⊛ Sets : an introduction.

Many modern programming languages like Java and Python have implemented a data structure called Set. One of the simplest way to implement set in any programming language is using Hash Table.

Definition of set :

A set is an unordered collection of items/elements which are distinct.

Typically we represent set using capital letters, A, B, C, and using curly braces.

$A = \{\overset{a_1}{1}, \overset{a_2}{2}, \overset{a_3}{3}, \overset{a_4}{4}, \overset{a_5}{5}\}$

$\{2, 3, 4, 1, 5\}$ ← element

Both are the same as we don't care about the ordering of the elements.

$\{1, 1, 2, 3, 4, 5\}$ ← Multiset (where elements can repeat)

Another way to represent set is using Venn Diagrams:

Venn Diagrams are a visual / graphical way to represent sets.

Singleton Set: A set which consists of only one item / element.

$A = \{a\}$

Finite set: If a set contains finite number of elements.

$A = \{1, 2, \ldots, 10\}$ — 10 elements ↑ Finite number

Cardinality / Size of a set: Number of elements in a set. It is represented as $|A|$.

For a finite set, the cardinality will always be a finite number.

Infinite set:

$A = \{$ list of all natural numbers $\}$

$= \{1, 2, 3, 4, \ldots\}$

The size of this set is infinity. Therefore, it is an infinite set.

Equality of sets: Every element that is present in one set is also present in the other set and vice versa, then both the sets are equal. The ordering of the elements donot matter.

$A = \{1, 2, 3, 4\}$ $B = \{2, 4, 1, 3\}$

$\therefore A = B$.

Null / Empty set :

A null set is a set whose cardinality is zero. That is, there are no elements in the set.

We represent Null set by :

$\{\}$, ϕ

E.g.: $A = \{ x \mid x \text{ is a prime number between 8 \& 10} \}$

(Another way to represent sets; $\mid$ = such that)

$= \{\}$

$= \phi$

Subset :

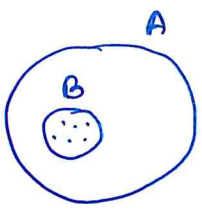
$A = \{1, 2, 3, 4, 5\}$

$B = \{1, 3, 5\}$

Every element present in B is also present in A but not necessarily vice-versa.

$B \subseteq A$: B is a subset of A.

($\subseteq$: subset)



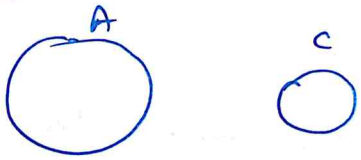
venn diagram

Note:

$A \subseteq A$
$\phi \subseteq A$

} Trivial (obvious) subsets of A are A and ϕ (phi).

E.g.

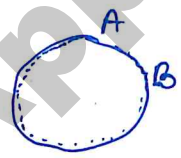


Here, $C \not\subseteq A$: C is not a subset of A.
(not a subset)

Proper subset: It is a subset that is not trivial.

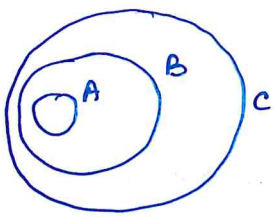
$B \subset A$: B is a proper subset of A.
(proper subset)

$A = B$ iff $A \subseteq B$ and $B \subseteq A$



If two sets are perfectly overlapping, then both the sets are the same. Therefore, we can also define equality of sets using the concept of subset.

If $A \subseteq B$ and $B \subseteq C$
then $A \subseteq C$



If $A = B$ and $B = C$

then $A = C$

Universal-Set: Set of all the elements that we care about in a given context.

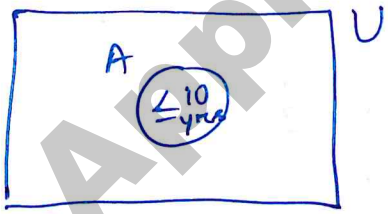
or,

set of all the elements which we care about in this discourse.

We use capital letter 'U' to represent a universal set. It's represented using rectangular box.

E.g. Suppose we are talking about — people living in India. Then the universe

U = set of people living in India.



A = set of all people ≤ 10 years of age in India.

The universal set changes with the context of the problem or the situation we are working in.

Power set: Given $A = \{1, 2, 3\}$; $|A| = 3$

Power set is the set of all subsets of A.

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

∴ We have :

(i) One subset of size zero — ϕ

(ii) Three subsets of size one — $\{1\}, \{2\}, \{3\}$

(iii) Three subsets of size two — $\{1,2\}, \{2,3\}, \{1,3\}$

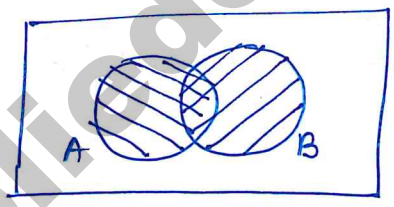
(iv) One subset of size three — $\{1,2,3\}$

∴ $P(A)$ is a set of all the subsets of A.

If $|A| = n$, then $|P(A)| = 2^n$.

⊛ Operations on sets :

① Union : $A \cup B$



$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

x is element of A or belongs to A

E.g. $A = \{1,2,3,4\}$

$1 \in A$

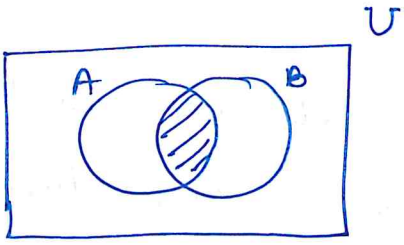
$2 \in A$

$5 \notin A$: 5 is not an element of A.

Note: $A \subseteq A \cup B$

$B \subseteq A \cup B$

② Intersection : $A \cap B$



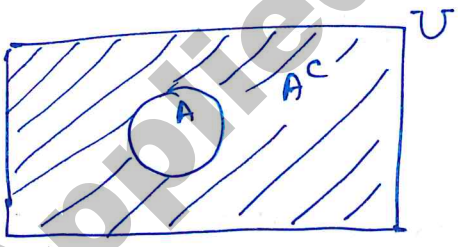
$A \cap B = \{x \mid x \in A \text{ AND } x \in B\}$

Note:

$(A \cap B) \subseteq A$

$(A \cap B) \subseteq B$

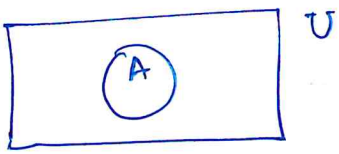
③ Complement: Given a set A, the complement of A is represented by $\bar{A}$ or A^c.



$\bar{A} = \{x \mid x \in U \text{ AND } x \notin A\}$

E.g.: U = population in India.

A = set of all males in India



$\bar{A}$ = set of all non-males in India

= set of all females or all the 3rd gender.

If $A \subseteq U$, then $\bar{A} \subseteq U$

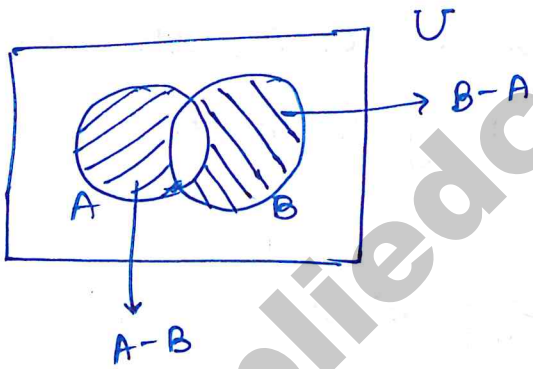
$A \cap \bar{A} = \phi$ [Here A and $\bar{A}$ are disjoint]

Disjoint sets : Two sets are called disjoint if they donot have any elements in common.

∴ A and $\bar{A}$ are also disjoint.

④ Relative complement / Difference between sets :

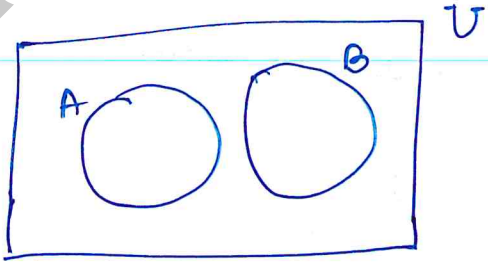
$A - B = \{x \mid x \in A \text{ AND } x \notin B\}$



$B - A = \{x \mid x \in B \text{ AND } x \notin A\}$

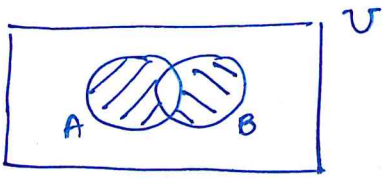
Properties :

1) If A and B are disjoint, then $A - B = A$ and $B - A = B$.

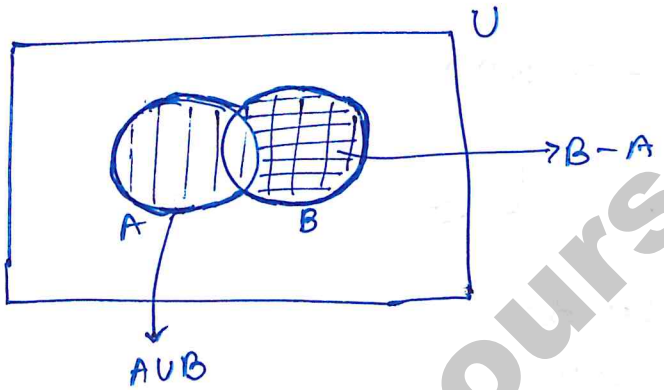


2.) If we have two sets, A and B, then (A−B) and (B−A) are disjoint.

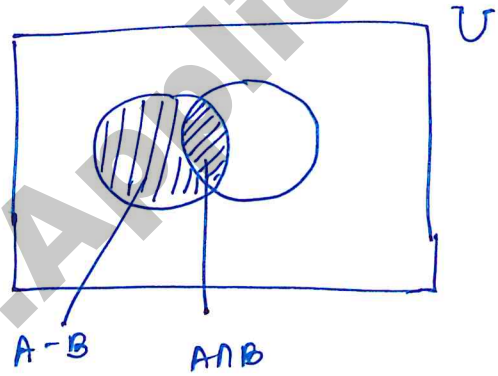
In other words, $(A-B) \cap (B-A) = \phi$.



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

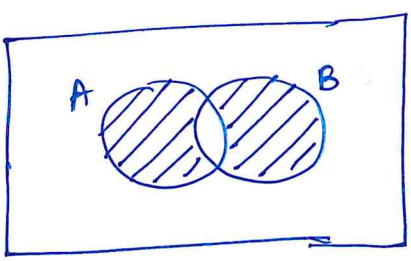


$A = (A \cap B) \cup (A - B)$



(5.) Symmetric Difference:

$$A \oplus B = (A \cup B) - (A \cap B) = \{x \mid x \in A \cup B \text{ AND } x \notin A \cap B\}$$



⊛ Properties of sets:

① Commutative laws:

$$A \cup B = B \cup A$$

$$\{x \mid x \in A \text{ or } x \in B\} = \{x \mid x \in B \text{ or } x \in A\}$$

Similarly,

$$A \cap B = B \cap A$$

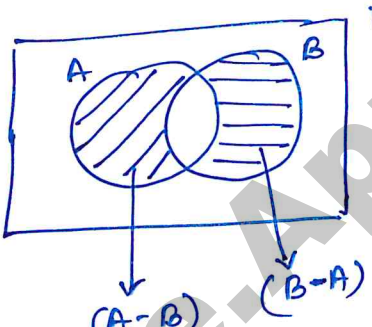
$$A \oplus B = B \oplus A$$

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

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

Note:

$$A - B \neq B - A$$



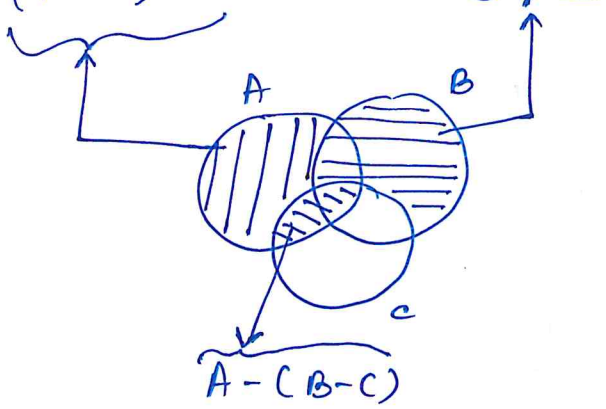
② Associative Laws:

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

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

$$(A \oplus B) \oplus C = A \oplus (B \oplus C)$$

$(A-B)-C \overset{?}{=} A-(B-C)$

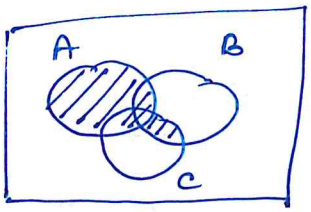


$\therefore \boxed{(A-B)-C \neq A-(B-C)}$

Note: $(A-B)-C = A-(B-C)$ iff $A \cap C = \phi$

Note: $\boxed{A-B = A \cap \bar{B}}$

(3) Distributive Laws:



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

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

(4) De-Morgan Law:

Note: $\bar{A} = A' = A^c$

(a) $\overline{(A \cup B)} = (A \cup B)'$

$= A' \cap B'$

$(A \cup B)'$

$\hookrightarrow x \notin A \cup B$

$\Rightarrow x \notin A$ AND $x \notin B$

$\Rightarrow x \in A'$ AND $x \notin B'$

$\Rightarrow x \in A' \cap B'$

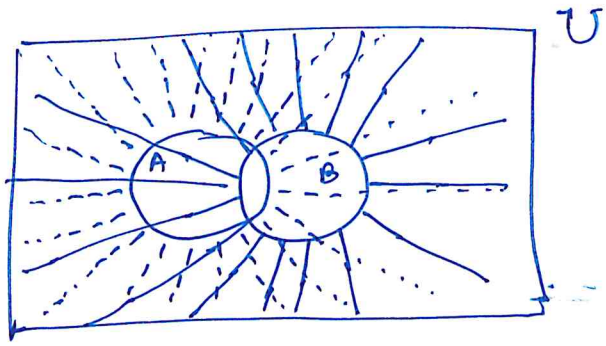
$x \in A \cup B$

$x \in A$ or $x \in B$

$x \notin A \cup B$

$x \notin A$ AND $x \notin B$.

Using Venn Diagram :



We can see that --- and —— line area/regions intersect in the region $(A \cup B)'$

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

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

LHS.

$x \notin A \cap B$

$\Rightarrow x \notin A$ or $x \notin B$

$\Rightarrow x \in A'$ or $x \in B'$

$\Rightarrow x \in (A' \cup B')$

(5) Idempotent Law :

$A \cup A = A$

$A \cap A = A$

(6) Identities :

$A \cup \phi = A$

$A \cap U = A$

$A \cup U = U$

$A \cup A' = U$

$A \cap A' = \phi$

$A \cup \phi = A$

⑦ Absorption Law:

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

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

⑧ Modular Law:

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

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

When will $(A \cap C) = C$?

$A \cap C = C$ when $A \subseteq C$

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

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

⑨ If we have 2 sets A and B,

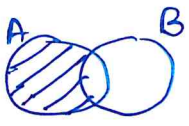
ⓐ $P(A \cap B) = P(A) \cap P(B)$

$x \in A$ and $x \in B$

ⓑ $P(A \cup B) = P(A) \cup P(B)$

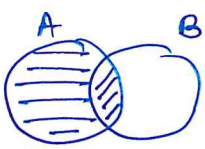
⑩ Formulae:

ⓐ $A - B = A \cap B'$



ⓑ $A - B = A - (A \cap B)$

ⓒ $A \cap B = A - (A - B)$



(d) $A \oplus A' = U$

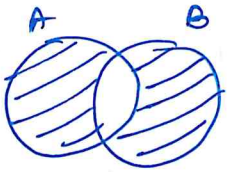
$\Rightarrow (A \cup A') - (A \cap A')$

$\Rightarrow U - \phi$

$\Rightarrow U$

(e) $A \oplus \phi = A$

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



(g) $((A \cap B) \cup C)' = (A' \cup B') \cap C'$

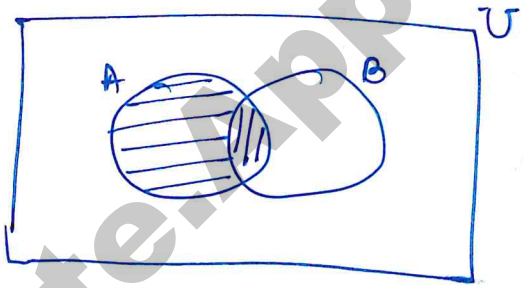
$= (A \cap B)' \cap C'$

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

} By applying Demorgan's Law.

$\equiv$ RHS.

(h) $(A - B)' = A' \cup (A \cap B)$



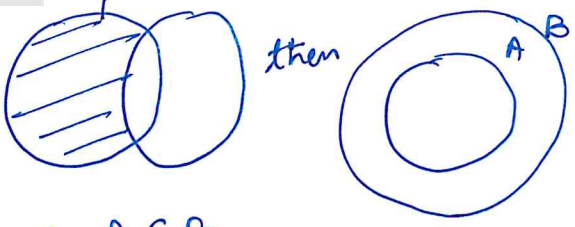
(i) $(A \oplus U) = \bar{A} = A'$

$\Rightarrow (A \cup U) - (A \cap U)$

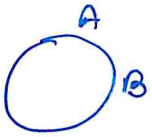
$\Rightarrow (U - A)$

(j) $(A - B) - C = (A - (B - C))$ iff $A \cap C = \phi$

(k) $A \subseteq B$ iff $A \cap \bar{B} = \phi$

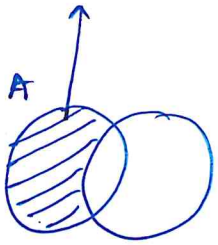


or

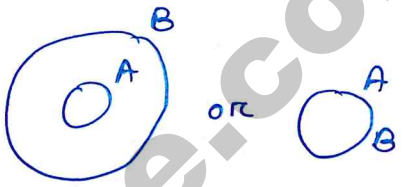


$\therefore A \subseteq B$

(l) $A \subseteq B$ iff $A - B = \phi$



then



$\therefore A \subseteq B$

(#) Cartesian Product and Multi-sets

Cartesian Product of sets:

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

$B = \{a, b\}$

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

Cartesian product returns us ordered pairs or 2-tuples.

$\therefore A \times B = \{(a,b) \mid a \in A, b \in B\}$

Note: We will also encounter the concept of Cartesian product in Databases and in Relations.

Let, $|A| = n$

$|B| = m$

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

∴ The set $(A \times B)$ will have $(n \times m)$ elements.

Note:

If $B = \phi$

then, $A \times B = \phi$

Similarly,

if $A = \phi$

then, $A \times B = \phi$

Reason is we can't form ordered pairs if one of A or B is ϕ.

Again,

$A \times B \neq B \times A$

∵ $(1, a) \neq (a, 1)$

order pairs of $(1, a)$ and $(a, 1)$ are not the same.

Note:

$\{a, 1\} = \{1, a\}$ as both are representing the same set.

Property:

if $A \times B = B \times A$

then $A = B$, $B = \phi$, $A = \phi$ } Atleast one of these three has to be true.

Multiset:

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

$A = \{a, a, b, b, b, c, c\}$ Not a set
It is a multiset.

$= \{2a, 3b, 2c\}$

Let, $A = \{3a, 2b, 1c\} = \{3a, 2b, 1c, 0d\}$

$B = \{2a, 3b, 4d\} = \{2a, 3b, 0c, 4d\}$

$A \cup B = \{3a, 3b, 1c, 4d\}$

$A \cup B$ is defined in such a way where:

$A \subseteq A \cup B$ and $B \subseteq A \cup B$

To define formally: $m_i \& n_i$ are multiplicities of a_i.

$A = \{m_1 a_1, m_2 a_2, \ldots m_k a_k\}$

$B = \{n_1 a_1, n_2 a_2, \ldots n_k a_k\}$

$A \cup B = \{\max(m_i, n_i) a_i\}$
for all $i : 1 \to k$

And, $A \cap B = \{2a, 2b\}$

$= \{\min(m_i, n_i) a_i \quad \forall i : i \to k\}$

$A - B = \{a, c\}$

In $(A - B)$, $a_i = \begin{cases} m_i - n_i \text{ times} & \text{if } m_i > n_i \\ 0, & \text{otherwise.} \end{cases}$

$A+B = \{5a, 5b, 4c, 4d\}$ $a_i = m_i + n_i$ times

⊛ Relations:

Relations are important because builds upon the concepts of sets and relations helps us understand what functions are.

Functions in mathematics are special types of relations.

The pratical implementation of relations can be seen in Databases where tables are relations.

Definition:

Given 2 sets A and B, a relation between A & B is any subset of the cross product of A×B.

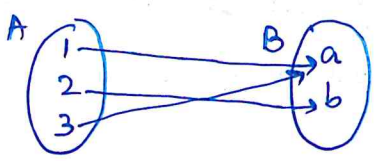
$A = \{1, 2, 3\}$

$B = \{a, b\}$

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

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

Another way to represent relation:



Diagrammatic way.

Another way to represent relation :

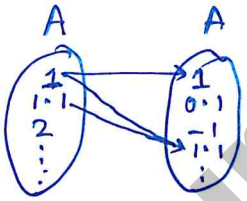
Matrix Method :

	a	b
1	1	0
2	0	1
3	1	0

E.g. A = set of all real numbers.

$R : A \rightarrow A$

$R \subseteq A \times A$



For, $2 \leq 3$
$2 \leq 2$
$2 \leq 4$

$\leq$ is a relation on a set of real numbers.

$\leq = \{(1,1), (-1,1), \ldots\} \subseteq A \times A$

$R_{\leq} = \{(x,y) \mid x \leq y ;\ x \in \mathbb{R},\ y \in \mathbb{R}\}$

$\downarrow$ on (A, A)

Mathematical / English based way to represent relation.

Similarly, $\geq, >, <, =, !=$ are all relations.

Let, $|A| = m$
$|B| = n$

(Q.) What is the total number of relations that are possible from A to B.

$R \subseteq A \times B$.

$|A \times B| = n \times m = k$

$A \times B = \{ \underbrace{- - - - -}_{k \text{ elements}} \}$

We can either chose an element out of k elements or not chose an element.

$\therefore$ Number of relations $= 2^{m*n} = 2^k$

#relations from set A to A $= 2^{(n^2)}$

Inverse Relation:

$R : A \to B$

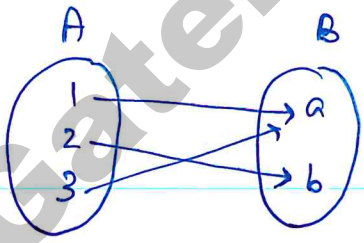
$R^{-1} = \{ (b, a) \mid (a, b) \in R \}$

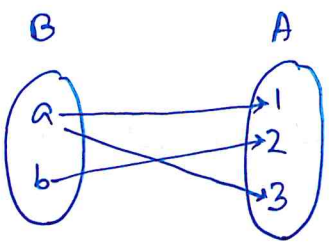
$\downarrow$

$B \to A$

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

$R^{-1} = \{(a, 1), (b, 2), (a, 3)\}$

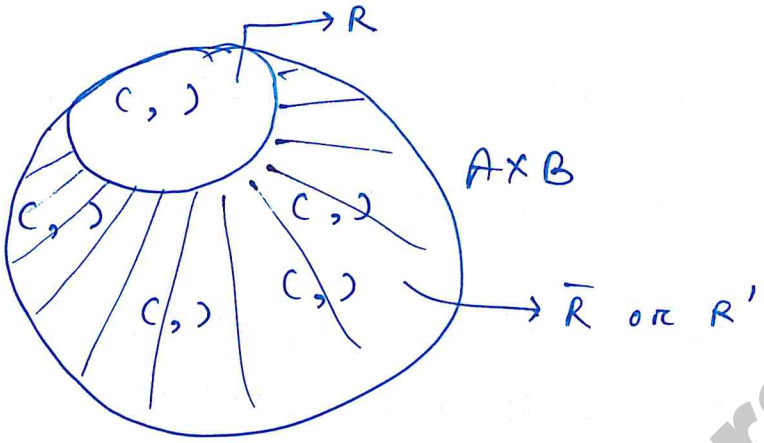




Complement of Relation R:

$R: A \rightarrow B$

$\bar{R}$ or $R' = (A \times B) - R$



Diagonal Relation (Δ_A): $A \rightarrow A$

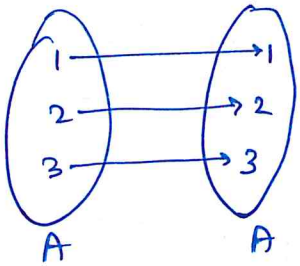
$$\Delta_A = \{ (x,x) \mid x \in A \}$$

E.g.: = relation.

A: real numbers

$x = x$

$x \neq y$



Matrix Representation:

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array} = I$$

= Identity matrix represents a diagonal relation.

* Reflexive and irreflexive relations :

A relation R is reflexive if $(x,x) \in R \quad \forall x \in A$

$R: A \to A \qquad A = \{a, b, c\}$

Let, $R = \{(a,a), (b,b), (c,c), (a,b)\}$

$\therefore$ R is reflexive.

$R_1 = \{(a,a), (a,b), (b,b), (c,b)\}$

$\because (c,c)$ is not present in R_1,

therefore R_1 is not reflexive.

E.g: $\leq$ on real numbers.

Is $\leq$ reflexive relation?

Yes it is reflexive.

Because any given number x,

$x \leq x \quad \forall x \in \mathbb{R}$

Similarly, $\geq$ is a reflexive relation.

Next, lets consider A : set of non-zero real numbers.

If we consider the division operator as a relation.

$\therefore$ x divides x $\quad \forall x \in A$

$\therefore$ Division on a set of non-zero real numbers is also a reflexive relation.

Properties :

① Any superset of reflexive relation is reflexive

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

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

$A \subseteq B$

If A is a subset of B, B is a superset of A

Let's have a reflexive relation $R \longrightarrow (x,x) \in R \quad \forall x \in A$

Say a new relation $R_1 \supseteq R$,

then all elements (x,x) present in R is also present in R_1, which makes R_1 also reflexive.

② If R is reflexive on set A, then R^{-1} is also reflexive on set A.

$\therefore (x,x) \in R \quad \forall x \in A$

$(x,x) \in R^{-1} \quad \forall x \in A$

which means R^{-1} is also reflexive trivially.

③ If R and S are reflexive on A, then $R \cup S$ and $R \cap S$ are also reflexive.

Since R and S, both have (x,x) pairs.

$\therefore$ Their intersection ($\cap$) will also contain the (x,x) pairs. And R Union S will anyway contain all (x,x) pairs.

④ Smallest reflexive relation on A = Diagonal relation
$= \Delta_A = \{(x,x) \mid x \in A\}$

If size of set is n,

$\therefore |A| = n$

then, $|\Delta_A| = n$

⑤ Largest reflexive relation on A = A × A

In A × A, all (x, x) pairs are present.

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

⑥ Let $|A| = n$;
what is the number of reflexive relations possible?

$A = \{a_1, a_2, a_3, \ldots, a_n\}$

To be reflexive, all the pairs (a_i, a_i) has to be present.

The total number of pairs is n^2

$\therefore (\_\_, \_\_) = n \times n = n^2$

Out of these n^2 pairs, n pairs (a_i, a_i) have to be present for the relation to be reflexive.

Now, out of n^2 pairs, we are left with (n^2-n) pairs. Out of these (n^2-n) pairs we can choose any subset of these pairs and place them as additional pairs.

∴ while creating the reflexive relations,

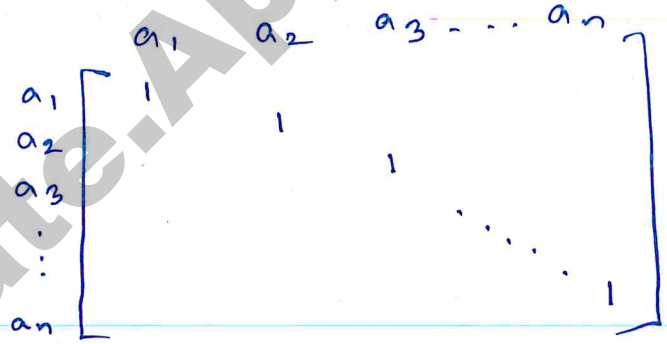
$$\{\underbrace{(a_i, a_i)}_{\text{This has to be present}}, \underbrace{(a_i, a_j)}_{(n^2-n)}\}$$

The # of subsets possible $= 2^{n^2-n}$

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

∴ # of reflexive relations possible $= 2^{n(n-1)}$

⑦ Matrix of reflexive relation on set A.



All the diagonal elements will be 1.
The non-diagonal elements maybe 1 or 0.

(8.) S = set of sets

In this case, relation subset '$\subseteq$' is a reflexive relation.

Let sets $s_1, s_2 \in$ set S.

$s_1 \subseteq s_1$

$\therefore (s_1, s_1)$ will be present.

Irreflexive relation:

$R: A \rightarrow A$ is irreflexive if $(a,a) \notin R \ \forall \ a \in A$

E.g.,

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

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

R is an irreflexive relation as (a,a) is not present.

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

R_1 is not an irreflexive relation as atleast one pair where we have the same element.

E.g. $<, >$ on real numbers

Is $x < x$? (NO) or $x > x$? (NO)

So, for all real numbers, the relations represented by $<$ and $>$ are irreflexive, because the relation will never contain a pair (x,x) for set of all real numbers.

Properties :

① If R is reflexive, then $\bar{R}$ is irreflexive

$\bar{R} = A \times A - R$

$R \longrightarrow (x,x) \in R \quad \forall x \in A$

$\bar{R}$: never have (x,x) as an element of $\bar{R}$ $\forall x \in A$

$\therefore \bar{R} : (x,x) \notin \bar{R} \quad \forall x \in A$

② Smallest irreflexive relation: ϕ

A null set (ϕ) of size zero is the smallest irreflexive relation because it doesnot contain any (x,x) pairs.

And, $|\phi| = 0$

Similarly, the largest irreflexive relation $= A \times A - \Delta_A$

And, $|A \times A - \Delta_A| = n^2 - n$

③ # irreflexive relations possible on A, such that $|A| = n$:

We can form n^2 pairs.

We are only allowed to have $(n^2 - n)$ pairs in the irreflexive relation.

Using (n^2-n) pairs, how many relations can we build?

we can have $2^{(n^2-n)} = 2^{n(n-1)}$ number of irreflexive relations on set A.

Note: Please understand that irreflexive doesnot mean non reflexive.

⊛ Symmetric, Antisymmetric, Asymmetric relations:

Symmetric relation:

For R on set A,

if xRy where $\forall x, y \in A$

then yRx

or,

if $(x,y) \in R$ where $\forall x, y \in A$

then $(y,x) \in R$

Note: $xRy \Leftrightarrow (x,y) \in R$

E.g. $A = \{1,2,3\}$

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

R_1 is a symmetric relation.

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

R_2 is not a symmetric relation as (2,1) is missing from R_2.

For A : set of real numbers, $x = x$

$\therefore$ '=' is a symmetric relation on a set of real numbers.

In Boolean Algebra, the complement operator is symmetric.

$\bar{1} = 0$

$\bar{0} = 1$

If complement operation is R, if $0 R 1$, then $1 R 0$.

Properties:

① If R is symmetric on set A, then R^{-1} symmetric

Symmetric basically means,

if aRb then bRa

$\equiv aRb \Rightarrow bRa$

And R^{-1} will have

$bR^{-1}a \Rightarrow aR^{-1}b$

$\because$ By definition of inverse relation,

$aRb \Rightarrow bR^{-1}a$

② If R & S are symmetric on A then R∪S & R∩S are also symmetric

R	R^{-1}
(x, y)	(y, x)
S	S^{-1}
(a, b)	(b, a)

R∪S will have all the symmetric pairs.

If x=a, y=b, then R∩S will have all the symmetric pairs as well.

③ Smallest possible symmetric relation on A

$= \phi$

Null set doesnot contain any pairs. And hence it is the smallest relation on A with zero elements.

Largest symmetric relation on A = A×A

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

A×A has both (a, b) & (b, a)

④ # of symmetric relations on A ; |A| = n

2 cases:

I.) $a \neq b$: (a, b) (b, a)

Here we have to choose 2 elements in ${}^nC_2$ ways $= \frac{n(n-1)}{2}$

$(\underline{a}, \underline{b})$ ⟶

II.) $a = b$: (a,a) ⟶ n ways (pick 1 element)

Total number of ways $= {}^nC_2 + n$

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

∴ How many symmetric relations are possible?

$2^{n(n+1)/2}$ ⟵ How many subsets can we form such that the subsets are themselves symmetric relations?

Anti-symmetric Relation :

Definition: If $(a,b) \in R$ and $(b,a) \in R$, then $a = b$.

or, if aRb and bRa then a should be equal to b.

E.g., $A = \{1, 2, 3\}$ $R = \{(1,1), (1,2), (1,3), (2,3)\}$

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

R_1 is not anti-symmetric because $(1,2)$ and $(2,1)$ exists but $1 \neq 2$.

E.g. $\leq$ on real numbers

$(a \leq b), (b \leq a) \Rightarrow (a = b)$

$\{(2,2), (2,3), (3,2)\}$ $\because 3 \neq 2$

(2,2) ✓ (2,3) ✓ (3,2) ✗

Similarly, $\geq$ on real numbers is also an anti-symmetric relation.

Properties:

① Smallest anti-symmetric relation: ϕ

$|\phi| = 0$

Largest anti-symmetric relation: ${}^nC_2 + n = n(n+1)/2$

There are two cases: (Given $|A| = n$)

(i) $a \neq b$ (a,b) or (b,a) $\longrightarrow {}^nC_2$ ways

(ii) $a = b$ (a,a) $\longrightarrow n$ ways

② If R & S are anti-symmetric then R∪S need not be antisymmetric

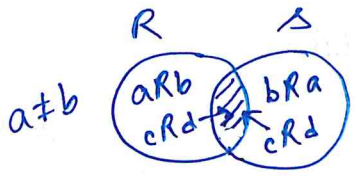
Let $(a,b) \in R$ and $(b,a) \notin R$ and $a \neq b$

Now, if $(b,a) \in S$, then R∪S will have

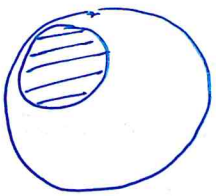
(a,b) and (b,a) and $a \neq b$

$\therefore$ R ∪ S need not be anti-symmetric.

Similarly, if R & S are antisymmetric, then $R \cap S$ is always antisymmetric.



(3) Every subset of an anti-symmetric relation is also antisymmetric.



$a \neq b \rightarrow aRb$ or bRa

$a = b \rightarrow aRa$

(4) Let R is an anti-symmetric relation,

then $R \cap R^{-1} \subseteq \Delta_A$

where $\Delta_A = \{(x,x) \mid x \in A\}$

For $R \cap R^{-1} \rightarrow a \neq b$: aRb or bRa

If $aRb \in R$, then $bRa \in R^{-1}$

and in $R \cap R^{-1}$, nothing will be present as $a \neq b$.

For $a=b$, if $aRa \in R$

then $aR^{-1}a \in R^{-1}$

or, $(a,a) \in R$ and $(a,a) \in R^{-1}$

$\therefore R \cap R^{-1} \subseteq \Delta_A$

(5) # possible anti-symmetric relations

(i) $a=b$; $aRa \longrightarrow$ n pairs possible, i.e., $n_{\wedge}$ such (a,a).
or
don't have it. $\therefore 2^n$ relations possible

(ii) $a \neq b$; $\longrightarrow$ we can have (a,b), (b,a) or none of the two in the relation.

$\therefore$ 3 possibilities.

For each of these possibilities, we have ${}^nC_2$ pairs.

$\therefore$ We have $3^{{}^nC_2}$ ways in which we can construct a relation.

$\therefore$ Total possible anti-symmetric relations

$= 2^n \cdot 3^{{}^nC_2}$

Asymmetric relation:

A relation R on set A is called asymmetric if $(x,y) \in R$, then $(y,x) \notin R \ \forall x,y \in A$.

E.g. $A = \{1,2,3\}$

$R_1 = \{(1,1), (1,2), (1,3)\}$ → anti-symmetric
→ Not asymmetric

Another definition:

A relation is called asymmetric if it is both antisymmetric and irreflexive.

E.g. $R_2 = \{(1,2), (1,3), (2,3)\}$ → asymmetric
→ antisymmetric

Note: Every asymmetric relation is antisymmetric relation but every antisymmetric relation need not be asymmetric.

E.g: $<, >$ on real numbers

$\therefore 2 < 3$ — ✓, $3 < 2$ — Not allowed
$2 < 2$ — Not allowed

$\therefore$ $<, >$ on real numbers are asymmetric relations.

Note: In set theory, there is a concept of strict subset ($\subset$).

$A \subset B$ iff $A \subseteq B$ & $A \neq B$

$\therefore$ If $A \subset B$ then $B \not\subset A$ and $A \not\subset A$.

$\therefore$ strict subset in set theory is an example of asymmetric relation.

Properties:

① Smallest asymmetric relation $= \phi$

ϕ is infact symmetric, asymmetric and antisymmetric.

And $|\phi| = 0$.

② Size of largest asymmetric relation $= {}^nC_2$
$= \frac{n(n-1)}{2}$

Let $|A| = n$.

If $a \neq b$,
we can have either (a, b) or (b, a)
but not both.

And $a = b$, doesnot arise for asymmetric relations.

③ # asymmetric relations on A, $|A| = n$.

For $a \neq b$, we can pick two elements in ${}^nC_2$ ways.

For every pair that we choose for $a \neq b$, we have 3 options: (a,b) or (b,a) or neither.

$\therefore$ Total number of asymmetric relations we can construct $= 3^{{}^{n}C_2}$

⊛ Transitive and Equivalence relations:

Transitive relation:

Definition: A relation on set A is said to be transitive if xRy and yRz then xRz $\forall x,y,z \in A$

In short,

$xRy, yRz \Rightarrow xRz \quad \forall x,y,z \in A$.

E.g.: $\leq$ on $\mathbb{R}$ (Real numbers)

$a \leq b, b \leq c \Rightarrow a \leq c$

$\therefore \leq$ is a transitive relation.

Similarly, $\geq$ is also a transitive relation.

E.g.: divides on $\mathbb{R}$

$x|y, y|z \Rightarrow x|z$

$\frac{6}{2} = \text{integer} = 3$

$2|6$

$x|y \Rightarrow \frac{y}{x} = \text{integer}$

x divides y.

$y|z \Rightarrow \frac{z}{y} = \text{integer}$

$\therefore \frac{z}{y} \cdot \frac{y}{x} = \frac{z}{x} = \text{integer}$

Since $\frac{z}{x} = \text{integer}$, it means x divides z.

∴ Divides on the set of real numbers is transitive relation.

E.g. 'is a subset of' relation on a set of sets (S).

Let, $A \subseteq B$, $B \subseteq C \Rightarrow A \subseteq C$

∴ $\subseteq$ is a transitive relation.

E.g. If $R = \phi$, then the empty relation R is transitive. Simply put ϕ is a transitive relation.

E.g. $R = \{(1, 2)\}$

If there is only a single pair, then trivially R is a transitive relation.

E.g. 'is mother of' — M

$a M b$, $b M c \not\Rightarrow a M c$

This relation is not transitive as a is a grandmother of c.

Properties :

① Smallest transitive relation :

The smallest transitive relation is a ϕ which contains 0 elements.

The largest transitive relation is $A \times A$

$|A \times A| = n \times n = n^2$ elements.

② # of transitive relations

If we have a set with $n=0$,

number of transitive relations = 1

$\therefore \phi$ is the transitive relation.

For $n=1$, let $A=\{1\}$,

number of transitive relations = 2

$\therefore \phi, \{(1,1)\}$

For $n=2$, we have 13 transitive relations.

For $n=3$, we have 171 transitive relations.

Note! we don't have a closed form formulae to count the number of transitive relations.

③ If R is transitive on a set A, then R^{-1} is transitive.

If $aRb, bRc \Rightarrow aRc$. $\forall a,b,c \in A$

$\therefore \underbrace{bR^{-1}a, cR^{-1}b \Rightarrow cR^{-1}a}_{cR^{-1}b, bR^{-1}a \Rightarrow cR^{-1}a}$ ✓

Now, if R is transitive on A, then $\bar{R}$ need not be transitive.

Let consider the relation = on $\mathbb{R}$.

We know that = is transitive

$\because$ $a = b$, $b = c \Rightarrow a = c$.

Now, complement of = is $\neq$.

$\neq$ on $\mathbb{R}$

$a \neq b$, $b \neq c \Rightarrow a \neq c$ ✗
$a \neq b$, $b \neq a \Rightarrow a \neq a$ ✗
} Fails.

(4) If R & S are transitive on a set A, then $R \cap S$ is transitive and $R \cup S$ is not transitive.

(5) A transitive relation is asymmetric iff it is irreflexive.

Transitive } $aRb, bRc \Rightarrow aRc$ $\forall a, b, c \in A$

Asymmetric } $aRb \Rightarrow b \not R a$ $\forall a, b \in A$

Irreflexive } $a \not R a$ $\forall a \in A$

$\therefore$ Another way to understand the definition is :

A transitive relation, if it is also irreflexive, then it is asymmetric.

$\therefore$ $aRb, bRa \Rightarrow aRa$ ✗ Not allowed as relation is irreflexive.

$\therefore$ $aRb \Rightarrow bRa$, which is nothing but asymmetric relation definition.

Equivalence relation :

A relation R is said to be an equivalence relation if it is reflexive, symmetric and transitive.

E.g.: $=$ on $\mathbb{R}$

$a=a \quad \forall a \in \mathbb{R}$ —— Reflexive

$a=b \Rightarrow b=a, \quad \forall a, b \in \mathbb{R}$ —— Symmetric

$a=b, b=c \Rightarrow a=c, \forall a, b, c \in \mathbb{R}$ —— Transitive.

E.g.: $\geq$ on $\mathbb{R}$

$a \geq a \quad \forall a \in \mathbb{R}$ —— Reflexive

$a \geq a \Rightarrow b \geq a$ ✗ $\forall a, b \in \mathbb{R}$ —— Not Symmetric

$a \geq b, b \geq c \Rightarrow a \geq c \quad \forall a, b, c \in \mathbb{R}$ — Transitive

$\therefore$ It is not an equivalence relation.

E.g.: ϕ

Since ϕ is an empty set, the relation represented by ϕ is not reflexive.

We need not check for symmetric and transitive.

$\therefore$ ϕ is not an equivalence relation.

Properties:

(1) Smallest equivalence relation $= \Delta_A$

To be an equivalence relation, the relation has to be a reflexive relation.

The smallest reflexive relation is Δ_A.

$\Delta_A = \{(x,x) \mid x \in A\}$

$|\Delta_A| = n$ elements.

And $\Delta_A = \{(x,x) \mid x \in A\}$

↳ reflexive

↳ $xRx \Rightarrow xRx$ (symmetric)

↳ Trivially transitive.

(2) Largest equivalence relation $= A \times A$

Because it contains all the pairs, therefore its size is n^2.

③ $R = \{(x,y) \mid (x-y) \text{ is an integer } \forall x,y \in R\}$

Reflexive:

$xRx \Rightarrow x-x = 0 = \text{integer}$

$\therefore$ R is reflexive.

Transitive:

$xRy, yRz \Rightarrow xRz$

$\left.\begin{array}{l} \therefore x-y = i \text{ (integer)} \\ y-z = j \text{ (integer)} \end{array}\right\} \Rightarrow x-z = i+j = k \text{ (integer)}$

$\therefore xRz$

Symmetric:

$xRy \Rightarrow yRx$

$x-y = i \text{ (integer)}$

$\Rightarrow y-x = -i = j \Rightarrow yRx$

integer

④ $R = \{(x,y) \mid (x-y) \text{ is divisible by } 5\}$ $x,y \in R$

It means, $\left(\frac{x-y}{5}\right) = \text{integer}$.

Reflexivity: $xRx \Rightarrow \frac{(x-x)}{5} = \text{integer} = 0$

Symmetric: $xRy \Rightarrow yRx$

$\frac{x-y}{5} = i \Rightarrow \frac{y-x}{5} = -i = j \Rightarrow yRx$

Transitivity:

$xRy, yRz \Rightarrow xRz$

$\frac{x-y}{5} = i \; ; \quad \frac{y-z}{5} = j$

$\Rightarrow \frac{x}{5} - \frac{z}{5} = \frac{x-z}{5} = i+j = k$

$\therefore xRz$

If i and j are integers, then k is also an integer.

⊛ Partial order relation & Hasse diagrams:

Partial ordering relation:

Defn: A relation is called a partial ordering relation if it is reflexive, anti-symmetric and transitive.

Eg. $\leq$ on $\mathbb{R}$ → Not equivalence relation because it was not symmetric.

Let's check if it is a partial ordering relation.

Reflexive: $a \leq a \quad \forall a \in \mathbb{R}$

Anti-symmetric: $a \leq b, b \leq a \Rightarrow a = b \quad \forall a, b \in \mathbb{R}$

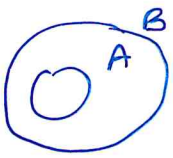
Transitive: $a \leq b, b \leq c \Rightarrow a \leq c \quad \forall a, b, c \in \mathbb{R}$

$\therefore \leq$ is a partial ordering relation.

E.g: $\subseteq$ on a set of sets — Not equivalence.

Because, symmetric doesnot hold.

$\because A \subseteq B \Rightarrow B \subseteq A$ ✗



Let's check if it is a partial ordering relation.

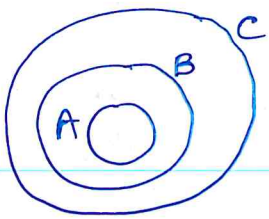
Reflexive: $A \subseteq A \quad \forall A \in S$ (S: set of sets)

Antisymmetric:

$A \subseteq B, B \subseteq A \Rightarrow A = B$

Transitive:

$A \subseteq B, B \subseteq C \Rightarrow A \subseteq C$

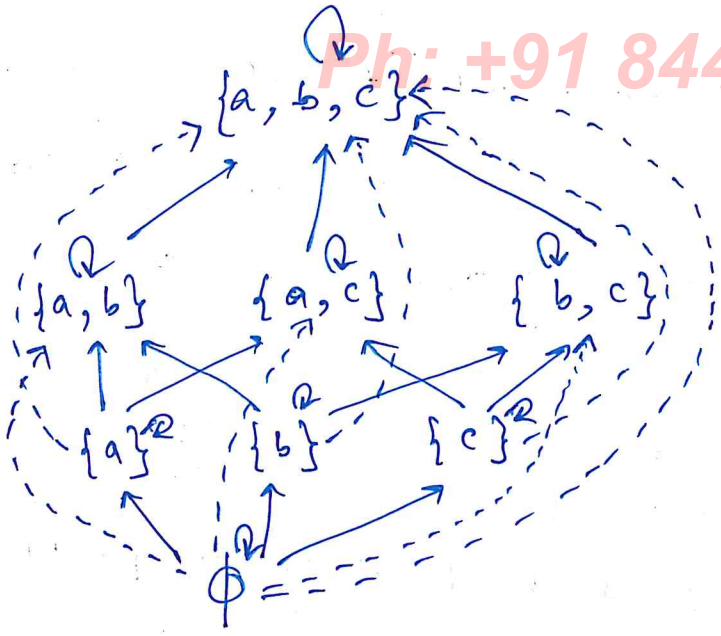


E.g:

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

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

Let, Relation : $\subseteq$

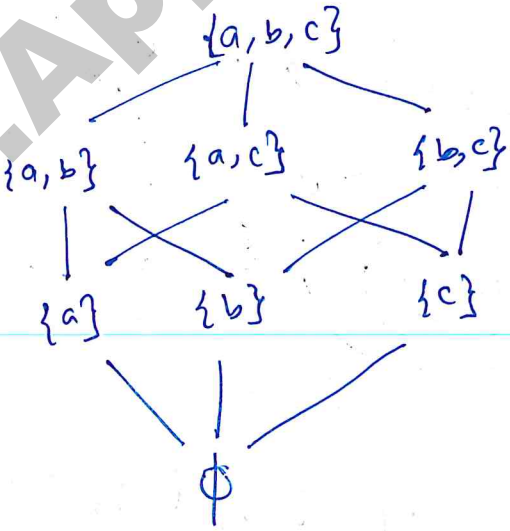


Diagrammatic way to represent Partial order Relation.

We use a strategy to simplify the diagram:

1. Omit all loops
2. Assume that all arrows point upwards
3. Skip all arrows that can be inferred using Transitivity.

Redrawing



Hasse diagram (A concise diagram)

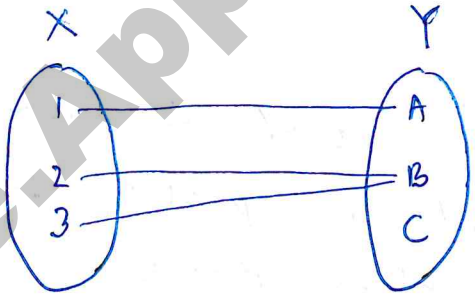
Functions : An introduction

Functions were formally studied in Real Analysis, in the framework of calculus in 17th and 18th centuries. In 19th century, set theory became a foundational topic.

Here we will learn the set theoretic formal definition of function.

Defn: A function is a relation (R) between X & Y such that: ① $\forall x \in X \quad \exists (x, y) \in R$

② if $(x, y) \in R$ and $(x, z) \in R$ where $x \in X$ & $y, z \in Y$ then, $y = z$.



Mapping diagram.

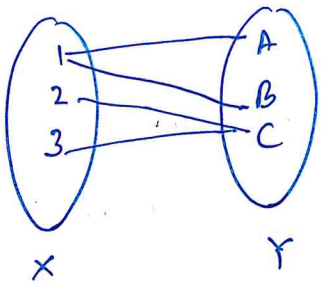
$(1, A) \in R$

Let's understand the definition:

① There is a mapping for every element in X to atleast one other element in Y.

② If $(1, A) \in R$ and $(1, B) \in R$, then $A = B$. But A and B are two distinct elements in Y. Then R is not a function.

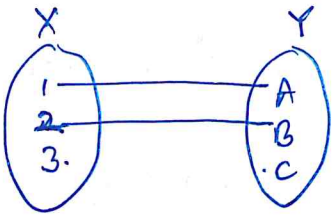
E.g.



(1, A), (1, B)

∴ Not a function.

E.g.



Not a function because 3 has to map to atleast an element of Y.

X : Domain

Y : Co-domain.

$Y' \subseteq Y$: Range or Image : The set of all elements in Y which are part of the relation is called Range.

$f : X \rightarrow Y$

f : name of function
X : Domain
Y : co-domain

Representation of a function: $f = \{(1,A), (2,B), (3,B)\}$ — set of ordered pairs

We can also write functions using algebraic or trigonometric expressions.

E.g.

$$f(x) = x^2$$

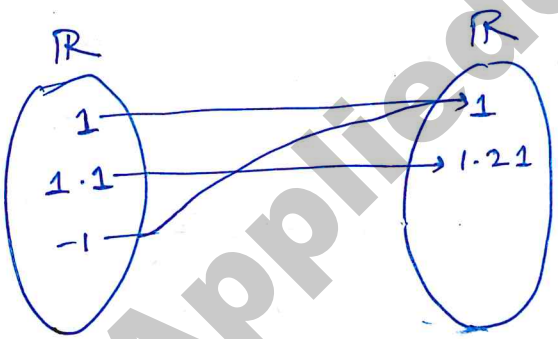
$y = f(x)$ ← output; ↑ input / argument

E.g. ① $f(x) = x^2$

$f : \mathbb{R} \to \mathbb{R}$

↑ Domain is set of all Real numbers

↑ codomain is set of all Real numbers



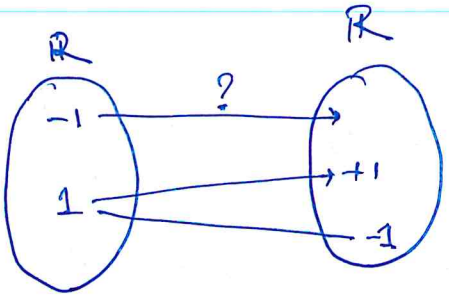
Conditions:

✓ 1. $\forall x \in X \ \exists (x, y) \in R$

✓ 2.

E.g. ② $f(x) = \sqrt{x}$

$f : \mathbb{R} \to \mathbb{R}$



$\sqrt{-1} = i \notin \mathbb{R}$

∴ Conditions:

1. ✗

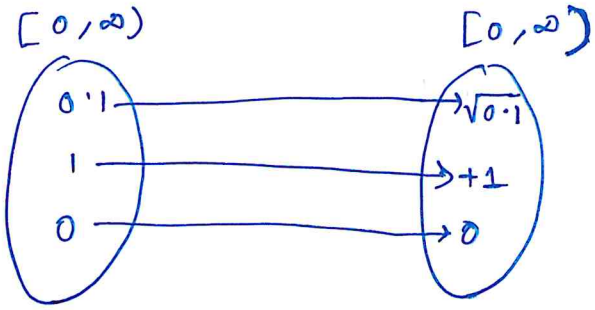
2. ✗

∴ Not a function.

Note: If we define the domain and range as:-

$f: [0, \infty) \rightarrow [0, \infty)$

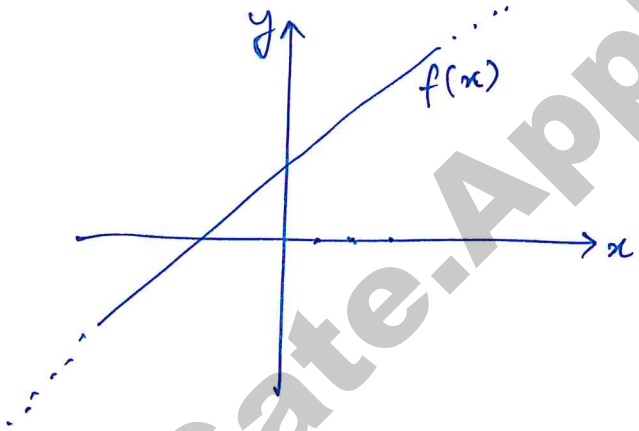
$[0, \infty)$: Non-negative numbers



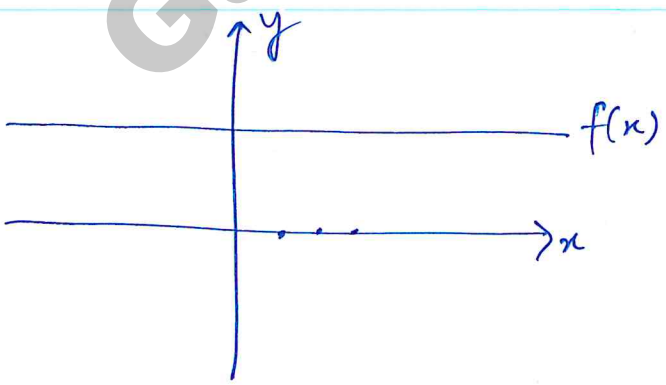
$\sqrt{0.1} > 0$

If domain and co-domain are defined in the above way, then $f(x) = \sqrt{x}$ is a function.

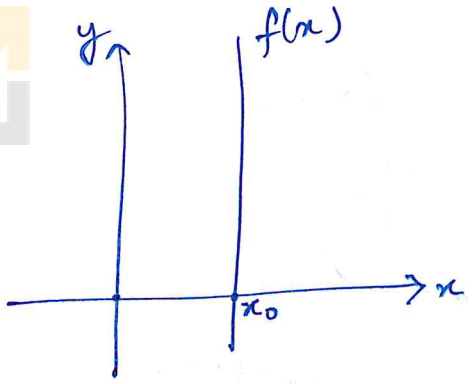
Functions can also be viewed in graph perspective:



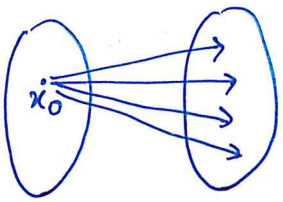
For every value on x, there is a unique value on y ∴ It is a function.



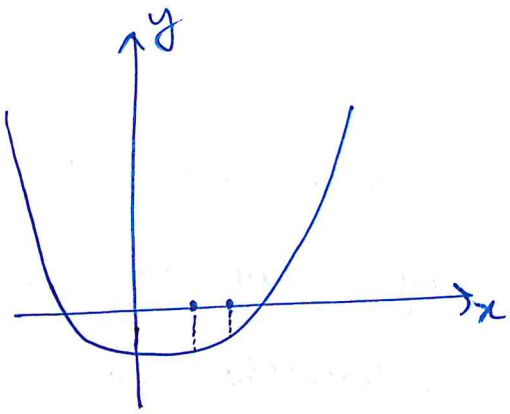
For the same reason mentioned above, this is also a function.



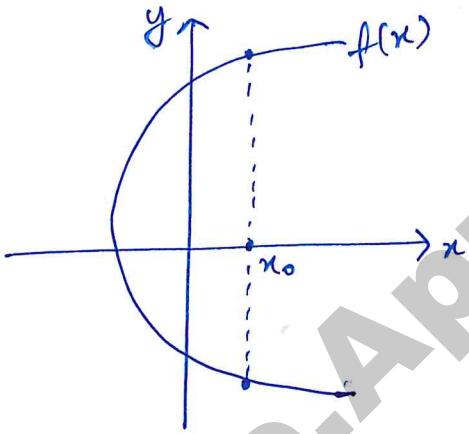
Here x_0 is mapping to infinite many values.

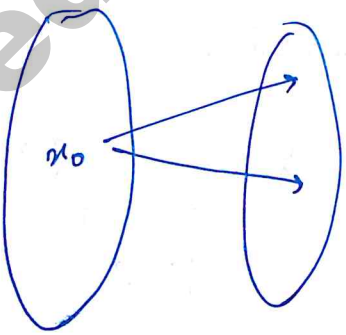


∴ Not a function.

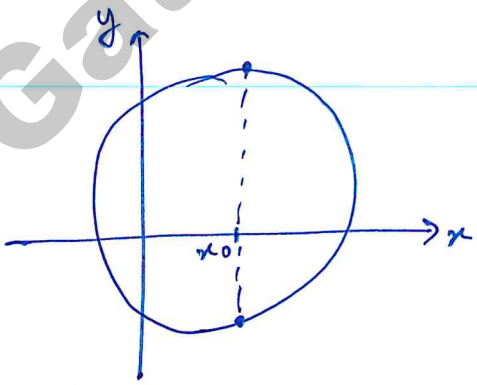


For every value in x, there is a unique value in y. ∴ It is a function.

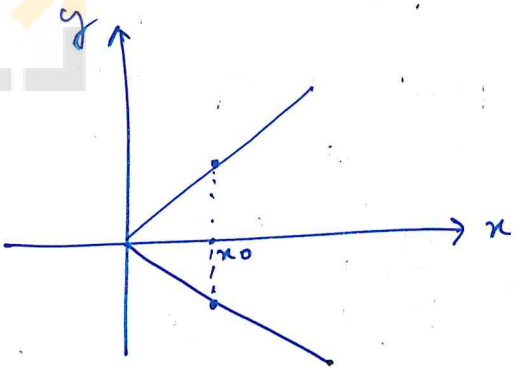


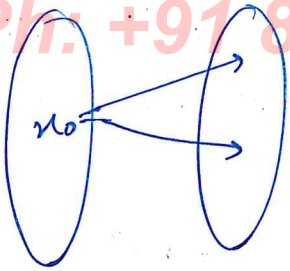


∴ Not a function.



∴ Not a function



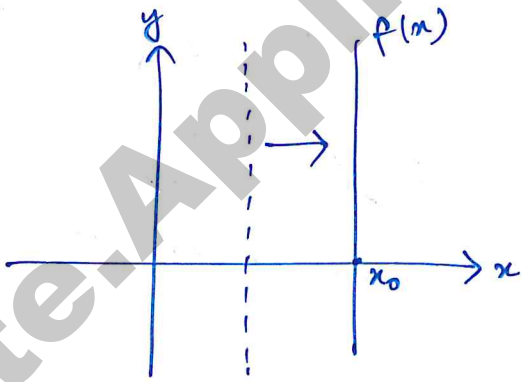


∴ not a function.

Shortcut trick :

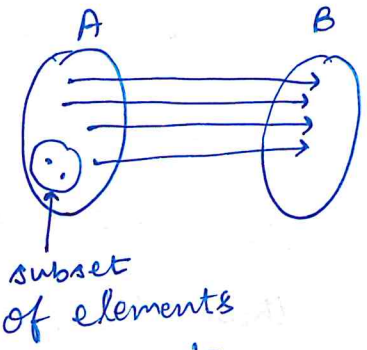
Consider an imaginary vertical line, move it along the x-axis. If for any value of x, the imaginary vertical line intersects the f(x) at more than 1 point, then f(x) is not a function.

E.g.



Types of functions:

① Partial function: If a subset of A has a mapping to elements in set B, then this relation is said to be a partial function.



Total function = function.

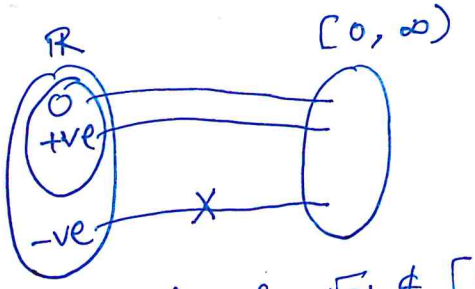
$= f: A \rightarrow B$

Note: Partial function is not a function

$f: A \dashrightarrow B$
$f: A \not\rightarrow B$
} Partial function notation.

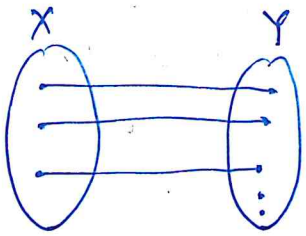
E.g. $f(x) = \sqrt{x}$

$f: \mathbb{R} \dashrightarrow [0, \infty)$

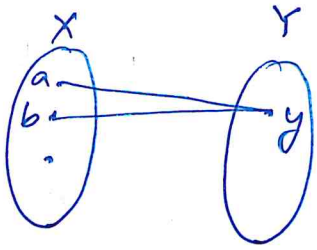


$\sqrt{-1} = i$ & $\sqrt{-1} \notin [0, \infty)$

② One-one (Injective)



one-one



many-one

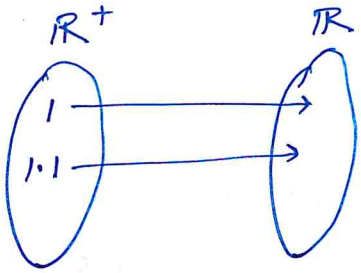
$f: X \to Y$ is one-one if $a \neq b$ and $\forall a, b \in X$ then $f(a) \neq f(b)$

For all a, b that belongs to set X, if $a \neq b$, then $f(a) \neq f(b)$, then it is said to be one-one.

e.g. $f(x) = x^2$

$f: \mathbb{R}^+ \to \mathbb{R}$

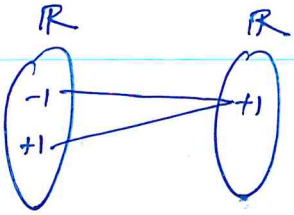
One-one



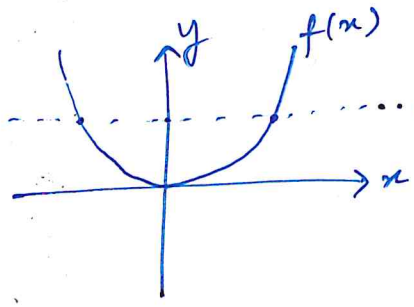
e.g. $f(x) = x^2$

$f: \mathbb{R} \to \mathbb{R}$

Many-one



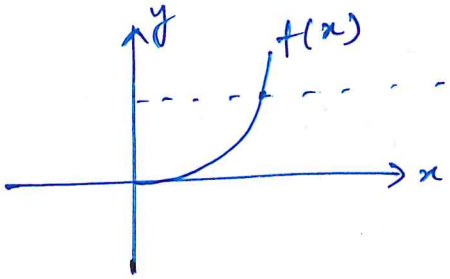
$f(x) = x^2$



$f: \mathbb{R} \to \mathbb{R}$

← Horizontal line to check at how many points does $f(x)$ intersect y. Many-one.

$f(x) = x^2$



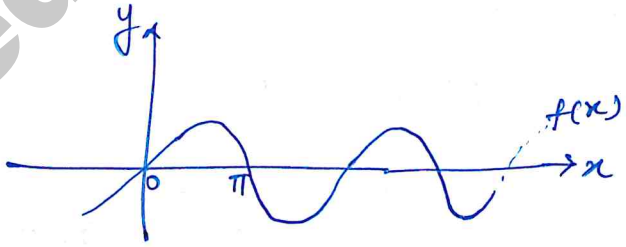
$f: \mathbb{R}^+ \to \mathbb{R}$

one-one.

e.g. $f(x) = \sin x$

$f: \mathbb{R} \to \mathbb{R}$

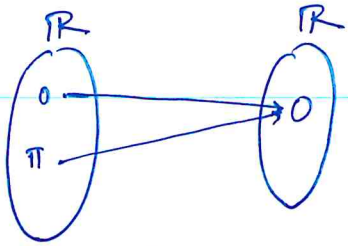
Many-one.



At 0, $f(x) = \sin x = 0$

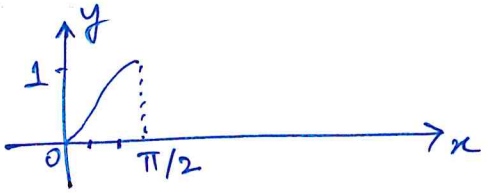
π, $f(x) = \sin x = 0$

∴



e.g. $f(x) = \sin x$

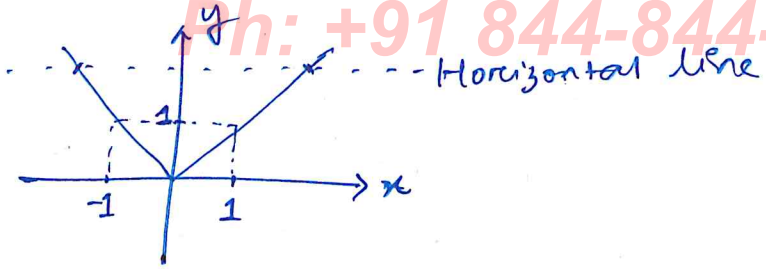
$f: [0, \pi/2] \to \mathbb{R}$



one-one

e.g. $f(x) = |x|$

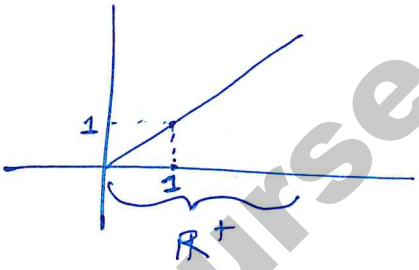
$f: \mathbb{R} \to \mathbb{R}$



Many-one

e.g. $f(x) = |x|$

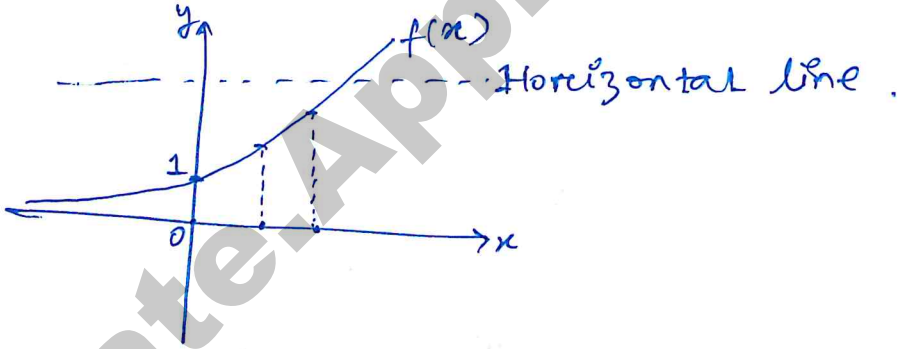
$f: \mathbb{R}^+ \longrightarrow \mathbb{R}$



One-one

e.g. $f(x) = e^x$

$f: \mathbb{R} \to \mathbb{R}$

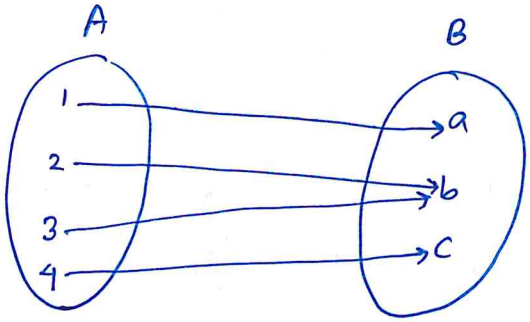


One-one function.

③ Onto & Into functions:

A function $f: A \to B$ is onto (surjective) iff

codomain (f) = B = range(f).



pre image of a = 1
" " b = {2,3}

codomain $(f) = \{a, b, c\}$

range $(f) = \{a, b\}$

For every value in B, there is a pre-image,

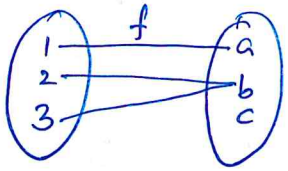
$\therefore$ f is ONTO.

or, $\forall b \in B$, $\exists (a,b) \in f$ s.t $a \in A$, then f is ONTO.

(s.t = such that)

INTO:

If Range$(f) \subset$ co-domain(f), then f is INTO.



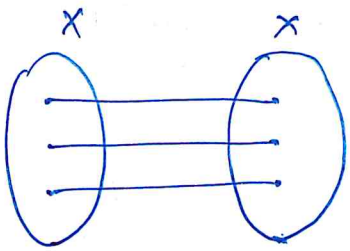
Here, range$(f) = \{a, b\}$

codomain$(f) = \{a, b, c\}$

$\therefore \{a,b\} \subset \{a,b,c\}$. $\therefore$ INTO function.

E.g.① $f: X \longrightarrow X$

$f(x) = x$ Identity function : Every value maps to itself.

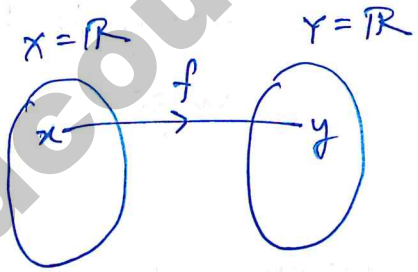


For every value of x, there is a preimage. It is trivially ONTO.

E.g.② $f: \mathbb{R} \longrightarrow \mathbb{R}$

$f(x) = 3x + 1 = y$

$\therefore x = \frac{y-1}{3}$

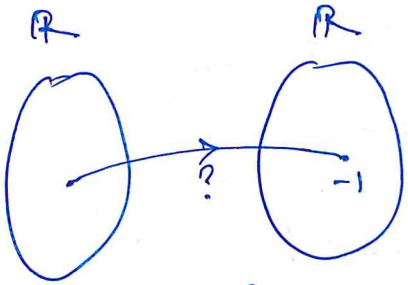


$\forall y \in \mathbb{R}, \exists (x, y) \in f$, where (such that) $x = \left(\frac{y-1}{3}\right) \in \mathbb{R}$.

This function is onto function.

E.g.③ $f(x) = x^2$

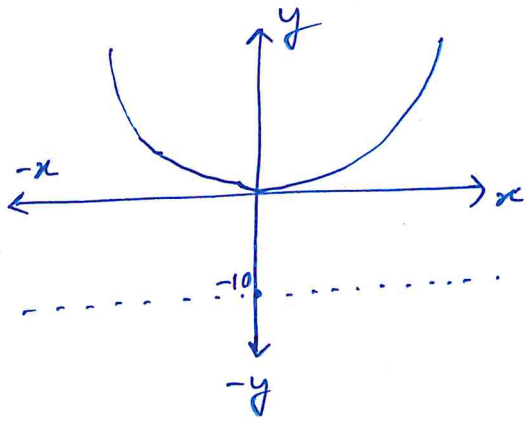
$f: \mathbb{R} \longrightarrow \mathbb{R}$



We can't find a pre-image for every real value

in the co-domain.

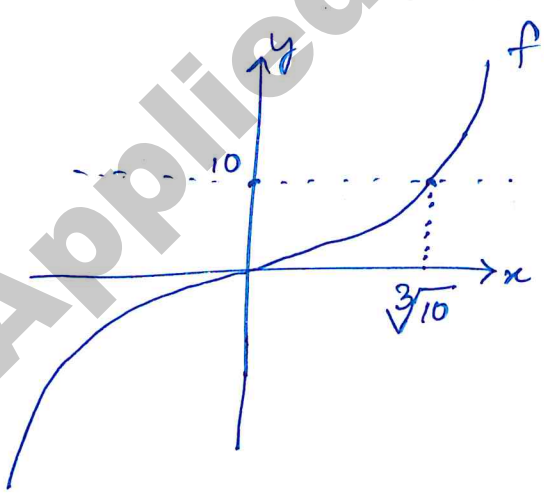
∴ This is an INTO function.



For $y = -10$, there is no corresponding x value as the point is not intersecting the points of the curve.

Eg ④ $f(x) = x^3$

$f: \mathbb{R} \to \mathbb{R}$

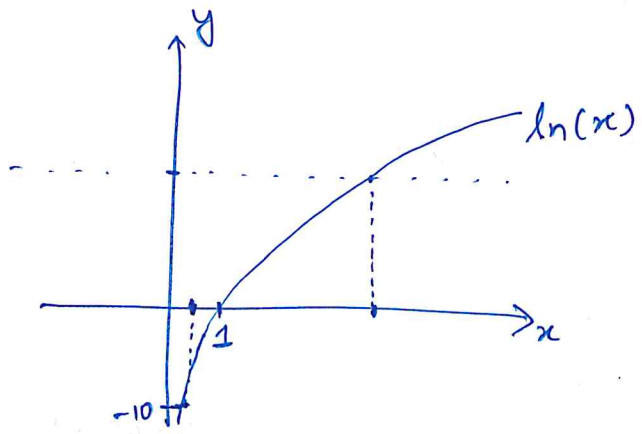


For every value of y, we can find the corresponding value of x, where $x = \sqrt[3]{y}$ for every y.

∴ It is an ONTO function.

E.g ⑤ $f(x) = \ln(x)$

$f: (0, +\infty) \to \mathbb{R}$

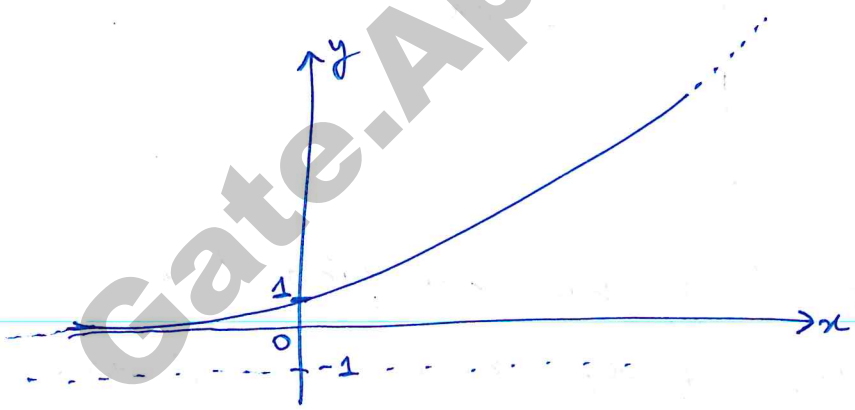


For every real value, we can find a preimage in the set $(0, +\infty)$.

0 is not included as because $\log_e 0$ is not defined. ∴ This is also ONTO function.

E.g ⑥ $f(x) = e^x$

$f: \mathbb{R} \to \mathbb{R}$



For $e^x = -1$, do such an x exist in the set of real numbers? — NO.

The horizontal line for $y = -1$ doesnot intersect the function $f(x)$ anywhere, which means there is no corresponding x such that

$e^x = -1$.

∴ This function is not ONTO, rather this function is INTO.

④ Bijection or Bijective function :

A function is said to be bijective if it is one-one and if it is ONTO.

E.g. $f : X \to X$

$f(x) = x$

It is one-one and ONTO.

∴ $f(x)$ is bijective.

E.g. $f : \mathbb{R} \to \mathbb{R}$

$f(x) = 3x + 1$

For every real value, $3x+1$ will give an exactly one value ∴ one-one.

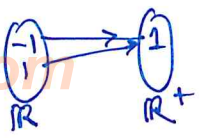
And it is ONTO as we have seen earlier.

∴ It is bijective

E.g. $f : \mathbb{R} \to \mathbb{R}^+$

$f(x) = x^2$

This function is NOT one-one, as it is many-one function.



∴ It is not bijective.

E.g. $f: \mathbb{R} \to \mathbb{R}$

$f(x) = e^x$

We have seen earlier that e^x is an INTO and not ONTO.

∴ It is not bijection.

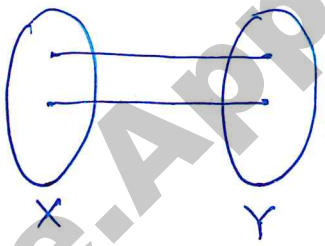
Note:

Interesting property:

$f: X \to Y$

if f is bijective

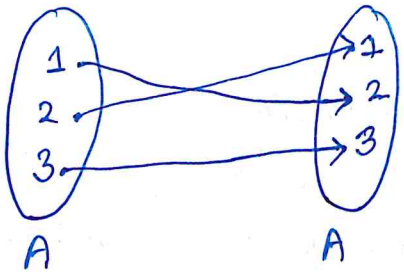
then $|X| = |Y|$



Note: A special type of bijection function is there, which is called permutation function.

A permutation function is a bijection from set A to itself.

$f: A \to A$



Bijection
- one-one
- onto

Let $f(x) = y$

x	y_1	y_2	y_3
1	2	1	3
2	1	2	1
3	3	3	2

permutation / re-ordering

⊛ Number of functions:

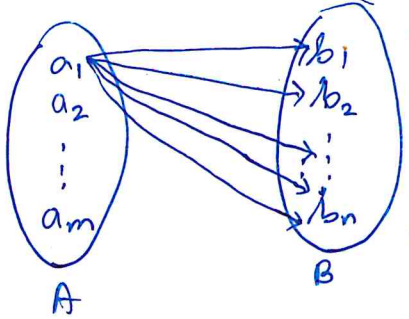
Here, we will try and count the number of functions that exists between two sets.

$f: A \longrightarrow B$

$|A| = m$

$|B| = n$

① # functions from set A to set B. $(A \longrightarrow B)$



for each a, we have n ways to connect any one of b. Because by definition of function, every element in A should map atmax. to one element in B.

$a_1 \longrightarrow n$

$a_2 \longrightarrow n$

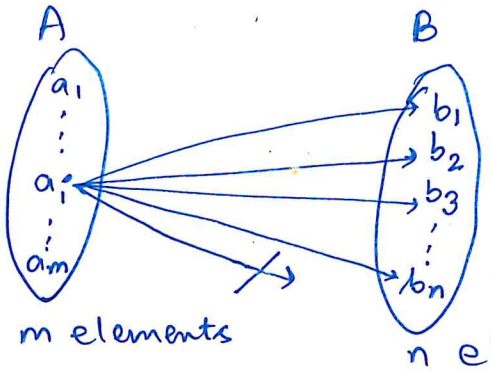
$\vdots$

$a_m \longrightarrow n$

$n^m = n \times n \times n \cdots m$ times

= total number of functions that exist between set A to set B.

② # partial functions $A \longrightarrow B$



In partial function, there can be elements in A that do not map to any element in B.

$\forall a_i \longrightarrow (n+1)$

not connecting is also an option

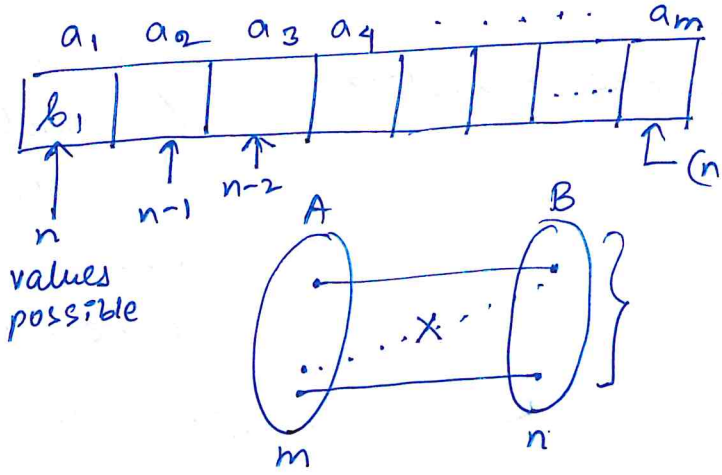
∴ Total number of partial functions

$= (n+1)^m$

③ # One-one functions:

We can think of functions like an array.

$f(a_1) = b_1$



∴ Total number of one-one functions

$= n(n-1)\cdot(n-2)\cdots(n-m+1)$

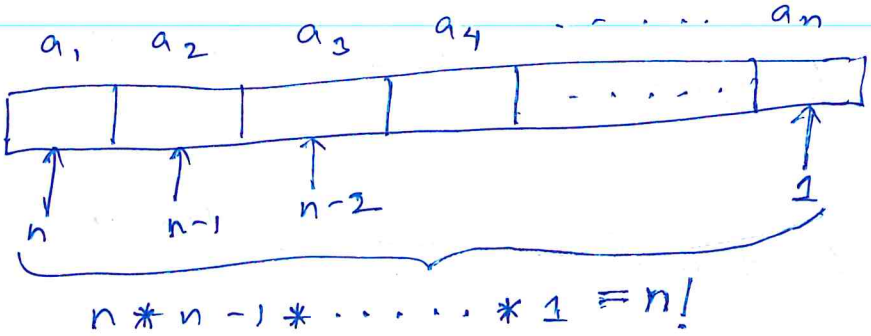
$= \frac{n!}{(n-m)!} = {}^{n}P_{m}$

④ # of Bijections: One-one & onto

Bijections

$f: X \to Y$, then $\boxed{n = m}$

(m, n)



permutation functions : $f: X \to X$ ($|X| = n$, $|X| = n$) } $n!$ bijections

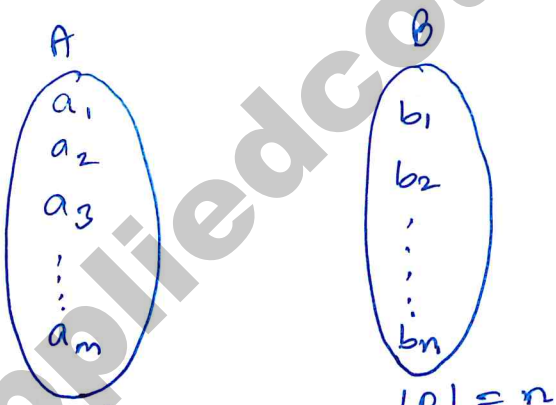
↓

bijection functions

Note: # Many-one functions = Total number of functions − number of one-one functions

$= n^m - {}^nP_m$

(5) # Into functions



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

functions where b_1 has no pre-image

$= (n-1)^m = |S_1|$

Set of functions where b_1 has no preimage

$= S_1$

Set of functions where b_2 has no pre-image

$= S_2$

And $|S_2| = (n-1)^m$

Note:

We calculate size of the set $|S_1|$ by imagining that b_1 doesnot exist in the set B.

$\therefore$ we get $(n-1)^m$ where number of elements in set B $= (n-1)$

.
.
.

Similarly, set of functions where b_n has no pre-image $= S_n$

& $|S_n| = (n-1)^m$

Therefore,

$S_1 \cup S_2 \cup S_3 \cup \ldots S_n$ = set of functions where atleast one element in B has no preimage

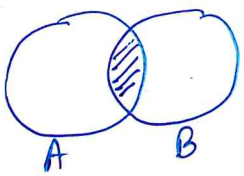
= set of INTO functions $A \to B$.

Now,

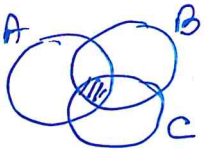
$|S_1 \cup S_2 \cup S_3 \cup \ldots S_n| = ?$

We look at the principle of Inclusion-Exclusion:

$|A \cup B| = |A| + |B| - |A \cap B|$



$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$.



We generalize :

$|S_1 \cup S_2 \cup S_3 \ldots \cup S_n|$ = $(|S_1| + |S_2| + \ldots + |S_n|)$ — one way

$- (|S_1 \cap S_2| + |S_1 \cap S_3| + \ldots$ all pairs) — two way intersections

$+ (|S_1 \cap S_2 \cap S_3| + |S_1 \cap S_2 \cap S_3| + \ldots$ all triplets) — 3 way intersections

$- (|S_1 \cap S_2 \cap S_3 \cap S_4| + \ldots$ all quadruplets) — 4 way intersections

Inclusion-Exclusion principle for n sets

$n(n-1)^m$

$- {}^nC_2 (n-2)^m$

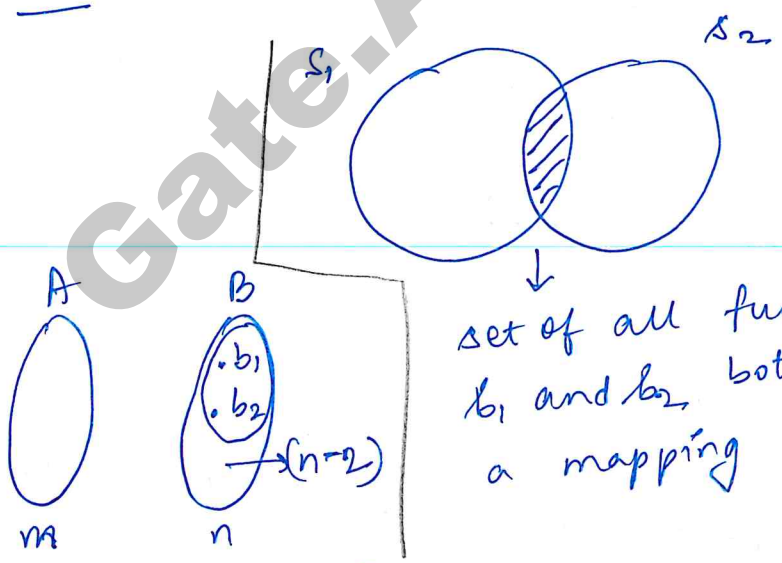
$+ {}^nC_3 (n-3)^m$

$- {}^nC_4 (n-4)^m$

$\vdots$

${}^nC_{n-1} 1^m$

Note:



set of all functions where b_1 and b_2 both don't have a mapping

functions possible $= (n-2)^m$

$\therefore$ # Into functions $= \sum_{i=1}^{n-1} {}^{n}C_i (-1)^{p+1} \cdot (n-i)^m$

$\therefore$ # onto functions $= n^m -$ # Into functions

(n^m = Total no. of functions)

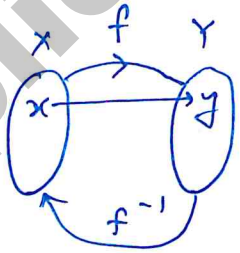
$= n^m - \sum_{i=1}^{n-1} {}^{n}C_i (-1)^{i+1} \cdot (n-i)^m$

(*) Inverse & Composition of functions :

Inverse of a function

$f : X \to Y$

$\hookrightarrow (x, y) \in f$



if $f(x) = y$ then $f^{-1}(y) = x$

$f^{-1} : Y \to X$

$= \{(y, x) \mid (x, y) \in f\}$

E.g. $f(x) = 2x + 3$

$f : \mathbb{R} \to \mathbb{R}$

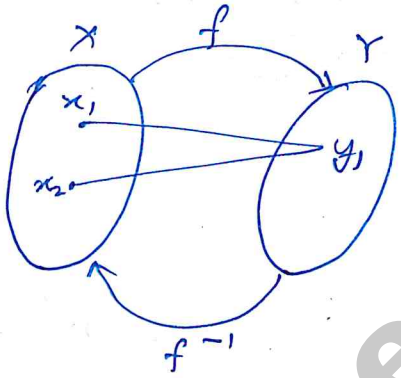
$2x + 3 = y$

$x = (y-3)/2$

$f^{-1}(x) = \frac{x-3}{2}$

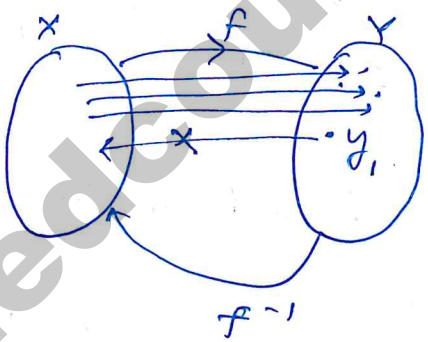
Theorem: f is invertible iff f is bijective (one-one & onto)

Let's say f is many-one then f^{-1} is not a function



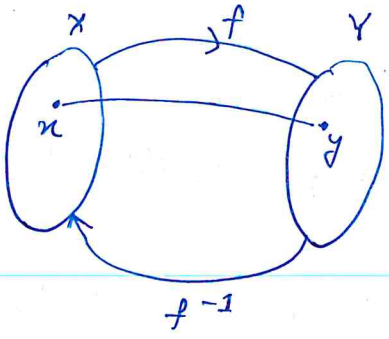
$f(x_1) = f(x_2) = y_1$

If f is not onto, then f^{-1} is not a function, rather it is a partial function.



Theorem: f is bijective iff f^{-1} is also bijective.

Theorem: $f^{-1}(f(x)) = x$



$f(x) = y$

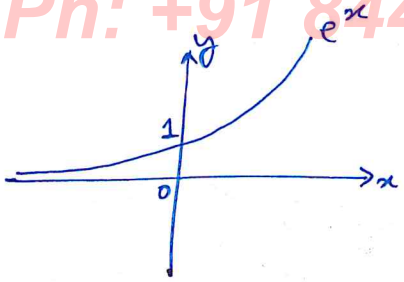
$f^{-1}(y) = x$

$f^{-1}(f(x)) = x$

Note: $f(f^{-1}(x)) = x$

E.g. $f(x) = e^x$

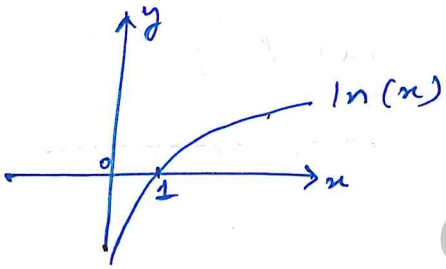
$f: \mathbb{R} \to (0, \infty)$



change x axis to y-axis and y-axis to x-axis we get inverse of a function.

$f^{-1}(x) = \ln(x)$

$f^{-1}: (0, \infty) \to \mathbb{R}$



Qn.) $f(x,y) = (x+y, x-y)$ ($x+y \to \mathbb{R}$, $x-y \to \mathbb{R}$)

$x \in \mathbb{R}$, $y \in \mathbb{R}$

ordered pair

$f: \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$

$f^{-1} = ?$

Let, $x+y = a$

$x-y = b$

$2x = a+b$

$x = (a+b)/2$

$y = (a-b)/2$

$\therefore f^{-1}(a,b) = \left(\frac{a+b}{2}, \frac{a-b}{2}\right)$

$\downarrow$

$f^{-1}(x,y) = \left(\frac{x+y}{2}, \frac{x-y}{2}\right)$

Composition of functions :

$f(x)$ & $g(x)$

$g(x) = y$, $f(y) = 3$ $\to$ $f(g(x)) = 3$

$= fog(x) = 3$

E.g.

$f(x) = 2x+3$

$g(x) = x^2$

$fog(x) = f(x^2) = 2x^2+3$

$gof(x) = g(2x+3) = (2x+3)^2$

$fog(x) \neq gof(x)$

$\therefore$ This composition is not commutative

Again,

$fo(goh)(x) = (fog)oh(x)$

$\therefore$ Associativity holds.

$fof^{-1}(x) = f(f^{-1}(x)) = x$

$f^{-1}of(x) = x$

} iff f^{-1} exists

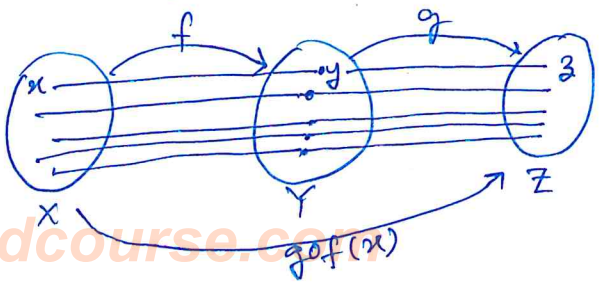
Identity function : $f(x) = x$

$fof^{-1} =$ Identity $= I(x)$

$f(I(x)) = f(x) = I(f(x))$

Properties :

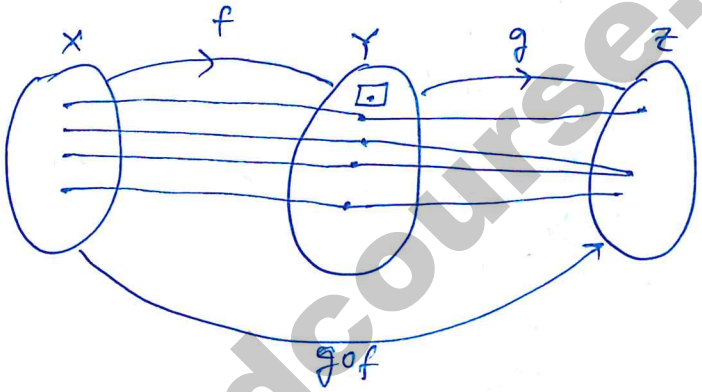
① if f and g are one-one then gof is also one-one



② if f & g are onto,
then $g \circ f$ is also onto

③ if f & g are bijective,
then $g \circ f$ is also bijective.

Qn) If $g \circ f$ is onto then f & g are also onto?
Is is True?



The co-domain of f is not the same as domain of g.

∴ $g \circ f$ is ONTO. g is also ONTO.

But f is not ONTO, because we have a value in the Y which doesnot have a preimage in X.

∴ The the given statement in the question is not always necessarily true.

⋆ Algebra of functions and special Functions:

Algebra of functions:

Given two functions $f(x)$ and $g(x)$, we can write,

① $(f+g)(x) = f(x) + g(x)$

Addition of two functions

② $(f-g)(x) = f(x) - g(x)$

Subtraction of two functions

③ $(f*g)(x) = f(x) * g(x)$

④ $(f/g)(x) = \frac{f(x)}{g(x)}$, if $g(x) \neq 0$

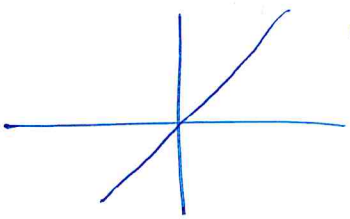
⑤ $K * f(x) = (k \cdot f)(x)$

K is constant or scalar

Special functions:

① Identity function : $I(x) = x$

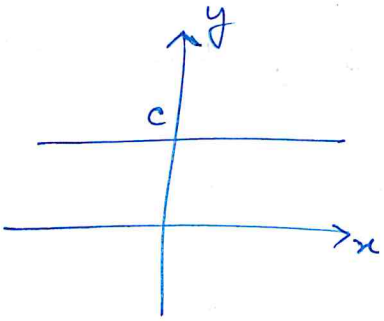
$I : \mathbb{R} \longrightarrow \mathbb{R}$



one-one onto

② Constant function: $f(x) = c \quad \forall x$

$f : \mathbb{R} \to \mathbb{R}$ (Into)

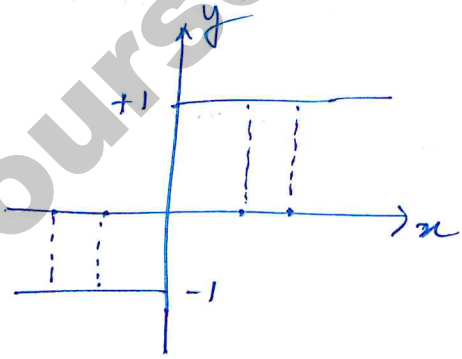


Many-one

$f : \mathbb{R} \to \{c\}$ (onto)

③ Sign function

$$f(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ -1 & \text{if } x < 0 \end{cases}$$



$f : \mathbb{R} \to \mathbb{R}$ (Into)

many-one

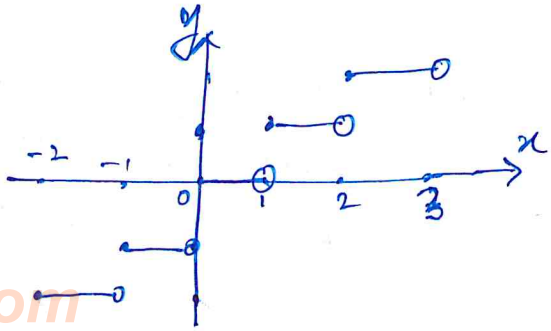
$f : \mathbb{R} \to \{+1, -1\}$ (onto)

codomain equals to the range

④ Greatest integer function: $[x] = n$, where n is an integer

if $n \leq x < n+1$

This function is referred to as floor in computer science.



For all the values of x which satisfies :-

$0 \leq x < 1$, the greatest integer function = 0

$1 \leq x < 2$, " " " " = 1

$2 \leq x < 3$, " " " " = 2

It is many-one function.

If this function is defined from :

$f: \mathbb{R} \longrightarrow \mathbb{R}$ (into)

If $f: \mathbb{R} \longrightarrow I$ (onto) — Because for every integer we can find a pre-image.

(*) POSET & TOSET : an Introduction

POSET (partially ordered set)

In relations, we have learnt about partial ordering relations and Hasse diagrams.

Note: Relations are special type of sets.
Functions are special type of relations.
POSET just like function is a special type of relation.

A partial ordering relation on a set S is a relation that is reflexive, antisymmetric & transitive

↳ aRa $\forall a$

↳ $aRb, bRa \Rightarrow a = b$

↳ $aRb, bRc \Rightarrow aRc$

where a, b, c are elements of the set on which the partial ordering relation is defined.

POSET: (non empty set, partial ordering relation)

E.g. $(\mathbb{R}, \leq)$ — whether it is a POSET?

Is it reflexive : $a \leq a \quad \forall a \in \mathbb{R}$

antisymmetric : $a \leq b, b \leq a \Rightarrow a = b, \forall a, b \in \mathbb{R}$

Transitive : $a \leq b, b \leq c \Rightarrow a \leq c, \forall a, b, c \in \mathbb{R}$

$\therefore (\mathbb{R}, \leq)$ is a POSET.

Similarly, $(\mathbb{R}, \geq)$ is also a POSET.

For $\mathbb{Z}$: set of integers,

$(\mathbb{Z}, \geq)$ is a poset

and

$(\mathbb{Z}, \leq)$ is also a POSET.

E.g. $A = \{1, 2, 3\}$

$(P(A), \subseteq)$ is also a POSET.

powerset, subset

Reflexivity : $B \subseteq B \quad \forall B \in P(A)$

Antisymmetry : $B \subseteq C, C \subseteq B \Rightarrow B = C \quad \forall B, C \in P(A)$

Transitivity : $B \subseteq C, C \subseteq D \Rightarrow B \subseteq D \quad \forall B, C, D \in P(A)$

E.g. $(Z, /)$

$/$: divisibility

$2/4$: 2 divides 4 $= 4/2 =$ integer

$4/8$: 4 divides 8 $= 8/4 =$ integer

x/y : x divides y = integer

$\therefore (Z, /)$

↓

set of all integer $= \{-1, -2, \ldots, 0, 1, 2, 3, \ldots\}$

Reflexivity : $i/i \ \forall i \in Z$

$0/0$ = undefined $\neq$ integer

$\therefore$ $(Z, /)$ not a poset.

Note:

$(Z^+, /) \rightarrow$ poset

$(Z^-, /) \rightarrow$ poset

TOSET (Totally ordered set) :

(S, R) is a TOSET iff ① (S, R) is a POSET

② $\forall x, y \in S$, xRy or yRx.

E.g. $A = \{1, 2, 3\}$, $(P(A), \subseteq) \rightarrow$ POSET ① ✓

$\{1\}, \{2\} \in P(A)$

$\{1\} \not\subseteq \{2\}$ or $\{2\} \not\subseteq \{1\}$

$\therefore$ ② condition is not satisfied.

$\therefore$ Not a TOSET.

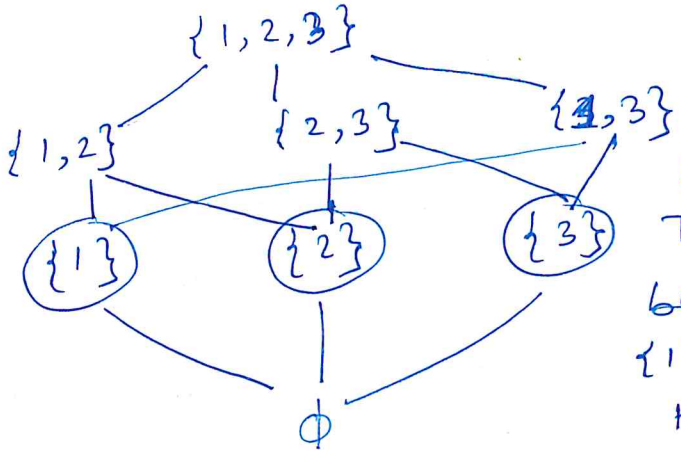


Fig: Hasse diagram

E.g.: There is no relation between the elements {1}, {2} and {3}. Hence, not a TOSET.

Note:

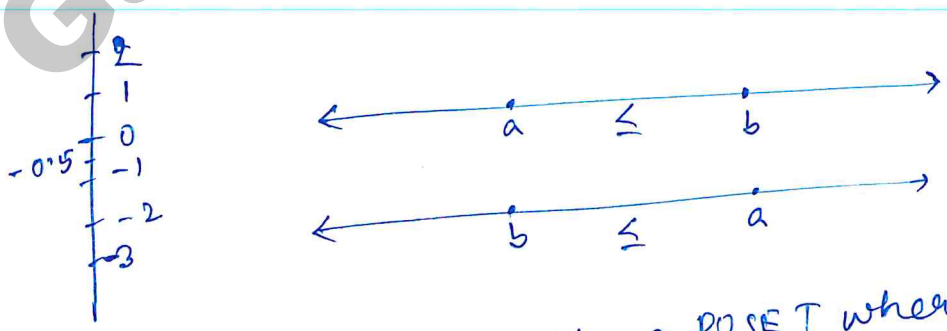
From Hasse diagram's perspective, TOSET's Hasse diagram is a chain.

∴ TOSETs are often referred to as chains or linearly ordered sets.

E.g. $(\mathbb{R}, \leq)$ → POSET — condition ① is satisfied

condition ②: $\forall a, b \in \mathbb{R}$

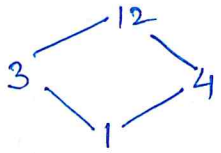
$a \leq b$ or $b \leq a$



Note: A TOSET is basically a POSET where every pair of elements are comparable / related.

E.g) $(Z^+, /) \rightarrow$ POSET

Hasse diagram :



It is not a chain,

∴ it is not a TOSET.

1/4 ✓
1/3 ✓
3/12 ✓
4/12 ✓

But, 3/4 ✗
4/3 ✗

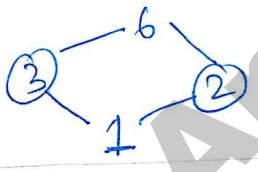
∴ 3 R 4 and 4 R 3

E.g.) D_n = set of divisors of n

E.g. $D_6 = \{1, 2, 3, 6\}$

$(D_n, /) \rightarrow$ POSET ✓

↘ ? TOSET



Not a chain,

∴ Not a TOSET

$(D_7, /) \rightarrow$ TOSET

$D_7 = \{1, 7\}$

(chain)

$(D_{prime}, /) \rightarrow$ TOSET.

(chain)

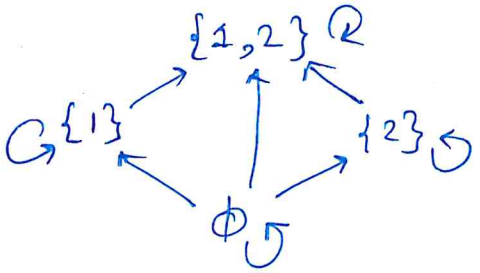
(*) Hasse diagrams & POSET properties:

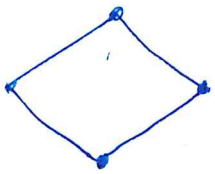
Hasse diagram — (Revisited)

$A = \{1, 2\}$; $|A| = n$

$P(A) = \{\phi, \{1\}, \{2\}, \{1,2\}\}$

$(P(A), \subseteq) \rightarrow$ POSET





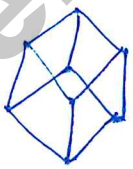
Few steps to simplify uncomplicate drawing Hasse diagram:

1. Remove self loops
2. all arrows are upwards (assumption)
3. skip arrows that can be inferred using Transitivity
4. Use a dot instead of an element.

$\#\text{vertices} = 2^n$

$\#\text{edges} = n \cdot 2^{n-1}$

Let, $A = \{1, 2, 3\}$; $|A| = n = 3$



$\#\text{vertices} = 2^3$

$\#\text{edges} = n \cdot 2^{n-1}$

$= 3 \cdot 2^2 = 12$.

Hasse diagram of $(P(A), \subseteq)$

Note! There are no cycles except self loops in the Hasse diagram of POSET.

For TOSET, (S, R) — S: set, R: Relation

$|S| = n$ elements

edges $= (n-1)$

(*) Maximal Element:

(S, R) or $(S, \leq)$

$a \in S$ is maximal iff $\nexists b \in S$ s.t $a \leq b$

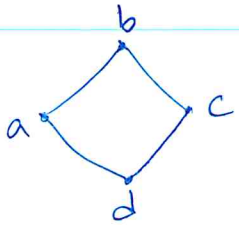
Here $\leq$ doesnot mean less than equal to.

It is just a symbolic way of saying set S with a relation called less than equal to. How less than equal to is defined, it is upto us.

(*) Minimal Element:

$(S, \leq)$

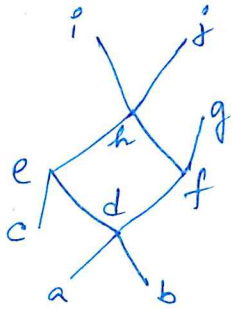
$a \in S$ is minimal iff $\nexists b \in S$ s.t $b \leq a$



maximal = {b}

minimal = {d}

E.g. $(S, \leq)$



Hasse diagram

maximal = {g, i, j}

minimal = {a, b, c}

(#) Greatest element : Represented with 1.

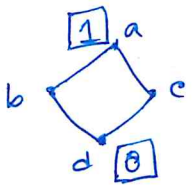
$(S, \leq)$

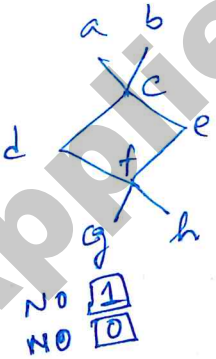
$a \in S$ is greatest element iff $b \leq a \ \forall b \in S$

(*) Least element : Represented with 0.

$(S, \leq)$

$a \in S$ is least element iff $a \leq b \ \forall b \in S$.



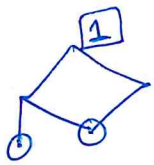


$a \geq b$?

For a to be the greatest element, it has to be greater than every other element.

Note: If the greatest and the least element exist, it is unique and it may not exist too.

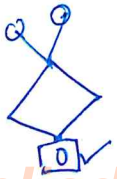
E.g.



No least element

But it has a greatest element.

E.g.



No 1

Note: A POSET that has both ⊥ & ⊤ is said to be 'bounded POSET'.

(*) Upper Bound (A):

$(S, \leq)$ $\quad A \subseteq S$; $a \in S$

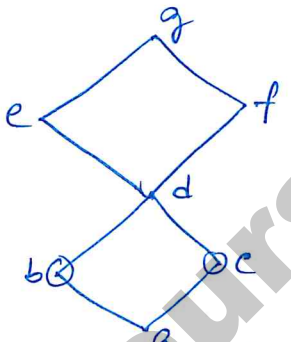
$a \in UB(A)$ iff $b \leq a \ \forall \ b \in A$

$A = \{b, c\} \subseteq S$

$UB(A) = \{d, e, f, g\}$

$B = \{b, d\}$

$UB(B) = \{d, e, f, g\}$



$(S, \leq)$

(*) Lower Bound (A): $A \subseteq S$; $a \in S$

$(S, \leq)$ $\quad a \in LB(A)$ iff $a \leq b \ \forall \ b \in A$

[Note: LB and UB are not unique and they may not exist as well.]

$LB(A) = \{a\}$

$LB(B) = \{b, a\}$

(*) Lowest Upper Bound (A) = LUB(A): $A \subseteq S$, $a \in A$

$(S, \leq)$

$a = LUB(A)$ iff

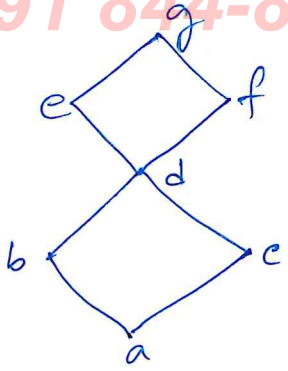
(i) $a \in UB(A)$

(ii) $a \leq b \ \forall \ b \in UB(A)$

$A = \{b, c\} \subseteq S$

$UB(A) = \{d, e, f, g\}$

$LUB(A) = \{d\}$



$B = \{b, d\}$

$UB = \{d, e, f, g\}$

$LUB = \{d\}$

(*) Greatest Lower Bound $(A) = GLB(A)$; $A \subseteq S$, $a \in S$

$(S, \leq)$

$a = GLB(A)$ iff

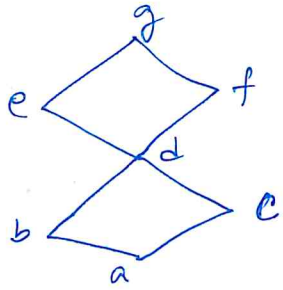
(i) $a \in LB(A)$

(ii) $b \leq a \quad \forall b \in LB(A)$

$A = \{b, c\}$

$LB(A) = \{a\}$

$GLB(A) = \{a\}$

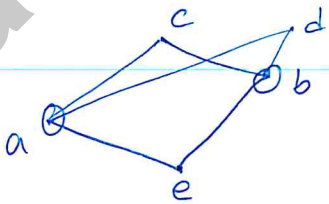


$B = \{b, d\}$

$LB(B) = \{b, a\}$

$GLB(B) = \{b\}$

E.g.



$A = \{a, b\}$

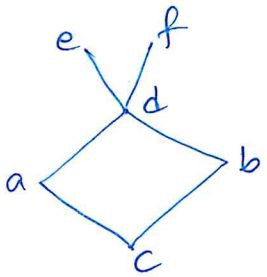
$LB(A) = \{e\}$

$GLB(A) = \{e\}$

$UB(A) = \{c, d\}$

$LUB(A) = \{\}$ or ϕ

E.g.



$A = S$

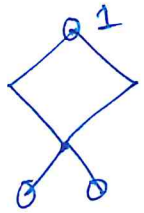
$LB(S) = \{c\}$

$GLB(S) = \{c\}$

$UB = \{\} = \phi$

$LUB = \phi$

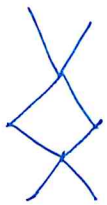
E.g.



$LB(S) = \phi$

$UB(S) = 1$

E.g.



$LB(S) = \phi$

$UB(S) = \phi$

Property: ① If $LUB(S)$ exists for $(S, \leq)$

then, $LUB(S) = 1$ (Greatest element)

② If $GLB(S)$ exists for $(S, \leq)$

then, $GLB(S) = 0$ (Least element)

(A) Lattice : an introduction.

Lattice:

Poset is a lattice iff $\forall a, b \in S$, $(S, \leq)$ and the LUB($\{a, b\}$) AND GLB($\{a, b\}$) exist.

LUB($\{a, b\}$) = Supremum(a, b) = Join(a, b) = $a \vee b$ → logical OR in Boolean Algebra.

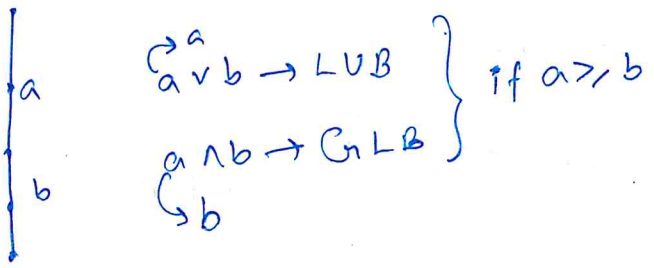
GLB($\{a, b\}$) = Infimum(a, b) = Meet(a, b) = $a \wedge b$ → logical AND

∴ POSET $(S, \leq)$ is a lattice if $\forall a, b \in S$ and $a \vee b$, $a \wedge b$ exist.

E.g., $(\mathbb{R}, \leq)$, $(\mathbb{Z}, \leq)$ — Both are POSETs; Both are TOSETs; Both are Lattices

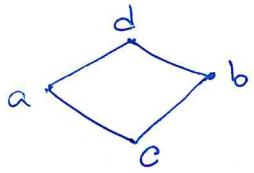
$a \leq b$ or $b \leq a$ where $a, b \in \mathbb{R}$ or $a, b \in \mathbb{Z}$.

Property: Every Toset is a lattice.



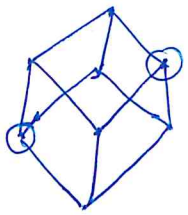
E.g., $(P(A), \subseteq)$ → POSET
↘ Lattice

$A = \{1, 2\}$



Every pair of element has a LUB and GLB. ∴ It is a lattice.

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



LUB and GLB exists for every pair of element.

∴ $(P(A), \subseteq)$ is a lattice.

E.g.

$(S, \subseteq)$ → poset
→ lattice

↓
set of all sets

$A = \{1, 2\}$ $B = \{3, 4\}$

$A \in S$ and $B \in S$

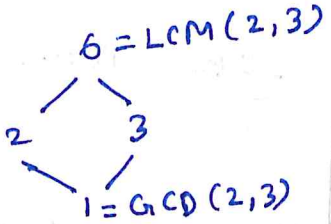
$A \vee B = LUB(\{A, B\}) = \{1, 2, 3, 4\}$
$= A \cup B \in S$

$\{1, 2, 3, 4\}$
$\{1, 2\}$ $\{3, 4\}$

$A \wedge B = GLB(\{A, B\}) = \phi \in S$
$= A \cap B$

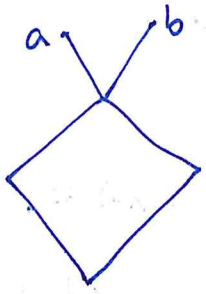
E.g.) $(Z^+, /)$ $\quad a, b \in Z^+$

↘ POSET



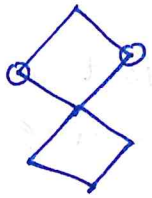
$LUB(\{a,b\}) = a \vee b = LCM(a,b)$

$GLB(\{a,b\}) = a \wedge b = GCD(a,b)$



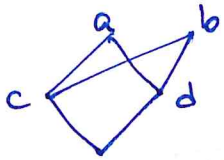
$LUB(\{a,b\}) = a \vee b = \phi$

$\therefore$ Not a Lattice



If we pick any 2 elements, there exists GLB and LUB

$\therefore$ It is a lattice.



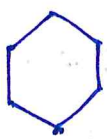
$LUB(\{a,b\}) = \phi$; $LUB(\{c,d\}) = \phi$

$\therefore$ Not a lattice

Note: $UB(\{c,d\}) = \{a,b\}$

But we can't compare a & b.

$\therefore$ LUB doesnot exist.



Lattice ✓

For every pair of elements, GLB and LUB exists.

Lattice ✓

For every pair of elements, GLB and LUB exists.

(*) Semi-Lattice:

A poset $(S, \leq)$ is a semi-lattice iff $\forall a, b \in S$ $a \vee b$ exists (LUB) Join SL

(OR)

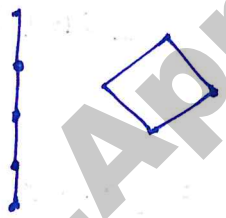
$\forall a, b \in S$ $a \wedge b$ exists (GLB) Meet Semi Lattice

Note: A lattice is a semi-lattice.

Note: For some pairs a, b, only $a \vee b$ exists, and for other pairs a, b, only $a \wedge b$ exists, it is not a semi-lattice.

$\forall a, b \in S$ ($a \vee b$ or $a \wedge b$) — Not a semilattice

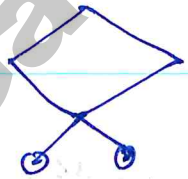
E.g.:



Both are lattices

⇓

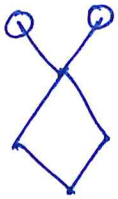
∴ They are semilattices.



LUB ({a, b}) $a \vee b$ exists $\forall a, b \in S$

GLB ({a, b} — Doesnot exists.

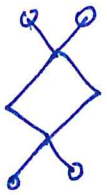
∴ It is a Join semilattice.



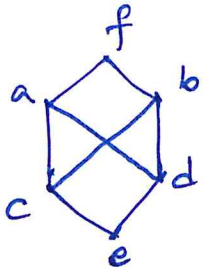
GLB exist $\forall a, b \in S$

$(a \wedge b)$

It is called a meet semi lattice.



Not a semi lattice



(a,b) $LB = \{c, d, e\}$

$GLB = \phi$

(c,d) $UB = \{a, b, f\}$

$LUB = \phi$

There exist one pair for which there is no GLB and there exist another pair for which there is no LUB.

∴ It is not a semi Lattice

⊛ Properties and Types of Lattices :

Lattice : $(S, \leq)$

① closure : $\forall a, b \in S$, $a \vee b \in S$ (LUB)
$a \wedge b \in S$ (GLB)

② Commutative : $\forall a, b \in S$, $a \vee b = b \vee a$
$a \wedge b = b \wedge a$

③ Associative : $\forall a, b, c \in S$

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

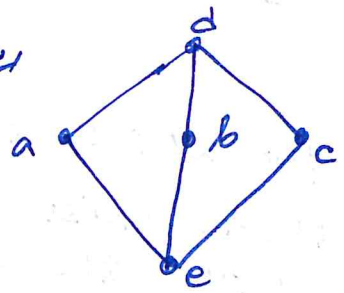
$$a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

④ Distributive : $a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c)$

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

Lattice is not distributive → Need not hold

E.g.:



Kite lattice

$\therefore a \vee e = a \Leftarrow a \wedge (b \wedge c)$; LHS

$\therefore d \wedge d = d \Leftarrow (a \vee b) \wedge (a \vee c)$; RHS

LHS $\neq$ RHS

Note: Distributive property need not hold for a lattice. If it holds, it is called distributive lattice.

⑤ Lattice need not be Bounded. Both 1, 0 should exist.

E.g.: $(Z, \leq)$

↳ No 1
↳ No 0

∴ It is an unbounded lattice.

Note: A finite lattice is always bounded.

$S = \{a_1, a_2, \ldots a_n\}$

$1 = a_1 \vee a_2 \vee a_3 \vee \ldots \vee a_n$

$0 = a_1 \wedge a_2 \wedge a_3 \ldots \wedge a_n$

⑥ Idempotent: $\forall a \in S$

$a \vee a = a$

$a \wedge a = a$

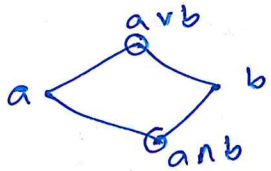
⑦ Absorption: $a \vee (a \wedge b) = a$ $\quad \forall a, b \in S$

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

⑧ Consistency: $\forall a, b \in S$

$a \leq a \vee b$ | $a \wedge b \leq a$

$b \leq a \vee b$ | $a \wedge b \leq b$



E.g) $a \le b$; $b \le c$

$a \wedge c = a$

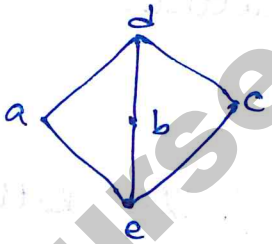
$a \vee c = c$

E.g.) $a \vee b = b \Rightarrow a \le b$

(9) Distributive inequality: $d \wedge d = d$

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

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



(10) Complement:

$\forall a \in S \ \exists a' \in S$

S.T $a \vee a' = 1$

AND $a \wedge a' = 0$

→ Complemented lattice.

Note: Every lattice is not a complemented lattice

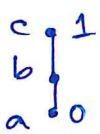
$1 \vee 0 = 1$

$1 \wedge 0 = 0$

Properties:

(*) A complemented lattice is always bounded

E.g.



$b' = ?$

$b \vee c = 1$

$b \wedge a = 0$

$b \wedge c = b$

$\begin{cases} b \vee b' = 1 \\ b \wedge b' = 0 \end{cases}$ $c \ne b'$

$b \vee c = 1$

$b \wedge c = b \ne 0$

$b \wedge a = 0$ $\quad a \neq b'$

$b \vee a = b \neq 1$

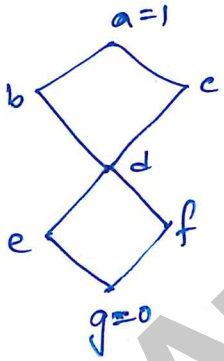
$\begin{cases} b \vee b = b \\ b \wedge b = b \end{cases}$

$\therefore$ This chain is not a COMPLEMENTED Lattice.

(*) A TOSET cannot be a complemented lattice if $|S| \geq 3$

TOSET is complemented Lattice iff $|S| = 2$

E.g.



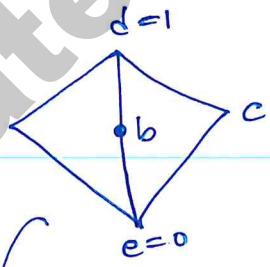
$b' = ?$ Does not exist

$b \vee c = 1$

$b \wedge c = d \neq 0$

It is a Lattice but it is not a complemented lattice.

E.g.



$a' = b, c \longrightarrow$ unique complements

$b' = a, c$

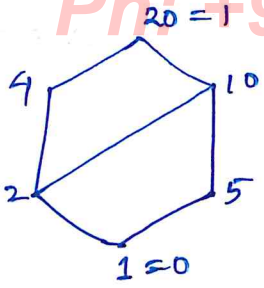
$c' = a, b$

Complemented lattice but the complements are not unique.

E.g. $(D_{20}, /)$

↓

Not complemented lattice



$2' = ?$

Do not exist

$2 \wedge 5 = 0$

$2 \vee 5 = 10 \neq 1$

(*) Distributive lattice

$(S, \leq)$ is Distributive lattice iff

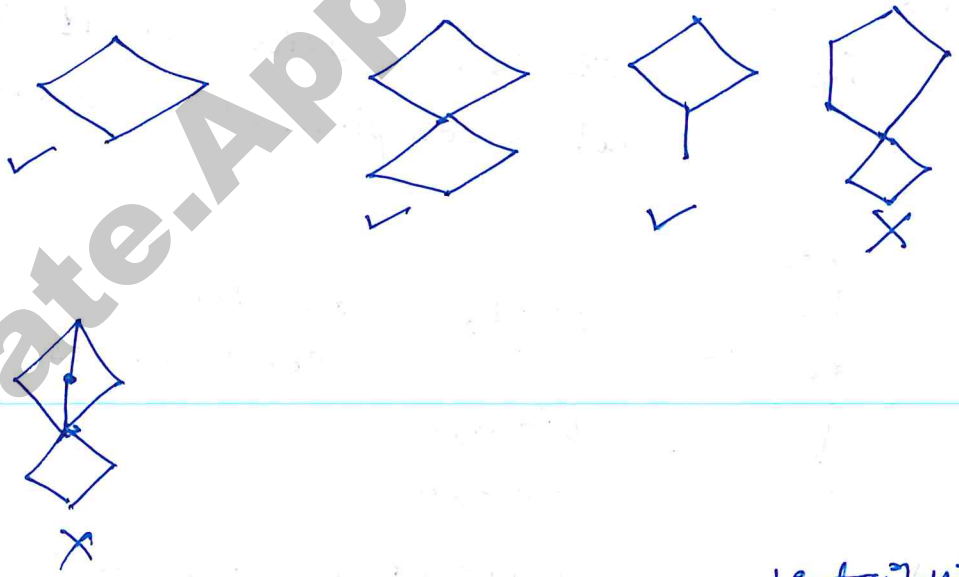
$\forall a, b, c \in S$

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

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

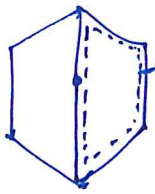
Properties:

1) A lattice is distributive iff it doesnot contain kite or pentagonal lattice as sub-lattice.



2) If a complemented lattice is distributive, then the complement of each element is unique.

E.g.



pentagonal
∴ Not distributive

Note: A lattice is a Boolean Algebra iff lattice is distributive, bounded and complemented.

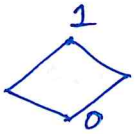
Sets → Relations → POSET → Lattice → B.A.

Boolean Algebra is foundational to computer science.

(#) In Boolean Algebra, every element has a unique complement.

$(P(A), \subseteq)$ → lattice : distributive, bounded and complemented.

$A = \{1, 2\}$



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

$\{n, /\}$ → B.A

(*) Lattice whose Hasse diagram is isomorphic to the Hasse diagram of $(P(A), \subseteq)$, then it is a Boolean Algebra.

(*) In Boolean Algebra,

$$\left.\begin{array}{l} a \vee b = a \vee c \\ \text{AND} \\ a \wedge b = a \wedge c \end{array}\right\} \Rightarrow b = c$$

$$\left\{\begin{array}{l} a \vee b = a \vee c \not\Rightarrow b = c \\ a \wedge b = a \wedge c \not\Rightarrow b = c \end{array}\right.$$

→ Cancellation doesnot hold for Boolean Algebra.

Note:
For real numbers on plus operator,

$$x + b = x + c \Rightarrow b = c$$

(*) Group Theory: An introduction

Group theory as mathematical subject is widely used in the areas of cryptography and network security.

Binary operation (*)

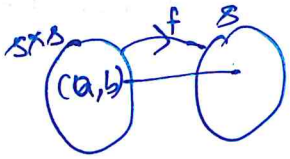
* is a binary operation defined on a non-empty set S as a mapping $f : S \times S \to S$

It can also be defined as:

(1) For $\forall a, b \in S$ $a * b$ is defined & $a * b \in S$

$f(a, b) = c$ is same as $a * b$.

($a \in S$, $b \in S$, $c \in S$)



① $\forall a, b \in S$ $a * b$ is unique

E.g. $a * b = a + b$ on $\mathbb{R}$

$(\mathbb{R}, +)$ $\forall a, b \in \mathbb{R}$, $a + b \in \mathbb{R}$

$\forall a, b \in \mathbb{R}$, $a + b$ is unique.

$\therefore$ It is a binary operation.

E.g. $a * b = a - b$ on $\mathbb{R}$

$(\mathbb{R}, -)$

$\therefore$ It is also a binary operation.

E.g. $a * b = \sqrt{ab}$ $(\mathbb{R}, *)$

$a = 1, b = 1$

$\therefore \sqrt{1} = +1 \in \mathbb{R}$

$-1 \in \mathbb{R}$

$\therefore \sqrt{ab}$ is not unique

$\therefore$ The operator is not unique

$\therefore$ It is not a binary operator.

E.g. $a * b = \frac{a}{b}$ $(\mathbb{R}, *)$

If, $b = 0$

& $a = 0$

We have $\frac{0}{0}$ = indeterminate $\notin \mathbb{R}$

$\therefore$ Not binary operator.

E.g. $a * b = \frac{a}{b}$ $(\mathbb{R} - \{0\}, *)$

Here $\frac{a}{b}$ is a binary operator.

Properties:

① **closure** : $(S, *)$

$a * b \in S \quad \forall a, b \in S$

$f: S \times S \rightarrow S$

Every binary operation is closed.

② **Associativity** : $\forall a, b, c \in S$

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

③ **Identity (e)** :

$\exists e \in S \quad s.t \quad \forall a \in S \quad a * e = e * a = a$

④ **Inverse**: $\forall a \in S \quad \exists a^{-1} \in S \quad s.t$

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

⑤ **Commutative** :

$\forall a, b \in S$

$a * b = b * a$

$(S, *)$

Semigroup → closure & Associative

Monoid → closure & Associative & Identity

Group → closure, Associativity, Identity, Inverse

Abelian Group → closure, Associativity, Identity, Inverse, commutative.

E.g. (1) :-

$(\mathbb{R}, *)$

$a * b = a + b$

closure : ✓

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

Identity : $a + e = e + a = a$

$\boxed{e = 0 \in \mathbb{R}}$

Inverse : $a + a^{-1} = a^{-1} + a = 0$

$\boxed{a^{-1} = -a \in \mathbb{R}}$

$\boxed{\text{For } \forall a \in \mathbb{R}, \; -a \in \mathbb{R}}$

Commutative : $a + b = b + a$

∴ Abelian group.

E.g. (2) :-

$(\mathbb{Z}, *)$

$a * b = a \times b$

closure : ✓

Associative : $a \times (b \times c) = (a \times b) \times c$

Identity : $a \times e = e \times a = a$

$e = 1 \in \mathbb{Z}$

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

$a^{-1} = \frac{1}{a}$

If $a = 2$, $\frac{1}{a} = a^{-1} = \frac{1}{2} \notin \mathbb{Z}$

$a = 0$, $\frac{1}{0}$ = Not determined.

∴ Inverse doesnot exist for all elements.

→ Monoid

Commutative: $a * b = b * a$

∴ Commutative Monoid.

E.g. ③ $(\mathbb{Z}, *)$

$a * b = a^b$ Closure: $a=2, b=-2 = 2^{-2} = \frac{1}{2^2} = \frac{1}{4} \notin \mathbb{Z}$

Not closed. ∴ Not a binary operator.

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

$a^{(b^c)} \neq (a^b)^c$

$2^{(2^3)} \neq (2^2)^3$

$2^8 = 256 \neq 4^3 = 64$

Identity: $a^e = e^a = a$

$a^1 = a \neq 1^a$

E.g. ④ $a * b = \max(a, b)$

$(\mathbb{Z}, *)$

Closure: ✓

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

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

Semigroup.

Identity:

$\max(a, e) = \max(e, a) = a$

Note: $e \neq -\infty$ as $-\infty \notin \mathbb{Z}$

∴ No identity exists.

Eg ⑤

*	a	b	c	d
e=a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Symmetric matrix
∴ It is also commutative

$S = \{a, b, c, d\}$

$(S, *)$

Closure: ✓

Associativity:

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

It is valid for all the triplets.

No. of triplets = ${}^4P_3$.

Identity: $b*e = e*b = b$

$e = a$

Inverse: $b * b^{-1} = e = a$

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

Commutative: ✓

∴ Abelian group.

Eg ⑥ $(Z, *)$ $a*b = a+b-ab$

Closure: ✓

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

$(a+b-ab)+c$

$-(a+b-ab)c$

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

$= a+b+c-bc$

$-a(b+c-bc)$

LHS = RHS as both sides cancel out.

Identity: $a*e = e*a = a$

$a+e-ae = a$

$\Rightarrow e-ae = 0$

$\Rightarrow e(1-a) = 0 \Rightarrow e = 0$

Inverse : $a * a^{-1} = e = 0$

$$a + a^{-1} - a a^{-1} = 0$$

$$\Rightarrow a^{-1}(1-a) = -a$$

$$\Rightarrow a^{-1} = \frac{-a}{1-a} = \frac{a}{a-1} \in Z \quad \forall a \in Z$$

If $a = 1$, $\frac{a}{a-1} = \frac{1}{1-1} = \frac{1}{0} \notin Z$

∴ Inverse doesnot exist, as we showed that for $a = 1$, inverse doesnot exist.

∴ It is a Monoid.

(*) Group Theory - II :

Properties of Group :

1. e is unique
2. Left identity = right identity

   $a * e = e * a$
3. a^{-1} is unique for all $a \in G$
4. $(a*b)^{-1} = b^{-1} * a^{-1} \quad \forall a, b \in G$

   $ab \in G$

   $(ab)(ab)^{-1} = e$

   $\Rightarrow a^{-1}(ab)(ab)^{-1} = a^{-1}e \Rightarrow (a^{-1}a)b(ab)^{-1} = a^{-1}a$

   $\Rightarrow b^{-1}b(ab)^{-1} = b^{-1}a^{-1}$

   $\Rightarrow (ab)^{-1} = b^{-1}a^{-1}$

⑤ $(a^{-1})^{-1} = a$

$a^{-1} = b$ iff $b^{-1} = a$

↳ $(a^{-1})^{-1} = a$

⑥ Left and right cancellation is allowed in a group.

$ab = ac \iff b = c$ for a group.

↳ True

But it is not true for a monoid.

Left cancellation:-

$a^{-1}ab = a^{-1}ac$

$\Rightarrow b = c$

Similarly, right cancellation:

$ba = ca \iff b = c$

$baa^{-1} = caa^{-1}$

$\Rightarrow b = c$

⑦ if $ax = b$

then $x = a^{-1}b$ is unique

if $xa = b$

then $x = ba^{-1}$ is unique

⑧ A cayley's Table of a finite group has no repetitions in any row/column.

$|G| =$ finite

operator

$*$	a	b
a	a	b
b	b	a

$G = \{a, b\}$

Cayley's Table

If cayley's Table is defined like :-

*	a	b
a	a	a
b	b	a

X This is not allowed.

Because here, ← Not unique

$a * a = a$

$a * b = a$

We know if $ax = b$, then x is unique.

∴ we cannot have repetitions in a row/column.

E.g

$(G, *)$

*	a	b	c	d
e = a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$d * b = a = e$

$d^{-1} = b$

$b^{-1} = d$

Let's look at properties of Abelian Group $(G, *)$

① $(G, *)$ is abelian Grp iff $a * b = b * a \ \forall a, b \in G$

② Grp: $\forall a \in G$, $a^{-1} = a \Rightarrow (G, *)$ is abelian

$a^{-1} = a$

↓

$a^2 = e$ (multiply both sides by a)

If $a, b \in G$, then ab is also an element of G, ie, $ab \in G$ (By closure property)

$\therefore (ab)(ab) = e$

$\Rightarrow abab\,ba = ba$

[we need to prove $ab = ba$ for abelian group. $\forall a, b$]

$\Rightarrow abaabba = ba$ ($bb = e$)

$\Rightarrow abaa = ba$ ($aa = e$)

$\Rightarrow \boxed{ab = ba}$ RHS.

② A group G $(G, *)$ is abelian iff $(ab)^2 = a^2b^2$

G is abelian $\iff (ab)^2 = a^2b^2$

Let's prove:

G is abelian $\Rightarrow (ab)^2 = a^2b^2$

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

(ba commutative with abb)

Now, let's prove: $(ab)^2 = a^2b^2 \Rightarrow G$ is abelian

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

$(ab)(ab) = aabb$

Inverse exists,

$a^{-1}(ab)(ab) = a^{-1}aabb$

$bab = abb$

Now, $babb^{-1} = abbb^{-1} \Rightarrow \boxed{ba = ab}$

Two special groups used in cryptography is called

(1) Addition modulo group : $(Z_m, +_m)$

$$Z_m = \{0, 1, 2, \ldots m-1\}$$

$$a +_m b = (a+b) \bmod m$$

The addition modulo operator on this group is actually an abelian group.

$+_m$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(Z_4, +_4)$

$(2+3) \bmod 3$
$= 5 \bmod 3$
$= 2$

Closed ✓

Associativity: $(a +_m b) +_m c$

$= a +_m (b +_m c) = (a+b+c) \bmod m$

Identity : 0

$\because a +_m 0 = a \bmod m = 0$

Inverse : $a +_m a^{-1} = 0$

$\Rightarrow (a + a^{-1}) \bmod m = 0 \Rightarrow a^{-1} = m - a$

Commutative : $(a+b) \bmod m = (b+a) \bmod m$

(ii) Multiplication modulo : $(Z_p, \times_p)$

$Z_p = \{1, 2, \ldots p\}$; p : prime

Note: Multiplication modulo is often defined on prime number. Prime numbers are extremely important in cryptography. Hence we use multiplication modulo in Cryptography.

For p is a prime number, we can show that $(Z_p, \times_p)$ is an abelian group, where

$a \times_p b = (a \times b) \bmod p$

Note: $e = 1$, where e = identity element.

(iii) Permutation group:

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

Let f be a function.

$f : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ (Input / output) permutation function

S = set of all permutation functions on A.

$|S| = 3! = 6$

$S = \{f_1, f_2, f_3, f_4, f_5, f_6\}$

$f \circ g = f(g(x))$

$(S, \circ)$ ← composition operator

↳ permutation group.

It satisfies:

↳ closure
↳ associativity
↳ inverse
↳ identity

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$$

$$\therefore \boxed{foI = Iof = f}$$

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

f_1 $\qquad$ $f_1^{-1} \in S$

It's not abelian group but it is a group.

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

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

(*) Powers of an element (a) in Grp $(G, *)$ (Group)

Let $\forall a \in G$ & $n \in Z$

then, $a^0 = e$

$a^1 = a$

$a^2 = a * a$

$a^3 = a^2 * a = a * a * a$

a^n = power of an element a, where n is an integer.

a^{-1} = inverse(a) = inv(a) = a^{-1}

a^n, $n = -1 \Rightarrow a^{-1}$.

$a^{-2} = (a^2)^{-1} = inv(a^2)$

$a^{1.5}$ is not defined as $1.5 \notin Z$

$(a^m)^n = a^{mn}$

$a^m . a^n = a^{m+n}$

(*) Order of a group & order of an element :

$(G, *)$

$o(G) = |G|$
↳ order of a group

Note: If group is an infinite set, then order of group can be infinity.

Let $a \in G$

$o(a) =$ smallest $n \in Z$ such that $a^n = e$
(smallest integer; e = identity element of the group.)

*	a	b	c	d
e = a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$o(a) = o(e) = 1 = a^1 = e$

$o(b) = b*b*b*b = a = e$
↳ 4 ∵ $b^4 = e$

$o(c) = 2$

$o(d) = 4$

Properties of order of an element and order of a group:

① $o(a) \leq o(G)$

$o(a) \mid o(G)$ for finite groups

for finite groups ; $O(a)$ exists & finite

② $O(G) = p$

Divisors of prime $p = 1, p$.

$\because o(a) \mid o(G)$,

$\therefore o(a) = 1$ or p

$o(e) = 1$

$o(a) = p \quad \forall a \in G$

$\therefore$ For $(p-1)$ elements, the order will be p and for the remaining 1 element which is the identity element, the order is 1.

This property is useful in cryptography, in the context of multiplication modulo.

$\therefore$ For multiplication modulo operator, we have Z_p and $|Z_p| = p$

③ $o(a*b) = o(b*a)$ ∀ groups

$o(ab) = n \iff (ab)^n = e$

$\underbrace{abababab\ldots ab}_{n \text{ times}} = e$

For groups, associativity holds,

$a(ba)(ba)(ba)\ldots = a(ba)^{n-1}b = e$

Note: We want to prove : $(ba)^n = e$

Now,

$a^{-1}a(ba)^{n-1}bb^{-1} = a^{-1}eb^{-1}$

$(ba)^{n-1} = a^{-1}b^{-1} = (ba)^{-1}$

$\boxed{(ba)^n = e}$

⑦ Cyclic groups and Subgroups :

Cyclic group :

A group $(G, *)$ is a cyclic group iff

$\exists g \in G$ s.t $\forall a \in G$, $a = g^n$, $n \in Z$

Note: Multiple g's may exist

If we have a g such that every element a in group can be represented as g^n, such a group is called the generator of the group.

E.g) $(\mathbb{Z}, +)$; $g = \underbrace{+1, -1}_{\text{two generators}}$

↑ Addition operation

$0 = 1^0$

$1 = 1^1$

$2 = 1^2 = 1+1 = 1*1$

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

⋮

$0 = -1^0$

$-1 = -1^1$

$-2 = (-1)^2 = -1 + -1$

⋮

Here, operator multiplication is defined as addition.

$-1 = 1^{-1}$

$-2 = 1^{-2}$

⋮

$1 = (-1)^{-1}$

⋮

Note: e cannot be a generator unless e is the only element in set G.

$\therefore G = \{e\}$.

*	e
e	e

$\therefore (\{e\}, *)$ is a group.

Properties:

① If g is a generator, then g^{-1} is also a generator of the group.

$\forall a$, $a = g^n$

$\Rightarrow a = (g^{-1})^{-n}$ $\quad \because (a^m)^n = a^{mn}$

(2) cyclic group is always abelian.

$\forall a, b \in G$, $a = g^n$, $b = g^m$, $n, m \in Z$

$$ab = g^n g^m = g^{n+m} = g^{m+n} = g^m \cdot g^n = ba$$

(3) An abelian group need not be cyclic

$(\mathbb{R}, +) \longrightarrow$ abelian group

↳ Not cyclic [∵ there exists no generator that generates all the numbers in the set of real numbers]

(4) A non-abelian group is always non-cyclic.

E.g.) $(Z_m, +_m)$ Addition modulo is cyclic

$g = 1, (m-1)$

E.g.)

*	a	b	c	d
e = a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$g \stackrel{?}{=} b$

$b^0 = a$
$b^1 = b$
$b^2 = c$
$b^3 = d$

All four elements are generated ∴ b is a generator

∴ $g = b$.

Also, we know that if g is a generator, then g^{-1} is also a generator.

$\therefore b^{-1} = d = g$

$\therefore g = \{b, d\}$

$\therefore$ The group is a cyclic group as generator exists.

properties of cyclic group:

① For prime ordered group,

if $o(G) =$ prime

then G is cyclic

gen = $G - \{e\}$

② $(G, *)$ is cyclic $\Leftrightarrow \exists a$ s.t $\boxed{o(a) = o(G)}$

$\phi(n)$ = Euler Totient function

$\phi(n)$ = # generators of a cyclic group of order n.

$\phi(n) = n - 1$ if n is prime

If n is not prime then we use the concept of prime factorization

$n = p_1^{n_1} p_2^{n_2} p_3^{n_3} \ldots$ (prime factorization)

If $n = 60 = 2^2 \times 3^1 \times 5^1$

$\phi(n) = (p_1^{n_1} - p_1^{n_1-1})(p_2^{n_2} - p_2^{n_2-1}) \ldots$

$= (2^2 - 2^1)(3^1 - 3^0)(5^1 - 5^0)$

$= (4-2)(3-1)(5-1) = (2)(2)(4)$

$= 16$

Note:

$n = p^1$

$\phi(n) = (p^1 - p^0) = (n-1)$

Again, $\phi(n)$ = number of integers i from i to n s.t GCD$(i, n) = 1$

Relative primes

[$\because$ i & n are rel. primes]

60 — 1 .... 60 — 16 numbers

$\therefore \phi(n) = \#$ relative primes of n.

(3) If $g_1, g_2, g_3, \ldots, g_k$ are generators of cyclic group of order n,

then,

$g_i = g_j^x \quad \forall g_i, g_j$

(4) $\because o(g_i)$ is a relative prime of $o(G)$

⊛ Subgroup : $(G, *)$

$(H, *)$ is a subgroup of $(G, *)$ iff

(i) $H \subseteq G$

(ii) $(H, *)$ is also group

E.g.) $(\{e\}, *)$ is a trivial subgroup of $(G, *)$.

Also, $(G, *)$ is a trivial subgroup of $(G, *)$.

E.g.) Non-trivial subgroups.

$(Z_4, +_4)$: Addition modulo 4

↳ $\{0, 1, 2, 3\}$

$(\{0, 2\}, +_4)$ — is it a subgroup?

Is it a group ?

$0 +_4 0 = 0$

$0 +_4 2 = 2$

$2 +_4 2 = 0$

} closed

⋮

Similarly we can prove the other properties.

Thus, it is infact a group and also it is therefore a subgroup of $(Z_4, +_4)$.

E.g) Check if $(\{0,1,2\}, +_4)$ is a subgroup or not.

Let's check closure property.

$1 +_4 2 = 3 \notin \{0,1,2\}$

$\therefore$ closure not satisfied

$\therefore$ NOT a group.

Properties:

① $A \subseteq G$; $B \subseteq G$

If A and B are subgroups of G, then $A \cap B$ is also a subgroup.

But, $A \cup B$ need not be a subgroup.

E.g.,

$A = (\{0,2\}, +_4)$ is a subgroup of $(Z_4, +_4)$

$B = (\{0,1\}, +_4)$ is also a subgroup of $(Z_4, +_4)$

But, $A \cup B = (\{0,1,2\}, +_4)$ is not a subgroup of $(Z_4, +_4)$

Theorem:

Lagrange's Theorem:

$o(H) \mid o(G)$ where H is a subgroup of $(G, *)$

Properties:

① If $|G| =$ prime;

$o(G) = p \rightarrow 1$, p

② If $(H, *)$, $(K, *)$ are subgroups of $(G, *)$

then $(H \cap K, *)$ is also a subgroup

similarly,

$(H \cup K, *)$ need not be subgroup.

③ If $(H, *)$, $(K, *)$ are subgroups of $(G, *)$

[$HK = \{h * k \mid h \in H, k \in K\}$ set]

then $(HK, *)$ is also a subgroup.

④ $o(HK) = \left[\frac{o(H) * o(K)}{o(H \cap K)}\right]$

$o(H \cap K) \leq o(H)$

$o(H \cap K) \leq o(K)$

$o(H \cap K) \mid o(H)$

$o(H \cap K) \mid o(K)$

$o(HK) \mid o(H)$

$o(HK) \mid o(K)$

Alternate definition of subgroup:

If $*$ is a binary operator on set H.

$(H, *)$ is a subgroup of $(G, *)$

(i) $H \subseteq G$

(ii) $a * b^{-1} \in H \quad \forall\, a, b \in H$

↳ we can prove H is a group (closure, associativity, identity, inverse)