Unit 2 Lattice

Topics:

- Different types of Relations
- Partially ordered set
- Totally ordered set
- Hasse diagram
- Lattice as Partially ordered set
- Properties of lattices
- Lattice as an algebraic system

Application:

Lattices have been used to design a wide range of cryptographic primitives, including public key encryption, digital signatures, encryption resistant to key leakage attacks, identity based encryption, and fully homomorphic encryption.

One of the most important applications of lattice theory **in modeling and simplifying switching or relay circuits**.

- **Power Set:**

- Power set of set A is the collection of all subset of A. It is denoted by P(A).
- Example : A = { 1, 2, 3 }
  Then P(A) = { Φ, {1}, {2}, {3}, {1, 2}, {2, 3}, {1, 3}, A}
- Note: If A has n elements then P(A) has 2^n elements.

- **Product set:**
- For any set A, the collection of all possible order pair (x, y) where x and y are elements of A is called product set of A. It is denoted by AxA.
- i.e. AxA = { (x, y) / x,y ϵ A}
- Example : A = { 1, 2 } Then AxA = { (1, 1), (1, 2), (2, 1), (2, 2) }

- **Relation :**
- For given set A, subset R of AxA is called relation on A.
- Example : If A = {a, b, c} then R = { (a, a), (a, b), (b, c) } is a relation on A.
- Here (a, b) ϵ R it means a is related to b. It is denoted by aRb
- R1 = { (a, a), (b, b), (b, c) }, R2 = { (a, a), (c, b), (b, c) }, R3 = { (a, -a), (b, b), (b, -c) } here R1 and R2 are relation on A but R3 is not subset of AxA so R3 is not relation on A.

- **Reflexive Relation :**
- A relation R is called reflexive relation on set A if (a, a) ϵ R for all a ϵ A i.e. aRa for all a ϵ A
- Example : If A = {1, 2, 3} then R = { (1, 1),(2, 2), (3, 3),(1,3),(1,2) } is a reflexive relation on A.
- R1 = { (1, 1), (2, 2), (1, 3) } is not a reflexive relation on A because (3, 3) is not in R1

- **Example: Check whether the following relations on Z are reflexive or not.**

  1) xRy if | x – y | = even number

  For integer a, | a – a | = 0 = even number
  Therefore R is reflexive relation on Z.

  2) xRy if xy ≥ 0

  For integer a, aa = $a^2 \geq 0$
  Therefore R is reflexive relation on Z.

  3) xRy if xy < 0

  For 2, 2*2 = 4 so 2 is not related to 2
  Therefore R is not reflexive relation on Z.

- **Symmetric relation:**

  A relation R is called symmetric relation on set A if (a, b) ϵ R for a, b ϵ A then (b, a) ϵ R

  i.e. if aRb then bRa for all a, b ϵ A

  Example : If A = {1, 2, 3} then R = { (1, 2), (2, 1), (3, 3) } is a symmetric relation on A.

  R1 = { (1, 2), (2, 1), (2, 3) } is not a symmetric relation on A because (3, 2) is not in R1

  Example: Check whether the following relations on Z are symmetric or not.

  1) xRy if | x – y | = even number

  For integers x, y, if xRy then | x – y | = even number

  ∴ | y – x | = even number

  ∴ yRx

  Therefore R is symmetric relation on Z.

  2) xRy if x ≥ y

  For integers x, y, if xRy then x ≥ y

  ∴ y can't be getter than x

  ∴ y is not related to x

  Therefore R is not symmetric relation on Z.

- **Anti - Symmetric relation:**

  A relation R is called Anti - symmetric relation on set A for a, b ϵ A a≠b if (a, b) ϵ R then (b, a) is not in R

  i.e. for a, b ϵ A a≠b if aRb then b is not related to a

  Example :If A = {1, 2, 3} then R = { (1, 2), (1, 3), (2, 2) } is Anti - symmetric relation on A.

  R1 = { (1, 2), (2, 1), (2, 3) } is not anti-symmetric relation on A because (1, 2), (2, 1) ϵ R

  Example: Check whether the following relations on Z are anti-symmetric or not.

  1) xRy if | x – y | = even number

  For integers x, y, if xRy then | x – y | = even number

  ∴ | y – x | = even number

  ∴ yRx

  Therefore R is not anti symmetric relation on Z.

  2) xRy if x ≥ y

  For integers x, y, if xRy then x ≥ y

  ∴ y can't be getter than x

  ∴ y is not related to x

  Therefore R is anti symmetric relation on Z.

  Example: A = Set of all males

  R = { (x, y) / x is brother of y } relation on A

  If x is brother of y then y is also brother of x

∴ If xRy then yRx

∴ R is symmetric

Example: A = Set of all males

R = { (x, y) / x is father of y } relation on A

If x is father of y then y can't father of x

∴ If xRy then y is not related to x

∴ R is anti symmetric

Example: On the set A = { 1, 2, 3, 4 } define

1. **Relation R which is symmetric but not anti symmetric**
2. **Relation R which is anti symmetric but not symmetric**
3. **Relation R which is both symmetric and anti symmetric.**
4. **Relation R which is neither symmetric nor anti symmetric.**

Answer :

1) R = { (1, 2), (2, 1), (3, 3) }
2) R = { (1, 2), (2, 4), (3, 3) }
3) R = { (1, 1), (2, 2), (3, 3) }
4) R = { (1, 2), (2, 1), (3, 4) }

- **Transitive relation:**

A relation R is called transitive relation on set A if (a, b), (b, c) ϵ R for a, b, c ϵ A then (a, c) ϵ R

i.e. if aRb and bRc then aRc for a, b, c ϵ A

Example :

If A = {1, 2, 3} then R = { (1, 2), (2, 1), (1, 1), (1, 3), (2, 1) } is a transitive relation on A.

R1 = { (1, 2), (2, 3), (2, 2) } is not a transitive relation on A because

(1, 3) is not in R1

Example: Check whether the following relations on Z are transitive or not.

1) xRy if | x – y | = even number

For integers a, b, c if aRb and bRc then

| a – b | = even number and | b – c | = even number

∴ |a – c| = |a - b| + | b – c | = even number + even number = even number

Therefore R is transitive relation on Z

2) xRy if x ≥ y

For integers a, b, c

If aRb and bRc then a ≥ b and b ≥ c

∴ a ≥ c

∴ aRb

Therefore R is transitive relation on Z.

3) xRy if xy < 0

(-3)*2 = - 6 **<** 0 and 2*(-4) = -8 **<** 0

$\therefore$ -3R2 and 2R(-4)

but $(-3)*(-4) = 12 > 0$

$\therefore$ -3 is not related to (-4)

Therefore R is not transitive relation on Z.

- **Equivalence relation:**

A relation R is called Equivalence relation on set A if R is Reflexive, Symmetric and Transitive relation on A

Example :

A = {a, b, c} and R = { (a, b), (b, a), (a, a), (a, c), (b, c), (b, b), (c, c), (c, b), (c, a) } is a relation on A

Here

R is reflexive

R is symmetric

R is transitive

$\therefore$ R is an equivalence relation on A.

Example: Check whether the following relations on Z are Equivalence relation or not.

1) xRy if | x – y | = even number

For integer a, $| a - a | = 0$ = even number

Therefore R is reflexive relation on Z.

For integers a, b, if aRb then $| a - b |$ = even number

$\therefore$ $| b - a |$ = even number

$\therefore$ bRa

Therefore R is symmetric relation on Z.

For integers a, b, c if aRb and bRc then

$| a - b |$ = even number and $| b - c |$ = even number

$\therefore$ $|a - c| = |a - b| + | b - c |$ = even number + even number = even number

Therefore R is transitive relation on Z.

Therefore R is equivalence relation on Z.

2) xRy if xy ≥ 0

For integer x, $x*x = x^2 \geq 0$

Therefore R is reflexive relation on Z.

For integers x, y, if xRy then $x y \geq 0$

$\therefore$ $yx \geq 0$

$\therefore$ yRx

Therefore R is symmetric relation on Z.

For integers x, y, z if xRy and yRz then $x y \geq 0$ and $yz \geq 0$

$\therefore$ x and y have same sign and y and z have same sign

$\therefore$ x and z have same sign

$\therefore$ xRz

Therefore R is transitive relation on Z.

Therefore R is Equivalence relation on Z.

Example: A = Set of all integers, R = { (x, y) / $x^2 = y^2$ } relation on A

Example: A = {a, b, c}, xRy if x is subset of y for x, y ϵ P(A)

Example: Check R is equivalence relation on real numbers, xRy if |x – y| =Odd number for real numbers x, y

- **Partially ordered set (POSET):**

If R is a relation on set A and R is reflexive, anti symmetric and transitive relation on A then (A, R) is called Poset.
It is also denoted by < A, R >
Example :
If A = {a, b, c} then R = { (a, b), (b, b), (a, a), (a, c), (b, c), (c, c) } is a relation on A.
Here
R is reflexive on A
R is anti symmetric on A
R is transitive on A
Therefore (A, R) is a Poset.

Example: Check whether the (Z, ≤) is Poset or not

For integer x, $x \le x$ so that xRx

∴ ≤ is reflexive relation on Z.

For integers $x \ne y$, if $x \le y$ then y can't less then x

∴ ≤ is anti symmetric relation on Z.

For integers x, y, z, if $x \le y$ and $y \le z$ then $x \le z$

∴ ≤ is transitive relation on Z.

∴ (Z, ≤) is Poset. .

Note:

S_n is the set of positive divisor of n Like $S_{12} = \{1,2,3,4,6,12\}$

D is a divides relation i.e. if a divides b then aDb Like 2D6, 5D30

Example: Check whether the (N, D) is Poset or not where D is divides relation.

For any x ϵ N, x = 1*x , 1 ϵ N

∴ xDx

∴ D is reflexive relation on N.

For any x, y ϵ N, $x \ne y$, if xDy then y = x*z where z ϵ N

∴ y can't divides x

∴ D is anti symmetric relation on N.

For x, y, z ϵ N if xDy and yDz then y = m*x and z = n*y where m,n ϵ N

∴ z = n*y = n*(m*x) = (m*n)*x where m*n ϵ N

∴ xDz

∴ D is transitive relation on N.

∴ (N, D) is Poset.

Example: Check whether the (Z, R) is Poset or not where aRb if and only if $a = b^n$ for positive integer n.

Example: Prove that (S_{60}, D) is Poset or not where D is divides relation

Example: Check whether the (Z, D) is Poset or not where D is divides relation

Example: Prove that $(P(A), \subseteq)$ is Poset where A = { a, b, c }

- **Comparable elements :**

Let (A, R) be a Poset. Two elements a, b ϵ A, a ≠ b are called comparable if aRb or bRa

Example :

(S_{18} , D) is a Poset. S_{18} ={ 1,2,3,6,9,18 }

Here 2D6 so 2 and 6 are called comparable elements.

But 2 does not divides 3 and 3 does not divides 2

So 2 and 3 are non comparable elements.

Totally ordered set (TOSET) or Chain :

A Poset (A, R) is called Toset (or Chain) if any two elements of A are comparable elements.

Example : **Check whether the (N, ≤) is Toset or not**

For positive integer x, x ≤ x so that xRx

∴ ≤ is reflexive relation on N.

For positive integer's x ≠ y, if x ≤ y then y can't less then x

∴ ≤ is anti symmetric relation on N.

For positive integers x, y, z, if x ≤ y and y ≤ z then x ≤ z

∴ ≤ is transitive relation on N.

∴ (N, ≤) is Poset.

For any two positive integers x ≠ y, either x ≤ y or y ≤ x

∴ Either xRy or yRx

∴ x and y are comparable elements.

∴ (N, ≤) is Toset (or Chain)

Example : **Check whether the (S_{64}, D) is Chain or not**

Here S_{64} ={ 1,2,4,8,16,32,64}

For any x ϵ S_{64} , x = 1*x , 1 ϵ N

∴ xDx

∴ D is reflexive relation on S_{64} .

For any x, y ϵ S_{64} , x ≠ y, if xDy then y = x*z where z ϵ N

∴ y can't divides x

∴ D is anti symmetric relation on S64 .

For x, y, z ϵ S_{64} if xDy and yDz then y = m*x and z = n*y where m,n ϵ N

∴ z = n*y = n*(m*x) = (m*n)*x where m*n ϵ N

∴ xDz

∴ D is transitive relation on S_{64} .

∴ (S_{64} , D) is Poset.

Now 1D2, 2D4, 4D8, 8D16, 16D32 and 32D64

∴ For any two elements of S_{64} x ≠ y, either xDy or yDx

∴ (S_{64}, D) is Chain

Example: Check whether the (Z^+, ≤) is Toset or not

- **Cover of an elements :**

Let (A, R) be a Poset. For elements a, b ϵ A, a ≠ b, b is called cover of a if aRb and there is no c ϵ A such that aRc and cRb

Example :

(S_{18} , D) is a Poset. S_{18} ={ 1,2,3,6,9,18 }

Elements	Cover of elements
1	2,3
2	6
3	6,9
6	18
9	18
18	------

Example :

$(P(A),\subseteq)$ is a Poset. A ={ 1,2,3 }

Elements	Cover of elements
Φ	{1}, {2}, {3}
{1}	{1,2}, {1,3}
{2}	{1,2}, {2,3}
{3}	{1,3}, {2,3}
{1,2}	A
{1,3}	A
{2,3}	A
A	--------

Hasse diagram:

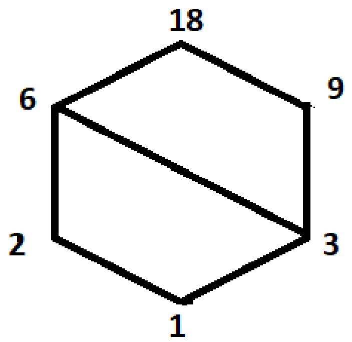
Hasse diagram is a graphical representation of Poset elements. Each elements of Poset is represented by a dot and join by lines according to following rules

1) If b is cover of a then dot corresponding a appears below in the diagram than the dot corresponding to b.
2) The two elements a and b are connected by line segment if either a is cover of b or b is cover of a.
3) it's upward orientation diagram

Example :

(S_{18} , D) is a Poset. S_{18} ={ 1,2,3,6,9,18 }

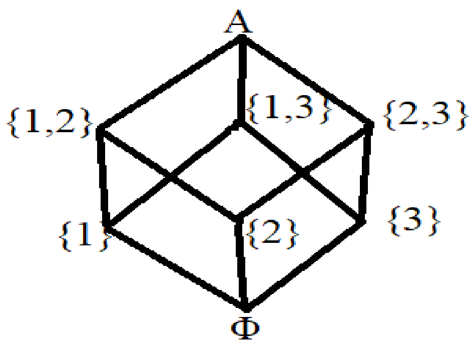
Elements	Cover of elements
1	2,3
2	6
3	6,9
6	18
9	18
18	------



Example :

is a Poset. A ={ 1,2,3 }

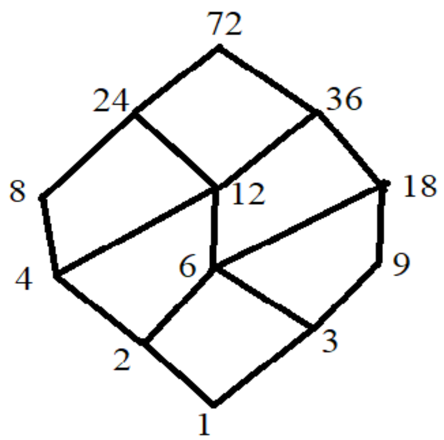
Elements	Cover of elements
Φ	{1}, {2}, {3}
{1}	{1,2}, {1,3}
{2}	{1,2}, {2,3}
{3}	{1,3}, {2,3}
{1,2}	A
{1,3}	A
{2,3}	A
A	--------



Example :

(S_{72} , D) is a Poset. S_{72} ={ 1,2,3,4,6,8,9,12,18,24,36,72 }

Elements	Cover of elements
1	2,3
2	4,6
3	6,9
4	8,12
6	12,18
8	24
9	18
12	24,36
18	36
24	72
36	72
72	-----



Example : Draw the Hasse diagram of (1) (S36, D)

(2) (S64, D)

(3) (S42, D)

Lattice as Partially ordered set

Lower bound :

Let (A, R) be a Poset and B is a subset of A then x ϵ A is called lower bound of B if xRy for all y in B.

Greatest Lower bound :

Let (A, R) be a Poset and B is a subset of A then x ϵ A is called greatest lower bound of B if (1) x is a lower bound of B (2) if a is any other lower bound of B then aRx

Example :

Let (N, ≤) be a Poset and B = {4,6,8,10}

Lower bounds = 1, 2, 3, 4

Greatest lower bound = 4

Upper bound :

Let (A, R) be a Poset and B is a subset of A then x ϵ A is called upper bound of B if yRx for all y in B.

Least upper bound :

Let (A, R) be a Poset and B is a subset of A then x ϵ A is called Least upper bound of B if (1) x is a upper bound of B (2) if a is any other upper bound of B then xRa

Example :

Let (N, ≤) be a Poset and B = {4,6,8,10}

Upper bounds = 10, 11, 12, ……

Least upper bound = 10

- **Lattice as Poset:**

Poset (A, R) is called lattice as Poset if glb(a, b) and lub(a, b) are in A for all elements a, b of A.
i.e. (A, R) is aPoset and for all a, b ϵ A , glb(a, b) ϵ A and lub(a, b) ϵ A
Note :
Let Poset (A, R) , for elements a, b ϵ A , we denotes glb(a, b) = a*b and lub(a, b) =a $\oplus$ b

Some standard relation and their glb(a, b) and lub(a, b)
1) D glb(a, b) = gcd(a, b)
lub(a, b) = lcm(a, b)
2) ≤ glb(a, b) = min(a, b)
lub(a, b) = max(a, b)
3) $\subseteq$ glb(a, b) = a $\cap$ b
lub(a, b) = a $\cup$ b

Example : Prove that (S_{30}, D) is a lattice as Poset.
Here first we prove that (S_{30}, D) is Poset
[Students can easily prove that D is reflexive, anti symmetric and transitive relation on S_{30}
So leave it for them]
Now we prove that for all a, b ϵ S_{30} , glb(a, b) = gcd(a, b) and lub(a, b) = lcm(a, b) ϵ S_{30}
S_{30} = {1,2,3,5,6,10,15,30}

gcd(a, b)	**1**	**2**	**3**	**5**	**6**	**10**	**15**	**30**
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
3	1	1	3	1	3	1	3	3
5	1	1	1	5	1	5	5	5
6	1	2	3	1	6	2	3	6
10	1	2	1	5	2	10	5	10
15	1	1	3	5	3	5	15	15
30	1	2	3	5	6	10	15	30

lcm(a, b)	**1**	**2**	**3**	**5**	**6**	**10**	**15**	**30**
1	1	2	3	5	6	10	15	30
2	2	2	6	10	6	10	30	30
3	3	6	3	15	6	30	15	30
5	5	10	15	5	30	10	15	30
6	6	6	6	30	6	30	30	30
10	10	10	30	10	30	10	30	30
15	15	30	15	15	30	30	15	30
30	30	30	30	30	30	30	30	30

In the above two tables all elements are from S_{30}.
So that for all a, b ϵ S_{30}, glb(a, b) = gcd(a, b) and lub(a, b) = lcm(a, b) ϵ S_{30}
(S_{30}, D) is a lattice as Poset

Example : Prove that (N, ≤) is a lattice as Poset.
Here first we prove that (N, ≤) is Poset
[Students can easily prove that ≤ is reflexive, anti symmetric and transitive relation on N.
So leave it for them]
Now we prove that for all a, b ϵ N, glb(a, b) = min(a, b) and lub(a, b) = max(a, b) ϵ N
For any a, b ϵ N, either a ≤ b or b ≤ a
So that either min(a, b) = a, max(a, b) = b or min(a, b) = b, max(a, b) = a
So in both case glb(a, b) = min(a, b) and lub(a, b) = max(a, b) ϵ N
∴ (N, ≤) is a lattice as Poset.

Example:
Prove that $(P(A), \subseteq)$ is a lattice as Poset where $A = \{2, 4, 6\}$.

Example : Prove that (N, D) is a lattice as Poset.

Properties of Lattice :

Let (A, R) be a Lattice.

1) Idempotent law

$$a * a = a$$

$$a \oplus a = a$$

2) Commutative law

$$a * b = b * a$$

$$a \oplus b = b \oplus a$$

3) Associative law

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

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

4) Absorption law

$$a * (a \oplus b) = a$$

$$a \oplus (a * b) = a$$

Lattice :

Let L be a non empty set and $*$ and $\oplus$ are two binary operations define on L. $(L, *, \oplus)$ Is called Lattice as an algebraic if L satisfied following properties

For all a, b, c $\in$ L

1) Commutative

$$a * b = b * a, \qquad a \oplus b = b \oplus a$$

2) Associative

$$(a * b) * c = a * (b * c), \qquad (a \oplus b) \oplus c = a \oplus (b \oplus c)$$

3) Absorption

$$a * (a \oplus b) = a, \qquad a \oplus (a * b) = a$$

Example :Check whether the (N, Min, Max) is a lattice.

For any a, b, c ϵ N, $a * b = \min(a, b)$ and $a \oplus b = \max(a, b)$

1) Commutative property

$$a * b = \min(a, b) = \min(b, a) = b * a$$
$$a \oplus b = \max(a, b) = \max(b, a) = b \oplus a$$

2) Associative property

$$(a * b) * c = \min(a, b) * c = \min(\min(a, b), c) = \min(a, b, c)$$
$$a * (b * c) = a * \min(b, c) = \min(a, \min(b, c)) = \min(a, b, c)$$
$$\therefore (a * b) * c = a * (b * c)$$

$$(a \oplus b) \oplus c = \max(a, b) \oplus c = \max(\max(a, b), c) = \max(a, b, c)$$
$$a \oplus (b \oplus c) = a \oplus \max(b, c) = \max(a, \max(b, c)) = \max(a, b, c)$$
$$\therefore (a \oplus b) \oplus c = a \oplus (b \oplus c)$$

3) Absorption property

For any a, b ϵ N, either $a \leq b$ or $b \leq a$

For $a \leq b$ $\min(a, b) = a$, $\max(a, b) = b$
$\therefore a * (a \oplus b) = a * \max(a, b) = a * b = \min(a, b) = a$
and $a \oplus (a * b) = a \oplus \min(a, b) = a \oplus a = \max(a, a) = a$

For $b \leq a$ $\min(a, b) = b$, $\max(a, b) = a$
$\therefore a * (a \oplus b) = a * \max(a, b) = a * a = \min(a, a) = a$
and $a \oplus (a * b) = a \oplus \min(a, b) = a \oplus b = \max(a, b) = a$

$\therefore$ (N, Min, Max) is a lattice.

Example : Prove that (S_{30}, GCD, LCM) is a lattice

Here $S_{30} = \{1,2,3,5,6,10,15,30\}$, for all a, b, c ϵ S_{30} $a * b = gcd(a, b)$, $a \oplus b = lcm(a, b)$

1) Commutative property

$$a * b = gcd(a, b) = gcd(b, a) = b * a$$
$$a \oplus b = lcm(a, b) = lcm(b, a) = b \oplus a$$

2) Associative property

$$(a * b) * c = gcd(a, b) * c = gcd(gcd(a, b), c) = gcd(a, b, c)$$
$$a * (b * c) = a * gcd(b, c) = gcd(a, gcd(b, c)) = gcd(a, b, c)$$
$$\therefore (a * b) * c = a * (b * c)$$

$$(a \oplus b) \oplus c = lcm(a, b) \oplus c = lcm(lcm(a, b), c) = lcm(a, b, c)$$
$$a \oplus (b \oplus c) = a \oplus lcm(b, c) = lcm(a, lcm(b, c)) = lcm(a, b, c)$$
$$\therefore (a \oplus b) \oplus c = a \oplus (b \oplus c)$$

3) Absorption property

For any a, b ϵ S_{30}, there are four cases

1) a divides b i.e. b = ma

$$a * b = gcd(a, b) = a \quad \text{and} \quad a \oplus b = lcm(a, b) = b$$
$$a * (a \oplus b) = a * b = a$$
$$a \oplus (a * b) = a \oplus a = a$$

2) b divides a i.e. a = mb

$$a * b = gcd(a, b) = b \quad \text{and} \quad a \oplus b = lcm(a, b) = a$$
$$a * (a \oplus b) = a * a = a$$
$$a \oplus (a * b) = a \oplus b = a$$

3) a and b are co prime |

$$a * b = \gcd(a,b) = 1 \quad \text{and} \quad a \oplus b = \operatorname{lcm}(a,b) = ab$$

$$a * (a \oplus b) = a * ab = \gcd(a, ab) = a$$

$$a \oplus (a * b) = a \oplus 1 = \operatorname{lcm}(a,1) = a$$

4) a and b has common factor m other then 1

a = mx and b = my where m,x,y are positive integers and $m \neq 1$

$$a * b = \gcd(a,b) = m \quad \text{and} \quad a \oplus b = \operatorname{lcm}(a,b) = mxy$$

$$a * (a \oplus b) = a * mxy = \gcd(a, ay) = a \quad (\because mx = a)$$

$$a \oplus (a * b) = a \oplus m = \operatorname{lcm}(a, m) = a \quad (\because mx = a)$$

$\therefore$ (S_{30}, Min, Max) is a lattice.

Example : Prove that (N, gcd, lcm) is a lattice.

Sub Lattice :

Let $(L, *, \oplus)$ be a Lattice and S is subset of L then $(S, *, \oplus)$ is a sub lattice of $(L, *, \oplus)$ if glb and lub of elements of S are in S. i.e. for all $a, b \in S$, $a * b \in S$ and $a \oplus b \in S$

Example : Check whether the following subsets are sub lattice of lattice (S_{24}, GCD, LCM)

1) A = {1,2,3,6}

To prove that A is Sub lattice we draw tables of lub and glb

gcd	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

lcm	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

Here all elements of this tables are from A

$\therefore$ A is sub lattice of S_{24}.

2) B = {1,2,3,8}

Here $2 \oplus 3 = \text{lcm}(2,3) = 6 \notin B$

$\therefore$ B is not sub lattice of S_{24}.

Example : Check whether the following subsets are sub lattice of lattice (N, GCD, LCM)

(1) A = { 1, 2, 5, 10 } (2) A = { 1, 2, 5, 7, 10, 14, 70 }

Distributive lattice :

A lattice $(L, *, \oplus)$ is called distributive lattice if $*$ and $\oplus$ satisfies distributive law

i.e. $a * (b \oplus c) = (a * b) \oplus (a * c)$

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

Note :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$\max(a, \min(b, c)) = \min(\max(a, b), \max(a, c))$$
$$\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c))$$
$$\gcd(a, \operatorname{lcm}(b, c)) = \operatorname{lcm}(\gcd(a, b), \gcd(a, c))$$
$$\operatorname{lcm}(a, \gcd(b, c)) = \gcd(\operatorname{lcm}(a, b), \operatorname{lcm}(a, c))$$

Example : Prove that (R, Min, Max) is a distributive lattice.

(R, min, max) is a lattice (Leave it on students)

4) Distributive property

$$a \oplus (b * c) = \max(a, \min(b, c))$$
$$= \min(\max(a, b), \max(a, c)) = (a \oplus b) * (a \oplus c)$$

$$a * (b \oplus c) = \min(a, \max(b, c))$$
$$= \max(\min(a, b), \min(a, c)) = (a * b) \oplus (a * c)$$

$\therefore$ (R, Min, Max) is a distributive lattice.

Example : Prove that (N, gcd, lcm) is distributive lattice.

Bounded lattice :

Lattice $(L , *, \oplus)$ is called bounded lattice if glb(L) and lub(L) are exist in L.

glb(L) is denoted by 0 element and lub(L) is denoted by I element

Bounded lattice is denoted by $(L , *, \oplus , 0 , I)$

Example:

(S_{24}, GCD, LCM) is lattice

$S_{24} = \{ 1,2,3,4,6,8,12,24\}$

For all $x \in S_{24}$ 1Dx and xD24

$\therefore$ $glb(S_{24}) = 0$ element $= 1$ and $lcm(S_{24}) = I$ element $= 24$

$\therefore$ (S_{24}, GCD, LCM) is bounded lattice

Complement elements :

Let $(L, *, \oplus, 0, I)$ be a bounded lattice then two elements a , b of L are called complement of each other if

$a * b = 0$ element and $a \oplus b = I$ element

Complement of a is denoted by a'

Complemented lattice :

A bounded lattice $(L, *, \oplus, 0, I)$ is called complemented lattice if each element of L has complement in L.

Complemented lattice is denoted by $(L, *, \oplus, ', 0, I)$

Example: Check whether the (S_{24}, GCD, LCM) is Complemented lattice or not.

S_{24} = { 1,2,3,4,6,8,12,24}, glb(S_{24}) = 0 element = 1 and lcm(S_{24}) = I element = 24

For 2 there is no element in S_{24} such that $2 * b = 0$ element and $2 \oplus b = I$ element

So 2 does not have complement therefore (S_{24}, GCD, LCM) is not Complemented lattice

Example : Check whether the is $(P(A), \cap, \cup)$ Complemented lattice or not, where A= {a ,b ,c , d}

First prove that $(P(A), \cap, \cup)$ is lattice.

Now Φ is subset of all elements of P(A) and all elements of P(A) are subset of A

$\therefore$ 0 element = Φ and I element = A

$$
\begin{array}{llll}
\Phi' = A & \{d\}' = \{a,b,c\} & \{b,c\}' = \{a,d\} & \{b,c,d\}' = \{a\} \\
\{a\}' = \{b,c,d\} & \{a,b\}' = \{c,d\} & \{b,d\}' = \{a,c\} & \{a,b,d\}' = \{c\} \\
\{b\}' = \{a,c,d\} & \{a,c\}' = \{b,d\} & \{c,d\}' = \{a,b\} & \{a,c,d\}' = \{b\} \\
\{c\}' = \{a,b,d\} & \{a,d\}' = \{b,c\} & \{a,b,c\}' = \{d\} & A' = \Phi
\end{array}
$$

All complements are in P(A)

$\therefore$ $(P(A), \cap, \cup)$ is complemented lattice.

Example : **Prove that (S_{30}, GCD, LCM) is a Complemented lattice.**