→ Set is unordered collection of distinct elements.
→ It can be finite or infinite.
→ Null set : { } or ϕ
→ for a set A, A and ϕ are trivial subsets.
→ If A is set (finite) then set of all subsets of A, called as power sets P(A).

|A| = Cardinality of set.

A = {a, b} |A| = 2

In power set include all subset

{ ϕ, {a}, {b}, {a,b} } → P(A)

$|P(A)| = 2^{|A|}$

A − B : elements belong to A only

$A \cap B = \phi$: Disjoint sets.

Symmetric difference / Booleansum

$A \Delta B$ / $A \oplus B$ XOR

$= (A - B) \cup (B - A)$

→ Sets are commutative and associative over, $(\cap, \cup, \oplus)$, and distributive over $(\cap, \cup)$.

→ $A - (B \cap C) = (A - B) \cup (A - C)$

Idempotent law

$A \cup A = A \cap A = A$

Absorption law

$A \cup (A \cap B) = A$

$A \cap (A \cup B) = A$

→ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Modular law

(1) $(A \cup B) \cap C = A \cup (B \cup C)$ iff $A \subseteq C$

(2) $(A \cap B) \cup C = A \cap (B \cap C)$ iff $C \subseteq A$

→ $A \cap P(A) = \phi$

→ $P(A) \cap P(P(A)) = \{\phi\}$

→ $A \oplus (B \cup C) \neq (A \oplus B) \cup (B \oplus C)$

$\oplus$ is not distributed over ($\cup$ or $\cap$).

Relations

→ Also called as cross product.

Cartesian Product : Consider two sets.

A = {1, 2, 3} B = {a, b}

$A \times B$ = {(1,a), (1,b), (2,a), (2,b), (3,a), (3,b)}

If |A| = n, |B| = m then $|A \times B| = m \times n$

Relation is subset of Cartesian Product.

R = {(1,a), (1,b)} : We can take any elements

1 R a can be said as (1,a) $\in$ R

No. of finite relations over cartesian product equals to N,

$N = 2^{m \times n}$

Ex → $R = \{(x, y) \in Z \times Z : x < y\}$

Z^+ → (+ve) integer Z^- → negative integers.

R = {(1,2), (2,3), (3,4), (1,4), (1,9), ...}

↳ It is infinite relation.

→ Relation can be finite or infinite depends on nature of cartesian product.

→ Relation can be defined on either two same sets (A × A) or different sets (A × B).

→ Reflexive Relation

A relation 'R' on a set 'A' is said to be reflexive if (x R x) $\forall$ $x \in A$.

Ex A = {1, 2, 3}

then R must contain {(1,1), (2,2), (3,3)}

R can also take other these elements but these elements should be there.

→ If |A| = n then smallest reflexive relation R_n contains 'n' order pair.

→ Largest reflexive relation contain all order pair, $|R_n| = n^2$ (here).

→ If A = {1, 2, 3, ... n} then no. of possible reflexive relation over A is equals to

$|R_n| = 2^{(\text{No. of non diagonal element})}$

$= 2^{m \times n - n} = \boxed{2^{n(m-1)}}$

So Ans = $\boxed{2^{n(n-1)}}$ [∵ m = n here]

No. of non-reflexive relation,

$= 2^{n^2} - 2^{n^2 - n}$

Note → ① The relation '≤' is reflexive on any set of real numbers. ($x \leq x \in R \times R$)

② The relation 'is a divisor of' is reflexive on any set of non-zero real no. ($x/x \in R \times R$)

③ The relation 'is a subset of' is reflexive on any collection of set. ($A \subseteq A$) $\in A$

④ The relation 'is parallel to' is reflexive on a set of all lines.

⑤ $R = \{(x,y) \in Z \times Z : x-y$ is even integer$\}$ $x-x=0$ (even).

→ '$x \equiv x \pmod 5$' on Z is reflexive)

→ If R_1, R_2 are reflexive then,
$R_1 \cap R_2$ → reflexive
$R_1 \cup R_2$ → reflexive
(Comparison on same set through of unity)

Ex = $A = \{1,2,3\}$

$R_1 = \{(1,1),(2,2),(3,3),(3,2),(1,2)\}$

$R_2 = \{(1,1),(2,2),(3,3),(2,3),(2,1)\}$

→ $R_1 \cap R_2$ and $R_1 \cup R_2$ both are reflexive

Irreflexive contains no diagonal elements. Even if a relation contain single diagonal element it will not irreflexive.

Ex → $A = \{1,2,3\}$

$R_1 = \{(1,1),(2,2),(3,3)\}$ → Reflexive

$R_2 = \{\}$ → Irreflexive

$R_3 = \{(2,2)\}$ → Neither reflexive nor Irreflexive

$R_4 = \{(1,2)(2,1)\}$ → Irreflexive but not reflexive

→ There is no relation which is both reflexive and Irreflexive.

→ If $|A| = n$ then,

→ Smallest irreflexive relation,
$R_n = \{\}$, $|R_n| = 0$

→ Largest irreflexive relation
$R_n = A \times A - \{$diagonal elements$\}$
$|R_n| = n^2 - n$

→ Say $|A| = n$ and relation defined on $A \times A$ then no. of irreflexive relation –

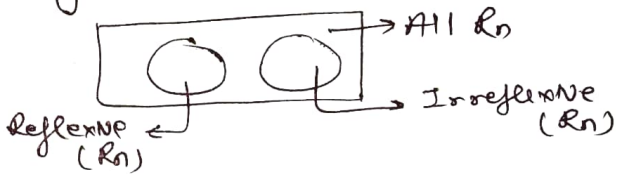
$A \times A = \{(1,1),(2,2)\ldots(n,n),(1,2),(2,1)\ldots\}$

No. of diagonal element $= n$

Total element $= n^2$

No of irreflexive relation $= 2^{n^2-n}$

So, no. of relexive relation equals to no. of irreflexive relation $= 2^{n^2-n}$



→ $|R_n|$ which are either $R(R_n)$ or $I(R_n)$
$= 2 \times 2^{n^2-n} = 2^{n(n-1)+1}$

→ $|R_n|$ which are neither $R(R_n)$ nor $I(R_n) = 2^{n^2} - 2^{n(n-1)+1}$

(or)

$|R_n| = (2^n - 2) \times 2^{n^2-n}$ → for other elements

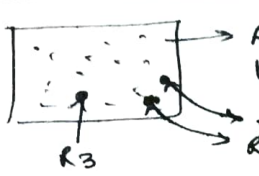
$(2^n - 2)$: all possible relation with (x,x) because each set contain 'n' (x,x) elements

Subtract two cases that either includes all (x,y) elements or non of (x,x) elements

→ The relation '$\leq$' on set of all real no., '$\subseteq$' on set of all sets and '$\perp$' on set of all lines are always irreflexive.

→ If R_1, R_2 are Irreflexive then $R_1 \cup R_2$ and $R_1 \cap R_2$ are Irreflexive.

Closed Under Operation

→ 

Say $R_1 (op) R_2 = R_3$

If R_3 belongs to same set then operation (op) can be said as closed. It means R_1 and R_2 are closed under operation (op).

Statement :

→ The set of all reflexive relations are closed under the operation set Union, Intersection only.

→ The set of all irreflexive relation are closed under the operation set Union, Intersection and set difference.

→ If R_1, R_2 is reflexive then, $R_1 - R_2$ is irreflexive always.

Symmetric Relations

A relation 'R' on a set 'A' is said to be symmetric if (xRy) then (yRx) $\forall x, y \in A$.

$A = \{1, 2, 3\}$

$R_1 = \{(1,2), (2,1)\}$ → Symmetric.

$R_2 = \{(1,1)\}$ → Symmetric

$R_3 = \{\}$ → Symmetric and Irreflexive

$R_4 = A \times A$ → Symmetric and Reflexive

Smallest symmetric relation R_3

$|R_3| = 0$

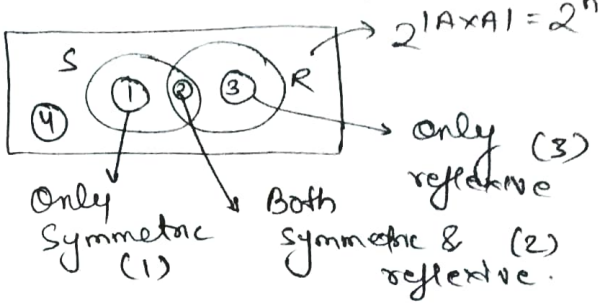
Largest symmetric relation R_4

$|R_4| = n^2$

Relationship between symmetric and reflexive relations

$|A| = n$, $R \in A \times A$

Consider a venn diagram as



→ Is it possible to form above diagram.

Ex → $A = \{1, 2, 3\}$

$R_1 = \{(1,2), (2,1)\}$ → (1)

$R_2 = \{(1,1), (2,2), (3,3)\}$ → (2)

$R_3 = \{(1,1), (2,2), (3,3), (1,2)\}$ → (3)

So, above diagram is valid.

$|S| = 2^n \cdot 2^{\frac{n(n-1)}{2}} = 2^{\frac{n(n+1)}{2}}$

$|R| = 2^{n(n-1)}$

Set of all relations which are both symm. and reflexive

$A \times A = \{(1,1), (2,2), \underbrace{\text{---}}_{n} (n,n), \underbrace{(1,2), (2,1) \text{ --- } \}}_{n^2 - n}$

make pairs of $(n^2 - n)$ elements.

$= 2^{\frac{n^2-n}{2}} = 2^{\frac{n(n-1)}{2}}$

Region (5) $= \underline{2^{\frac{n(n-1)}{2}}} = |S \cap R|$

$|S - R| = n(S) - n(S \cap R)$

$= \underline{2^{\frac{n(n+1)}{2}} - 2^{\frac{n(n-1)}{2}}}$

$|R - S| = n(R) - n(S \cap R)$

$= 2^{n(n-1)} - 2^{\frac{n(n-1)}{2}}$

$= \underline{2^{\frac{n(n-1)}{2}} \left(1 - \frac{1}{\sqrt{2}}\right)}$

$\overline{n(S \cup R)} = 2^{n^2} - \left[n(S) + n(R) - n(S \cap R)\right]$

If R_1 and R_2 are symmetric then $(R_1 \cap R_2)$, $(R_1 \cup R_2)$ and $(R_1 - R_2)$ are symmetric relations or closed relation.

No. of symmetric relation possible

$|A| = n$, $(A \times A)$

$A = \{1, 2, 3\}$

$A \times A = \{(1,1)\ (2,2)\ (3,3)\ (1,2)\ (2,1)\ (1,3)\ (3,1)\ (2,3)\ (3,2)\}$

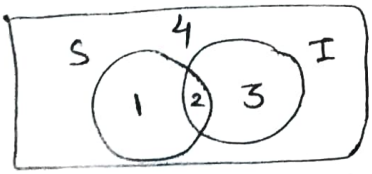
(1,1), (2,2), (3,3) → 2 × 2 × 2; (1,2), (2,1) → 2; (1,3), (3,1) → 2; (2,3), (3,2) → 2

No. of relation symmetric $= 2^n \times 2^{\frac{n^2-n}{2}}$

Here, $n^2 - n$ is an even number.

Relation btw Symmetric and Irreflexive :

$|A| = n$ $\quad A \times A \rightarrow$ set.



We are trying to validate the above venn diagram.

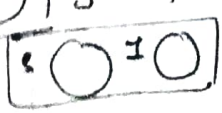
$R_S = \{(1,2)\ (2,1), (1,1)\} \rightarrow (1)$

$R_I = \{(1,2)\} \rightarrow (3)$

$R_{I \cap S} = \{(1,2), (2,1)\} \rightarrow (2)$

So, above diagram is possible.

$R_4 = \{(1,2), (1,1)\} \rightarrow (4)$

→ If  gets failed then go for  (Disjoint sets).

$n(S) = 2^{\frac{n(n-1)}{2}} \cdot 2^n = \boxed{2^{\frac{n(n+1)}{2}}}$

$n(I) = \boxed{2^{n^2-n}}$

$n(S \cap I) = \boxed{2^{\frac{n^2-n}{2}}}$

$n(S \cup I) = n(S) + n(I) - n(S \cap I)$

$n(S - I) = n(S) - n(S \cap I)$

$n(I - S) = n(I) - n(S \cap I)$

$\overline{n(S \cup I)} = 2^{n^2} - n(S \cup I)$

Antisymmetric Relations

A rel^n is antisymmetric if $(x R y)$ and $(y R x)$ then $x = y$ $\forall$ $x, y \in R$

$A = \{1, 2, 3\}$

$R_1 = \{(1,2)(2,1)\}$ Not Antisymmetric

$R_2 = \{(1,1)\}$ Symmetric, Antisymmetric

$R_3 = \{(1,2), (1,1)\}$ Antisymmetric

$R_4 = \{(2,3)\}$ Not Antisymmetric and not symmetric

$R_5 = \{\} \rightarrow$ Smallest antisymmetric Relation

$A \times A = \{(1,1)(2,2)(3,3)$ $(1,2)(2,1)$ $(3,1)(1,3)$ $(2,3)(3,2)\}$ Pairs

$R_7 = \{(1,1), (2,2), (3,3), (1,2), (3,1), (3,2)\} \rightarrow$ Largest Antisymm

We can choose only one order pairs from pairs

If $|A| = n$ for $A \times A$ then cardinality for largest antisymmetric relation is –

$|R_n| = n + \frac{n^2-n}{2}$

$= \boxed{\frac{n(n+1)}{2}}$

No. of antisymmetric relⁿ possible

$|A| = n \quad |A \times A| = n^2$

Ex → $A = \{1,2,3\}$

$A \times A$

$= \underset{\downarrow 2}{(1,1)} \; \underset{\downarrow 2}{(2,2)} \; \underset{\downarrow 2}{(3,3)} \; \underset{\downarrow 3}{(1,2)(2,1)}$

$\underset{\downarrow 3}{(1,3)(3,1)} \quad \underset{\downarrow 3}{(2,3)(3,2)}$

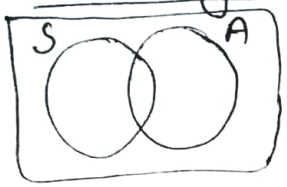
3 cases bcoz either include (1,3), or (3,1) or non from them.

$= 2^3 \times 3^3$

for $|A| = n$

No. of antisymmetric relations are $= \boxed{2^n \times 3^{\frac{n^2-n}{2}}}$

Relation between no. of symmetric and antisymmetric relation.



$|U| = 2^{n^2}$

$n(S) = 2^{\frac{n(n+1)}{2}}$

$n(A) = 2^n 3^{n(n-1)/2}$

$A = \{1,2\}$

$R = \{(1,1),(2,2)\}$ is a symmetic as well as antisymmetric

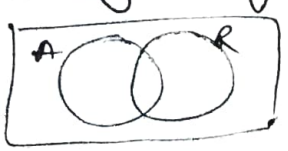
$|R| = 2^n = n(S \cap A)$

$n(S \cup A) = n(S) + n(A) - n(S \cap A)$

$n(\overline{S \cup A}) = n(U) - n(S \cup A)$

$n(S - A) = n(S) - n(S \cap A)$

Relation between reflexive and antisymmetric



$n(A) = 2^n 3^{n(n-1)/2}$

$n(R) = 2^{n(n-1)}$

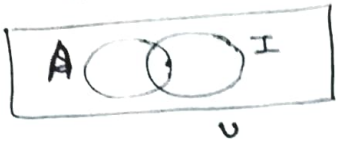
$n(U) = 2^{n^2}$

for male reflexive we need to include all (x,x) element. So they have no choice to exclude

$n(A \cap R) = 3^{\frac{n(n-1)}{2}}$

$n(A \cup R) = n(A) + n(R) - n(A \cap R)$

Relation btw irreflexive and anti-symmetric



$|A| = n, \; A \times A$

$n(U) = 2^{n^2}$

$n(A) = 2^n 3^{n(n+1)/2}$

$n(I) = 2^{n(n-1)}$

R is a relⁿ which is asymmetric as well as Irreflexive

$R = \{(1,2)\}$

$n(A \cap I) = 3^{n(n-1)/2}$

Now you can solve any query over it.

The relation '$\leq$' or '$<$' is anti-symmetric on any set of real numbers.

The relation '$\subseteq$' or '$\subset$' (Proper subset) is also anti-symmetric over any collection.

Asymmetric relation

→ Stricter version of anti-symmetric.

→ We are not allowing even (x,x).

A relⁿ is asymmetric if $(x R y)$ then $(y \not R x) \; \forall \; x, y \in A$,

$A = \{1,2,3\}$

$R_1 = \{(1,2)\}$ → Asymetric and Anti-symmetric.

$R_2 = \{(1,2)(2,2)\}$ → Not asymetric but Asymetric.

→ Diagonal element can be present in anti-symmetric but not in asymmetric.

$R_3 = \{\}$ → Asymmetric and antisymmetric both.
↳ Also symmetric too.

$R_4 = \{(1,2),(2,1)\}$ → Not asymmetric and antisymmetric.

|Smallest| = 0 : { }

Largest Asymmetric Relation

$$|\text{Largest}| = \frac{n^2 - n}{2} \quad , |A| = n$$

No. of asymmetric relations

$|A| = n$, $A \times A \subseteq R$

$A = \{1, 2, \cdots n\}$ $\quad |A \times A| = n^2$

$A \times A = \{$ diagonal + non diagonal $\}$

diagonal: n — only 1 choice

non diagonal: $(n^2-n)/2$ — include only one from any pair

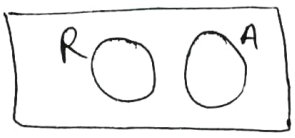
→ We can't include diagonal elements

→ We have 3 choices for non-diagonal

$$|\text{Asymmtric}| = 3^{\frac{n(n-1)}{2}}$$

→ If a relation is reflexive then it can't be asymmetric.

So,



$n(A) = 3^{n(n-1)/2}$

$n(R) = 2^{n(n-1)}$

$n(A \cup R) = n(A) + n(R)$

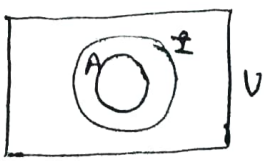
$n(A \cap R) = 0$

$n(A - R) = n(A)$, $n(R - A) = n(R)$

$n(\overline{R \cup A}) = n(U) - n(R \cup A)$

Relation between asymmetric and Irreflexive

→ Every asymmetric relation is Irreflexive, but converse is not true.



$n(I) = 2^{n(n-1)}$, $n(A) = 3^{n(n-1)/2}$

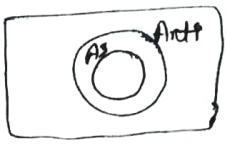
$n(I \cup A) = n(I)$ | $n(I - A) = n(I) - n(A)$

$n(I \cap A) = n(A)$ | $n(A - I) = 0$

$n(\overline{I \cup A}) = n(U) - n(I)$

Relation between Asymmetric and Antisymmetric

→ Every Asymmetric relation is antisymmetric.



$n(A) = 3^{n(n-1)/2}$

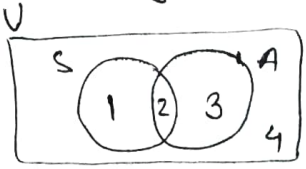
$n(Anti) = 2^n 3^{n(n-1)/2}$

$n(A \cup Anti) = n(Anti)$

Similarly we can find more values.

Relation between symmetric and Asymmetric

$R = \{\}$ is symmetric and asymmetric both.



$|U| = n^2$

$R_1 = \{(1,1)\}$ | $R_3 = \{(1,2)\}$

$R_2 = \{\}$ | $R_4 = \{(1,1), (1,2)\}$

$n(S \cap A) = 1$

$n(S) = 2^{n(n+1)/2}$

$n(A) = 3^{n(n-1)/2}$

$n(S \cup A) = n(S) + n(A) - 1$

$n(\overline{S \cup A}) = n(U) - n(S \cup A)$

Asymmetric relations are closed under subset, intersection and set difference operation.

Transitive Relations

If (xRy) and (yRz), then (xRz) $\forall x, y, z \in A$.

If $a < b$ and $b < c$ then $a < c$. So it is transitive.

Similarly, $>$, $\subseteq$, $\subset$, $\supseteq$, $\supset$, $/$, are transitive.

→ Closed under $\cap$ not $\cup$.

Equivalence relation

→ If the relation is reflexive, symmetric and transitive then it called as equivalence relation.

R = {diagonal elements only} is the smallest equivalence relation.

$|R| = n$ (for smallest reln)

$|R| = n^2$ (for largest reln)

→ Closed under $\cap$ not $\cup$

Partial Order Relation (POR)

→ A relation on set 'A' is POR if it follow all these properties reflexive, transitive and antisymmetric together.

POset → Partial Order Set

Ex of POR

$R = \{(1,1), (2,2), (3,3)\}$

↳ Above Relation is both POR and equivalence relation.

→ The set that holds a partial order relation 'R' on it called as Poset.

→ It is denoted as $[A; R]$ (A: set, R: POR)

Ex: $[R; \leq]$, $[R; \geq]$, $[S; \subseteq]$, $[S; \supseteq]$, $[S; /]$

R → set of all real no.

S → set of all sets.

$\supseteq$ → Superset $\supset$ → Proper superset

TOS (Totally Ordered Set)

Linearly ordered set or chain.

A Poset $[A; R]$ is called as 'TOS' if every pair of elements in A are comparable, i.e; aRb or bRa $\forall$ $a, b \in A$.

Ex → If 'A' is any set of real no's then poset $[A; \leq]$ is a TOS.

Explanation: If you choose any two no from the set of real no's you can apply '$\leq$' symbol to compare. Either both will be equal or any one of them should be smaller one.

② If $A = \{1, 2, 6, 30, 60, 300\}$ then $[A; /]$ is TOS.

→ In finding TOS order of selection doesn't matter as you can think 1 can devides every no's similarly 2 can divides all no's on RHS but how 2 can devide 1. so we divide 1 by 2 ∴ it is not case we are just choosing (1,2) are applying division as (2/1) in both cases either (1,2) or (2,1).

Partial Orders and Lattice

→ Hasse diagram (Poset diagram)

Let [A; R] be a poset. The poset diagram is as follows.

(1) There is a vertex corresponding to each element of 'A'.

(2) An edge between the elements 'a' and 'b' is not present in the diagram, if there exists an element $x \in A$ such that (aRx) and (xRb).

→ We don't represent any transitive relation.

(3) An edge btw the elements 'a' and 'b' is present iff (aRb) and there no element 'x' $\in A$ such that (aRx) and (xRb).

Ex $A = \{1,2,3\}$ Relation: '$\leq$'

$R = \{(1,1), (2,2), (3,3), (1,2), (2,3), (1,3)\}$

3 ↻ 2 ↻ 1 ↻ we can do this for (1,1) (2,2) (3,3) but we know that it is poset and all posets are reflexive so, we have no need to make self loop in Hasse diagram.

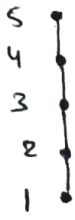
So,

→ No need bcoz we can go from 1 to 3 using 2 already!

Also we have no need to mark the arrows bcoz it is already understood from levels in diagram

→ It refers (1,2) bcoz 2 at upper level in diag.

Ex → ① $A = \{1,2,3,4,5\}$ $[A; \leq]$



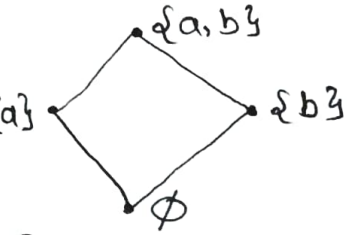
→ Loops and transitive relations are included.

→ It is a total order relation and like a chain.

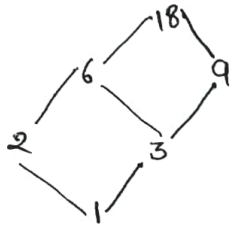
② $S = \{\phi, \{a\}, \{b\}, \{a,b\}\}$

$S = P(A)$: $A = \{a,b\}$

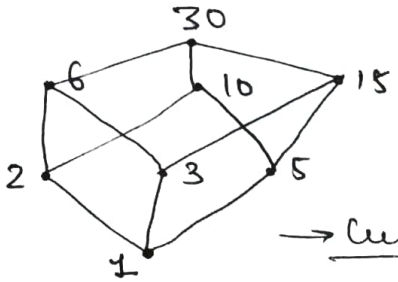
Relation $[S, \subseteq]$



③ $A = \{1,2,3,9,6,18\}$ $[A, /]$



$A = \{1,2,3,5,6,10,15,30\}$ $[A, /]$



→ Cube.

→ It is not necessary to always get a closed figure.

LUB → Least Upper Bound

(LUB or Join or Supremum)

Let [A; R] be a poset for $a, b \in A$, if there exist an

element $c \in A$ such that

(1) aRc and bRc

(2) if there exist any other element 'd' such that (aRd) and (bRd) then (cRd), then C is called LUB of 'a' & 'b'.

Ex → (a,c) and (b,c) : C is upper bound.

Ex

$(\{a\}, \{a,b\})$ $(\{b\}, \{a,b\})$

So, here, LUB = $\{a,b\}$

Similarly $(\phi, \{a\})$ $(\{a\}, \{a\})$ and $(\phi, \{b\})$ $(\{b\}, \{b\})$

So, $\{a\}$ and $\{b\}$ both are LUB. Now apply Rule 2 because $(\{a\}, \{a,b\})$ $(\phi, \{a,b\})$ are also in the bucket.

So, $c = \{a\}$, $d = \{a,b\}$. Or (cRd) LUB = $c = \{a\}$.

→ So, Or $(\{a\}, \{a,b\})$ and $(\{b\}, \{a,b\})$ and $(\phi, \{a,b\})$

LUB = $\{a,b\}$

→ Or $(\phi, \{a\})$, $(\{a\}, \{a,b\})$

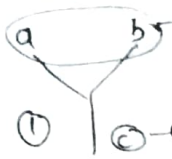
LUB = $\{a\}$

→ Or $(\phi, \{b\})$, $(\{b\}, \{a,b\})$

LUB = $\{b\}$

→ Maximal, Minimal element

If in a poset, an element is not related to any other element, called maximal and if in a poset, no related element for an element called minimal



Maximal = $\{a, b, c\}$
Minimal = $\{a, b, c\}$

→ 2nd Hasse diagram have reflexive property and also showing a Poset

max = $\{d, e, b, i\}$
min = $\{f, g, h\}$

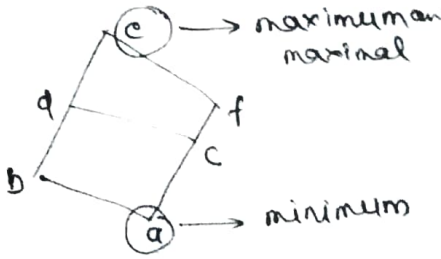
→ Each diagram must have min. 1, maximal or minimal elements

→ Maximum and Minimum element

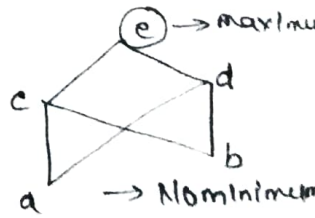
for maximum, it should be maximal and every elements related to it.

for minimum, it should be minimal and it is related to every element in poset.

No maximum
d, e not related to each other.



a, b are minimal but not minimum because not related.



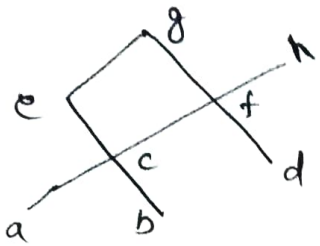
No minimum but a, b are minimal

• a → Both maximum and minimum

• • • a b c → No maximum and minimum.

We need single bottom or single top.

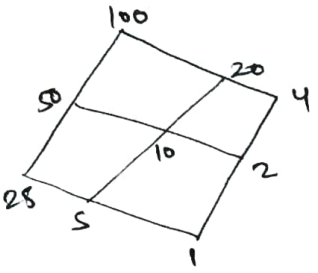
Upper Bound and Lower Bound



A = {a, b, c, d, e, f, g}
B = {e, c}
L.B(B) = {a, b, c}
U.B(B) = {g, e}

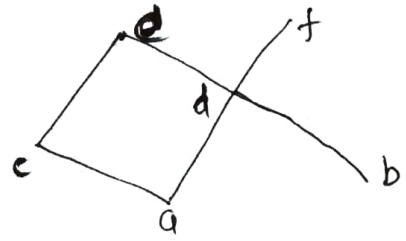
We consider e, c in L.B and U.B bcoz of self loop

B = {c, f, d}
L.B(B) = ϕ
U.B(B) = {f, g, h}

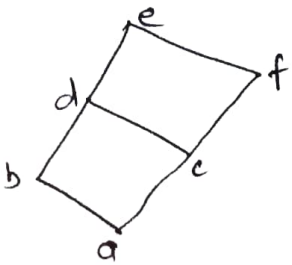


L.B(B) = {1, 2, 5, 10}
U.B(B) = {100, 50}
B = {5, 10}

Least Upper Bound (Join, Supremum, V)
Greatest Lower Bound (Intimum, meet, ∧)



B = {c, d}	B = {a, b}	B = {e, f}
UB(B) = {e}	UB = {e, d, f}	UB = {ϕ}
LB(B) = {e}	LB = ϕ	LB = {a, d, b}
LUB(B) = {e}	LUB = {d}	LUB = {ϕ}
GLB(B) = {a}	GLB = ϕ	GLB = {d}



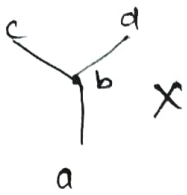
B = {a, c, f}	B = {d, c}
UB = ef	UB = e, d
LUB = f	LUB = d
LB = a	LB = ac
GLB = a	GLB = c

Join Semi-Lattice

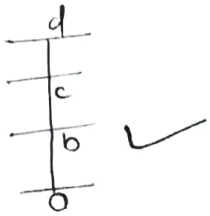
→ We fix the number of element in the set as 2 for which we are finding UB and LB.

→ In a poset if LUB exist for every pair of elements, then poset is called as Join semi-lattice.

→ If you are able to find any single pair for which Join doesn't exist then poset is not Join semi-Lattice.



X

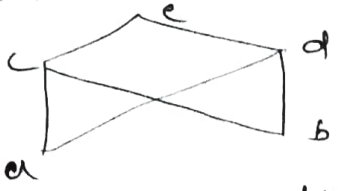


L

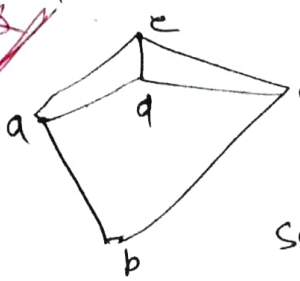
→ To find join for any pair find out the point where they met firstly.

→ In case if there are more than 2 candidates for LUB then it will not Join semi-Lo

Ex



c, d both are the candidates.



→ Here are two candidate, d, e but both are join. So, we can take decision.

→ No single top → No Join semi lattice

Meet semi-Lattice

In a poset if GLB / MEET / $\wedge$ exists for every pair of elements then poset is called meet-semi lattice.

Lattice → If both LUB and GLB are exist for every pair of elements.

Ex → A $\{1, 2, 3, \ldots 10\}$ $[A, /]$ is a meet semi lattice.

→ To verify take any pair and find its GCD, it will belong to A.
Here, GCD and GLB are same

(1) $S = \{\{a\}, \{b\}, \{a, b\}\}$ $[S, \subseteq]$ is a join semi-lattice.

→ To verify you can find union of any two element means in case of subset Union acts as LUB.

→ for GLB use intersection.

(3) $A = \{1, 2, 3, 4\}$ $[A, \leq]$

→ It is a lattice
GLB and LUB both exists

Properties of Lattice

for 3 elements in a lattice all these are true.

(1) Commutative over $\wedge$ or $\vee$
$a \vee b = b \vee a$ → LUB
$b \wedge a = a \wedge b$ → GLB

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

(3) Itempodent law
$A \vee a = a$
$a \wedge a \; a$

(4) Absorption law
$a \vee (a \wedge b) = a = a \wedge (a \vee b)$

(5) Distribution law doesn't holds good for all lattice, only hold for distributive lattice.

→ In a lattice $(a \vee b) = b$ iff $(a \wedge b) = a \; \forall \; a, b \in$ Lattice

Distributive Lattice and Sub-Lattice

(1) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
(2) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
If a lattice satisfies above two properties called as distributive lattice.

Sub-lattice:

Finding distributive lattice is a hectic task, so we use sub-lattice concept to reduce complexity.

Let 'L' be a lattice $[L, \vee, \wedge]$. A subset 'M' of 'L' is called a sublattice if
1) M is a lattice
2) for any pair of elements $a, b \in M$ the LUB and GLB are same in 'M' and 'L'.

A (Set) → A × A → Relation (R, A, T) → POR
(R, A, T) → Reflexive, Antisymmetric, Transitive
POR → Poset $[A, R]$ ← Lattice ← Distributive Lattice
Lattice → Sub-lattice

In a bounded lattice, the following properties holds good.

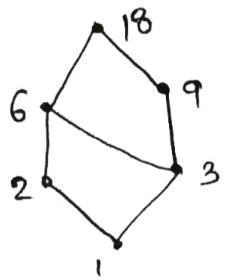
Say $I \rightarrow$ Upper bound
$0 \rightarrow$ lower bound.

1) LUB of a and I i.e $a \vee I = I$
2) GLB of a and I i.e $a \wedge I = a$
3) LUB of a and 0 i.e $a \vee 0 = a$
4) GLB of a and 0 i.e $a \wedge 0 = 0$

(a, I) $(0, a)$
GLB LUB GLB LUB

→ D_n = set of all positive divisors of n.

Ex, $[D_{18}, /]$



Bounded lattice

Lattice that have both lower and upper bound.

→ In the given poset check for lattice, if and only if it has single top or single bottom

Upper bound of Lattice 'L', if there exist an element I, such that $\forall a \in L$, $(a \leq I)$ then, I is called upper bound.

Lower bound of lattice '0', if all the elements in L have $(0 \leq a) \forall a \in L$.

→ for infinite lattice no upper and lower bound exist. Basically it exist but we can't find it

→ for any set upper bound is Universal set and lower bound is ϕ.

$A \cup U = U$	$a \vee I = I$
$A \cap U = A$	$a \wedge I = a$
$A \cup \phi = A$	$a \vee 0 = a$
$A \cap \phi = \phi$	$a \wedge 0 = 0$

→ Bounded lattice must have lower or upper bound means finite lattice, not infinite

We know,

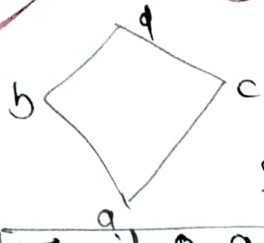
$A \cup A^c = U$	$a \vee a^c = I$
$A \cap A^c = \phi$	$a \wedge a^c = 0$

So, we can find complement of element using bounded lattices.

Complement of an element in a lattice

In a bounded lattice 'L' for any element $a \in L$, if there exist an element $b \in L$ such that $a \vee b = I$, $a \wedge b = 0$, that 'b' is called complement of 'a', we can say 'a', 'b' are complement of each other.

$I^c = O$, $O^c = I$



$a \vee d = d$

$a \wedge d = a$

So, a, d are complement

$I = d, O = a$

→ for '$\vee$' go for first meet of both elements on the upper side.

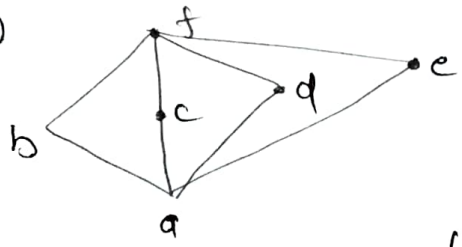
→ for '$\wedge$' go for first meet of both elements on lower side.

$b \vee c = d$

$b \wedge c = a$

So, b, c are complement of each other

(e)



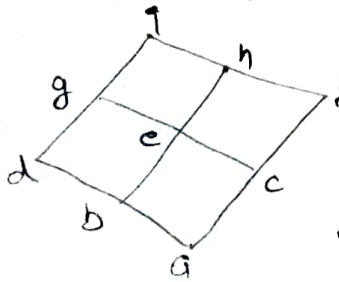
(a, f) are complement pair.

$b^c = c, d, e$ | $e^c = b, c, d$

$c^c = b, d, e$ | $d^c = b, c, e$

In set theory there should exist atleast and only one complement.

→ In lattice it is not necessary that there should exist a complement and there is need not be only one complement.



(d, e) are not complement

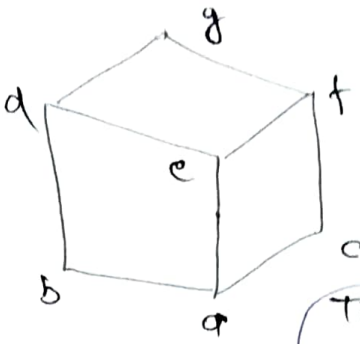
$d \vee e = g$ not i

$d \wedge e = b$ not a

i → GLB → I

a → LUB → O

$a^c = i$, $d^c = f$, there is no complement for b, c, e, g, h.



$b^c = c, f$

$a^c = g$, $d^c = c$

$c^c = b, d$

$f^c = b$

There is no complement for e.

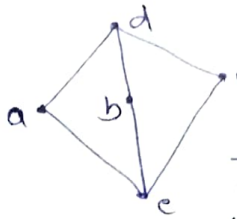
Distributive Lattice

A lattice is said to be distributive if $\forall a, b, c \in L$

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

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

Eg:



LHS

$a \vee (b \wedge c)$

$a \vee e = a$

RHS

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

$(a \vee c) = d$

$a \neq d$, so distributive law doesn't follow.

But checking property for each order pair of 3 elements is a tedious test. So we go for a trick.

→ In a distributive lattice, every element have atmost 1 complements.

In above diagram,

$a^c = b, c$ | $c^c = a, b$

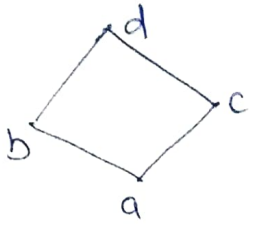
$b^c = a, c$

So, not a distributive lattice.

→ It is the easiest way to find distributive lattices.

Complemented Lattice

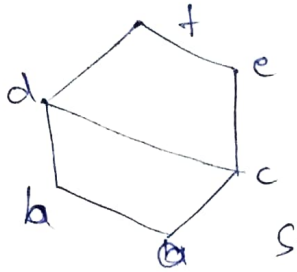
If lattice is said to be complemented if each element have atleast 1 complements



$a^c = d$

$b^c = c$

Lattice is both distributed and complemented if each element must have only one complement



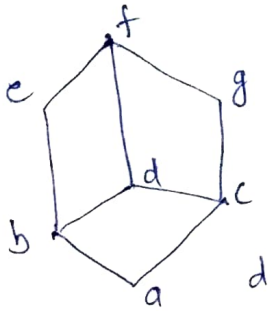
$a^c = f$

$b^c = e$

d^c = no complement

So it is not a complemented lattice.

→ If you have direct path then no need to go for other paths



$a^c = f, f^c = a$

$b^c = g, c^c = e$

$e^c = g, c, g^c = e, b$

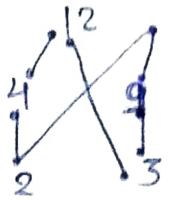
d → no complement

→ Not a complemented lattice.

Boolean Algebra: A lattice 'L' is said to be boolean algebra, if it is complemented & distributive.

→ Each element have exactly one complement

Ex [{2, 3, 4, 9, 12, 18}, /]



Hasse diagram

→ It is not a lattice, just a Poset.

② [R, ≤] $R \in (-\infty, \infty)$

→ Unbounded lattice

→ It is distributive bcoz we will get no complement due to absence of upper and lower bound.

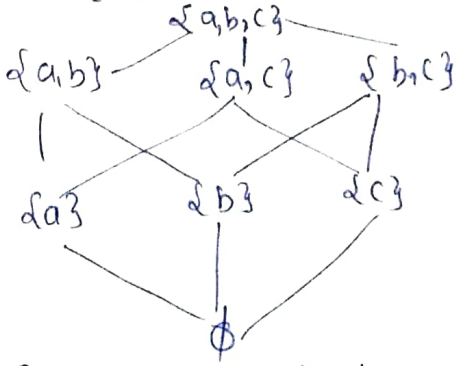
③ [D81, /]

D = {1, 3, 9, 27, 81}

→ Bounded lattice but distributive and not complemented Lattice.

④ {P(A), ⊆} A = {a, b, c}

P(A) = {ϕ {a}, {b} {c} {a, b} {b, c} {a, c} {a, c, b}}



Every, P(A) is boolean algebra w.r. to its sets

Groups

Algebric Structure

A non-empty set 'S' is called an algebric structure w.r.to binary operation 'op' if $(a \, op \, b) \in S \; \forall \; a, b \in S$ i.e op is closure operation.

Ex → ① $S = \{1, -1\}$

op → *

$(S, *) = \{(1 * -1) = -1 \in S\}$

or $(1 * 1)$ or $(-1 * 1) \in S$

So, $(S, *)$ is algebric structure.

② $S = \{\phi, \{a\}, \{b\}, \{a, b\}\}$

op → ∪

$(S, \cup)$ is also a algebric structure. You can perform union in between any two elements of S and you will get the o/p lies within S.

③ $A = \{1, 2, 3\}$

R → Reflexive relation}

$(R, \cup)$ and $(R, \cap)$ are algebric structures.

④ $(R, +)$ is closed under addition. So, set can be finite or infinite

→ ~~Algebric str also called as abelian str.~~

⑤ $S = \{1, 2, 3\}$

then, $(S, *)$ is not an algebric structure.

Semi-Group

: An algebric structure $(S, *)$ is called a semi group if $(a * b) * c = a * (b * c) \; \forall \; a, b, c \in S$ i.f '*' is associative on S.

Ex- ① $(N, +) \rightarrow a + (b + c) = (a + b) + c$

so, it is a semi group.

② $(N, *) \rightarrow a \times (b \times c) = (a \times b) \times c$

So, it is a semi group.

③ $(Z, -)$ → it is only algebric str. but not semi group.

④ $(Q^*, +)$ ⟼ it is not algebric str.

Q → set of rational no.

Q^* → $Q - \{0\}$

Ex → $(2 + (-2)) = 0$ but Q^* doesn't included 0.

⑤ $(Q^*, *)$ → it is also an semi-group.

⑥ $(P(A), \cup)$, $(P(A), \cap)$ both are semi-groups.

Monoid

: A semigroup $(S, *)$ is called a monoid if there exist an element $e \in S$ such that

$(a * e) = (e * a) = a, \; \forall \; a \in S$.

e → identity element of S w.r.to operation (*).

① $(N, *)$: $a * e = a$ [So, $e = 1$]

→ it is monoid for $e = 1$ bcoz $e \in N$.

② $(N, +)$: $a + e = a$ [So, $e = 0$]

but $0 \notin N$. So it is not a monoid.

③ $(Z, +)$: $a + e = a$ [So, $e = 0$]

→ it is monoid for $e = 0$.

Before finding 'e' verify that it should be semi-group.

④ $(P(A), \cup)$: $a \cup e = a$

so $\boxed{e = \phi, a}$ but we choose $e = \phi$. so it is monoid.

Groups: A monoid $(S, *)$ with identity element 'e' is called a group if to each element $a \in S$, there exist an element $b \in S$, such that $(a*b) = (b*a) = e$.

then 'b' is inverse of an element 'a', denoted by a^{-1}.

Note →

Algebric Str. → Closure propety

↓

Semi-group → Associativity

↓

Monoid → Identity element

↓

Group → Inverse element.

Ex-① $(Z, +)$: here $e = 0$

$a + b = b + a = e$

$a + b = b + a = 0$

$\Rightarrow \underline{b = -a \in Z}$. $\forall a \in Z$

So it is a group.

② $(Q, *)$: $e = 1$

$a * b = b * a = 1$

$\boxed{b = 1/a}$ but Q includes 0 and $\frac{1}{0} = \infty$ doesn't belong to Q. So it is not a group.

③ $(Q^*, *)$ → It is a group with $\boxed{b = 1/a \ \forall \ a \in Q}$

④ $(P(A), \cup)$: Not a group.

$a \cup b = b \cup a = \phi$.

We can't find any 'b' for this condition.

Abelian Group

→ In a group $(G, *)$, the following properties must holds good.

① Identity element and inverse element of 'G' is unique.

② Inverse of 'e' is 'e' itself.

③ Cancellation law can be applied.

$(a*b) = (a*c) \Rightarrow \underline{b = c}$ | $(a*c) = (b*c) \Rightarrow a = b$

④ $(a*b)^{-1} = b^{-1} * a^{-1} \ \forall a, b \in G$

A group $(G; *)$ is abelian if $(a*b) = (b*a) \ \forall \ a, b \in G$. It is also called commutative group.

Ex → $(Z, +)$, $(R^*, *)$, $(M, *)$

M → Set of Non-singular matrices of $(n \times n)$ size.

Algebric structure and also $(AB)C = A(BC)$ and also $e = I$ (Identity matrix)

It also have inverse bcoz Non-singular so it is a group.

but $AB \neq BA$. So it is not abelian group.

① In a group $(G, *)$ with identity 'e', if $a*a=a$ then $a=e$.

$\Rightarrow a*a=a$

$\Rightarrow a*a=a*e$

$\Rightarrow \boxed{e=a}$ → True.

② In a group $(G, *)$ if $x^{-1}=x \ \forall x \in G$ then G is abelian group.

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

$(a*b) = b*a$] → True.

→ so it is abelian group

③ In group $(G, *)$ if $(a*b)^2 = a^2*b^2 \ \forall a, b \in G$ then G is abelian group.

$\Rightarrow (a*b)^2 = a^2*b^2$

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

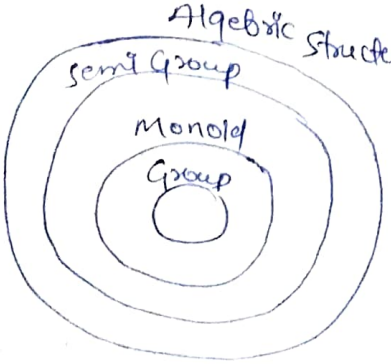
$a*(b*a)*b = a*(a*b)*b$

$\Rightarrow a*b = b*a$

So it is abelian.

→ '*' is not multiplication, it can be any operation.

Ex-4



Q Let $A=\{x \mid 0<x\leq 1 \text{ and } x \in R\}$ then 'A' w.r.to multiplication is —

a) a semigroup but not monoid
b) monoid but not a group
c) a group
d) Not a semi-group.

$x \in (0,1] = A$

A → algebric str. and semi group.

$e=1$ here so monoid.

$b=1/a \notin x$ so, inverse existence is not possible.

So, it is not a group.

b) monoid but not a group.

Q Let A is set of all integers and a binary operation '*' is defined by $(a*b)=\min(a,b)$, then $(A, *)$ is —

① Algebric structure ✓

② semi group: It also follows associativity so, semigroup

③ Monoid : $a*e=a$

We can't find a finite e, so that it work as identity. (e can be ∞)

→ $(A, *)$ is a semi group only.

Q Let S be the string set of all bits accepts the null strings $\in$? '+' denotes string concatenation. $(S, +)$ is.

$S=\{\in, 0, 1, 00, 11, 01, 001, \ldots\}$

Set is algebric structure for $(S, +)$

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

$abc = abc$

→ So it is semi group

→ Identity element $e = \in$ here. So its monoid.

→ $a + e = \in$, it is never possible.

So, $(S, +)$ is monoid only, not a group.

Note → ① for identity element

$$a * e = a$$

② for inverse element

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

$*$ → it can be any operation

Finite Group → Group with finite no. of elements.

$O(G)$ → Order of finite group means no. of elements present in group.

Ex. → $(\{0\}, +)$ → it is AS, semi-group, $e = 0$ (so its monoid).

$\Rightarrow a^{-1} = 0$ so its group.

→ It is only finite group over Real nos containing one element over '+' operator.

$(\{1\}, *)$ → it is also a finite group.

Only a finite group over '*' for real nos with one element.

$(\{1, -1\}, *)$

	1	−1
1	1	−1
−1	−1	1

All element in composition table lies in set, so it is algebric structure

$*$ → it is associative

$e = 1$ (Identity element)

→ It also have inverse as for 1 inverse is 1 and for −1 inverse is −1. So it is a finite group.

$(\{1, \omega, \omega^2\}, *)$; $\omega^3 = 1$

	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

So, it is alg. structure.

$*$ is associative, so it is semi-group.

$e = 1$ here as identity element

Inverse of $1 \to 1$,

$\omega \to \omega^2$, $\omega^2 \to \omega$. So for all element inverse exist so its a group.

→ Above is cube root of unity.

$(\{0, 1, 2, \ldots (m-1)\}, \oplus m)$

$\oplus m$ → Addition modulo m. It means first sum and the find % m.

If $(a+b) < m$ then $o/p = (a+b)$

$(a+b) > m$ then $o/p = (a+b)\%m$

$1 \oplus_4 2 = 3\% 4 = 3$

$3 \oplus_4 4 = 7\% 4 = 3$

In modulo 'm' o/p range is always $[0 \to (m-1)]$

→ Above set is a group bcoz it has both identity and inverse bcoz range is upto $(m-1)$. Hence it

if we also include 'm' then we will found 'no' Inverse for 'm'. So it will not a group with $S = \{0, 1, \cdots (m)\}$.

→ for multiplication modulo m $\otimes_m$, '1' is Identity element generally.

→ for $\oplus_m$, '0' is an Identity element generally.

Order → It defines on element of group (finite group).

Let $(G, *)$ be a group, and $a \in G$, then order of element 'a' is the smallest +ve Integer n such that a^n is identity element.

Ex → $(\{1, -1\}, *)$

Here, $e = 1$ (identity element)

So, $(1)^n = e \Rightarrow (1)^n = 1$

So, $n = 1$ [Smallest]

$(-1)^n = e = 1$

$\Rightarrow n = 2$ [Smallest]

$O(-1) = 2$, $O(1) = 1$.

Order of Identity element is always 1. $O(1) = 1$

$(\{1, \omega, \omega^2\}, *)$

Here $e = 1$

So, $O(1) = 1$

$O(\omega) = 3$

$O(\omega^2) = 3$

$\therefore (\omega^3) = 1 = \omega^6$.

O(Group) = no. of elements present in group.

Order of element always divide order of a group.

$(\{0, 1, 2\}, \oplus_3)$ $O(G) = 3$

$I = 0$

$0^1 = 0$ $O(0) = 1$

$1 \oplus_3 1 \oplus_3 1 = 3 \% 3 = 0$

$2 \oplus_3 2 \oplus_3 2 = 6 \% 3 = 0$

$O(1) = O(2) = 3$.

→ Order of element a and a^{-1} is going to be same.

$O(\omega) = O(\omega^2) = 3$ bcoz both are Inverse of each other.

Subgroups

Let $(G, *)$ be a group. A subset 'H' of 'G' is called a subgroup of 'G' if $(H, *)$ is a group.

① → A group is subgroup of itself.

② → Group with set containing only identity elements are also called subgroup.

→ In above ② statement subgroups defined are called as trivial subgroup.

→ All subgroup other than this called proper subgroup.

Ex → $G = (\{1, -1, i, -i\}, *)$

Then, $H = (\{1, -1\}, *)$ is a proper subgroup.

$(\{1\}, *)$ → Trivial Subgroup and G

Theorems ($*$ → Any operation)

① Let 'H' be a non-empty subset of a group $(G, *)$. 'H' is a subgroup of 'G' iff $a * b^{-1} \in H$ $\forall$ $a, b \in H$.

→ H means if you choose any pair of (a, b) from H, 'H' should satisfy the property $a * b^{-1} \in H$.

② Let 'H' be a non-empty finite subset of a group $(G, *)$. 'H' is a subgroup of 'G' iff $(a * b) \in H$ $\forall$ $a, b \in H$

③ **Lagrange's Theorem**

If 'H' is a subgroup of finite group $(G, *)$, then $O(H)$ is the divisor of $O(G)$.

The converse of Algo. need not be true.

$O(G) = m$ $O(H) = n$ then m/n should exist.

→ Using this we can directly discard some sets.

Ex Say $O(G) = 10$, $O(H) = 3$

then H will not be subgroup but it can be subset.

→ But if divides then only we check for H is subgroup or not.

→ H is a kind of (-ve) test.

Ex → $G = (\{0, 1, 2, 3, 4, 5\}, (+)6)$

Which of the following is subgroup of G.

① $H_1 = \{1, 3\}$

$O(G) = 6$ $O(H_1) = 2$

$6/2 = 3$. So H_1 can be group.

Now apply theorem ②

	1	3
1	②	④
3	doesn't belong to H_1	

So, it doesn't follow closure property hence it is not a subgroup.

② $H_2 = \{1, 5\}$

$O(G)/O(H) = 3$

	1	5
1	②	0
5		

→ 2 is not present in H_2

③ $H_3 = \{0, 3\}$

$O(G)/O(H) = 3$

	0	3
0	0	3
3	3	0

So all the elements are present

So it is a subgroup

④ $H_4 = \{0, 2, 4\}$

$O(G)/O(H_4) = 2$

	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

→ It is a subgroup

(c) $H_5 = \{0, 2, 3, 5\}$

$O(G)/O(H_5) = 3/2 = 1.5$

So, it is not a subgroup.

→ Let $(G, *)$ be a group of order P where P is a prime no, then the no. of proper subgroups of G is 0.

$O(G) = P$. (Given)

$O(H)$ can be $= \{1, P\}$ bcoz prime no. is only divisible by 1 and itself.

→ $O(H) = 1$ and P both denotes trivial subgroup.

So, no. of proper subgroup is 0.

→ $(S_8, \oplus_8) = (\{0, 1, 2, 3 \cdots 7\}, \oplus_8)$

Which of the following are not true?

① The union of two subgroups of 'G' is also a subgroup of 'G'. → false

Ex → $(S_8, \otimes_8)$

$= (\{1, 3, 5, 7\}, \otimes_8)$

So, $H_1 = (\{1, 3\}, \otimes_8)$ $H_2 = (\{1, 5\}, \otimes_8)$

	1	3
1	1	3
3	3	1

	1	5
1	1	5
5	5	1

Both are subgroup

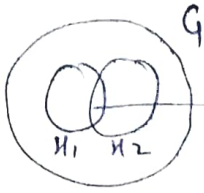
$H_1 \cup H_2 = \{1, 3, 5\}$

But $3 * 5 = 15\%8 = 7$

but 7 doesn't $\in H_1 \cup H_2$

So, it is false statement.

② The intersection of two subgroups of 'G' is always a subgroup of G. → True.

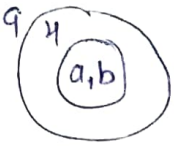


all elements in this area should satisfy Closure property

③ The union of two subgroup H_1 and H_2 is also a subgroup

↳ false.

④ Every subgroup of an abelian group is also an abelian group. → True



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

Cyclic Groups : A group $(G, *)$ is called as a cyclic group if there exists an element $a \in G$ such that element in 'G' can be written as a^n for some integer 'n'. Then 'a' is called generator or generating element.

Ex → $G = (\{1, -1\}, *)$

$(-1)^2 = 1 \quad (-1)^1 = -1$

$G = (\{1, \omega, \omega^2\}, *)$

$(\omega)^1 = \omega, \; (\omega)^2 = \omega^2$

$(\omega)^3 = 1$

ω^2, ω → generating elements

find out all the generator of Group.

Ex → $G = (\{1,2,3,4,5,6\}, \otimes_7)$

→ No. of elements that can be works as generator is 'n'. To compute n find $\phi(6) = S_6 = \{1,5\}$

S_6 → Elements less than 6 and relatively prime.

So, n=2 here (if it is cyclic)

Now find the generating element

On doing some calculate we will get that 3 is generator So, it is cyclic, Hence we can say that,

$3^1 \% 7$ and $3^5 \% 7$

↓ ↓

3 5

So, 3, 5 are two generators.

Theorems

Note:-

Two numbers are relatively prime if they nothing in common factor other than 1.

In $\{1,2,3,4,5,6\}$

factor of	factor	Relatively prime to $6 = \{1,5\}$
1	1	
2	1, 2	because 2 and 6 have 2 as common and
3	1, 3	3 and 6 have 3 as common
4	1, 2, 4	
5	1, 5	
6	1, 2, 3, 6	

Similarly relatively prime to $5 = \{1,2,3,4\}$

because 1, 2, 3, 4 have no common element other than 1.

Theorem 1:

Let $(G, *)$ be a cyclic group of order 'n' with generator 'a', then

(i) The number of generators is $G = \phi(n)$

$\phi(n)$ → Euler's function of 'n'

(ii) a^m is also a generator G if $GCD(m,n) = 1$

$\phi(3)$ → no. of integers less than 3 which are relatively prime to 3

$\phi(3) = \{1,2\} = 2$

$\phi(7) = \{1,2,3,4,5,6\} = 6$

But it is valid for cyclic group only.

Ex → Let $(G, *)$ be a cyclic group of order 8 with generator 'a'.

(1) Number of generator in G is $\phi(8)$.

$\phi(8) = S_8 = \{1,3,5,7\}$

$= 4$

a^1, a^3, a^5, a^7 are generating

(2) which of the following is not a generator

① a^2 ② a^3 ③ a^5 ④ a^7

① If $n = pq$ then

$\phi(n) = \phi(p) \cdot \phi(q)$

$\forall$ p, q distinct values and prime

② $\phi(p) = p - 1$ $\forall$ $p \in$ Prime no's

③ Ex: $\phi(77) = \phi(7) \cdot \phi(11)$

$= 6 \cdot 10$

$= 60$

$\phi(35) = \phi(7) \cdot \phi(5)$

$= 6 \cdot 4$

$= 24$

Exception:

① for $\phi(25) = \phi(5^2)$

$= 5^2 - 5^1 = 20$

gmp

$\phi(p^n) = p^n - p^{n-1}$

$\forall$ $p \in$ Prime number

→ This formula is only applicable to repetitions.

② $\phi(84) = \phi(2^2 \times 3 \times 7)$

$= \phi(2^2)\,\phi(3)\,\phi(7)$

$= (4-2) \times 2 \times 6$

$= 24$.

→ If $(G, *)$ is a cyclic group with generator 'a' then

① a^{-1} is also a generator

② The order of generator $= O(G)$

Ex → $(\{0, 1, 2, 3\}, \oplus_4)$

$1^1 = 1$ $1^2 = 2$ $1^3 = 3$

$1^4 = 0$ → order

$3^1 = 3$ $3^2 = 2$ $3^3 = 1$

$3^4 = 0$ → order

for $e = 0$ (1, 3) are inverse of each other.

So, property 1 follows.

$O(2) = O(3) = O(G) = 4$. So it also satisfy point ② but only for cyclic groups.

Properties of Cyclic group

① Every cyclic group is abelian group.

② Every group of prime order is cyclic and so every group of prime order is abelian group.

③ Every subgroup of a cyclic group is also cyclic, but the generator of the subgroup need not be same as that of the cyclic group.

Ex: $G = \{1, -1, i, -i\}$, $H = \{1, -1\}$

So, H is a subgroup of G.

Generators of $G = i, -i$, generator of $H = -1$.

④ Let $(G, *)$ be a group of even order, then there exist at least one element $a \in G$ $(a \neq e)$ such that $a^{-1} = a$

→ for first statement

$a * b = g^n * g^m = g^{n+m} = g^{m+n}$

$= b * a$

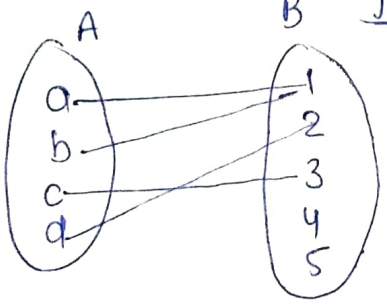
So every cyclic group is abelian.

g → any generator and in cyclic group we can write elements in power of generators.

Functions

A relation 'f' from a set 'A' to a set 'B' is called a function if to each element $a \in A$, we can assign an unique element of 'B'.

$f: A \to B$



$f = \{(a,1), (b,1), (c,3), (d,2)\}$

Domain = $\{a, b, c, d\} = A$

Co-domain = $\{1, 2, 3, 4, 5\} = B$

Range = $\{1, 2, 3\}$

→ 'Each element' in A must be related to B and each element in A should get only one image in B.

In $(a, 1) \to 1$ is image of a and 'a' is pre-image of 1.

→ In relation, 'B' can have more than one pre-image but 'A' can't have more than one image.

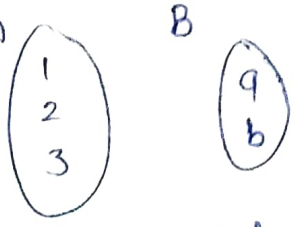
→ Range $\subseteq$ Co-Domain

Count the no's of function

$f: A \to B$

$|A| = m \quad |B| = n$

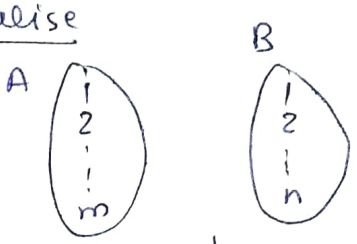
Ex-



Each element in A have 2 choices to choose in B.

= No. of fn possible = $2 \times 2 \times 2 = 8$.

Generalise



Each element have n choices.

No. of function = $n^m = |B|^{|A|}$

→ Every relation is not a function.

No. of Relations possible over A and B which are not functions = N(R)

= Total no. of relation − Total no. of functions.

Total no. of relation $N = 2^{mn}$

So, $N(R) = 2^{mn} - n^m$

for $f: A \to A \quad |A| = n$

then,

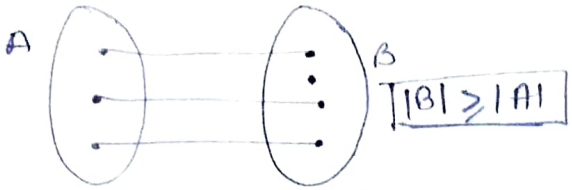
No of function = n^n

No. of relations = 2^{n^2}

$N(R) = 2^{n^2} - n^n$

One-one function

→ Also called injection.



Each element in A have distinct image in B.

→ If there are exactly one-one functions possible from A → B then which of following is not true

a) |A| = 5 & |B| = 5 → $5P_5$

b) |A| = 4 & |B| = 5 → $^5P_4$

c) |A| = 3 & |B| = 6 → $^6P_3$

d) |A| = 5 & |B| = 4 → ✗

No. of one-one fn = m·(m-1)·(m-2) ··· (m-n+1)

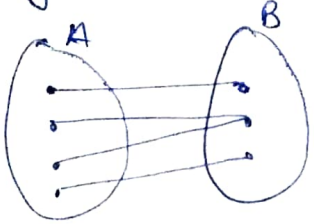
= ^mP_n

|A| = n , |B| = m

Onto functions (Surjective)

A function f: A → B is said to be onto if each element of B is mapped to atleast one element in A.

Range = Co-Domain



|B| ≤ |A| → Necessary Condition, not sufficient condition.

→ function that shows both the properties injective and surjective called bijective.

Bijective → one-one & onto

→ If one-one function have |A| = |B| then it is onto.

→ If |A| = |B| = n then no. of onto functions = n! and no. of one-one function = n!

→ If |A| = m and |B| = n, (m > n) then the no. of onto functions possible from A → B is,

$n^m - {}^nC_1(n-1)^m + {}^nC_2(n-2)^m - \cdots (-1)^{n-1}\,{}^nC_{n-1}(1)^m$

Ex: |A| = 6 |B| = 3, no. of onto functions from A → B.

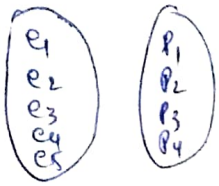
m = 6 , n = 3

$3^6 - {}^3C_1(2)^6 + {}^3C_2(1)^6 - {}^3C_3(0)^6$

= 540.

Ex → In how many ways we can assign 5 employees to 4 project so that every employee is assigned to only one project and every project is assigned to atleast one employee.

m = 5 n = 4



required ways =

$4^5 - {}^4C_1 3^5 + {}^4C_2 2^5 - {}^4C_3 1^5 + 0$

= 240