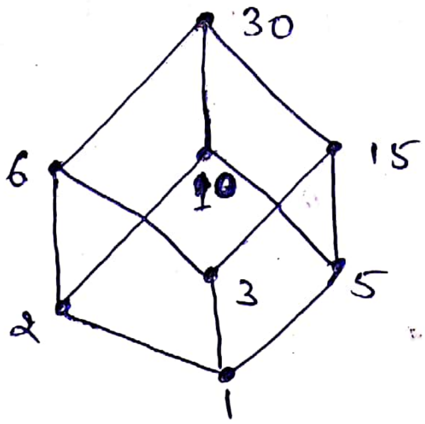
Ex. Let A be the set of factors of a particular positive integer m and let $\leq$ be the relation "divides" i.e. $\leq = \{(x,y) : x \in A, y \in A \text{ and } x \mid y\}$ Draw Hasse diagram for.

a) $m=12$ b) $m=30$ c) $m=45$

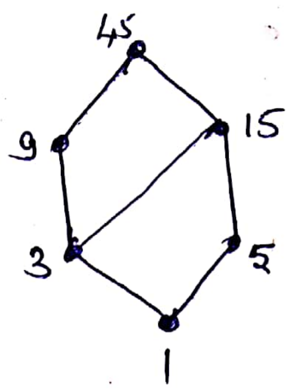
Sol a) $A = \{1,2,3,4,6,12\}$



b) $A = \{1,2,3,5,6,10,15,30\}$



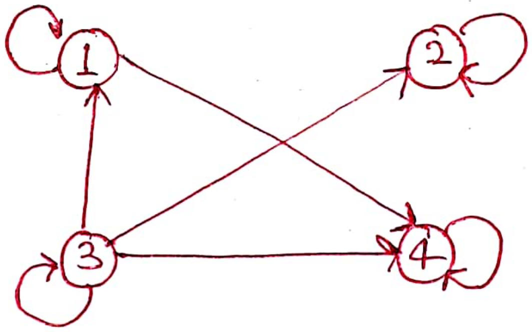
c) $A = \{1,3,5,9,15,45\}$



Scanned with CamScanner

Ex The directed graph G for a relation R on set $A = \{1, 2, 3, 4\}$ is shown in fig –

i) verify that (A, R) is a poset and find its Hasse diagram



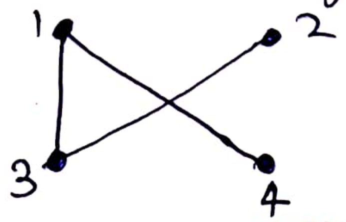
Solution :– The relation R corresponding to the given diagraph is $R = \{(1,1), (2,2), (3,3), (4,4), (3,1), (3,2), (3,4), (1,4)\}$

1) Reflexive since $aRa \; \forall a \in A$ Hence it is reflexive

2) Antisymmetric since aRb and bRa then we get $a = b$. Hence, it is antisymmetric.

3) Transitive for every aRb and $bRc \Rightarrow aRc$ hence it is transitive.

therefore we can say (A, R) is poset.



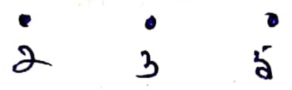
Scanned with CamScanner

Ex Draw the Hase diagrame for the given Sets with relation $\preceq$, where $\preceq$ denoted $a|b$.

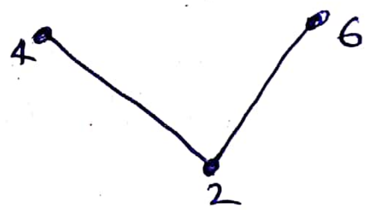
$A = \{2, 3, 5\}$, $B = \{2, 3, 4\}$, $C = \{2, 3, 6\}$,
$D = \{2, 4, 6\}$, $E = \{2, 4, 8\}$

Sol

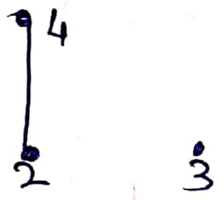
A)



D)

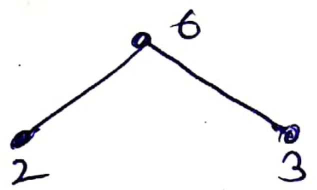


B)



E)

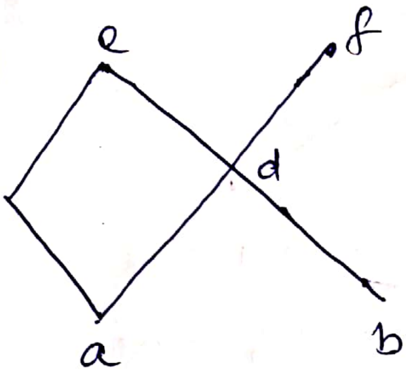
C)



Examples for join & meet

Check whether the given Diagrams have meet & join semi-lattice or not.

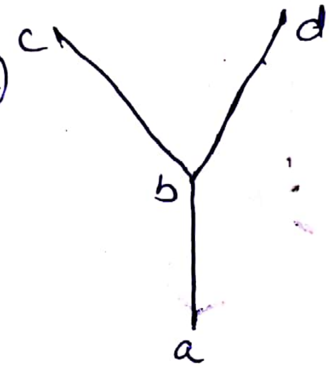
(1)



$e \vee f = \times$

$a \wedge b = \times$

(2)



$c \vee d = \times$

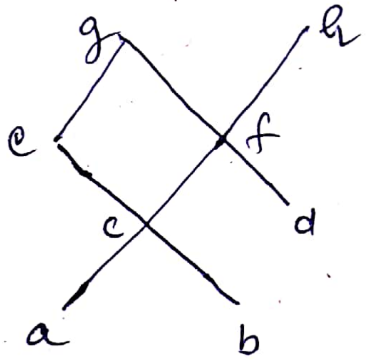
meet = ✓

(3)

meet = ✓

join = ✓

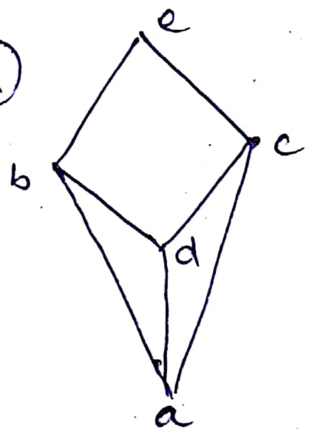
(4)



join = ×

meet = ×

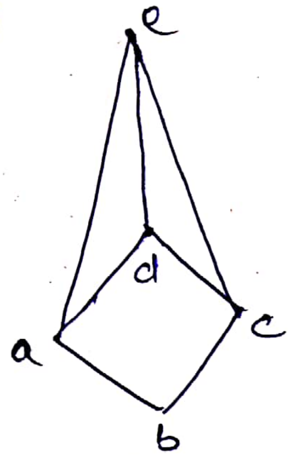
(5)



join = ✓

meet = ✓

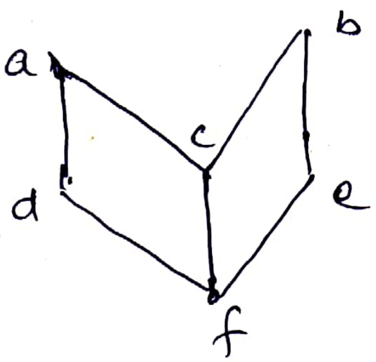
(6)



join = ✓

meet = ✓

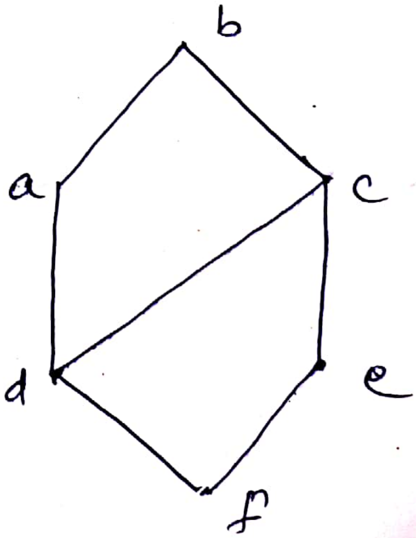
(7)



$a \vee b = \times$

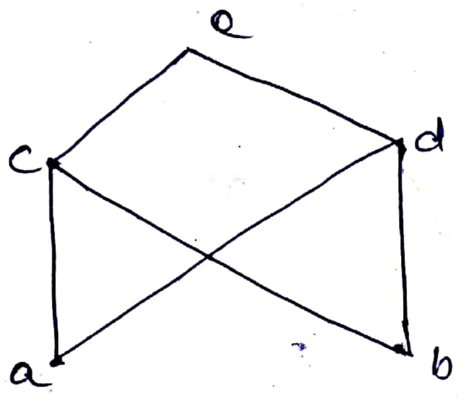
meet = ✓

(8)



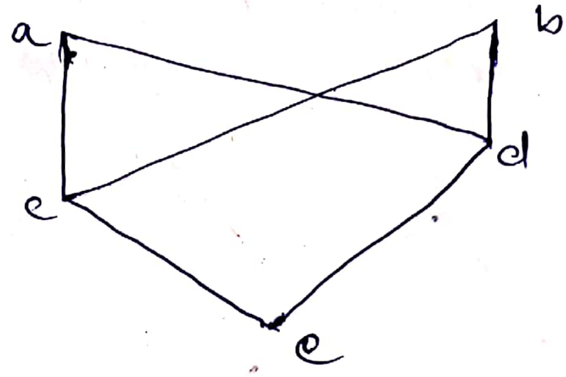
join = ✓

meet = ✓



$a \vee b = X$

$c \vee d = e$



$c \wedge d = e$

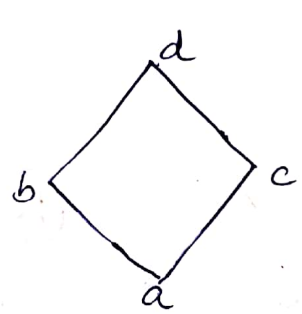
$a \wedge b = X$

Properties of lattice:-

1) Idempotent law:-

$a \vee a = a$

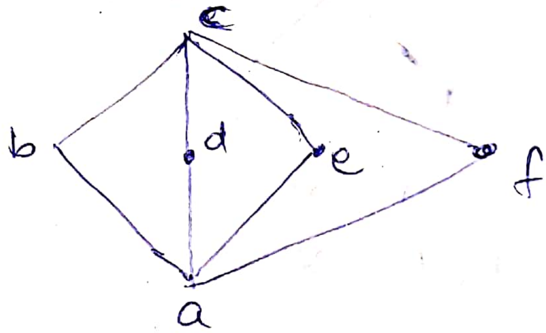
$a \wedge a = a$



2) Associative law:-

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

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



3) Commutative law:

$a \vee b = b \vee a$

$a \wedge b = b \wedge a$

Ex. Associative $(b \vee d) \vee e = b \vee (d \vee e)$

$\Rightarrow c \vee e = b \vee c$

$\Rightarrow c = c$

Ex. Commutative

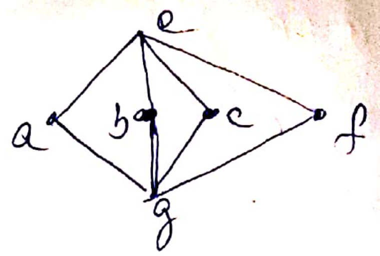
$b \vee d = c = d \vee b$

$b \wedge d = a = d \wedge b$

4) **Distributive ~~lattice~~ law :-**

$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

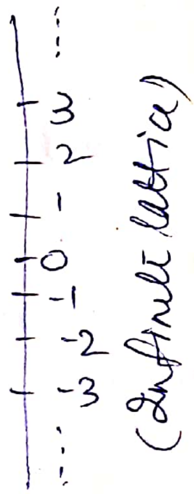
$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$



Ex. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

$a \vee g = e \wedge e$

$a \neq e$



5) **De-Morgan's law :-**

$(a \vee c)^c = a^c \wedge c^c$

6) Complement

Bounded lattice (1) maximum, Greatest, (I) upperbound — in a lattice 'L' if there exists an element I, such that $\forall a \in L$ $(a R I)$ then I is called upper bound of lattice.

(2) minimum, least, (O), lower bound : In a lattice 'L' if there exists an element 'O' such that $\forall a \in L$ $(O R a)$, then O is called lower bound of lattice.

Note :- If for any lattice there exists upper bound & lower bound both then that lattice is called as bounded lattice.

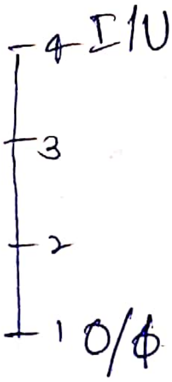
* A bounded lattice is also a finite lattice.

$\star$ $a \vee a^c = I$

$a \wedge a^c = 0$

$I^c = 0$

$0^c = I$



$a \vee I = I$ | $A \cup U = U$

$a \wedge I = a$ | $A \cap U = A$

$a \vee 0 = a$ | $A \cup \phi = A$

$a \wedge 0 = 0$ | $A \cap \phi = \phi$

$A \cup A^c = U$ $\quad U^c = \phi$

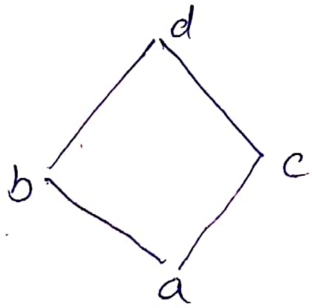
$A \cap A^c = \phi$ $\quad \phi^c = U$

Complement of an element in a lattice:-

In a bounded lattice L, for any element $a \in L$ if there exist an element $b \in L$. Such that -

$a \vee b = I$, $a \wedge b = 0$, that b is called complement of a. we can say 'a' and 'b' are complements of each other.

(1)



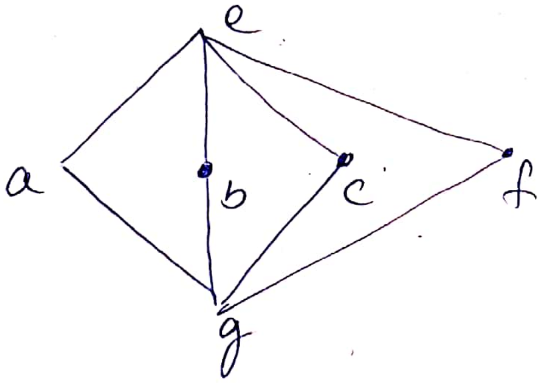
$I = d$

$0 = a$

$a^c = d$ $\quad b^c = c$

$d^c = a$ $\quad c^c = b$

(2)



$I = e$

$0 = g$

$a^c = b, c, f$

$b^c = a, c, f$

$c^c = a, b, f$

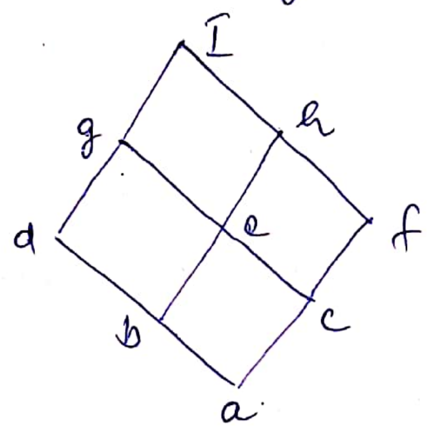
$f^c = a, b, c$ | $e^c = g$

$g^c = e$

Scanned with CamScanner

Complement of an element :- ① when performing join with any element we get I. ② when performing meet operation with any element we get 0.

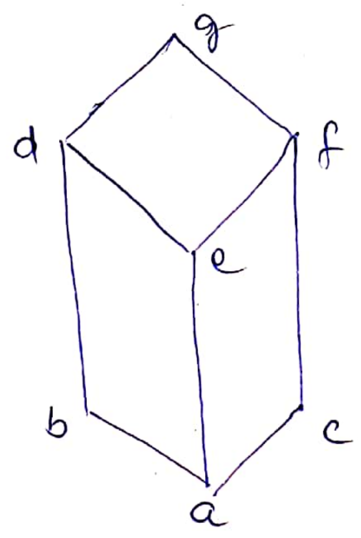
(3)



$a^c = I$
$I^c = a$
$d^c = f$
$f^c = d$

b, c, h, g, e (no complements)

(4)



$a^c = g$
$g^c = a$

$b^c = c, f$ $e = \times$ (no com
$c^c = b, d$

<u>Complemented lattice</u> :- A lattice L is said to be complemented if every element $\forall a \in L$ must have at least one complement.

<u>Distributive lattice</u> :- It has at most one complement for each element or zero ~~element~~ Complement.

Modular lattice :- A lattice $(L, \leq)$ is said to be modular if

$$a \vee (b \wedge c) = (a \vee b) \wedge c$$

whenever $a \leq c$ for all $a, b, c \in L$

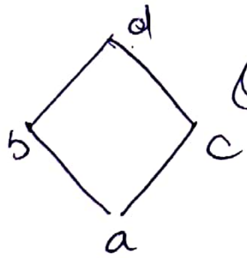
Theorem :- Every distributive lattice is modular

Proof – Let $(L, \leq)$ be distributive lattice and $a, b, c \in L$ such that $a \leq c$, as $a \leq c$ we have $a \vee c = c$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$$

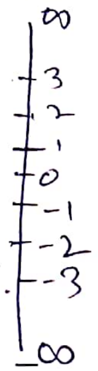
Hence every distributive lattice is modular.

Complete lattice: In (A, R) lattice, each non empty subset of A has a join $\vee$ (LUB) and meet $\wedge$ (GLB) will called complete lattice.



(complete)

finite lattice



(not complete)

infinite lattice

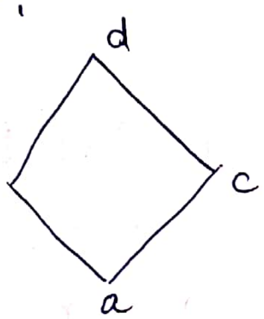
Note :- every finite lattice is a complete lattice.

Boolean Algebra :- A lattice 'L' is said to be boolean algebra if it is complemented and distributed.

or

If each element in a Hasse diagram has exactly one complement.

I



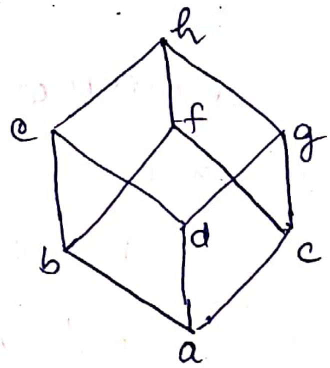
$V = 4 = 2^2$
$e = 4$
$n = (a, b)$ $P(S) = 2^2 = 4$
So $V = 4$
$e = 2 \cdot 2^{2-1} = 4$

$a^c = d$
$d^c = a$
$b^c = c$
$c^c = b$

(Boolean Algebra) ✓ Yes

II

$V = 8$
$e = 12$



for $n = 3$ (a, b, c)
In $P(S) = 2^3 = 8$ elements
then
$V = 8$
$e = 3 \cdot 2^2 = 3 \cdot 4 = 12$

Property

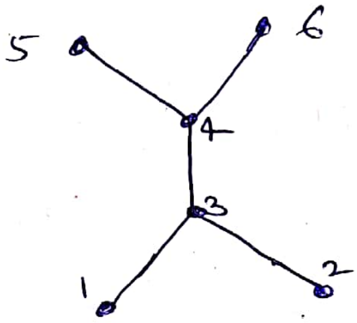
⇒ Number of vertices in POSET must be 2^n form.
⇒ Number of edges must be $n \cdot 2^{n-1}$.

Upper bound :- If $[A, R]$ is a poset
$a \in A$ is called upper bound of subset B
$(B \subseteq A)$ if xRa, $\forall x \in B$

Lower bound :- $a \in A$ is lower bound of B where
$B \subseteq A$ if aRx, $\forall x \in B$

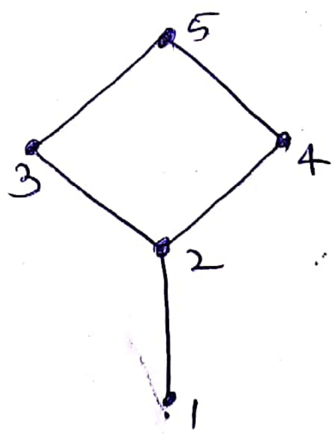
Note :- Upper bound & lower bounds are considered in case of given subsets.

Ex.



Upper bound :- $\{4, 5, 6\}$ lower bound :- $\{1, 2, 3\}$

Ex.



$B_1 = \{4, 5\}$

$UB = \{5\}$

$LB = \{1, 2, 4\}$

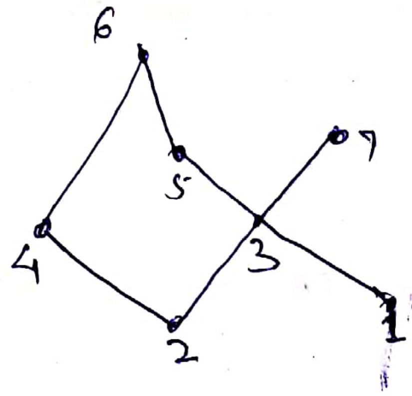
$B_2 = \{1, 2\}$

$UB = \{2, 3, 4, 5\}$

$LB = \{1\}$

Scanned with CamScanner

Ex



① $B = \{3,4\}$
② $B = \{2,5\}$
③ $B = \{4,7\}$
④ $B = \{1,5\}$

Sol i) $UB = \{6\}$
$LB = \{2\}$

ii) $UB = \{5,6\}$
$LB = \{2\}$

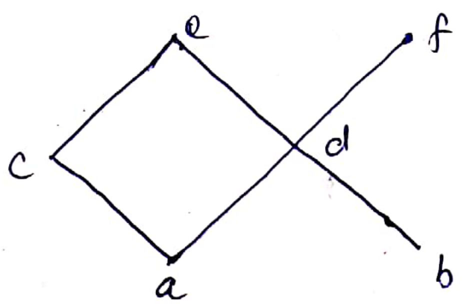
iii) $UB = \{$doesnot exist$\}$
$LB = \{2\}$

iv) $UB = \{5,6\}$
$LB = \{1\}$.

Least upper bound :- LUB, Supremum, Join, $\vee$ (disjun)
least (minimum) element in upper bound.

Greatest lower bound :- GLB, Infimum, meet, $\wedge$ (conj)
Greatest (maximum) element in lower bound.

Ex



$B = \{c,d\}$
$B = \{a,b\}$
$B = \{e,f\}$

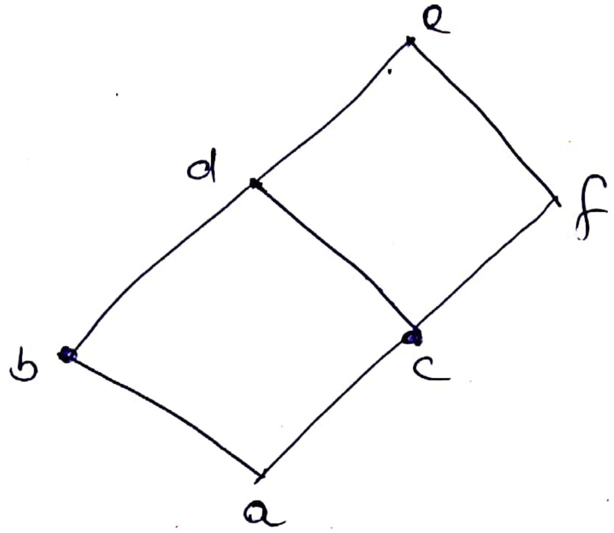
$B = \{c,d\}$
$UB = \{e\}$
$LUB = \{e\}$
$LB = \{a\}$
$GLB = \{a\}$

$B = \{a,b\}$
$UB = \{d,e,f\}$
$LUB = \{d\}$
$LB = \{x\} = \phi$
$GLB = \{x\} = \phi$

$B = \{e,f\}$
$UB = \{$doesn't exist$\}$
$LUB = \{$doesn't exist$\}$
$LB = \{a,d,b\}$
$GLB = \{d\}$

Scanned with CamScanner

Ex



B = {a, c, f}

B = {d, c}

B = {a, c, f}

UB = {e, f}

LUB = {f}

LB = {a}

GLB = {a}

B = {d, c}

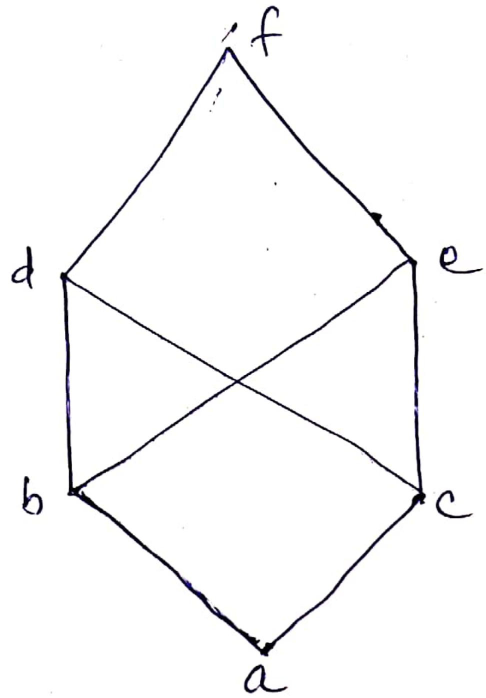
UB = {d, e}

LUB = d

LB = a, c

GLB = c

Ex



B = {d, e}

B = {b, c}

(I) B = {d, e}

UB = f

LUB = f

LB = b, a, c

GLB = ϕ

(II) B = {b, c}

UB = d, e, f

LUB = ϕ

LB = a

GLB = a

Example 33: *Consider the partially order set* $A=\{2, 4, 6, 8\}$ *where* $2|4$ *means* 2 *divide* 4 *show with reason whether the following statements are true or false.*

(i) *Every pair of elements in the poset has a greatest lower bound.*

(ii) *Every pair of elements in the poset has a least upper bound.*

(iii) *This poset is a lattice.* **[U.P.T.U. (B.Tech.) 2002]**

Solution: Now first we draw the Hasse diagram under relation of divisor

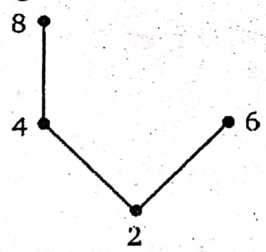


Fig. 6.63

(i) True, its g.l.b. table is

$\wedge$	2	4	6	8
2	2	2	2	2
4	2	4	2	4
6	2	2	6	2
8	2	4	2	8

Here $a \wedge b = \text{H.C.F of } (a, b)$. Hence every pair of elements has g.l.b.

(ii) False, since there exists no l.u.b. of 6 and 8

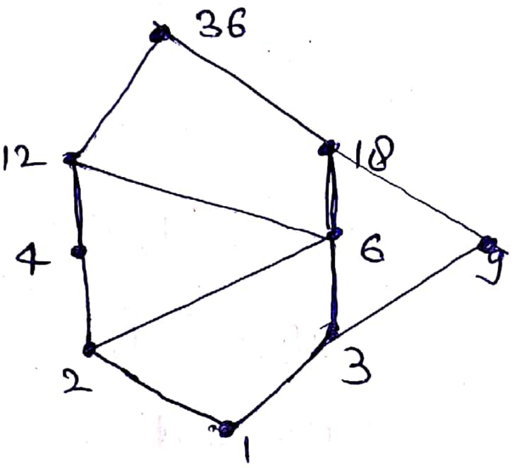
(iii) False, since 6 and 8 has no l.u.b. This is not a lattice.

Ex. Consider the poset $A = (\{1,2,3,4,6,9,12,18,36\}, |)$

i) Draw the Hasse diagram for the given Poset.

ii) Find the Infimum (GLB) and supremum (LUB) of sets $\{6,18\}$ and $\{4,6,9\}$.

Sol



$B = \{6,18\}$

$B = \{4,6,9\}$

Sol i) $B = \{6,18\}$

LB = 1, 2, 3, 6

GLB = 6

UB = 18, 36

LUB = 18

Sol ii) $B = \{4,6,9\}$

LB = 1

GLB = 1

UB = 36

LUB = 36

Join Semi lattice:- In a poset if LUB / Join / supremum / $\vee$ exist for every pair of elements, this poset is called join ~~Meet~~ - Semi - lattice.

Meet - Semi - lattice:- In a poset if GLB / Meet / Infimum / $\wedge$ exist for every pair of elements, this poset is called Meet - Semi - lattice.

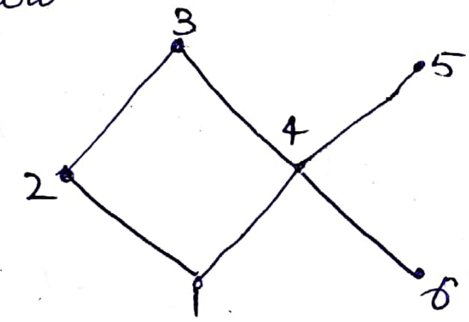
Scanned with CamScanner

Maximal and Minimal Elements :-

An element belonging to a point $(A, \leq)$ is said to be Maximal element of A if there is no element c in A such that $a \leq c$. An element $b \in A$ is said to be minimal element of a if there is no element c in A such that $c \leq b$ (more than on elements are allowed).

Ex. Find all the maximal and minimal elements of posets whose Hasse diagrams are given in the figures below.

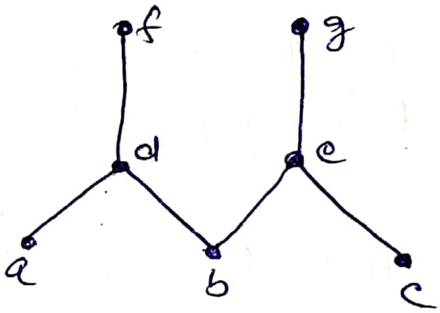
i)



maximal - 3, 5

minimal - 1, 6

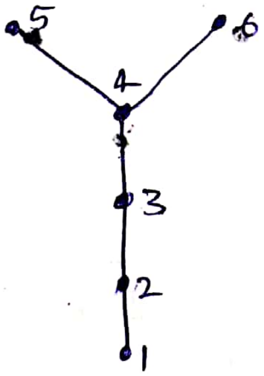
ii)



Maximal - f, g

Minimal - a, b, c

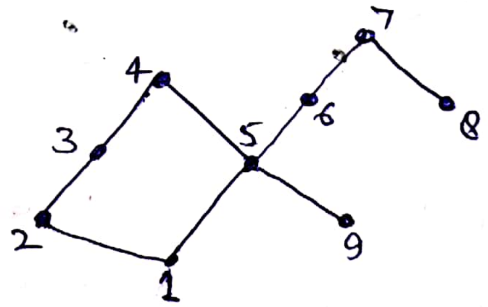
iii)



maximal - 5, 6

minimal - 1

iv)



Maximal - 4, 7

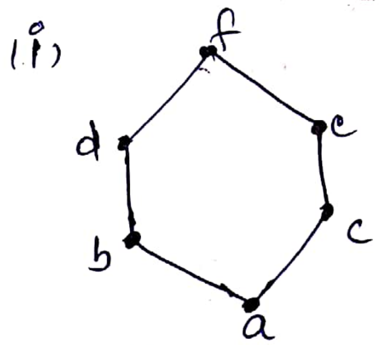
minimal - 1, 9, 8

Greatest Element and Least Element :-

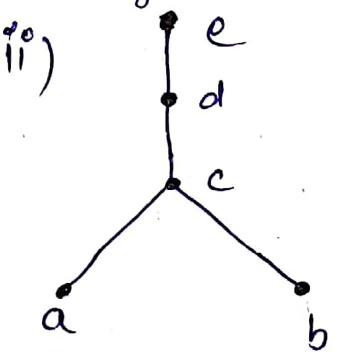
An element $a \in A$ is said to be a Greatest (Last, unit) Element of A if $x \leq a$ for all $x \in A$. An element $a \in A$ is called a least element (first or zero element) of A if $a \leq x$ for all $x \in A$. The least element if exists is unique. It may happen that the least element does not exist. The least element generally denoted by 0. The greatest element if exists is unique. It may happen that the greatest element does not exist. The greatest element is generally denoted by 1. (must be unique)

Ex Find the greatest and least elements of following Hasse diagrams.

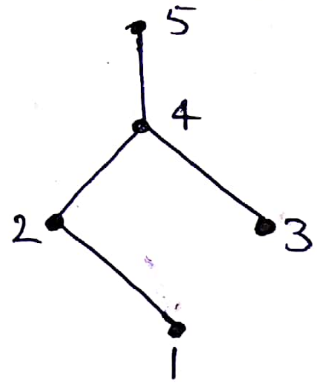
(i)



(ii)



(iii)

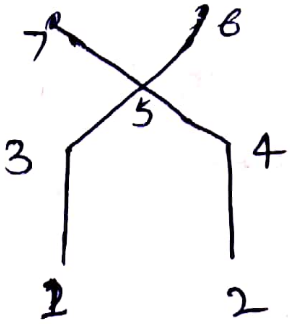


greatest = f
least = a

greatest = e
least = none

greatest = 5
least = none

(iv)



greatest = none
least = none

General properties of a group.

1) The identity element in a group is unique.

proof Let us suppose that $a \in G$ and, e, e' be the two identities in G.

$$e \in G \quad a \in G \Rightarrow ae = a \qquad \text{--- (i)}$$

$$e' \in G \quad a \in G \Rightarrow ae' = a \qquad \text{--- (ii)}$$

from (i) and (ii), we get

$$ae = ae' \Rightarrow e = e'$$

Hence the identity element of a group is unique.

2) The inverse of each element of a group is unique.

proof Let $a \in G$ and $e \in G$

Let b and c be the two inverses of a in G.

$$a \in G \quad b \in G \Rightarrow ab = e \qquad \text{--- (i)}$$

$$a \in G \quad c \in G \Rightarrow ac = e \qquad \text{--- (ii)}$$

$$ab = ac$$

$$b = c$$

Hence inverse element in a group is unique.

Order of a finite group

The number of element in a finite group is called the order of the group. An infinite group is said to be of infinite order. We shall denote the orders of a a group G by the symbol O(G)

Ex: Let $A = \{a, b\}$, which of the following tables define a semi group? which defines a monoid on A.

*	a	b
a	b	a
b	a	b

(i)

*	a	b
a	b	b
b	a	a

(ii)

*	a	b
a	a	b
b	b	a

(iii)

Sol
we have from (i)

a) closure - Since all the entries in composition table are in A. Hence closure property satisfied.

b) Associative :- Since there are only two elements in the set A. Hence associativity is always satisfied.

c) Identity :- $\forall$ elements of A $\exists$ an element $b \in B$ such that $b * a = a$ and $b * b = b$

Hence (i) is semi group as well as monoid

(ii) Again table no (ii) satisfied closure and associativity and there is no identity. Hence it is semi group but not monoid.

(iii) In table no (iii) we have closure, Associativity as well as Identity. Therefore, it is semi group as well as monoid.

Ex Show that the group $G = \{1,2,3,4,5,6\} \times_7$ is cyclic. How many generators are there.

Sol :- Let a be generator of G. Then $O(a) = O(G) = 6$

Now $3^1 = 3$, $3^2 = 3 \times_7 3 = 2$, $3^3 = 3 \times_7 3 \times_7 3 = 6$

$3^4 = 6 \times_7 3 = 4$, $3^5 = 4 \times_7 3 = 5$, $3^6 = 5 \times_7 3 = 1$

Hence G is cyclic group with generator 3

$$G = \{3, 3^2, 3^3, 3^4, 3^5\}$$

Similarly 5 is also generator of G.

Order of an element of a group :-

If a is an element of group G and n is a positive integer such that $a^n = e$, then $O(a) \leq n$, when n is a least positive integers satisfying $a^n = e$ then $O(a) = n$ and there exists any positive integer $m\ (<n)$ such that $a^m = e$ then $O(a) < n$.

Ex find the orders of each element of the multiplicative group $G = \{1, -1, i, -i\}$

Sol - Since 1 is the identity element, therefore $\underline{O(1) = 1}$

Now $(-1)^1 = -1$, $(-1)^2 = 1$

$\underline{O(-1) = 2}$

Similarly $(i)^1 = i$; $(i)^2 = -1$, $i^3 = -i$, $i^4 = 1$

$O(i) = 4$

Scanned with CamScanner

$(-i)^1 = -i$; $(-i)^2 = 1$, $(-i)^3 = i$, $(-i)^4 = -1$

$$O(i) = 4$$

Hence $O(1) = 1$, $O(-1) = 2$, $O(i) = 4$, $O(-i) = 4$

Ex find the order of each element of the group $G = \{0, 1, 2, 3, 4, 5\}$, the composition in G is addition modulo 6.

Sol The Identity element of group $(G, +_6)$ is 0, therefore the order of this element is 1

$$O(0) = 1$$

Now $1^1 = 1$, $1^2 = 1 +_6 1 = 2$, $1^3 = 1 +_6 1 = 1 +_6 2 = 3$ (Identity)

$1^4 = 1 +_6 1 +_6 1 +_6 1 = 1 +_6 3 = 4$, $1^5 = 1 +_6 4 = 5$, $1^6 = 1 +_6 5 = 0$

$$O(1) = 6$$

$2^1 = 2$, $2^2 = 2 + 2 = 4$, $2^3 = 2 + 4 = 0$ (Identity)

$$O(2) = 3$$

$3^1 = 3$, $3^2 = 3 + 3 = 0$ (Identity)

$$O(3) = 2$$

$4^3 = 3(4) = 12 \pmod 6 = 0$

$$O(4) = 3$$

Similarly $O(5) = 6$

Permutation group of Symmetric Group

Let S be finite set consisting n elements, then the set of all one-one onto mapping from S to S forms a group with respect to composition of mapping. This group is called Permutation group or Symmetric group on n symbols of degree n and is denoted by S_n.

If $S = \{a_1, a_2, a_3, --- a_n\}$ then we can write an element $f \in S_n$ as

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & --- & a_n \\ f(a_1) & f(a_2) & f(a_3) & & f(a_n) \end{pmatrix}$$

when $f(a_1), f(a_2), --- f(a_n)$ are the f-images of $a_1, a_2 --- a_n$ respectively. So it is permutation of n symbols

Equal permutation :-

Let S be non empty set. The permutation f and g defined on S is said to be equal if

$$f(a) = g(a) \; \forall a \in S$$

Ex let $S = (1, 2, 3, 4)$ and $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$

and $g = \begin{pmatrix} 4 & 1 & 3 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$, we find

$f(1) = g(1) = 3$, $f(2) = g(2) = 1$, $f(3) = g(3) = 2$

$f(4) = g(4) = 4$

Product of permutation or composition of permutation

Ex. Let $S = \{1,2,3\}$ and $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ be two permutation on S then.

$$fog = fg = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$gof = gf = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\therefore fog \neq gof.$$

inverse of permutation

if f is a permulation on $S = (a_1, a_2, a_3 --- a_n)$ such that

$$f = \begin{bmatrix} a_1, & a_2 & a_3 & --- & a_n \\ b_1 & b_2 & b_3 & --- & b_n \end{bmatrix}$$

then there exists a permutation called inverse f and denoted by f^{-1} such that $fof^{-1} = f^{-1}of = I$

$$f^{-1} = \begin{bmatrix} b_1 & b_2 & --- & b_n \\ a_1 & a_2 & --- & a_n \end{bmatrix}.$$

Ex If $A=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$, $B=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$

then find AB, BA and A^{-1}

Sol we have

$$AB = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$$

$$BA = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Posets and Lattice theory

Partially ordered set (POSET)

A relation R on a set A is called a partial order if R is reflexive, antisymmetric and transitive. The set A together with the partial order R is called Partially ordered set or simply a poset and we will denote this poset by (A, R).

The relation R is often denoted by the symbol $\preceq$ which is different from the usual less than or equal to symbol $\leq$. A partial order is denoted by

$x \preceq y$ means x precedes y

$x \prec y$ means x strictly precedes y

Q) Show that the relation $\geq$ is a partial ordering on the set of integers Z.

Sol (i) since $a \geq a$ for every a, $\geq$ is reflexive

(ii) $a \geq b$ and $b \geq a$ imply $a = b$, $\geq$ is antisymmetric

(iii) $a \geq b$ and $b \geq c$ imply $a \geq c$, $\geq$ is transitive

That means, $\geq$ is a partial ordering on the set of integers and $(Z, \geq)$ is a poset.

Q Let $A = \{2, 3, 6, 12, 24, 36\}$ and R be the relation in A which is defined by a divides b then R is partial order in A.

Solution :- The relation divisor is a partial order if it satisfies the following conditions.

① Reflexivity : Since $a|a \ \forall a \in A$ ∴ 'R' is reflexive

② Antisymmetric If $a|b$ and $b|a \ \forall a, b \in A$ then $a=b$

③ Transitivity If $a|b$ and $b|c \ \forall a, b, c \in A$ then $a|c$

for ex $2|6$, $6|12 \Rightarrow 2|6$

Hasse Diagram :- A graphical representation of a partial ordering relation in which all arrow heads are understood to be pointing upward is known as the Hasse diagram of the relation.