3 Rings

Date 10/11/21
Page L&W

ii) $(Q, +)$
a) Asso ✓
b) Identity ✓
c) Inverse ✓ eg: $a = -1/2$ $a^{-1} = 1/2$
$a = -1$ $a^{-1} = 1$
d) commu property ✓
e) semigroup
f) distributive ✓

$\therefore (Q, +, \cdot)$ is a ring

iv) $(R, +, \cdot)$ is a ring

v) $Z_4 = \{0, 1, 2, 3\}$
↑
set of integers under modulo 4.

vi) $+_4$
↑
addⁿ modulo 4

$2 +_4 2 = 0$ $2 + 2 = 4$
$2 +_4 3 = 1$ $2 + 3 = 5$

$+_4$ ⇒ Hi te pahile add kra simply ani mg tya new no la modulo under kay ahe tya no ni divide kr ani remainder sang

$2 + 3 = \underline{5}$
↑

Wise

$$\frac{1}{4\sqrt{5}} \quad \frac{-4}{}$$

① ← $2 +_4 3$

v) $(Z_4, +_4, \times_4)$

$Z_4 = \{0, 1, 2, 3\}$

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

i) Asso ✓

ii) identity ✓

iii) Inverse ($a+b = b+a = 0$)

Here $0+0$ in table is present

for 1 : $1+3 = 0$

2 : $2+2 = 0$

3 : $3+1 = 0$.

Thus it satisfy inverse property (In short check out whether 0 is present in every row).

Date / /
Page L&W

d) comm property

eg $1+1=2$

$\rightarrow 2+3=1$ ~~$3+2=1$~~

$\rightarrow 2+1=3$ ~~$1+2=3$~~

e) semi group ✓

f) distributive. ✓

Thus it is a ring.

Rings.

Algebraic structure $(R, +, \cdot)$ is said to be ring

If

i) $(R, +)$ is an abelian group.

ii) $(R, \cdot)$ is semigroup.

iii) Distribute laws holds. ($\cdot$ → multiplication)

eg. $(Z, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$

$(Z_4, +_4, \times_4)$, $(M_{22}, +, \times)$.

Ex: $(Z_5, +_5, \times_5)$ ✓

★ Types of Rings.

1) commutative Ring.

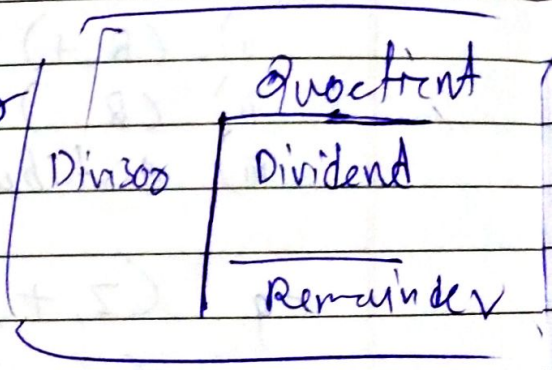
Ring = Abelian Group under addition (already commutative)

A Ring $(R, +, \cdot)$ is called commutative ring if $a.b = b.a$ for every $a, b \in R$.

Ex: $(Z, +)$, $(Q, +)$, $(R, +, \cdot)$
$(Z_4, +_4, \cdot)$ $(Z_n, +_n, \times_n)$

$(M_{22}, +, \times)$ is not commutative Ring.

★ Ring with zero divisor



Suppose A & B are

If $a.b = 0$ where a & b are non zero elements of $(R, +, \cdot)$

then a & b are called as divisors of zero & $(R, +, \cdot)$ is called ring with zero divisors.

Ex: $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

$(Z_6, +_6, \times_6)$.

$a = 2 \neq 0$, $b = 3 \neq 0$.

But $a.b = 2.3 = 0$.

2 & 3 are called zero of divisor.
3 & 4 are called zero of divisor.
$(Z_6, +_6, \times_6)$ ring with zero divisor.

~~4~~ Ring without zero divisor.

$(R, +, .)$ is called ring without zero divisor If $a.b = 0$
$\Rightarrow a = 0$ or $b = 0$.

In other words.

$a \neq 0$, $b \neq 0$ then $a.b \neq 0$.

Ex: $(Z_p, +_p, \times_p)$ where p is prime no.
$(Z_7, +_7, \times_7)$, $(Z_5, +_5, \times_5)$
$(Z, +, \times)$ $(R, +, \times)$.

Integral domain:

A commutative Ring $(R, +, \cdot)$ without unity and with zero divisor is called as integral domain.

Ex: $(Z_5, +_5, \times_5)$, $(Z_p, +_p, \times_p)$.
$(Z, +, \cdot)$ $(Q, +, \cdot)$ $(R, +, \cdot)$,

Field.

A commutative Ring with unity is called field.

If every nonzero element has multiplicative inverse.

eg. $(Z, +, \cdot)$ ⇒ It is not a field

$(Q, +, \cdot)$ ✓ $(R, +, \cdot)$

Q. $Z_4 = \{0, 1, 2, 3\}$
Is $(Z_4, +_4, \times_4)$ Field.

⇒ $Z_4^* = Z_4 - \{0\} = \{1, 2, 3\}$.

$\times_4$	1	2	3
1	(1)	2	3
2	2	0	2
3	3	2	(1)

inverse of 2 is not exist

so (Z_4, X_4, t_4) is not field.

Ex: $Z_5 = \{0, 1, 2, 3, 4\}$.

$\Rightarrow$ $Z_5^* = Z_5 - \{0\} = \{1, 2, 3, 4\}$.

X_5	1	2	3	4
1	(1)	2	3	4
2	2	4	(1)	3
3	3	(1)	4	2
4	4	3	2	(1)

(Z_5, t_5, X_6) a field.

Ex: $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

$\Rightarrow$ $Z_6^* = Z_6 - \{0\} = \{1, 2, 3, 4, 5\}$.

X_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

It is not field.

Date / /
Page L&W

Ex $(Z_3, +_3, \times_3)$

$\times_3$	1	2
1	1	2
2	2	1

It is field.

★ $(Z_p, +_p, \times_p)$ is field where p is prime.

$(Z_n, +_n, \times_n)$ is not field where n is not prime.

↳ Every Field is integral domain.

↳ converse need not be true.

↳ Every integral domain need not be field.

eg: $(Z, +, \cdot)$.

↳ Every finite integral domain is field.

Date 12/11/21
Page L&W

Revision

* Subring of ring.

Let R is a ring and S be the non-empty subset of R. then S is said to be subring of R. If following condition holds.

i) for all $a, b \in S$ then $a-b \in S$, $a.b \in S$

Ex: Is $S = \{0, 3\}$ is subring of ring $(Z_6, +_6, \times_6)$ under operation $+_6$ & $\times_6$

⇒

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

$S = \{0, 3\}$.

If $a = 0, b = 3$

$a - b = -3 \Rightarrow 3$

$-3 = 6(-1) + 3$

$a = 3 \quad b = 0$

$3 - 0 = 3$

$0 - 0 = 0 \quad 3 - 3 = 0$

* Subgroup of group

Subgroup of group

Subset H is said to be subgroup of group G. If

i) If $a, b \in H$ then $a * b \in H$.

ii) $e \in H$

iii) If $a \in H$ then $a^{-1} \in H$.

Ex: $G = Z_6 = \{0, 1, 2, 3, 4, 5\}$

$G = (Z_6, +_6)$

$H = \{0, 3\}$

Is H is subgroup of G under addition modulo 6.

⇒

$+_6$	0	3
0	0	3
3	3	0

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

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

(1), (2), (3) property satisfied

$-_6$	0	3
0	0	3
3	3	0

$\times_6$	0	3
0	0	0
3	0	3

Property satisfied so S is subring of Z_6.

Ex: $R = (Z, +, \cdot)$ $S = (2Z, +, \cdot)$

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

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

⇒ S is subset of R.

subtraction of even integer is even
multiplication of even integer is even.

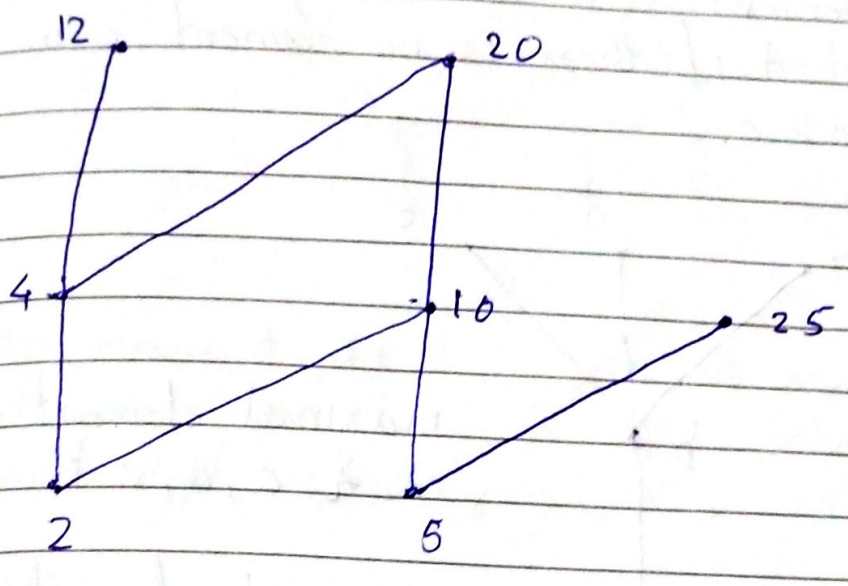
S(2Z) is subring of Ring of Z

* Z has infinite number of subring.

Date 15/11/21
Page L&W

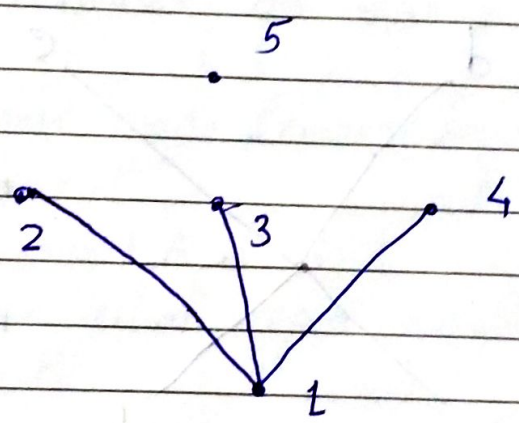
Extra example.

Ex.1



Minimal element = {2, 5}
Maximal element = {12, 20, 25}.

Ex.2

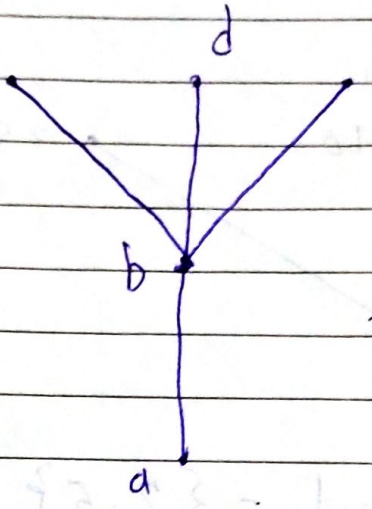


Minimal element = {1}
Maximal element = {2, 3, 4}.

Date 11/12/21
Page

* An element $a \in A$ is called maximal element of set A if there is no element c in A such that $a < c$.

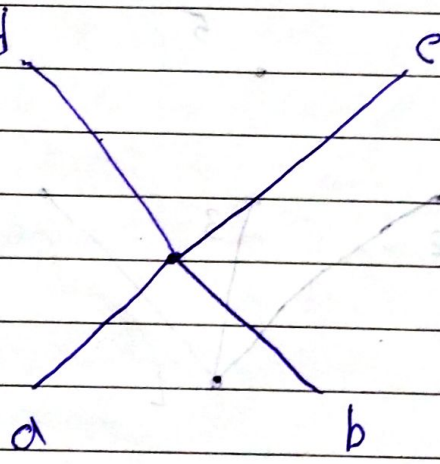
ex:1)



maximal element
$\Rightarrow \{c, d, e\}$.

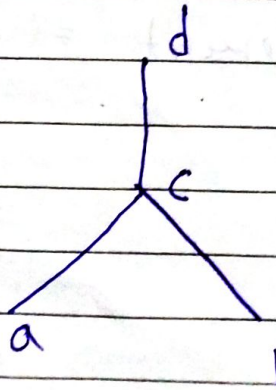
minimal element
$\Rightarrow \{a\}$.

2)



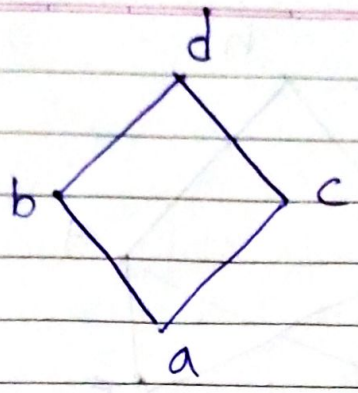
maximal
$= \{d, e\}$
minimal
$= \{a, b\}$

3)



maximal
$= \{d\}$
minimal
$= \{a, b\}$

4)



maximal = {d}

minimal {a}.

* An element $a \in A$ is called minimal element of set A if there is no element c in A such that $a > c$.

↳ If there is single minimal element it's called minimum element. or least element.

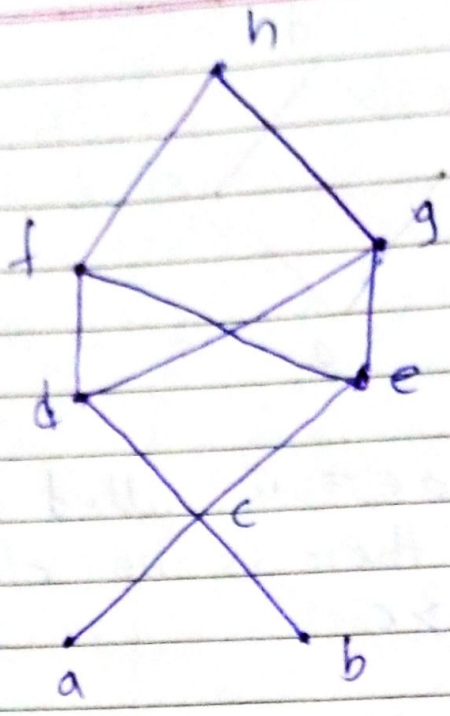
↳ If there is single maximal element it's called greatest element or maximum.

* Upper bounds and lower bounds.

consider a poset A & subset B of A an element $a \in A$ is called an upper bound of B if $b \leq a$ for all $b \in B$.

Ex: Consider the ~~case~~ poset

$$A = \{a, b, c, d, e, f, g, h\}.$$



$B = \{a, b\}$

Upper bound

$= \{c, e, g, d, f, h\}$

$B_1 = \{c, d, e\}$

Upper bound

$= \{f, g, h\}$.

* Lower bound :

An element $a \in A$ is called Lower bound of B If $a \leq b$ for all $b \in B$.

$B_2 = \{a, b\}$

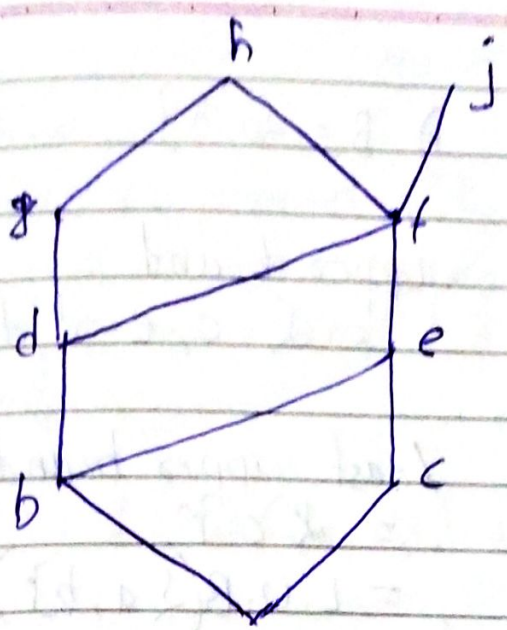
Lower bound

$= \{\phi\}$.

$B_4 = \{c, d, e\}$.

Lower bound $= \{a, b, c\}$.

Ex:



i) $B = \{a, b, c\}$.

Upper bound
$= \{e, f, \phi, j, g, h\}$
$= \{e, f, j, h\}$

Lower bound
$= \{a\}$.

ii) $B = \{j, h\}$.

Upper bound
$= \{\phi\}$

Lower bound
$= \{f, d, e, b, c, a\}$.

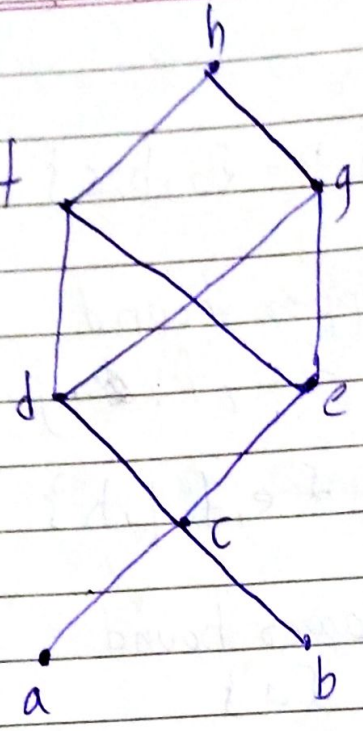
* Least upper bound of set: (L.U.B)

An upper bound of set which is less than all other upper bounds.

* Greatest lower bound of set (G.L.B)

An lower bound of set which is greater than all other lower bound.

Ex:



i) $B = \{a, b\}$

upper bound
$= \{c, e, d, f, g, h\}$

Least upper bound (L.U.B)
$= \{c\}$.
$= L.U.B(\{a, b\}) = c$.

Lower bound $= \phi$
= doesn't exist.

ii) $B = \{c, d, e\}$

upper bound
$= \{f, h, g\}$

Least upper bound = doesn't exist.

Lower bound
$= \{a, b, c\}$.

greater upper lower bound = c.
$G.L.B(\{c, d, e\} = c$.

V = join.
∧ = meet.

Date / /
Page L&W

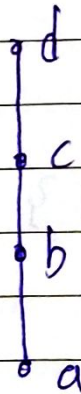
#poset = partial order pair.

Lattice

lattice is a poset $(L, \leq)$ in which every subset of $\{a,b\}$" consisting of two element has least upper bound (L.U.B) & greatest lower bound.

$$L.U.B(\{a,b\}) = a \vee b = a \text{ "join" } b$$

$$G.L.B(\{a,b\}) = a \wedge b = a \text{ "meet" } b$$



i) $\{a,b\}$.

U.B = $\{b, c, d\}$.

L.U.B = $\{b\}$.

L.B = $\{a\}$.

G.L.B = $\{a\}$.

ii) $\{a,c\}$

U.B = $\{c, d\}$

L.U.B = $\{c\}$.

L.B = $\{a\}$

G.L.B = $\{a\}$.

iii) $\{a,d\}$

U.B = $\{d\}$

L.U.B = $\{d\}$

L.B = $\{a\}$

G.L.B = $\{a\}$.

iv) $\{b,c\}$

U.B = $\{d, c\}$

L.U.B = $\{c\}$

L.B = $\{b, a\}$

G.L.B = $\{b\}$

v) $\{b,d\}$

U.B = $\{d\}$

L.U.B = $\{d\}$

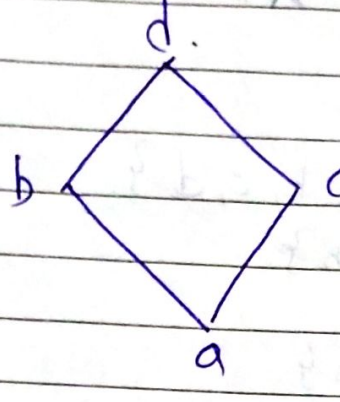
L.B = $\{b, a\}$

G.L.B = $\{b\}$.

vi) {c, d}.
U.B = {d}
L.U.B = {d}
L.B = {c, a, b}
G.L.B = {a}.

For all pair L.U.B & G.L.B exist so this hasse diagram is lattice.

Ex2



i) {a, b}.
U.B = {b, d}
L.U.B = {b}
L.B = {a}
G.L.B = {a}.

ii) {a, d}
U.B = {d}
L.U.B = {d}
L.B = {a}
G.L.B = {a}.

iii) {a, c}.
U.B = {c, d}
L.U.B = {c}
L.B = {a}
G.L.B = {a}

iv) {b, c}
U.B = {d}
L.U.B = {d}
L.B = {a}
G.L.B = {a}

v) (c, d)
U.B = {d}
L.U.B = {c}
L.B = {c, a}
G.L.B = {a}.

vi) $\{b, d\}$

$U.B = \{d\}$

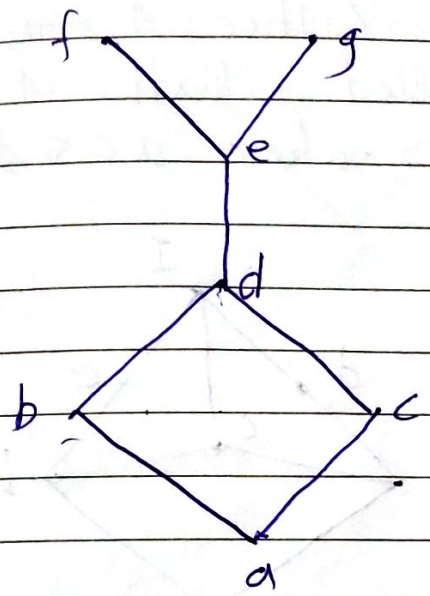
$L.U.B = \{d\}$

$L.B = \{b, a\}$

$G.L.B = \{a\}$.

It is lattice because all two element pair exist L.U.B & G.L.B.

Ex:3

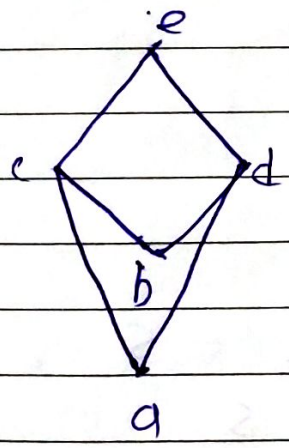


i) $\{f, g\}$

It doesn't have Least upper bound.

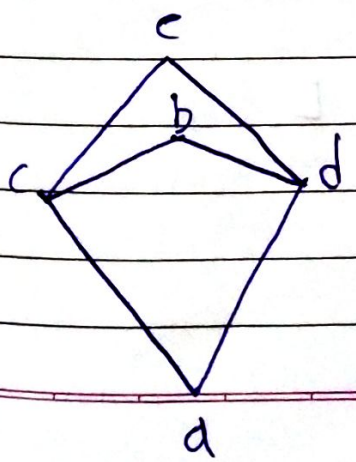
so it is not lattic

Ex:4



i) $\{a, b\}$

a & b are incomparible element.



i) $\{e, b\}$

e & b are incomparable element.

Date 20/11/21
Page L&W

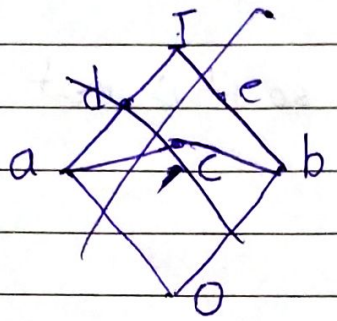
(meet) & (join) are binary operation on set.

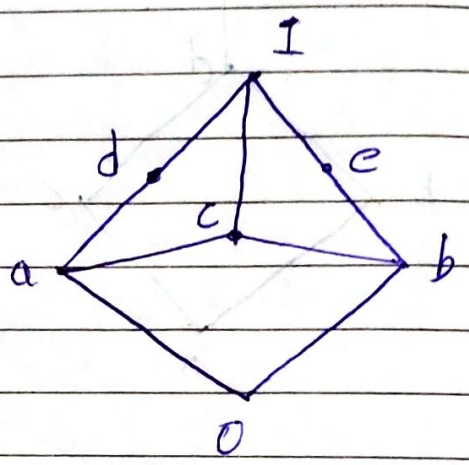
~~(L, V, Λ)~~ (L, V, Λ).

Sublattice

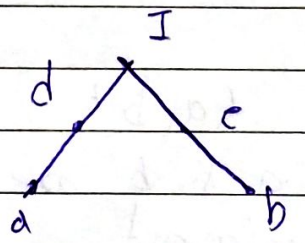
Let $(L, \leq)$ be Lattice, A non-empty subset S of L is called sublattic of L if $a \vee b \in S$ & $a \wedge b \in S$. where $a \in S$ & $b \in S$.

Ex:





i)

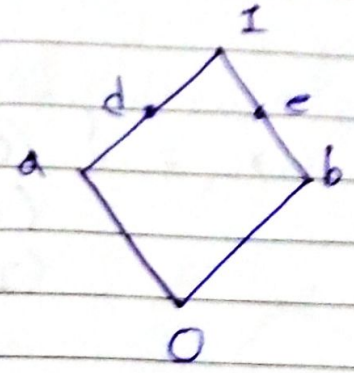


$L.U.B\{a, b\} = a \vee b = I \in S$

$G.L.B\{a, b\} = a \wedge b \notin S$

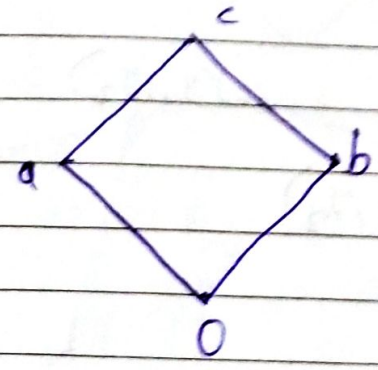
S is not sublattice of L.

ii)



Sublattice.

iii)

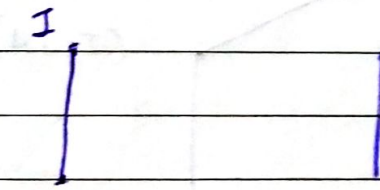


sublattice.

Product of two lattices

$(L_1, \leq)$ & $(L_2, \leq)$ then $L = L_1 \times L_2$ is lattice.

ex:



then $L = L_1 \times L_2$

$L_1 = \{0, I\}$ $0 \leq I$

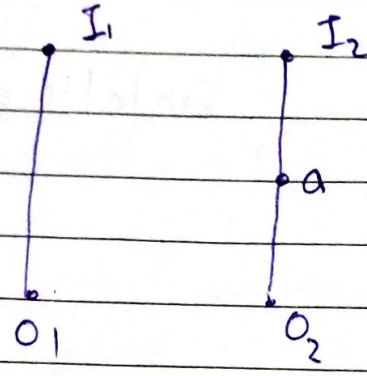
$L_1 \times L_2 = \{(0,0)\ (I,I)\ (I,0)\ (0,I)\}$

$(0,0) \leq (I,I)$ $\quad (I,I) \geq (0,I)$

$(0,0) \leq (0,I)$ $\quad (I,I) \geq (I,0)$

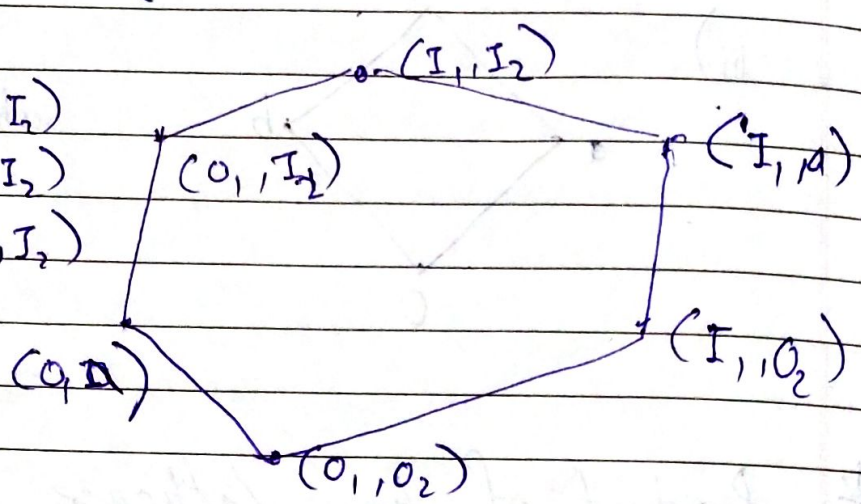
$(0,0) \leq (0,I)$

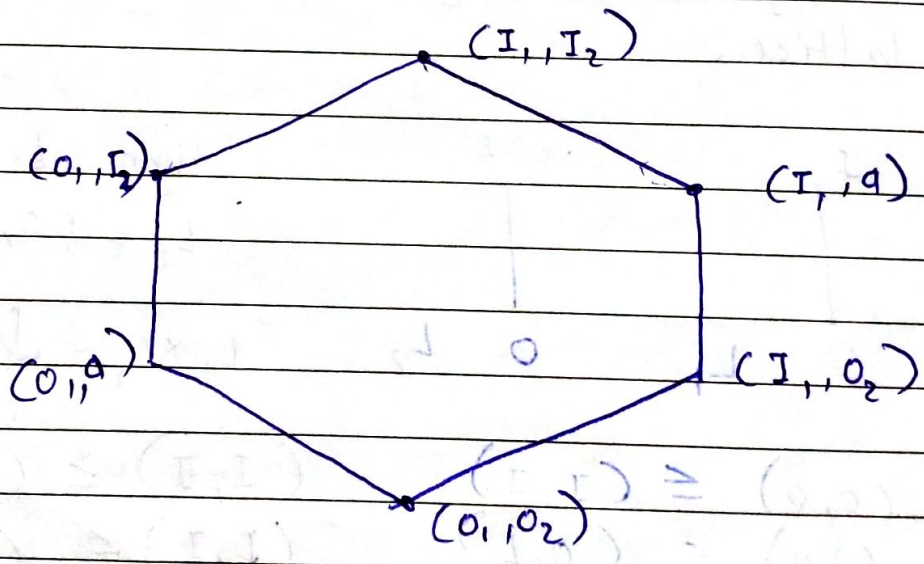
Ex:2



$L_1 \times L_2 = \{ (O_1, O_2)\ (O_1, a)\ (O_1, I_1)\ (I_1, O_2)\ (I_1, a)\ (I_1, I_2) \}$

$(O_1, O_2) \leq (I_1, I_2)$
$(O_1, a) \leq (I_1, I_2)$
$(O_1, I_2) \leq (I_1, I_2)$





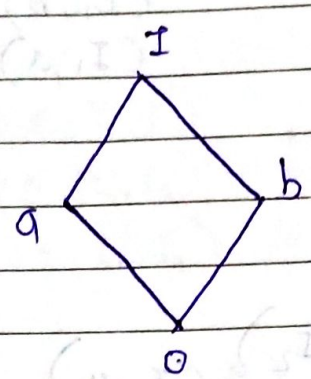
Date / /
Page L&W

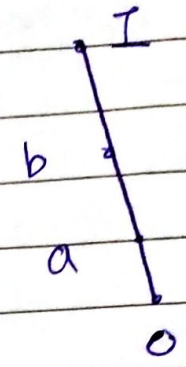
★ Special types of lattice.

1) Bounded Lattice

A lattice is said to be bounded if it has greatest element I & least element O.

e.g





$O \vee I = I$
$O \wedge I = O$
$I \wedge I = I$
$I \vee I \quad I$

$O \vee O = O$
$O \wedge O = O$

$A \cup A^c = U$
$A \cap A' = \phi.$

a = element

a join (∨) $(a^c) = I$
a meet $(a') = O$

$a \vee a = a$
$a \vee b = I$
$a \wedge b = O$

$a \quad a^c = b$

$\vee$ = join
$\wedge$ = meet

Date 21/11/21
Page L&W

compliment of 0 $\boxed{0^c = I}$

$0 \vee I = I$
$0 \wedge I = 0$

$U^c = \phi$

$\phi^c = U$.

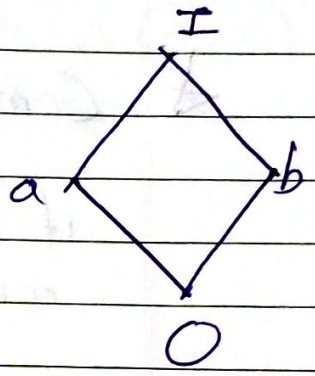
* Complement of element in lattice.

Let L be the bounded lattice with greatest element (I) & least element (0). An $A' \in L$ is called compliment of element A a If $A \vee A' = I$ & $A \wedge A' = 0$.

Ex:

$0 \vee I = I$
$I \wedge I = I$
$I \vee I = I$

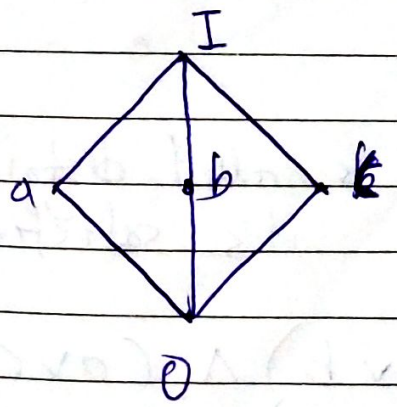
$0 \wedge I = 0$.
$0 \vee 0 = 0$
$0 \wedge 0 = 0$.



$a \vee b = I$
$a \vee a = a$
$a \wedge a = a$

$a \wedge b = 0$
$b \vee b = b$
$b \wedge b = b$.

Ex:

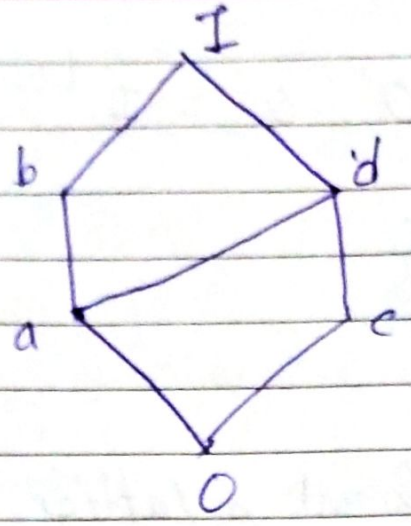


$a \vee c = I$
$a \wedge c = 0$

$a \vee b = I$
$a \wedge b = 0$

$a^c = b$ & c.
$b^c = a$ & c
$c^c = a$ & b

Ex:



$I^c = O$

$O^c = I$

~~$a^c = b$ & d~~

$a \vee c = d$

$a \wedge c = O$.

$a \vee b = b$.

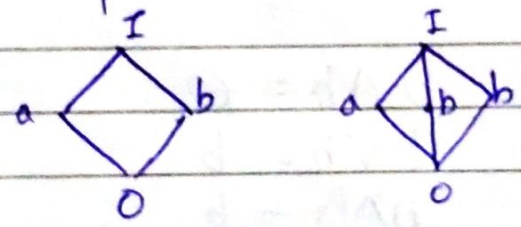
$a \vee d = d$.

Element a has no compliment.

★ Complimented Lattice.

Lattice L is called complemented if it is bounded and every element has complement (At least one).

Ex:



★ Distributive Lattice

Lattice L is called distributive if for every $a, b, c \in L$ it's satisfied distributive if

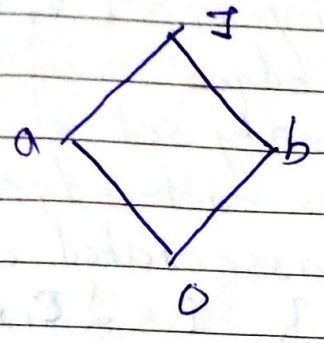
i) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

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

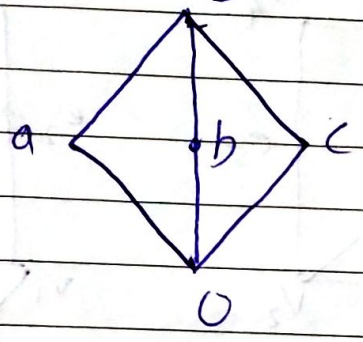
Date / /
Page L&W

* Every element at most 1 compliment.

Ex:



Ex:



L.H.S = $a \vee (b \wedge c)$

$= a \vee O$

$= a$

R.H.S = $(a \vee b) \wedge (a \vee c)$

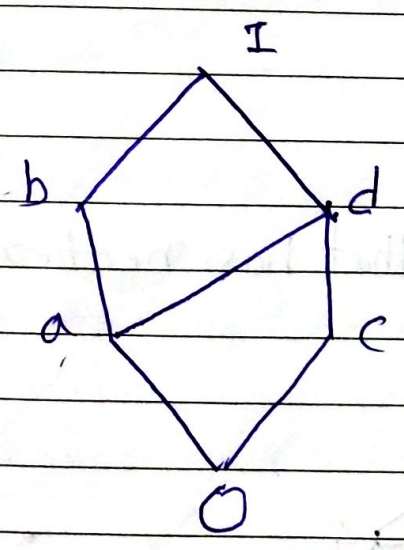
$= I \wedge I$

$= I.$

L.H.S $\neq$ R.H.S

This is non-distributive lattice.

Ex:



Every element has at most 1 complement

So this is distributive lattice.