UNIT-3

Algebraic Structures

Definition :- A non-empty set having one or more binary operations is called an algebraic structure.

Let G is a non-empty set

If $f: G \times G \rightarrow G$ then f is called a binary operation on G.

$$G \times G = \{(a,b) \,;\, a \in G, b \in G\}$$

The symbols $+, \cdot, o, *$ etc are used to denote binary operations on a set

Thus $+$ will be a binary operation on G if and only if $a+b \in G \; \forall \, a,b \in G$ and $a+b$ is unique.

Ily $*$ will be a binary operation on G if and only if $a*b \in G, \forall \, a,b \in G$ and $a*b$ is unique.

$\rightarrow$ $N \leq Z \leq Q \leq R \leq C$

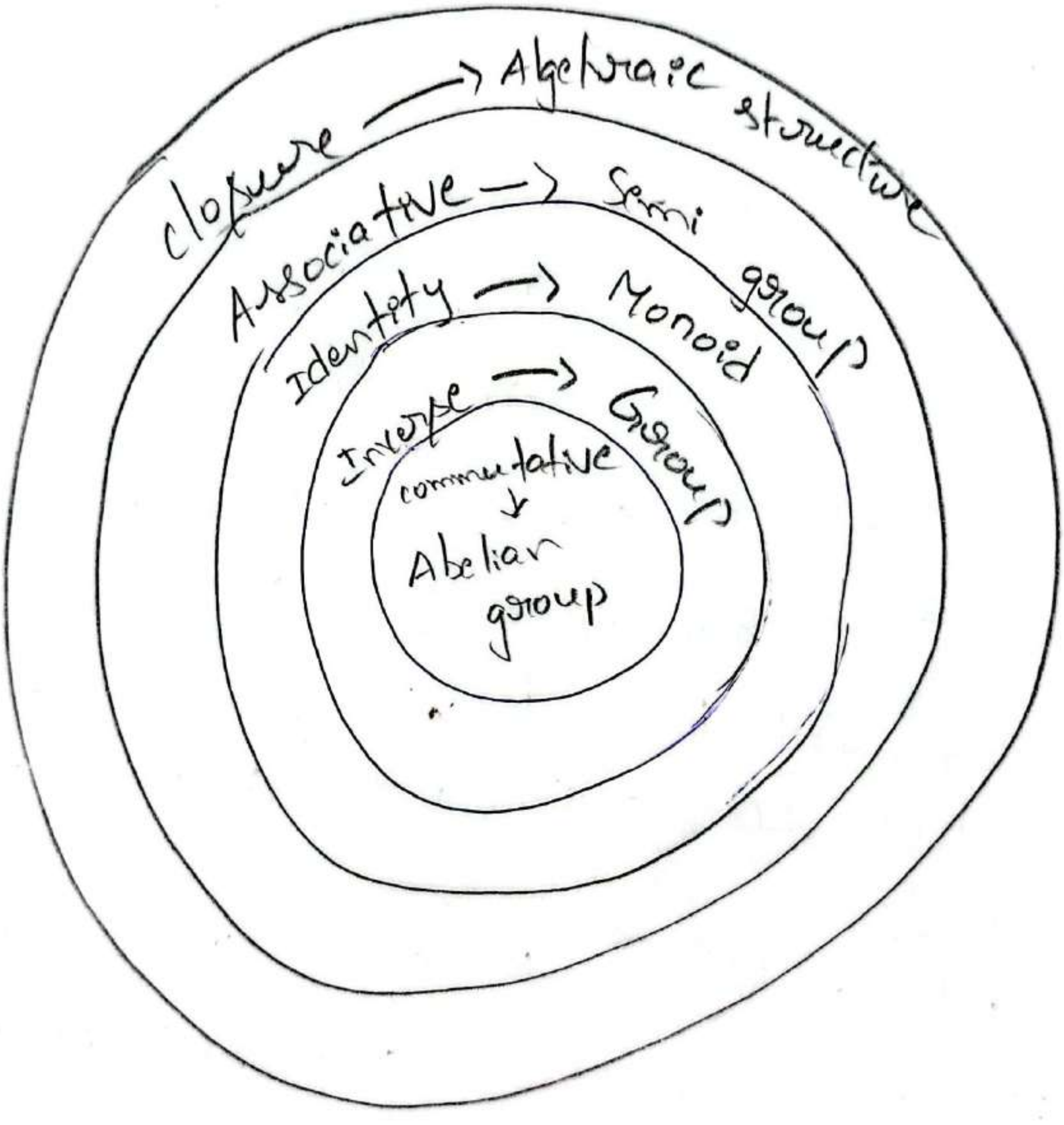
N → set of Natural numbers

Z → set of integers

Q → set of Rational nos

R → set of Real no's

C → set of complex no.s


closure → Algebraic structure
Associative → Semi group
Identity → Monoid
Inverse → Group
commutative
↓
Abelian group

Algebraic system :- A system consisting of a non-empty set and one or more n-ary operations on the set is called an algebraic system.

→ An algebraic system will be denoted by $\{S, f_1, f_2 \cdots\}$ where S is the non-empty set $f_1, f_2, \ldots$ are n-ary operations on S

→ we will mostly deal with algebraic systems with $n = 0, 1, \& \ 2$ containing one or two operations only

$\{S, +\}, n=1$
$\{S, +, *\}$ $n=2$

General properties of algebraic systems

Let $\{S, *, +\}$ be an algebraic system where $*$ and $+$ are binary operations on S.

1. **closure property** : For an $a, b \in S$

$a * b \in S$

Eg:- If $a, b \in Z$, $a+b \in Z$ and $a*b \in Z$

where + and * are the operations of addition and multiplication.

② Associative property:

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

Eg:- If $a, b, c \in Z$
$(a+b)+c = a+(b+c)$ and
$(a*b)*c = a*(b*c)$

③ commutative Property

for any $a, b \in S$
$a*b = b*a$

Eg:- If $a, b \in Z$
$a+b = b+a$ and
$a*b = b*a$

④ Identity element property;

there exists a distinguished element e, $e \in S$ s.t for any element 'a', $a \in S$

Then $a*e = e*a = a$

The element $e \in S$ is called the identity element of S w.r.t the operation $*$

Eg:- 0 & 1 are the identity elements of Z w.r.t the operations of addition and multiplication respectively.

since for any element a, $a \in Z$

$$a+0 = 0+a = a$$
$$a*1 = 1*a = a$$

(5) <u>Inverse element</u> :

for each element 'a', $a \in S$ there exists an element $\bar{a}^1$, $\bar{a}^1 \in S$

s.t $a * \bar{a}^1 = \bar{a}^1 * a = e$

the element $\bar{a}^1$ is called the inverse of a under the operation $*$

e is called identity element w.r.t the operation $*$.

Eg:- for each $a \in z$, $-a$ is the inverse of a under the operation addition, since

$a+(-a)=0$

where '0' is the identity element of z under addition.

(6) Distributive property :

for any three elements $a,b,c \in S$

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

In this case, the operation $*$ is said to be distributive over the operation '+'

Eg:- for any 3 elements $a,b,c \in z$

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

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

(7) cancellation property

for any three elements $a,b,c \in S$ and $a \neq 0$,

$a*b = a*c \Rightarrow b=c$

$b*a = c*a \Rightarrow b=c$

Eg:- cancellation property holds good for any $a, b, c \in Z$ under addition and multiplication.

(8) Idempotent property :-

An element a, $a \in S$ is called an Idempotent element w.r.t the operation $*$, If

$$a * a = a$$

Eg:- $0 \in Z$ is an idempotent element under addition.

$$0 + 0 = 0$$

$0, 1 \in Z$ are idempotent element under ~~addition~~. Multiplication

$$0 \times 0 = 0 \; \& \; 1 * 1 = 1$$

Semi group

Let S be non-empty set and $*$ be any binary operation on S then Algebraic system $\langle S, * \rangle$ is called a semi group it satisfies the following properties.

① closure property

for any two elements a, b where $a, b \in S$ then $a * b \in S$

Associative property :-

for any three elements a, b, c where $a, b, c \in S$ then

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

Eg :- E is the set of positive numbers

(E, +) , (E, *) are semi groups.

(N, +) is a semi group

→ prove (E, *) is a semi group.

suppose $E = \{2, 4, 6, 8, 10 \ldots\}$

take two elements $a, b \in E$

$a = 2, b = 4$.

closure property :-

$a, b \in E$ where $a = 2, b = 4$

$a * b \in E$ i.e $2 * 4 \in E$

$8 \in E$ true

closure property satisfied.

Associative property

$a, b, c \in Z$ ~~where~~ where $a = 2, b = 4, c = 6$

$$a * (b * c) = (a * b) * c$$
$$2 * (4 * 6) = (2 * 4) * 6$$
$$48 = 48$$

Associative property satisfied.

Monoid

Let S be a non-empty set and $*$ be a binary operation S, then the algebraic system $\langle S, * \rangle$ is called a Monoid iff it satisfies the following properties:

① **closure property**:

for any any two elements a, b; s.t $a * b \in S$ where $a, b \in S$

② **Associative property**:

for any three elements

$a, b, c \in S$ such that

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

(iii) Identity element :

there exists a distinguished

element e. $e \in S$ s.t
identity

$$a + e = e + a = a , \quad \forall a \in S$$

Eg :- $\langle W, + \rangle$ is a Monoid.
$\langle N, + \rangle$ is not a Monoid

where W = set of whole numbers
$= \{0, 1, 2, 3, 4, 5 \ldots\}$
N = set of natural numbers
$N = \{1, 2, 3, 4, 5 \ldots\}$

Note : A monoid is always a semigroup.

such a structure consisting of a non-empty set S and a binary operation defined in S is called a groupoid.

Group :- Let $(G, *)$ be an ~~alg~~ algebraic structure where $*$ is a binary operation then $(G, *)$ is called a group under this operation if the following conditions are satisfied.

1. closure
2. Associative
3. Identity
4. Inverse.

Monoid :- An algebraic structure $(S, *)$ is called a monoid if the following conditions are satisfied

1. closure
2. Associative
3. Identity

Semi group :- An algebraic structure $(S, *)$ is called a semigroup if the following conditions are satisfied

1. closure
2. Associative

Groupoid :- Let $(S, *)$ be an algebraic structure in which S is a non-empty set and $*$ is a binary operation on S Thus S is closed with the operation $*$

(3) show that $(Z, *)$ is a group, where $*$ is defined by $a*b = a+b+1$

Sol :- we have to prove that $(Z, *)$ is a group.

we have to satisfy all the following properties

(1) closure

Let $a, b \in Z$ so that both 'a' and 'b' are integers.

$\therefore a*b = a+b+1$ is also an integer.

Hence $a*b \in Z$

this is the closure property

(2) Associative :

$(a*b)*c = (a+b+1)*c$

$= a+b+1+c+1$

$= a+b+c+2$

Also $a*(b*c) = $ ~~a+b~~ $a*(b+c+1)$

$= a+b+c+1+1$

$= a+b+c+2$

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

(3) identity :- If 'e' is the identity.

Then $a*e = a \Rightarrow a+e+1$

$a = a+e+1$

$e = -1 \in Z$

(1) show that the binary operation $*$ defined on $(R, *)$ where $x * y = x^y$ is not associative

Sol :- $(x * y) * z = x^y * z$

$= (x^y)^z$

$= x^{yz}$

again $x * (y * z) = x * y^z$

$= x^{y^z}$

$(x * y) * z \neq x * (y * z)$

(2) prove that the fourth roots of unity $1, -1, i, -i$ from an abelian multiplicative group.

(or) prove that $G = \{-1, 1, i, -i\}$ is an abelian group under multiplication.

Sol :- let $G = \{-1, 1, i, -i\}$

Know we from the composition table

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

and in this case

$a*(-1) = a+(-1)+1$
$= a$

$\therefore$ Identity element is -1

(4) Inverse : $a*b = a+b+1 = -1$ the identity

$\Rightarrow a+b = -2$
$b = -2-a \in Z$

$\therefore -a-2 = b$ is the inverse of a

Hence $(Z,*)$ is an abelian group.

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

Sol :- Let $G = \{1,2,3,4,5\}$

the operation addition modulo 6 is denoted by $+_6$

Def :- Addition modulo m : If a and b be two integers then by addition modulo m expressed as $a +_m b$ equals to the least non-negative number r which is the remainder when $a+b$ is divided by m.

eg:- $3 +_6 20 = 23$

$= 6(3)+5 = 5$

we say $20 \equiv (\bmod 6)$

lly $-20 +_6 5 = -15 = 6(-3)+3 = 3$

we can operate $+_6$ on the elements in G and prepare the composition table as in the system $(G, +_6)$

$2 +_6 5 = 1$ for $2+5 = 7 = 1\times 6+1$

$1 +_6 4 = 5$ for $1+4 = 5$

$3 +_6 5 = 2$ for $3+5 = 8 = 1\times 6+2$ etc.

Hence the composition table is

$+_6$	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

Def : Multiplication modulo m :

If 'a' and 'b' be two integers then by multiplication modulo m expressed as $a \times_m b$ equals to the least non-negative number r which is the remainder when ab is devided by m.

Eg:- $3 \times_7 20 = 60 = 7(8) + 4 = 4$;
$-4 \times_5 11 = -44 = 5(-9) + 1 = 1$

The operation multiplication modulo 6 is denoted by $\times_6$

In the system $(G, \times_6)$

$2 \times_6 5 = 4$ for $2 \times 5 = 10 = 1 \times 6 = 4$

$3 \times_6 4 = 0$ for $3 \times 4 = 12 = 2 \times 6 + 0$

Hence the composition table is

$\times_6$	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

8 mod 6

$6)8(1$
$\underline{6}$
2

From the composition table, It is clear that all the entries in the composition table do not belong to G.

in particular of G.

Hence not closed w.r.t $\times_6$

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

---

(1) Show that if a, b are arbitrary elements of a group G. Then $(ab)^2 = a^2b^2$ if and only if G is abelian.

Sol :- Let 'a' and 'b' be arbitrary elements of a group G.

Suppose $(ab)^2 = a^2b^2 \longrightarrow (1)$

To prove G is an abelian

$(ab)^2 = a^2b^2 = (ab)(ab) = (aa)(bb)$

$= a(ba)b = a(ab)b$ (Associative)

$= (ba)b = (ab)b$ (left cancellation law)

$= ba = ab$ (Right cancellation law)

Again Suppose G is abelian so then

$ab = ba, \forall a, b \in G$

To prove that $(ab)^2 = a^2b^2$ —(2)

Now $(ab)^2 = (ab)(ab)$

$= a(ba)b$

$= a(ab)b \quad (\because ②)$

$= (aa)(bb)$

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

Hence proved

Sub group :- Let $\{G, *\}$ be a group. If H be a finite subset of group G then H is a subgroup of G if and only if it satisfies the following property w.r.t the operation *

① closure property

Let a & b are two elements in H i.e $a, b \in H$ then $a * b \in H, \forall a, b \in H$

② Associative property

Let a, b and c are 3 elements in H i.e $a, b, c \in H$ then

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

③ Identity property :-

Let a is an element in H.

i.e $a \in H$ $\exists$ a special element e in H i.e $e \in H$. where e is an identity element s.t

$$a * e = e * a = a \quad , \forall a \in H$$

$$a * 1 = 1 * a = a$$

[$\because$ 1 is the identity element w.r.t $*$]

④ Inverse property: Let a is an element in H i.e $a \in H$ $\exists$ it inverse a^{-1} is also in H i.e $a^{-1} \in H$ s.t

$$a * a^{-1} = a^{-1} * a = e \quad , \forall a \in H$$

$$(\because e = 1)$$

where e is an identity element w.r.t $*$

a^{-1} is the inverse of a.

H satisfies 4 properties

Hence H is a subgroup of G.

prob ① Let $\{G, *\}$ is a group ⑨

$G = \{1, -1, i, -i\}$ and $\{H, *\}$ is a subgroup of $\{G, *\}$ check whether $\{1, -1\}$ is a subgroup of G or not.

sol :- $\{G, *\}$ is a group

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

$\{H, *\}$ is a subgroup of $\{G, *\}$

Then $H = \{1, -1\}$ is a subgroup, if it satisfying the following properties.

① closure property :-

Let us take any two elements a & b, $a, b \in H$ then

$a * b \in H, \forall a, b \in H$

composition table

*	1	-1
1	1	-1
-1	-1	1

$1 \in H, -1 \in H$

Eg :- $a = 1, b = 1$

$1 * -1 \in H$

$-1 \in H$

∴ closure property satisfied.

② Associative property :

for any $a, b, c \in H$ then

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

Eg:- $a = 1,\ b = -1,\ c = 1$

$$1 * (-1 * 1) = (1 * (-1)) * 1$$

$$1 * -1 = -1 * 1$$

$$-1 = -1 \quad , -1 \in H$$

$\therefore$ Associative property is satisfied.

(3) Identity property:

take any elent a, Here $a \in H$ then

$a * e = e * a = a$.
where e is identoty element $= 1$

Eg:- $a = -1, \quad a \in H$

$$-1 * 1 = 1 * -1 = -1 \in H$$

$\therefore$ Identity property is satisfied.

(4) Inverse property :-

Take any one elent 'a' Here $a \in H$
$\exists$ an elent a^{-1} in H i.e $a^{-1} \in H$ then

$a * a^{-1} = a^{-1} * a = e$
where e is the identity elent its
its value is equal to 1

a inverse is a^{-1}
a^{-1} " " a

Eg :- Let us take $a = 1$ where $a \in H$

Now its inverse is $a^{-1} = 1$

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

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

$\therefore$ 1 inverse is 1

-1 " is -1

suppose $a = -1$, when $a \in H$

a inverse is $a^{-1} = -1$

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

$-1 * -1 = -1 * -1 = e$

$1 = e$

$\therefore$ Inverse property is also satisfies

$\therefore H = \{1, -1\}$ satisfying 4 property

Hence $\{H, *\}$ is a subgroup of $\{G, *\}$

where $H = \{-1, 1\}$

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

(i) prepare the composition table w.r.t $+_6$ (Addition Modulo 6)

(ii) prove that G is an abelian group

(iii) Find the inverse of each and every element in G.

(iv) Find the order of each and every element in a group.

(v) Find out the subgroups generated by each and every element in G.

sol:-

(i) composition table w.r.t Addition modulo 6 $(+_6)$

$+_6$	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

$2 +_6 2 = 4$

$4 \% 6$

$6)4(0$
$\underline{0}$
4

$5 +_6 5 = 10$

$10 \div 6$

$6)10(1$
$\underline{6}$
4

(ii) Inverse of each element in G

Identity element for the above composition table is 0

Inverse of each element is

$0^{-1} = 0$ $\quad$ $3^{-1} = 3$

$1^{-1} = 5$ $\quad$ $4^{-1} = 2$

$2^{-1} = 4$ $\quad$ $5^{-1} = 1$

(2) Now we will prove G is an abelian group.

(i) Closure property :- for any two elements $a +_6 b \in G$

Let us take $a = 2, b = 3$
$2 +_6 3 \in G$
$5 \in G$

$a = 4, b = 5$
$a +_6 b = 4 +_6 5$
$= 3 \in G$

$\therefore$ satisfies the closure property

(ii) Associative property : For any three elements $a, b, c \in G$.

$$(a +_6 b) +_6 c = a +_6 (b +_6 c)$$

Let us take $a = 2, b = 3, c = 4$

$(a +_6 b) +_6 c = a +_6 (b +_6 c)$

$(2 +_6 3) +_6 4 = 2 +_6 (3 +_6 4)$ $\quad 3 +_6 4 = 7$

$5 +_6 4 = 2 +_6 1$ $\quad 7 \div 6$

$3 = 3$ True $\quad 6)7(1$

$\quad \quad \quad \quad 1$

It satisfies the associative property.

(3) Identity property :

Here the identity element is $e = 0$

for any element a, $a \in G$

$a +_6 e = e +_6 a = a$

Let us take $a = 2$

$2 +_6 0 = 0 +_6 2 = 2$

It satisfies the Identity property.

(4) Inverse property : for each and every element in the Group G, Inverse of that element also exist in the same group G.

$0^{-1} = 0$ $\quad 3^{-1} = 3$

$1^{-1} = 5$ $\quad 4^{-1} = 2$

$2^{-1} = 4$ $\quad 5^{-1} = 1$

It satisfies the inverse property.

(5) commutative property :: For any two elements a, b. $a, b \in G$ then

$$a +_6 b = b +_6 a$$

Let us take $a = 3$, $b = 4$

$$a +_6 b = b +_6 a$$
$$3 +_6 4 = 4 +_6 3$$
$$1 = 1 \quad \text{True}.$$

It satisfying the commutative property.

$\therefore$ Addition Modulo $+_6$ satisfies the above 5 properties

Hence $+_6$ is abelian group.

Order of an element of a group

Let $(G, *)$ be a group 'a' is an element of G.

i.e $a \in G$ the order of an element 'a' is denoted by $o(a)$

$$o(a) = n$$

where 'n' is the smallest possible integer which satisfying the eqn $a^n = e$

where e is the identity element

Note : (1) order of identity element is always 1

(2) order of an element and its inverse is always same

Eg(1) Let $(Z_4, +)$ is a group. find out the order of each element ?

Sol :- $(Z_4, +)$ is addition modulo 4

$(Z, +)$ Addition Modulo 4

$Z = \{0, 1, 2, 3\}$

$0 \bmod 4 = 0$

$4 \overline{)0}(0$
$\quad 0$
$\quad \overline{(0)}$

$3 \bmod 4 = 3$

$4 \overline{)3}(0$
$\quad 0$
$\quad \overline{(3)}$

$1 \bmod 4 = 1$ $\qquad$ $2 \bmod 4 = 2$

$4 \overline{)1}(0$
$\quad 0$
$\quad \overline{(1)}$

$4 \overline{)2}(0$
$\quad 0$
$\quad \overline{2}$

$Z = \{0, 1, 2, 3\}$

$a^n = e$
$0^n = 0$
0

$0^0 = 0$

$0^1 = 0$

$0^2 = 0 +_4 0 = 0$

$0^3 = 0 +_4 0 = 0$ $\qquad$ $\therefore O(0) = 1$

$1^1 = 1$

$1^2 = 1 +_4 1 = 2 \bmod 4 = 2$

$1^3 = 1 +_4 1 +_4 1 = 3 \bmod 4 = 3$

$1^4 = 1 +_4 1 +_4 1 +_4 1 = 4 \bmod 4 = 0$

$o(1) = 4$

$4) 3 (0$
$\underline{0}$
3

$2^1 = 2$

$2^2 = 2 +_4 2 = 4 \bmod 4 = 0$

$2^3 = 2 +_4 2 +_4 2 = 6 \bmod 4 = 2$

$2^4 = 2 +_4 2 +_4 2 +_4 2 = 8 \bmod 4 = 0$

$4) 6 (1$
$\underline{4}$
2

$o(2) = 2$
(least power)

$3^1 = 3$

$3^2 = 3 +_4 3 = 6 \bmod 4 = 2$

$3^3 = 3 +_4 3 +_4 3 = 9 \bmod 4 = 1$

$3^4 = 3 +_4 3 +_4 3 +_4 3 = 12 \bmod 4 = 0$

$o(3) = 4$

composition table :

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\therefore$ 0 is the identity element

(i) Let $(Z_6, +)$ is a group find out the order of each element?

Sol:- $(Z_6, +)$ is addition modulo 6

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

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

$\therefore$ Identity element is 0

$a^n = e$

$a^n = 0$

$0^1 = 0$

$0^2 = 0 +_6 0 = 0$

$0^3 = 0 +_6 0 +_6 0 = 0$

$0^4 = 0 +_6 0 +_6 0 +_6 0 = 0$

$0^5 = 0 +_6 0 +_6 0 +_6 0 +_6 0 = 0$

$o(0) = 1$

$1^1 = 1$

$1^2 = 1+1 = 2$ mod

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

$1^4 = 1+1+1+1 = 4$

$1^5 = 1+1+1+1+1 = 5$

$1^6 = 1+1+1+1+1+1 = 6$

$6 \bmod 6 = 0$

$o(1) = 6$

$2^1 = 2$

$2^2 = 2+2 = 4 \bmod 6 = 4$

$6)\,4\,(0$
$\;\;\underline{0}$
$\;\;\;4$

$2^3 = 2+2+2 = 6 \bmod 6 = 0$

$2^4 = 2 +_6 2 +_6 2 +_6 2 = 8 \bmod 6 = 2$

$2^5 = 2 +_6 2 +_6 2 +_6 2 +_6 2 = 10 \bmod 6 = 4$

$2^6 = 2 +_6 2 +_6 2 +_6 2 + 2 +_6 2 + = 12 \bmod 6 = 0$

$o(2) = 3$ (least power)

$3^1 = 3$

$3^2 = 3+3 = 6 \bmod 6 = 0$

$3^3 = 3+3+3 = 9 \bmod 6 = 3$

$3^4 = 3+3+3+3 = 12 \bmod 6 = 0$

$3^5 = 3+3+3+3+3 = 15 \bmod 6 = 3$

$3^6 = 3+3+3+3+3+3 = 18 \bmod 6 = 0$

$o(3) = 2$

$4^1 = 4$

$4^2 = 4+4 = 8 \bmod 6 = 2$

$4^3 = 4+4+4 = 12 \bmod 6 = 0$

$4^4 = 4+4+4+4 = 16 \bmod 6 = 4$

$4^5 = 4+4+4+4+4 = 20 \bmod 6 = 2$

$4^6 = 4+4+4+4+4+4 = 24 \bmod 6 = 0$

$5^1 = 5$

$5^2 = 4$

$5^3 = 3$

$5^4 = 2$

$5^5 = 1$

$5^6 = 0$

$o(5) = 6$

$o(4) = 3$

$\therefore o(5) = 6$

$\therefore (Z_6, +)$ is abelian group

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

Group :- A non-empty set G, together with a binary operation $*$ is said to form a group, if it satisfies the following conditions:

1. closure property
2. Associative property
3. Identity
4. Inverse

(1) closure property : The binary operation $*$ is a closed operation.
i.e $a*b \in G$ for all $a, b \in G$

(2) Associative property : The binary operation $*$ is an associative operation
i.e $a*(b*c) = (a*b)*c$ for all $a, b, c \in G$

(3) Identity : there exists an identity element i.e for every $a \in G$ there exists an unique element $e \in G$ s.t $e*a = a*e = a$
eg:- $5+0=5$

(4) Inverse : For each a in G there exists an element a' (inverse of a) in G s.t

$$a * a' = a' * a = e.$$

General properties of Groups

(1) The left identity e is also the right identity i.e $a*e = a = e*a \ \forall a \in G$

proof :- If a^{-1} be the left inverse of a,

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

$= e*e$

$= e$

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

$a*e = a$

Hence e is also the right identity of an element of a group..

(2) The left inverse of an element is also its right inverse i.e $a^{-1}*a = e = a*a^{-1}$

proof :- Now $a^{-1}*(a*a^{-1}) = (a^{-1}*a)*a^{-1}$ (Associative)

$= e*a^{-1}$

$= a^{-1}*e$

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

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

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

thus the left inverse of an element in a group is also its right inverse

(3) The Identity element e in a group is unique.

proof:- If possible be two identity elements $e_1 \& e_2 \in G$.

Then $ae_1 = a$ and $ae_2 = a$

$\Rightarrow ae_1 = ae_2$

$\Rightarrow e_1 = e_2$ (left cancellation)

Hence the identity element e in a group is unique.

(4) The inverse of an element in a group is unique.

Sol:- Let a be an element of the group having two inverses $b \& c$

Then $ab = e = ba \rightarrow$ ($\because b$ is inverse of a)

~~$acb = e = bc$~~

$ab = e = ca$ ($\because c$ is inverse of a)

$ab = e = ac$

$b = c$ (left cancellation)

(or) $ba = ca \Rightarrow b = c$ (Right cancellation)

Hence the inverse of an element in a group is unique.

Lattice

Def :- A lattice is a partially order set $(L, \leq)$ in which every pair of elements such as $a, b \in L$ has a Greatest Lower Bound [GLB] and a least upper Bound [L.U.B]

-) The LUB (supremum) of a subset $\{a, b\} \subseteq L$ is denoted by $a \vee b$ (or) $a \oplus b$ and is called the Join (or) sum of 'a' and 'b'

-) GLB (Infimum) of a subset $\{a, b\} \subseteq L$ denoted by $a \wedge b$ (or) $a * b$ and is called the meet (or) product of 'a' and 'b'

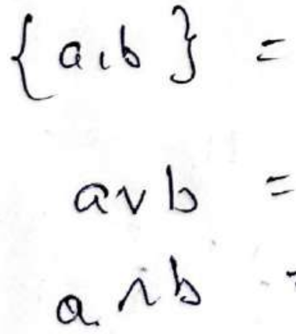
$GLB\{a, b\} = a \wedge b$ (or) $a * b$ (meet or product of a & b)

$LUB\{a, b\} = a \vee b$ (or) $a \oplus b$ (Join or sum of a & b)

i.e $a \vee b = LUB\{x, y\}$

$a \wedge b = glb\{x, y\}$

Eg :-



LUB table

$\vee$	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

GLB table

$\wedge$	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

∴ for every pair of elements in the given poset both, lub, glb exist

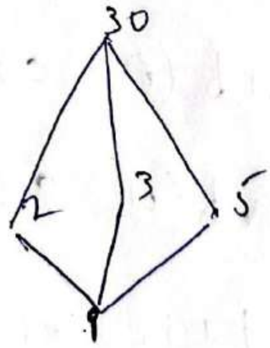
Hence we can say that poset is a lattice.

② eg-2: Let $L = \{1, 2, 3, 5, 30\}$ and R be the relation "is divisible" defined on set L. show that L is lattice or not.

sol:- $L = \{1, 2, 3, 5, 30\}$

R is a divisibility relation defined on L

Hasse diagram:



LUB table

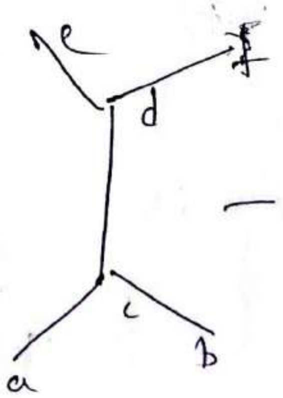
$\vee$	1	2	3	5	30
1	1	2	3	5	30
2	2	2	30	30	30
3	3	30	3	30	30
5	5	30	30	5	30
30	30	30	30	30	30

GLB Table

$\wedge$	1	2	3	5	30
1	1	1	1	1	1
2	1	2	1	1	2
3	1	1	3	1	3
5	1	1	[illegible]	5	5
30	1	2	1	3	30

∴ we can say that for every pair of elements in set L have least upper bound LUB & GLB.
Hence we can say that L is lattice.

(3) check the following Hasse-diagram is lattice or not.



→ Hasse diagram.

sol:- $L = \{a, b, c, d, e, f\}$

for every pair of elements of L has LUB & glb Hence we can say that 'L' is lattice other wise L is not a lattice.

lub table

∨	a	b	c	d	e	f
a	a	c	c	d	e	f
b	c	b	c	d	e	f
c	c	c	c	d	e	f
d	d	d	d	d	e	f
e	e	e	c	d	e	—
f	f	f	f	f	-	f

for the element e & f and f & e lub ~~does~~ not exist.

So we can say that L is not lattice

∴ Glb table

∧	a	b	c	d	e	f
a	a	—	a	a	a	a
b	—	b	b	b	b	b
c	a	b	c	c	c	c
d	a	b	c	d	d	d
e	a	b	c	d	e	d
f	a	b	c	d	d	f

~~not lattice~~

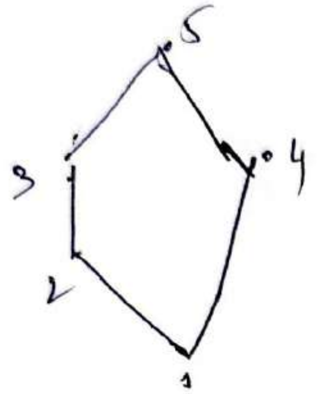
Here for the element a & b and b & a does not exist glb.

So we can say that L is not lattice.

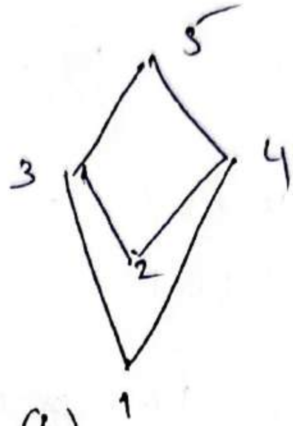
∴ The given hasse diagram is not a lattice.

H.W

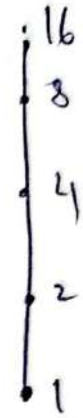
(4) Check wether the following Hasse diagrams, varify are lattices



(a)
lattice



(b)
not lattice
glb of 3 & 4 is 2 & 1
so not possible



lattice.

properties of lattices

Let $(L, \leq)$ be a lattice. L satisfies the following properties of the two binary operations of meet & join denoted by $\wedge$ & $\vee$. for any $a, b, c \in L$ we have

(1) Idempotent property

(i) $a \vee a = a$ (ii) $a \wedge a = a$ $\forall a \in L$

(2) commutative property :

(i) $a \vee b = b \vee a$ (ii) $a \wedge b = b \wedge a$

(3) Associative property.

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

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

(4) Absorption law property

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

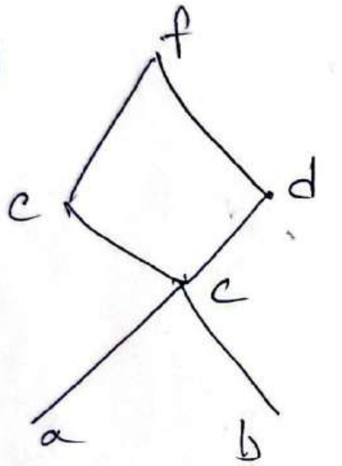
(ii) $a \wedge (b \vee c) = a$

Meet semi lattice

Def:- In a poset, for every pair of elements, If Glb (or) Meet (or) Infimum (or) $\wedge$ exists, then the poset is called "Meet semi lattice"

eg:- check whether the following poset's are meet semi lattice or not

(1)

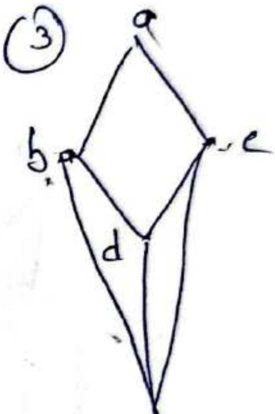


glb not exist
not a meet semi lattice

(2)

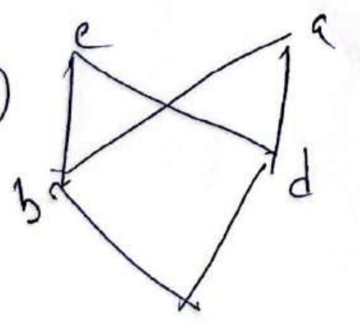
glb exists
so, meet semi lattice

(3)



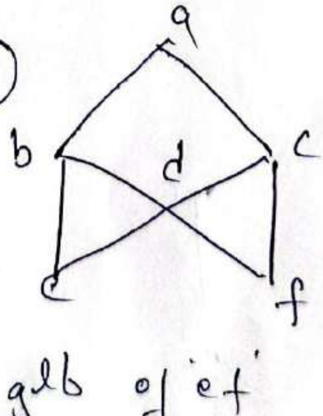
glb of b c is de so not meet semi lattice

(4)



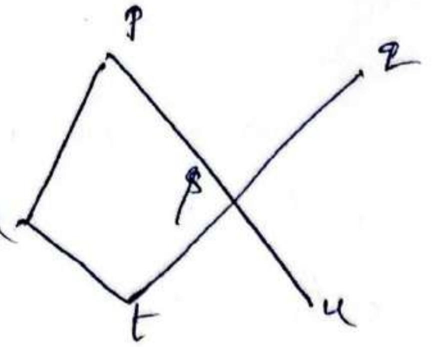
glb not exist
so not a meet semi lattice

(5)



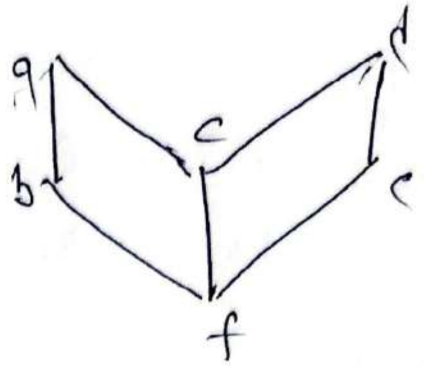
glb of e f not exist
not a meet semi lattice

(6)



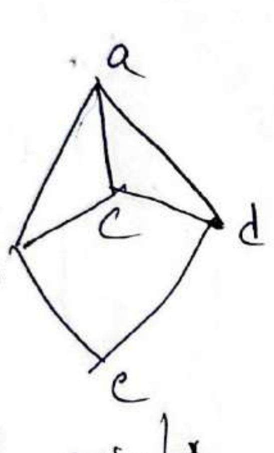
glb of tu does not exist
so not a meet semilattice

(7)



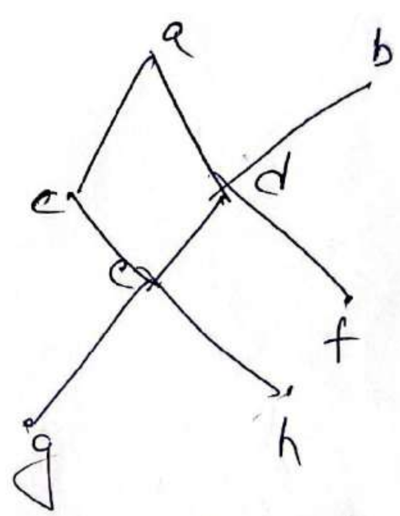
glb of ad is cf so not a meet semi lattice

(8)



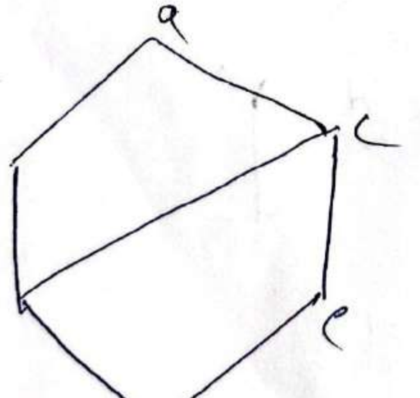
glb exists
so meet semi lattice

(9)



glb for cf & gh doesnot exist
so not meet semi lattice

(10)



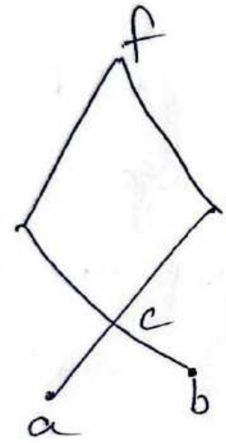
glb exists
meet semi lattice

Join Semi Lattice (24)

Def:- In a poset, for every pair of elements, if lub (or) join (or) supremum (or) v exists then the poset is called "Join semi lattice"

example: check whether the following posets are Join semi lattice or not

(1)

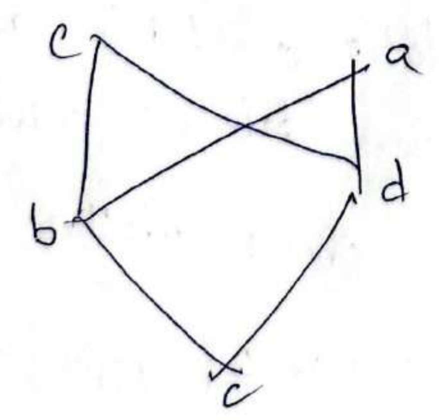


→ we can take any pair of elements in a poset exist lub so it is "join semi lattice"

(2)

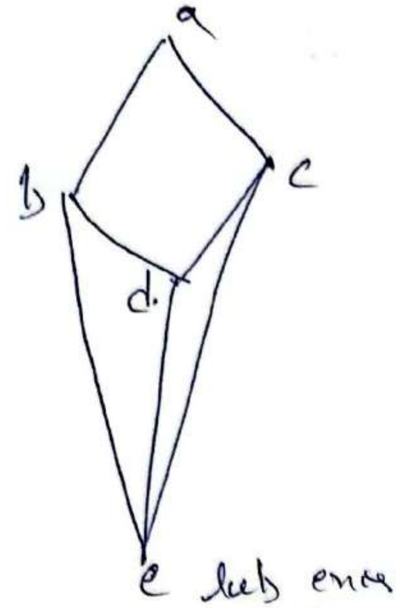
→ least u.b exists so it is a semi lattice

(3)



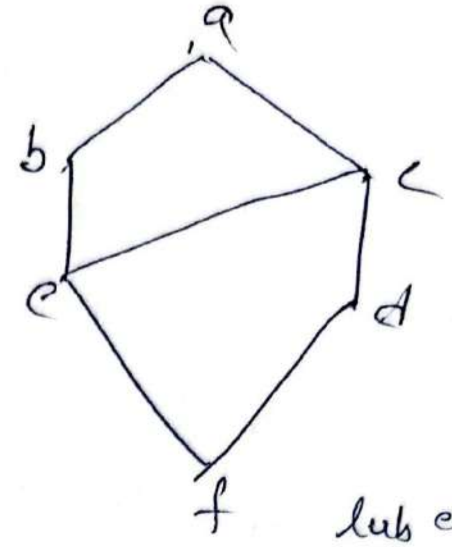
→ not a join semi lattice
lub of bd is c a so ~~need~~ have two lubs, so not exist.

(4)



e lub exists
join semi lattice

(5)



lub exists
join semi lattice

Sublattices

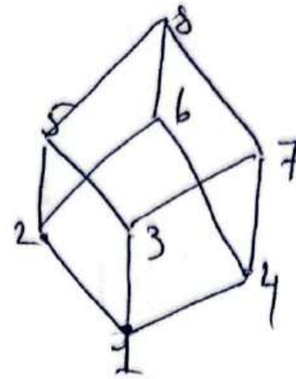
Def:- Let $(L, \vee, \wedge)$ be a lattice and let $S \subseteq L$ be a subset of L. The algebraic system $(S, \vee, \wedge)$ is a sublattice of $(L, \vee, \wedge)$ if and only if S is closed under both the operations $\vee$ and $\wedge$.

→ From the above definition, it is obvious that the sublattice itself is a lattice with r.t $\vee$ and $\wedge$

Eg:- (1) consider the lattice (L, R) represented by Hasse diagram shown below where $L = \{1, 2, 3, 4, 5, 6, 7, 8\}$ check whether the following sets $M_1 = \{1, 2, 4, 6\}$, $M_2 = \{3, 5, 7, 8\}$ and $M_3 = \{1, 2, 4, 8\}$ are sublattices of L or not

(22)

~~sol~~ — Given ~~R,~~ ~~$L = \{1, 2, 3, 4, 5, 6, 7, 8\}$~~



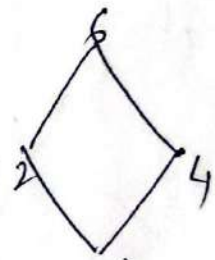
Given Hasse diagram

sol! - Given $L = \{1, 2, 3, 4, 5, 6, 7, 8\}$

(L, R)

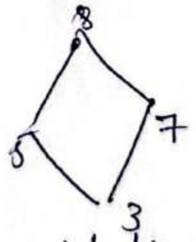
(M_1, R) is a sublattice of (L, R)

$M_1 = \{1, 2, 4, 6\}$



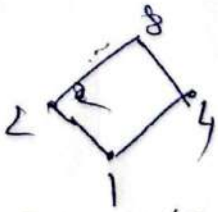
(M_1, R) is a sublattice of (L, R)

$M_2 = \{3, 5, 7, 8\}$



(M_2, R) is a sublattice of (L, R)

$M_3 = \{1, 2, 4, 8\}$



lub of $(2, 4)$ ~~is~~ $= 8$ for M_3

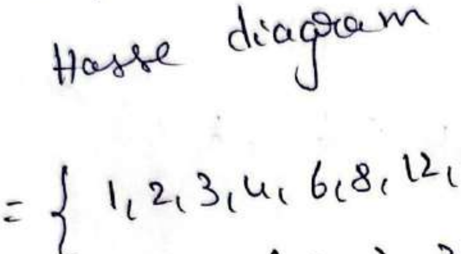
lub of $(2, 4) = 8$

- lup of $(2,4)$ does not exist

Hence we can say that (M_3, R) is not a sub lattice

=.

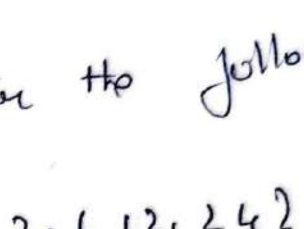
② consider the lattice $(S, /)$ represented by Hasse diagram shown below where $S = \{1, 2, 3, 4, 6, 8, 12, 24\}$ check whether the following sets $M_1 = \{1, 2, 3, 6, 12\}$ $M_2 = \{1, 2, 6, 12, 24\}$ $M_3 = \{1, 2, 4, 8, 24\}$ are sublattices of S or not.



Hasse diagram $(S_{24}, /)$

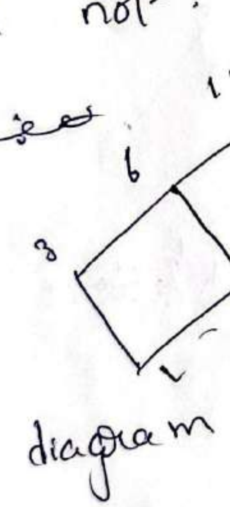
$\langle M_1, / \rangle$

M_1 is a sublattice of $(S_{24}, /)$



$(M_2, /)$

M_2 is a sub-lattice of $(S_{24}, /)$



$(M_3, /)$

M_3 is a sublattice of $(S_{24}, /)$

∴ Ans. both M_1, M_2, M_3 are sublattices of S

=.

Lattices as algebraic systems

Def:- A Lattice is an algebraic system $(L, \vee, \wedge)$ with two binary operations $\vee$ and $\wedge$ defined on L. If and only if both operations satisfies the following laws (or) properties.

For any three elements of L i.e $a, b, c \in L$.

(i) commutative law

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

(ii) Associative property

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

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

(iii) Absorption property

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

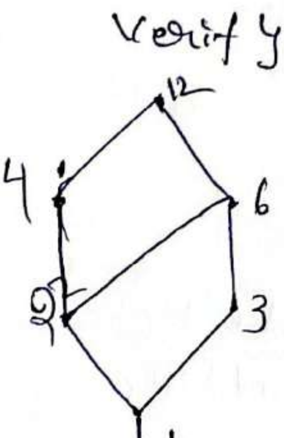
(b) $a \wedge b \vee c) = a$

complete Lattice

Def:- A lattice L is said to be complete lattice if each of its non-empty subsets has a lub and a glb.

Eg:- consider the following Hasse diagram defined on the set $L = \{1, 2, 3, 4, 6, 12\}$ with the relation "Divisibility relation" $(L, |)$ is a Lattice verify. L is complete lattice or not.

Sol:-



consider the set $L = \{1, 2, 3, 4, 6, 12\}$

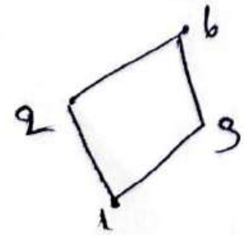
now the subsets of L are

$L_1 = \{1, 2, 3, 6\}$ $\quad L_2 = \{1, 2, 4, 12\}$

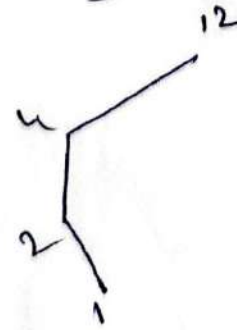
$L_3 = \{1, 3, 6, 12\}$ $\quad L_4 = \{1, 2, 6, 12\}$

$L_5 = \{1, 2, 3, 6, 12\}$ $\quad L_6 = \{2, 3, 4, 6\}$

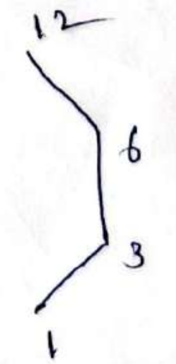
Sol:-



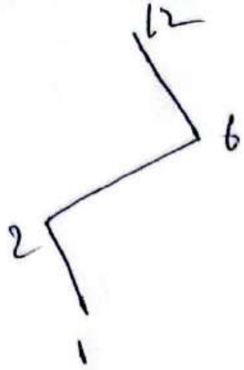
$(L_1, |)$



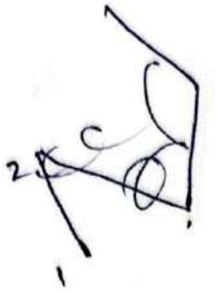
$(L_2, |)$

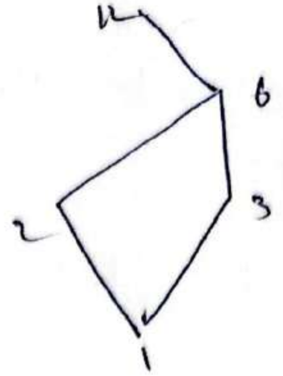


$(L_3, |)$

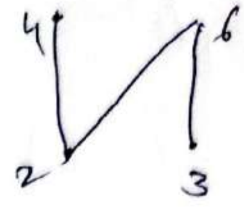


$(L_4, |)$





$(L_5, |)$



$(L_6, |)$

↓
glb not exist
lub also not exist so
$<L_6, |>$

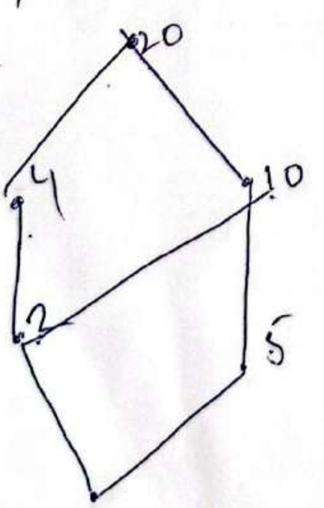
Hence we can say that it is not a comple lattice

② Is $D_{20} = \{S_{20}, |\}$ is a complete lattice ?

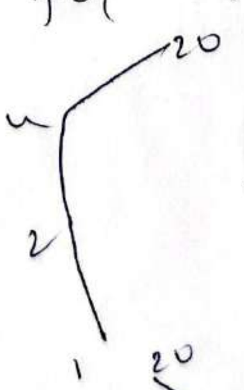
Sol:- Here $D_{20} = \{1, 2, 4, 5, 10, 20\}$

Its Hasse diagram

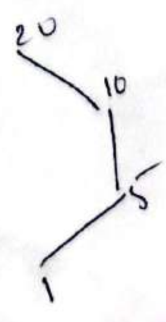
sep:



for the subsets



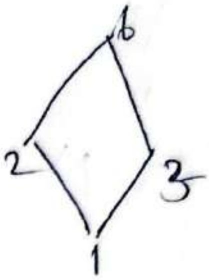
→ has lub & glb so it is complete lattice



→ has lub & glb so it is complete lattice

3) Let $L = \{1, 2, 3, 6\}$ The lattice $(L, /)$ is complete lattice?

Sol:- Let $L = \{1, 2, 3, 6\}$



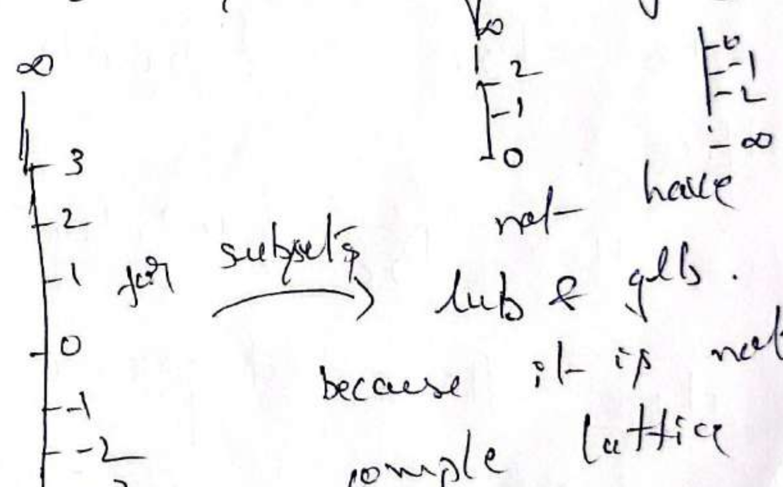
subsets $S_1 = \{1, 2\}$

$S_2 = \{1, 2, 6\}$

$S_3 = \{1, 3, 6\}$ → follow division relation

subsets has a lub & glb so it is comple lattice.

(4) $(Z, \leq)$, Z = set of integers

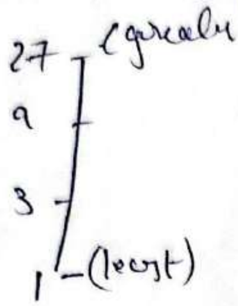


for subsets → not have lub & glb. because it is not comple lattice

Bounded lattice

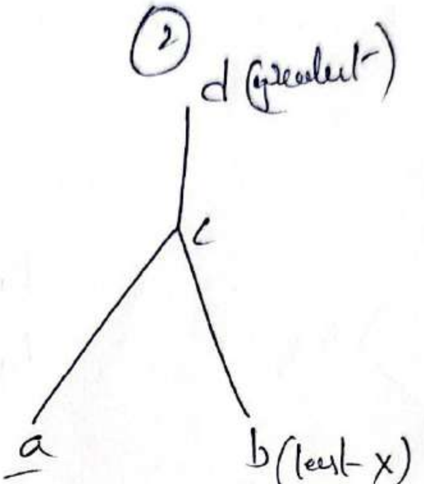
Def:- A lattice which has both elements least & greatest (denoted by 0 & 1 respectively) is called a bounded lattice. It is denoted by $(L, \vee, \wedge, 0, 1)$

Eg:- (1)



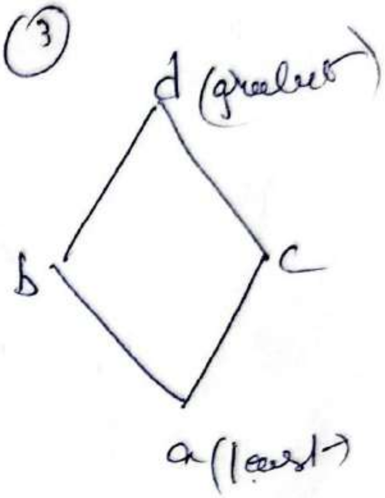
In this lattice has least - 1
greatest - 27
so Bounded lattice

(2)



In this lattice least element of this ~~greatest~~ lattice ~~of each~~ not exist.
so, not bounded lattice

(3)



has both least & greatest so it is bounded lattice

Note: least element is denoted by 0
greatest " " " " 1

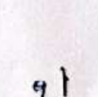
properties of bounded lattice

(1) $0 \wedge a = 0 = a \wedge 0, \forall a \in L$

(2) $0 \vee a = a = a \vee 0, \forall a \in L$

(3) $1 \wedge a = a = a \wedge 1, \forall a \in L$

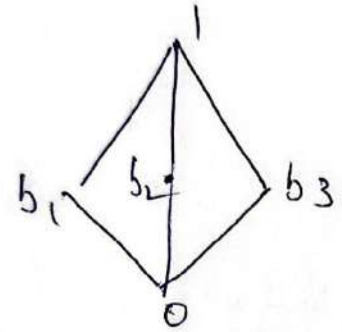
(4) $1 \vee a = 1 = a \vee 1, \forall a \in L$

complemented lattice :

In a bounded lattice $(L, \vee, \wedge, 0, 1)$ an element $b \in L$ is called a complement of an element $a \in L$ if $a \wedge b = 0$ and $a \vee b = 1$
where 0 & 1 are lower and upper bounds of L

Eg:-



b_1, b_2

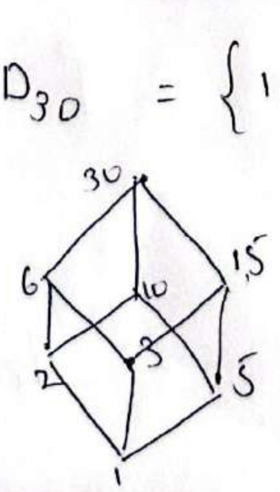
$b_1 \wedge b_2 = 0$
$b_1 \vee b_2 = 1$

So it is complemented lattice

A lattice L is called completed lattice if its bounded and if every element in L has at least one complement.

(1) consider the Bounded lattice $(D_{30}, /)$ and $(D_{20}, /)$ the hasse diagram are shown below. check whealther the above bounded lattices are complemented lattice or not.

Sol :- $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$



$\left\{ \begin{array}{l} a \vee b = \text{LCM of } a \,\&\, b \\ a \wedge b = \text{GCD of } a \,\&\, b \end{array} \right\}$

① 1 & 30

$a=1,\ b=30$

$a,b \in D_{30}$

① $1 \vee 30 = LCM(1,30) = 30$

$1 \wedge 30 = GCD(1,30) = 1$

$1' = 30,\ 30' = 1$

② 2 & 15

$a=2,\ b=15,\ a,b \in D_{30}$

$2 \vee 15 = LCM(2,15) = 30$

$2 \wedge 15 = GCD(2,15) = 1$

$2' = 15,\ 15' = 2$

2) 15 (7
14
1) 2 (1
2
0
Gcd = 1

③ 6 & 5

$6,5 \in D_{30}$

$6 \vee 5 = LCM(6,5) = 30$ (lub)

$6 \wedge 5 = GCD(6,5) = 1$ (glb)

$6' = 5,\ 5' = 6$

④ 3 & 10

$a=3,\ b=10,\ a,b \in D_{30}$

$3 \vee 10 = LCM(3,10) = 30$

$3 \wedge 10 = GCD(3,10) = 1$

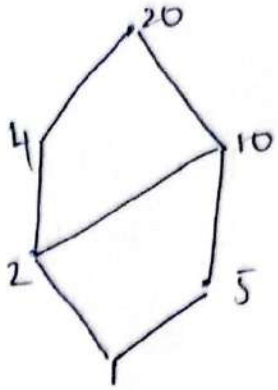
$3' = 10,\ 10' = 3$

$1' = 30,\ 2' = 15,\ 6' = 5,\ 3' = 10$

$30' = 1,\ 15' = 2,\ 5' = 6,\ 10' = 3$

$\therefore (D_{30}, /)$ is a complemented lattice

$D_{20} = \{1, 2, 4, 5, 10, 20\}$



(1) 1 & 20

$a=1, b=20, a, b \in D_{20}$

$1 \vee 20 = LCM(1, 20) = 20$

$1 \wedge 20 = GCD(1, 20) = 1$

$1' = 20, 20' = 1$

(2) 4 & 5

$a=4, b=5, 4, 5 \in D_{20}$

$4 \vee 5 = LCM(4, 5) = 20$

$4 \wedge 5 = GCD(4, 5) = 1$

$4' = 5, 5' = 4$

(3) 2 & 10

$a=2, b=10, 2, 10 \in D_{20}$

$2 \vee 10 = LCM(2, 10) = 10 \neq 20$ (greater)

$2 \wedge 10 = GCD(2, 10) = 2 \neq 1$ (least)

$2' \neq 10, 10' \neq 2$

(4) 4 & 10

$a=4, b=10, 4, 10 \in D_{20}$

$4 \vee 10 = LCM(4, 10) = 20$

$4 \wedge 10 = GCD(4, 10) = 2 \neq 1$

$4' \neq 10$

$10' \neq 4$

elements 2 & 10 does not have complexity

$\therefore$ It is not a complemented lattice.

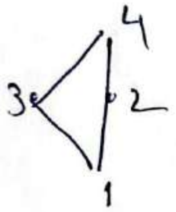
Distributive lattice :- A lattice $(L, \leq)$ is said to be Distributive lattice if and only if it satisfies the following properties

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

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

where a,b,c are any three elements of L i.e $a, b, c \in L$.

Eg:- verify the following Hasse diagrams (or) lattices are Distributive lattice or not-

(a) 

Sol:- consider lattice $L = \{1, 2, 3, 4\}$

L is said to be distributive lattice If it satisfies two properties

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

$a = 1,\ b = 2,\ c = 3$

$1 \vee (2 \wedge 3) = (1 \vee 2) \wedge (1 \vee 3)$

$1 \vee 1 = 2 \wedge 3$

$1 = 1$ (satisfies)

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

$1 \wedge (2 \vee 3) = (1 \wedge 2) \vee (1 \wedge 3)$

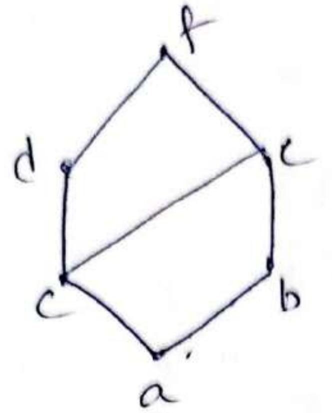
$1 \wedge 4 = 1 \vee 1$

$1 = 1$ (satisfies)

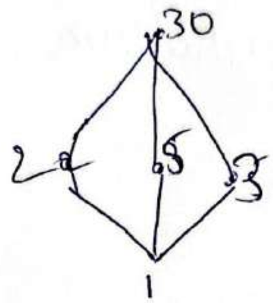
$\therefore$ satisfies 2 property so it is distributive lattice.

H.W

→ (1) find if it is distributive lattice or not



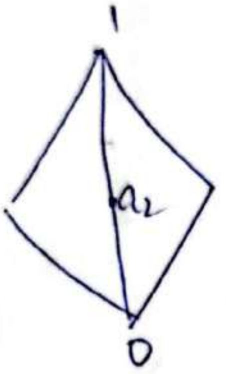
→ (2) $A = \{1, 2, 3, 5, 30\}$ distributive lattice or not.



Modular lattice

Def:- A lattice $(L, \leq)$ is said to be modular lattice if $a \vee (b \wedge c) = (a \vee b) \wedge c$ whenever $a \leq c$, $\forall\ a, b, c \in L$

Eg:- check whether the following lattice is modular or not.



$L = \{0, 1, a_1, a_2, a_3\}$

Take $a = 0$, $b = a_1$, $c = a_3$

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

$0 \vee (a_1 \wedge a_3) = (0 \vee a_1) \wedge a_3$

$0 \vee 0 = a_1 \wedge a_3$

$0 = 0$ (satisfies)

(ii) $0, a_2, a_3 \in L$

$a = 0$, $b = a_2$, $c = a_3$

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

$0 \vee (a_2 \wedge a_3) = (0 \vee a_2) \wedge a_3$

$0 \vee 0 = a_2 \wedge a_3$

$0 = 0$ (satisfies)

(iii) $a_2, a_3, 1 \in L$

$a = a_2$, $b = a_3$, $c = 1$

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

$a_2 \vee (a_3 \wedge 1) = (a_2 \vee a_3) \wedge 1$

$a_2 \vee a_3 = 1 \wedge 1$

$1 = 1$ (satisfies)

$\therefore$ The given lattice is modular lattice

Boolean Algebra

Def! ① A lattice is said to be boolean algebra, if it is both distributive and complemented.

Def :② A non-empty set B with two binary operations + and • a unary operation ' (complement), and two distinct element 0 and 1 is called a Boolean algebra. denoted by (B, +, •, ', 0, 1) If and only if the following properties are satisfied.

Axioms of Boolean Algebra

If a, b, c ∈ B then

① commutative laws

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

② Distributive laws

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

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

③ Identity laws

(a) $a+0 = a$ (b) $a \cdot 1 = a$

④ complement laws

(a) $a+a' = 1$ (b) $a \cdot a' = 0$

Basic Theorem

let $a, b, c \in B$ then

(1) Idempotent laws

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

(2) Boundedness laws

(a) $a+1=1$

(b) $a \cdot 0 = 0$

(3) Absorption laws

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

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

(4) Associative laws

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

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

(5) uniqueness of complement

$a+x=1$ and $a \cdot x = 0$ then $x=a'$

(6) Involution laws

$(a')' = a$

(7) complement laws

(a) $0'=1$ (b) $1'=0$

(8) De morgan's laws

(a) $(a+b)'=a' \cdot b'$

(b) $(a \cdot b)' = a'+b'$

Transposition Theorem

ST: Transposition theorem can be defined by the following Boolean $AB + \bar{A}C = (A+C)(\bar{A}+B)$

proof:- let us take RHS:-

$$(A+C)(\bar{A}+B)$$

$$\Rightarrow (A.\bar{A}) + AB + \bar{A}.C + BC$$

$$\Rightarrow 0 + AB + \bar{A}C + BC$$

($A.\bar{A} = 0$ or $A.A' = 0$)

$$\Rightarrow AB + \bar{A}C + BC$$

$$\Rightarrow AB + \bar{A}C + BC(1)$$

$$\Rightarrow AB + \bar{A}C + BC(A+\bar{A})$$

$$\Rightarrow AB + \bar{A}C + ABC + \bar{A}BC$$

($BC(1) = BC$, $A+\bar{A} = 1$)

$$\Rightarrow AB + ABC + \bar{A}C + \bar{A}BC$$

$$\Rightarrow AB(1+C) + \bar{A}C(1+B)$$

($\because 1+B(\text{any}) = 1$)

$$\Rightarrow AB(1) + \bar{A}C(1)$$

$$\Rightarrow AB + \bar{A}C$$

$$= L.H.S$$

$\therefore$ R.H.S = L.H.S

consensus Theorem

ST: consensus theorem is defined by the following Boolean expressions $AB+\bar{A}C+BC = AB+\bar{A}C$

proof :- let us take L.H.S

$AB + \bar{A}C + BC$

$\Rightarrow AB + \bar{A}C + BC(1)$ $[\because BC(1) = BC]$

$\Rightarrow AB + \bar{A}C + BC(A+\bar{A})$ $(\because A+\bar{A}=1)$

$\Rightarrow AB + \bar{A}C + ABC + \bar{A}BC$

$\Rightarrow AB + ABC + \bar{A}C + \bar{A}CB$

$\Rightarrow AB(1+C) + \bar{A}C(1+B)$

$\Rightarrow AB(1) + \bar{A}C(1)$ $(\because 1+C=1$
$1+B=1$
$1+A=1)$

$\Rightarrow AB+\bar{A}C$

$\Rightarrow$ R.H.S (1+any literal = 1)

$\therefore$ L.H.S = R.H.S

Hence proved.

Demorgan's laws

Demorgan's law-1: The complement of a sum of variables is equal to the product of their individual complements

$$\boxed{\overline{A+B} = \bar{A} \cdot \bar{B}}$$

where A and B are two variables.

Truth table for $\overline{A+B} = \bar{A} \cdot \bar{B}$

A	B	$\bar{A}$	$\bar{B}$	$\bar{A} \cdot \bar{B}$	A+B	$\overline{A+B}$
0	0	1	1	1	0	1
0	1	1	0	0	1	0
1	0	0	1	0	1	0
1	1	0	0	0	φ	0

$\therefore$ L.H.S = R.H.S

$\overline{A+B} = \bar{A} \cdot \bar{B}$ is proved.

($n=2$ (A & B)
$2^2 = 4$.
i.e 00,0
10,11)

Demorgan's law-2 :

The complement of a product of variables is equal to the sum of their individual complements

$$\boxed{\overline{A \cdot B} = \bar{A} + \bar{B}}$$

where A and B are two variables.

Truth table for $\overline{A \cdot B} = \bar{A} + \bar{B}$:

A	B	AB	$\overline{AB}$	$\bar{A}$	$\bar{B}$	$\bar{A} + \bar{B}$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

L.H.S = R.H.S

$\overline{AB} = \bar{A} + \bar{B}$

Hence proved.

Duality law / Duality principle

Boolean algebra we can produce dual by changing all "+" signs to "." signs all "." signs to "+" signs and complementing all 0's to 1's and all 1's to 0's. The variables are not complemented in this procedure

serial number	expression	Dual
1	$\bar{0} = 1$	$\bar{1} = 0$
2	$0 \cdot 1 = 0$	$1 + 0 = 1$
	$0 \cdot 0 = 0$	$1 + 1 = 1$
3	$1 \cdot 1 = 1$	$a + 0 = 0$
4	$A \cdot 0 = 0$	$A + 1 = 1$
5	$A \cdot 1 = A$	$A + 0 = A$
6	$A \cdot \bar{A} = 0$	$A + \bar{A} = 1$
7	$A \cdot B = B \cdot A$	$A + B = B + A$
8	$A(B \cdot C) = (A \cdot B) \cdot C$	$A + B = B + A$
9	$A \cdot (A \cdot B) = A \cdot B$	$A + (B + C) = (A + B) + C$
10		
11	$A \cdot (A \cdot B) = A \cdot B$	$A + (A + B) = A + B$

serial number	expression	Dual
11	$\overline{(A\cdot B)} = \bar{A}+\bar{B}$	$\overline{A+B} = \bar{A}\cdot\bar{B}$
12	$\overline{(A+B)} = \bar{A}\cdot\bar{B}$	$\overline{A\cdot B} = \bar{A}+\bar{B}$
13	$A+B = AB+\bar{A}B+A\bar{B}$	$A\cdot B = (A+B)+(\bar{A}+B)+(A+\bar{B})$
14	$(\bar{A}+C)(A+B)+(B+C)$ $(\bar{A}+C)(A+B)$	$= \bar{A}\cdot C + AB + B\cdot C$ $= \bar{A}\cdot C + A\cdot B$
15	$\overline{\bar{A}B+\bar{A}+AB} = 0$	$\overline{A+B\cdot\bar{A}\cdot(A+B)}$
16	$A+AB = A$	$A(A+B) = A$
17)	$A\bar{B}$ nis,	

Axioms (or) postulates of Boolean Algebra

Axioms or postulates of Boolean algebra are a set of logical expressions that we accept with out proof and upon which we can build a set of useful theorems.

Actually, axioms are definitions of the three basic logical operations that we have already discussed: AND, OR, NOT

Each axiom can be in Interpreted as the outcome of an operation performed by a logic gate (AND, OR, NOT)

AND operation (·)

Axiom 1 : 0.0 = 0

2 : 0.1 = 0

3 : 1.0 = 0

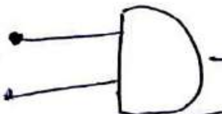
4 : 1.1 = 1

A	B	A·B (or) A AND B
0	0	0·0 = 0
0	1	0·1 = 0
1	0	1·0 = 0
1	1	1·1 = 1

$2^n = 2^2 = 4$

AND operation represented by ·, ∧, ∩

Inputs { A, B



A·B
c (output)

AND gate

OR operation (+)

Axiom 5 : 0+0 = 0

6 : 0+1 = 1

7 : 1+0 = 1

8 : 1+1 = 1

A	B	A OR B (or) A+B
0	0	0+0 = 0
0	1	0+1 = 1
1	0	1+0 = 1
1	1	1+1 = 1

OR operation is represented by +, ∪, ∨

OR operation

A+B
c

OR gate

NOT operation

Axiom 9 : $\bar{1} = 0$ (or) $1' = 0$

10 : $0' = 1$ (or) $\bar{0} = 1$

NOT operation is represented by :-

A	$\bar{A}$
0	1
1	0

B	$\bar{B}$
0	1
1	0

$n = 1$
$2^n = 2^1 = 2$ inputs

$\boxed{\text{Not Gate}}$

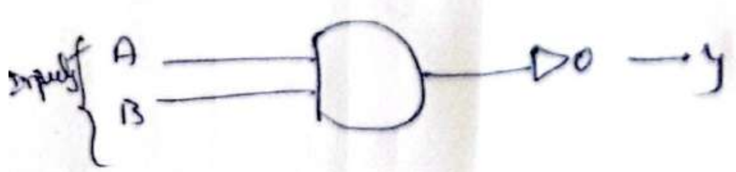
universal gates :

① Nand gate :

Nand = not + And (·)

A	B	y
0	0	1
0	1	1
1	0	1
1	1	0

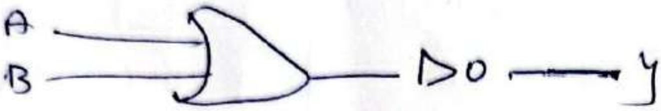
(or)



② NOR gate :

NOR = NOT + OR (+)

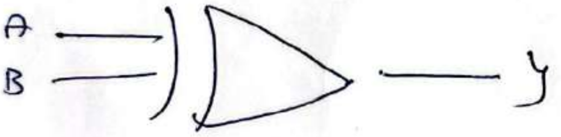
(या)



A	B	y
0	0	1
0	1	0
1	0	0
1	1	0

③ EX-OR gate (+)

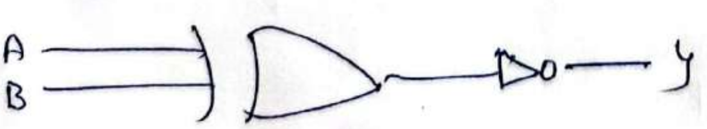
(या)



A	B	y
0	0	0
0	1	1
1	0	1
1	1	0

~~EX-NOR~~ EX-NOR = (EXOR + NOT)

(या)



A	B	y
0	0	1
0	1	0
1	0	0
1	1	1