

DT :- 30/01/24

DISCRETE MATHEMATICS

MOD-1

SET THEORY

①

- Set :- A collection of well defined distinct objects is known as set.

→ It is denoted as the capital English Alphabet i.e. A, B, C, D etc.

→ A set A is defined as :-

$$A = \{x_1, x_2, x_3, \dots, x_n\}$$

where, $x_1, x_2, x_3, \dots, x_n$ are elements of set A.

→ EX :- $B = \{2, 4, 6, 8\}$

→ Element of set B

$2 \in B$ → element

→ 2 belongs to set B

EX :- $A = \{a, e, i, o, u\}$

$a \in A$

Read as :- a is an element of set A
or

a belongs to set A.

- Representation of a set :- A set is represented by capital English alphabet & elements are enclosed by $\{a, b, c\}$

① Tabular form
or
List form
or
Roster form

EX :- $A = \{a, e, i, o, u\}$

② Set-Builder form
or
Set-Selector form
or
Rule form

EX :- $A = \{a, e, i, o, u\}$
↓
Roster form

$A = \{x : x \text{ is a vowel of E. Alpha}\}$

$C = \{x : x \in \mathbb{N}, x < 5\}$ s-B form
 $= \{1, 2, 3, 4\}$ Roster form

- Types of sets :-

① Singleton set :- let $A = \{a\}, a \in A$

→ A set having only one element is known as singleton set.

EX :- $B = \{2\}$ or $A = \{a\}$

- (2) finite set :- $A = \{a, e, i, o, u\}$ The set having finite no of elements.
 $B = \{1, 2, 3, 4, 5\}$

at first :- Remark :-
countable :- we can count the number of elements present in a set.

Definition :- A set having finite no of elements is known as finite set.

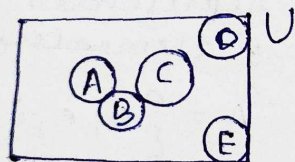
- (3) Infinite set :- A set having infinite no of elements is known as infinite set.

EX :- set of Natural no = $\{1, 2, 3, 4, \dots\}$

- (4) Empty set :- A set having no elements.
 It is denoted by $\phi = \{ \}$

- (5) universal set :-

$$N = \{1, 2, 3, 4, 5, \dots\}$$



$$0 \notin \phi$$

cardinality of $\phi =$ The no of elements in ϕ set.

$$|\phi| = 0$$

$$\text{EX :- } \phi = \{x : x \neq x \text{ if } x \in N\}$$

$$\phi = \{x : x \neq 1 \text{ if } x \in N\}$$

cardinality of set :- The no of elements present in a set is known as cardinality of that set.

$\rightarrow$ It is defined as $|A|$ if A is a set (finite)
 $\hookrightarrow$ or $n(A)$
 or $\text{ord}(A) \rightarrow$ order of set A

EX of representation of set :-

EX :- $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

1...10 are elements of set A.

$5 \in A$
↓
Belongs to

$12 \notin A$

Dt:- 06/02/24

Infinite set :-

EX :-

$$N = \{1, 2, 3, 4, \dots\}$$

↓

(natural no set)

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

(whole no set)

$$\mathbb{Z} \text{ or } \mathbb{I} = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}$$

(Integer set)

$$= \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}$$

Rational number = A no is written in the form of p/q where $p, q \in \mathbb{Z}$ and p and q are coprime.

EX $\mathbb{R} = \left\{ 3, \frac{11}{23}, \frac{5}{7}, 8, 0, \dots \text{etc} \right\}$

(6) Rational no set :-

$$(\mathbb{Q}) = \left\{ x : x = \frac{p}{q}, p, q \in \mathbb{Z}, q \neq 0 \right\}$$

(7) Irrational no set :- $\mathbb{Q}'$ = Those numbers are not rational

$$\mathbb{Q}' = \{\sqrt{2}, \sqrt{3}, \dots, \pi, e, \dots\}$$

where $\pi \approx \sqrt{10}$

$$e \approx 2.718283 \dots$$

(8) Real numbers ^{Set} (R) :- All rational and irrational numbers are known as real numbers.

$$(R) = Q \cup Q'$$

SUBSET :- If all elements of set A are in set B.
Then set A is subset of set B.

→ It is defined as $A \subseteq B$.
↓
denoted

$\subseteq$ → subset

$\subset$ → proper subset.

$\supseteq$ → superset.

EX :- $A = \{2, 4, 8, 10\}$

$$B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$A \subset B \rightarrow \boxed{A \subset B}$$

↓
proper subset

EX :- 2 :- $A = \{x : 2x^2 + 5x + 3 = 0, x \in \mathbb{R}\}$

$$\therefore 2x^2 + 5x + 3 = 0.$$

$$\Rightarrow 2x^2 + 2x + 3x + 3 = 0.$$

$$\Rightarrow 2x(x+1) + 3(x+1) = 0$$

$$\Rightarrow (x+1)(2x+3) = 0$$

$$\Rightarrow \boxed{x = -1} \text{ or } 2x = -3$$

$$\Rightarrow \boxed{x = -\frac{3}{2}}$$

$$B = \{-1, -\frac{3}{2}\}$$

$$A \subseteq B.$$

$$\text{or } B \supseteq A.$$

$\supseteq \rightarrow$ superset.

• Set operation :-

(1) union set :- $A \cup B = \{x: x \in A \text{ or } x \in B\}$ or $= \{x: x \in A \vee x \in B\}$.

(2) Intersection set :- $A \cap B = \{x: x \in A \text{ or } x \in B\}' = \{x: x \in A \wedge x \in B\}$.

(3) Difference between 2 sets :- $A - B$ or $A - B$ or $A \setminus B$ or $A \setminus B$.

$$A - B = \{x: x \in A \text{ but } x \notin B\}.$$

(4) Symmetric difference between 2 sets :- It is denoted as $A \Delta B$.

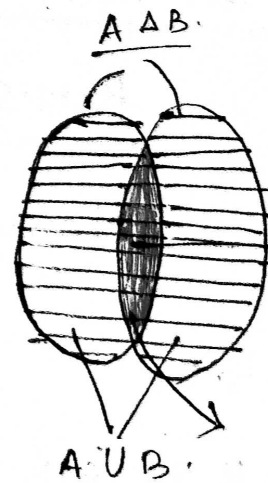
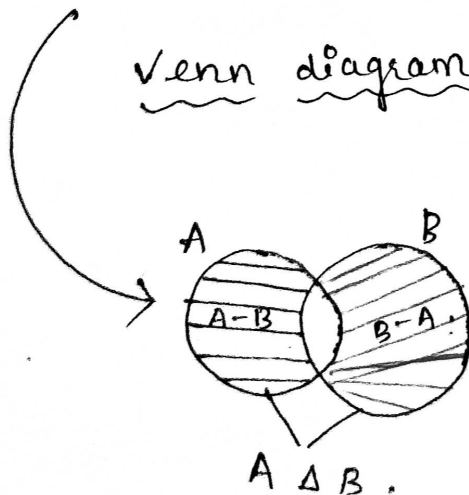
$\rightarrow$ It is defined as

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

or

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

Venn diagram :-



$\rightarrow$ It also can't be fixed

EX :-

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

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

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

$$= \{a, b, c, d, e\} - \{a, b, c\} = \{d, e\}.$$

Principle of Inclusion & Exclusion :-

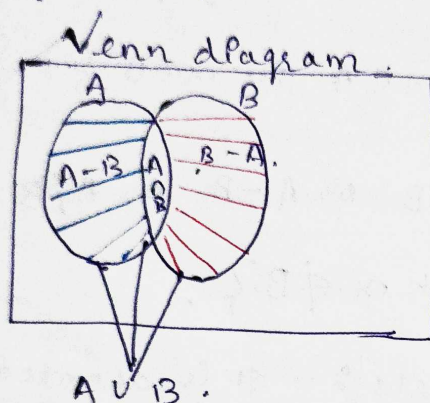
→ If A & B be any 2 sets, then

$$\boxed{|A \cup B| = |A| + |B| - |A \cap B|}$$

Cardinality

PROOF :-

By help of Venn diagram, we can prove,



We know that,

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

$$\Rightarrow |A - B| = |A| - |A \cap B|$$

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

$$\Rightarrow |B - A| = |B| - |A \cap B|$$

$$\underline{\text{L.H.S}} = |A \cup B|$$

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

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

$$\boxed{= |A| + |B| - |A \cap B|}$$

R.H.S

Hence proved

Remark :-

If A, B & C are 3 sets, then,

$$\boxed{\text{IMP } |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|}$$

Proof :- L.H.S = $|A \cup B \cup C|$

$$= |A \cup D|$$

let $B \cup C = D$.

→ Applying Inclusions and Exclusions

$$= |A| + |D| - |A \cap D|$$

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

by distributive law

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

$$= |A| + |B| + |C| - |B \cap C| - |E \cup F| \quad \text{where } E = A \cap B$$

$$F = A \cap C$$

$$= |A| + |B| + |C| - |B \cap C| - [|E| + |F| - |E \cap F|]$$

$$= |A| + |B| + |C| - |B \cap C| - |E| - |F| + |E \cap F|$$

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

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

$$= \underline{\text{R.H.S}}$$

Hence proved

Mathematical Induction :-

or

Principle of Mathematical Induction :-

→ The proof of a statement consists of 3 steps :-

STEP-1 :- called the Basis of Induction :- checking if $P(m)$ is true for $m \in \mathbb{N}$.

STEP-2 :- called the Induction Hypothesis :- Assuming that $P(m)$ is true for $m \in \mathbb{N}$. (arbitrary natural no.) where $m \geq n$.

STEP-3 :- called the Induction step :- showing that $P(m+1)$ is true, by a direct or indirect method of proof.

Remark :-

Statement :- A sentence which infer true or false value is known as a statement :

→ It is known as a proposition.

(Statement / proposition) → It is denoted as $P(m)$.

EX :-

	<u>Sentence</u>	<u>Statement</u>
(1)	Puri is famous for Lord Jagannath.	✓ T
(2)	Kapilash is famous for Lord Krishna.	✓ F
(3)	Dhenkanal is famous for Vidyata Bara.	✓ T
(4)	B.T.B college is in Sambalpur.	✓ F
(5)	How old are you?	→ not a statement.
(6)	May god bless you!	→ not a statement.

Remark :- Every statement is a sentence.

but Every sentence need not be a statement.

IMPORTANT QUESTION :-



Question related to principle of Mathematical Induction.

Prob-1 :- To prove,
 $1+2+3+\dots+n = \frac{n(n+1)}{2}$

By principle of Mathematical Induction.

Ans let us consider,

$P(n)$ be a statement i.e. $P(n) : 1+2+3+\dots+n = \frac{n(n+1)}{2}$

By Mathematically Induction process.

(i) let $\boxed{n=1}$, $P(1) = \text{LHS} = 1$.

$$\text{RHS} = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

Here LHS = RHS. So, $P(1)$ is true. ✓

let $\boxed{n=m}$, $P(m) = 1+2+3+\dots+m = \frac{m(m+1)}{2}$

(ii) Assume that, $P(m)$ is true,

$$\boxed{1+2+3+\dots+m = \frac{m(m+1)}{2}} \quad \text{--- (i)}$$

We shall have to prove,

$P(m+1)$ is true

i.e. to prove

$$P(m+1) = 1+2+3+\dots+m+(m+1) = \frac{(m+1)((m+1)+1)}{2}$$

↓
 We have to prove this.

PROOF :-

$$\text{LHS :- } 1+2+3+\dots+m+(m+1)$$

$$= [1+2+3+\dots+m] + (m+1)$$

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

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

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

$$= (m+1)(m+1)$$

$$= \frac{(m+1)[(m+1)+1]}{2} = \text{RHS}$$

Here LHS = RHS

So, $P(m+1)$ is true.

Here, we have

(i) $P(1)$ is true

(ii) $P(m)$ is true.

$\Rightarrow P(m+1)$ is true.

So,

$P(n)$ is true by principle of mathematical Induction.

$$\text{Hence, } P(n) : 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}.$$

Hence proved

Homework :-

(Q) By method of Induction :-

$$\left. \begin{array}{l} (1) 1^2 + 2^2 + 3^2 + 4 \dots + n^2 = \frac{n(n+1)(2n+1)}{6} \\ (2) 1^3 + 2^3 + 3^3 + \dots + n^3 = \left[\frac{n(n+1)}{2} \right]^2 \end{array} \right\}$$

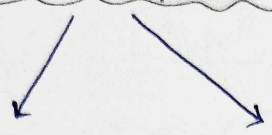
- Logic and method of proofs :-

- Propositional logic :-

→ Every statement or proposition is a sentence, but every sentence need not be a statement.

→ G. Frege (1884 - 1925) developed the idea, regarding a mathematical theory as applied system of logic.

- Types of proposition :-



(1) primary (primitive) proposition (2) compound or composite or molecular proposition.

(1) Primary or primitive proposition :-

→ A proposition consisting of only a single propositional variable, or a single propositional constant is called a primary (primitive proposition) or simply proposition.

→ primitive proposition can't be subdivided further.

(2) Molecular or composite or compound proposition :-

→ A proposition obtained from the combination of 2 or more propositions by means of logical operators or connectives of 2 or more propositions or by negating the a single proposition is referred to molecular or composite or compound proposition.

Connectives :- The words or phrases or symbols used to form compound proposition are called connectives.

- Types of connectives :-

→ There are 5 basic connectives called :-

(i) Negation :- ($\sim$) not

(ii) Conjunction :- ($\wedge$, and)

(22)

Disjunction :- ($\vee$, or)

(2v)

Implication or conditional :- ($\rightarrow$ or $\Rightarrow$)

(v)

Equivalence or biconditional :- ($\leftrightarrow$ or $\Leftrightarrow$) $\downarrow$ or double implication $\rightarrow$ if ... then $\Leftrightarrow$ if and only if.

(222)

(i)

Negation :- If p is any proposition, the negation of p , denoted by $\sim p$ or not p EX :- All students are intelligent.Ans :- $\sim p =$ (1) Truth table :-For negation

p	$\sim p$
T	F
F	T

(22)

(2) Conjunction (and) :-Conjunction of 2 statements p & q is denoted by $p \wedge q$ and can have truth values if both p & q are true otherwise false.AXIOM :- (conjunction) $\rightarrow$ If both statements p & q are true, then their conjunction statement is true otherwise false.Truth table for conjunction :-

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

(iii) Disjunction (V or or) :-
 If p and q are proposition, then the ^{disjunction of} ~~proposition~~ p or q is denoted by $p \vee q$ and can have true value if any one of p and q ~~have~~ are true otherwise false.

Truth Table :-

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

• Definition of (Ring sum) $(p \oplus q)$ (exclusive or) :-

Ring sum :- If p and q are propositions then exclusive "or" of p and q is denoted by " $p \oplus q$ "

$\rightarrow$ It is defined as a proposition i.e. true when exactly one of p and q is true otherwise false.

Truth Table :- (Ring sum) :-

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

(iv) Implication or conditional :- ($\rightarrow, \Rightarrow$)

$\rightarrow$ If p and q are two proposition, then p implication q is denoted by $p \rightarrow q$ or $p \Rightarrow q$.

and it is defined as a proposition which is false only when p is true & q is false otherwise true.

$\hookrightarrow$ $\downarrow$
 Hypotheses. conclusion.

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Dt:- 12/02/24

(V) Double Implication or Biconditional :-

→ let p and q be any 2 propositions, then double implication or biconditional then p and q is denoted as $p \leftrightarrow q$ or $p \Leftrightarrow q$. and it is defined as true, when p and q have same truth values. otherwise false.

Truth Table :-

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

• converse, Inverse and contrapositive of a statement :-

If $S: p \leftrightarrow q$ is a statement, then,

(i) converse of S :-

If $p \leftrightarrow q$
then its converse is,
 $q \leftrightarrow p$.

(ii) Inverse of S :-

If $S: p \rightarrow q$ is a statement
then its Inverse is

$$\sim p \rightarrow \sim q$$

(iii) contrapositive of S :-

let $S: p \rightarrow q$ be a statement, then the contrapositive of S is $\boxed{\sim q \rightarrow \sim p}$

• Propositional Equivalence :-

→ If 2 propositions $p(p, q, \dots)$ and $q(p, q, r, \dots)$ where $p, q, \dots$ are propositional variables have the same truth values in every possible case, the propositions are called logically equivalent or propositional equivalent.

→ It is denoted by $p(p, q, \dots) \equiv q(p, q, \dots)$

• How to test propositional equivalence?

→ To test whether two proposition p & q are logically equivalent, the steps are followed :-

(i) Construct the TT for p .

(ii) Construct the TT for q using the same propositional variable.

(iii) Check each combinations of truth values of the propositional variables to see whether the value of p is the same as the Truth value of q .

→ If in each row, the truth value of p is the same, as the truth value of q . then p and q are logically equivalent.

• Tautology :-

→ If a composite statement (i.e 2 or more statements combined by means of connectives) is always true irrespective of the truthness of individual statement. then that composite statement is turned as a Tautology.

Truth table :-

p	q	$p \wedge q$	$\sim(p \wedge q)$	$\sim(p \wedge q) \vee q$
T	T	T	F	T
T	F	F	T	T
F	T	F	T	T
F	F	F	T	T

• predicates and Quantifiers :-

- The propositional equivalence doesn't allow us to represent many of the statements, that we use in mathematics, computer science and in our daily life
- However, predicate calculus is a generalisation of propositional calculus. It contains all the components of propositional calculus along with the propositional variable constants.

• predicates :-

- There are some type of statements which are neither true nor false unless or until the values of variables are specified.

• EX :- $x > 30 \rightarrow x$ is greater than 30.

$$x + y = 5$$
$$\Rightarrow 3x + 2y = 72.$$

In the above three statements, it is impossible to judge the truthness of the statements unless we specify the values of the variables for which we denote.

$P(x) : x > 30$, then $P(31)$ and $P(35)$

$x = 31$, $P(31) : 31 > 30$ (True)

$x = 35$, $P(35) : 35 > 30$ (True)

But, $x = 29$, $P(29) : 29 > 30$ (False)

$x = 28$, $P(28) : 28 > 30$ (False)

- The statements x is greater than 30 has 2 parts, where ^{the} first part is the variable x and the second part is greater than 30.
- So the second part is otherwise termed as predicate. It is denoted by 'P'

(Q) If $Q(x, y) : x + y = 5$, what are the truth values of the proposition $Q(1, 2)$ and $Q(4, 1)$?

Ans

Given that $Q(x, y) : x + y = 5$

then, if we set $x = 1$ and $y = 2$ in above predicate of 2 variables, we get,

$$Q(1, 2) : 1 + 2 = 5 \text{ (which is false)}$$

Again, if we set $x = 4$, $y = 1$ in the above predicate of 2 variables,

we get,

$$4+1=5 \text{ (which is true)}$$

(Q) let X be the set of integers be the inverse of discourse and consider the statement :

$$\forall n \in \mathbb{Z}, n^2 = n$$

$$(\exists n \in \mathbb{Z}), n^2 = n$$

find the truth value of each of the statements .

Ans let $p(n)$ be the proposition $n^2 = n$

Then $\forall n, p(n)$ is false because $p(3) : 3^2 = 3$ (false)

and $\exists n, p(n)$ is true, because atleast one proposition $p(n)$ is true .

In fact, exactly two of them are true

namely $p(0)$ and $p(1)$

Dt 8-19/04/24

Problem-1

Indirect Method :-

Proof by contradiction

(Q) To prove $\sqrt{2}$ is an irrational number.

Ans Proof - Let $\sqrt{2}$ is a rational number.

We will show that this leads to contradiction.

Let $\sqrt{2} = \frac{p}{q}$ where $p, q \in \mathbb{Z}$ and p and q are coprime and $q \neq 0$

Squaring both sides, $2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2$ — (i)

$\Rightarrow p^2$ is even

$\Rightarrow p$ is even.

Let $p = 2m, m \in \mathbb{Z}$.

$\Rightarrow p^2 = 4m^2$ — (ii)

From eqn (i) and (ii), we have

$$2q^2 = 4m^2$$

$$\Rightarrow q^2 = \frac{4m^2}{2} = 2m^2$$

$\Rightarrow q^2$ is even.

$\Rightarrow q$ is even

Since p and q are both even,

they have a common factor '2' which is the contradiction to our assumption that p & q have no common factor other than 1 i.e. $\gcd(p, q) = 1$
 $\downarrow$
 coprime.

So $\sqrt{2}$ is an irrational no.

Hence proved

Some important terms :-

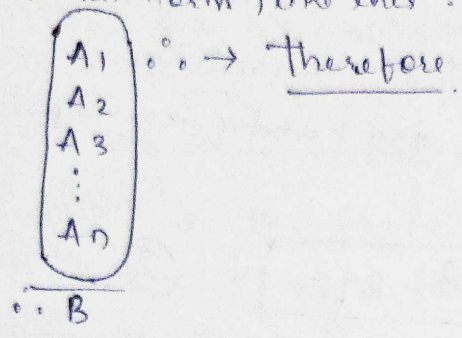
(1) Premises :- An argument is a finite collection of statements $A_1, A_2, A_3, \dots, A_n$ called premises or Hypothesis

$\rightarrow$ followed by a statement B called conclusion.

$\swarrow P \rightarrow q$
Hypothesis $\downarrow$ conclusion.

• validity proposition :- such an argument is valid if whenever $A_1, A_2, A_3 \dots A_n$ are all true (tautology) after that we can say it as a validity statement / proposition.

→ It is even often convenient to write an elementary argument in column form, like this.



(Q) Problem-1 :- Determine the following argument is valid

- Stated
- A₁ - If I like Biology, then I will study it.
 - A₂ - Either I study Biology, or I fail the course.
 - A₃ - If I fail the course, then I do not like Biology.

Ans

let p be the statement $\Rightarrow p$: I like Biology
 let q be another statement, q : I will study Biology.
 r : I fail the course.

In the symbol of argument, we have to check

$$\begin{array}{l} p \rightarrow q \\ q \vee r \\ \hline r \rightarrow (\sim p) \\ \quad \downarrow \\ \quad (\sim p) \end{array}$$

p	q	r	$p \rightarrow q$	$q \vee r$	$\sim p$	$r \rightarrow (\sim p)$
T	T	T	T	T	F	T
T	T	F	T	T	F	T
T	F	T	F	T	F	F
T	F	F	F	F	F	T
F	T	T	T	T	T	F
F	T	F	T	T	T	T
F	F	T	T	T	T	F
F	F	F	T	F	T	T

P	q	$\neg p$	$p \rightarrow q$	$q \vee \neg p$	$\sim p$	$p \rightarrow (\sim p)$
T	T	F	T	T	F	T
T	F	T	F	T	F	F
F	T	F	T	T	T	F
F	F	T	T	T	T	T
T	T	F	T	T	F	T
T	F	T	F	T	F	T
F	T	F	T	T	T	T
F	F	T	T	T	T	T

→ Invalid.

If all the truth values are true then it is valid. otherwise Invalid statement.

Dt :- 20/04/24

• Rules of Inference :-

① Modus ponens OR (Modus ponens - Mode that affirms)

Law of Detachment

$$\begin{array}{c} p \\ p \rightarrow q \\ \hline \therefore q \end{array} \rightarrow \text{Formula of Modus ponens.}$$

∴ corresponding Tautology :- $(p \wedge (p \rightarrow q)) \rightarrow q$
we can write this also

Proof using Truth Table :- Tautology

P	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	$(p \wedge (p \rightarrow q)) \rightarrow q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Example :- let P: "It is snowing".
q: "I will study discrete Mathematics".

It is snowing, then I will study discrete Mathematics.

"∴ it is snowing" $\xrightarrow{\quad}$
$$\begin{array}{c} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

Therefore, I will study DM.

②

Modus Tollens :-

$$\begin{array}{l} \neg q \text{ or } \neg q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

Corresponding Tautology :-

$$((\neg q) \wedge (p \rightarrow q)) \Rightarrow (\neg p)$$

Example :-

Let p : "It is snowing"

q : "I will study DM".

$p \rightarrow q \rightarrow$ If it is snowing, then I will study DM

$\neg q \rightarrow$ I will not study DM.

$\therefore$ It is not snowing.

$\therefore$ Therefore,

$$\begin{array}{l} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$$

③

Hypothetical Syllogism :-

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$$

Corresponding Tautology :-

$$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$$

Example :-

Let p : "It snows"

q : "I will study DM"

r : "I will get an A"

$p \rightarrow q \rightarrow$ If it snows, then I will study DM.

$q \rightarrow r \rightarrow$ If I study DM, then I will get an A.

~~Therefore~~

If it snows, I will get an A.

(4)

Disjunctive syllogism :-
or

Disjunction Elimination :-

$$\frac{\text{Formula} - \begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}}{\text{Proof :-}}$$

Corresponding Tautology

$$\boxed{((p \vee q) \wedge (\neg p)) \rightarrow q}$$

Example -

let p :-

"I will study DM"

let q :-

"I will study EL"

$p \vee q$ = "I will DM or I will study EL"

$\neg p$ = "I will not study DM"

$\therefore$ I will study EL.

P	q	$\neg p$	$p \vee q$	$(p \vee q) \wedge (\neg p)$	$(p \vee q) \wedge (\neg p) \rightarrow q$
T	T	F	T	F	T
T	F	F	T	F	T
F	T	T	T	T	T
F	F	T	F	F	T

(5)

Addition :-

$$\boxed{\frac{p}{\therefore p \vee q}}$$

Corresponding Tautology

$$\boxed{p \rightarrow (p \vee q)}$$

Example :-

let p : "I will study DM".

let q : "I will visit Kanark Temple".

Ans - P : "I will study DM".

$p \vee q$: "I will study DM" or I will visit Kanark Temple"

(6)

Simplification :-

or

Conjunction Elimination :-

Corresponding Tautology

$$\boxed{\frac{p \wedge q}{p}}$$

$$\boxed{(p \wedge q) \rightarrow p}$$

TT for addition

P	q	$P \vee q$	$P \rightarrow q$ $P \vee q$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

TT for simplification :-

P	q	$P \wedge q$	$P \wedge q \rightarrow P$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

Example :- Let p : "I will study DM"
 q : "I will study EL".

$p \wedge q$: "I will study DM and I will study EL".

or
 "I will study DM or EL"

$\therefore$ Therefore p is true.

(7) conjunction :-

P
q
$\therefore P \wedge q$

$$(P) \wedge (q) \rightarrow (P \wedge q)$$

Truth table

P	Q	(P)^(Q)	$(P) \wedge (Q) \rightarrow (P \vee Q)$	$P \vee Q$
T	T	T	T	T
T	F	F	T	T
F	T	F	T	T
F	F	F	T	T

- (8) Resolution :- Resolution plays an important role in AI and is used in the programming language. (prolog)
 → DM is applicable there.

formula :-

$$\begin{array}{l} P \vee Q \\ \neg P \vee R \\ \hline \therefore Q \vee R \end{array}$$

Corresponding Tautology

$$(P \vee Q) \wedge (\neg P \vee R) \rightarrow (Q \vee R)$$

Truth table

P	Q	R	$\neg P$	$P \vee Q$	$\neg P \vee R$	$(P \vee Q) \wedge (\neg P \vee R)$	$Q \vee R$	$(P \vee Q) \vee (\neg P \vee R) \rightarrow (Q \vee R)$
T	T	T	F	T	T	T	T	T
T	F	T	F	T	T	T	T	T
F	T	T	T	T	T	T	T	T
F	F	T	T	F	T	F	T	T
T	T	F	F	T	F	F	T	T
T	F	F	F	T	F	F	F	T
F	T	F	T	T	T	T	T	T
F	F	F	T	F	T	F	F	T

Example :-

Let P: "I will study DM".

Let Q: "I will study DataBases".

Let R: "I will study EL".

Let $P \vee Q$: "I will study DM or I will study DBs. → T or T
 Let $\neg P \vee R$: "I will not study DM or I will study EL". → F or T

∴ $Q \vee R$ true

Tautology

Both T.

Proof by cases :-

(1) Disjunction elimination

Formula

$$\begin{array}{l} p \rightarrow q \\ r \rightarrow q \\ p \vee r \\ \hline \therefore q \end{array}$$

$$(p \rightarrow q) \wedge (r \rightarrow q) \wedge (p \vee r) \rightarrow q$$

By Truth Table

p	q	r	$p \rightarrow q$	$r \rightarrow q$	$p \vee r$	$(p \rightarrow q) \wedge (r \rightarrow q) \wedge (p \vee r)$	$\wedge (p \vee r) \rightarrow q$
T	T	T	T	T	T	T	T
T	F	T	F	F	T	F	T
F	T	T	T	T	T	T	T
F	F	T	T	F	T	F	T
T	T	F	T	T	T	T	T
T	F	F	F	T	T	F	T
F	T	F	T	T	F	F	T
F	F	F	T	T	F	F	T
T	T	T	T	T	T	T	T
T	F	T	F	F	T	F	T
F	T	T	T	T	T	T	T
F	F	T	T	F	T	F	T
T	T	F	T	T	T	T	T
T	F	F	F	T	T	F	T
F	T	F	T	T	F	F	T
F	F	F	T	T	F	F	T

Ex :- let p : "I will study DM"
 let q : "I will study CS"
 let r : "I will study DBS"

Ans
 $p \rightarrow q$: "If I will study DM then I will study CS"
 $r \rightarrow q$: "If I will study DBS then I will study CS"
 $p \vee r$: "I will study DM or I will study DBS"

$\therefore$ Therefore I will study CS.
 $\downarrow$
 q .

(2) Constructive :- It is also called disjunction of Modus ponens

↳ DILEMA

$$\begin{array}{l} p \rightarrow q \\ r \rightarrow s \\ p \vee r \\ \hline \therefore q \vee s \end{array}$$

Corresponding Tautology

$$(p \rightarrow q) \wedge (r \rightarrow s) \wedge (p \vee r) \rightarrow (q \vee s)$$

p	q	r	s	$p \rightarrow q$	$r \rightarrow s$	$p \vee r$	$q \vee s$	$(p \rightarrow q) \wedge (r \rightarrow s) \wedge (p \vee r) \rightarrow (q \vee s)$
T	T	T	T	T	T	T	T	T
T	F	T	T	F	T	T	F	T
F	T	T	T	T	T	T	T	T
F	F	T	T	T	T	T	F	T
T	T	F	T	T	T	T	T	T
T	F	F	T	F	T	T	F	T
F	T	F	T	T	T	F	T	T
F	F	F	T	T	T	F	F	T
T	T	T	F	T	F	T	T	T
T	F	T	F	F	F	T	F	T
F	T	T	F	T	F	T	T	T
F	F	T	F	T	F	T	F	T
T	T	F	F	T	T	T	T	T
T	F	F	F	F	T	T	F	T
F	T	F	F	T	T	F	T	T
F	F	F	F	T	T	F	F	T

• Important Example :-

Let p : "I will study DM"

q : "I will study CS"

r : "I will study protein structure"

s : "I will study Biochemistry"

$p \rightarrow q$: "If I will study DM, then I will study CS"

$r \rightarrow s$: "If I will study PS, then I will study Biochemistry"

$p \vee r$: "I will study DM or I will study P.S"

$\therefore q \vee s$: I will study CS or I will study Biochemistry.

→ It is constructive dilemma.

(4) Absorption -
$$\frac{p \rightarrow q}{\therefore p \rightarrow (p \wedge q)}$$

Corresponding Tautology

$$(p \rightarrow q) \rightarrow (p \rightarrow (p \wedge q))$$

Truth Table :-

P	Q	$P \rightarrow Q$	$P \wedge Q$	$P \rightarrow (P \wedge Q)$	$(P \rightarrow Q) \rightarrow (P \rightarrow (P \wedge Q))$
T	T	T	T	T	T
T	F	F	F	F	T
F	T	T	F	T	T
F	F	T	F	T	T

Example :-

let p : "I will study DM".

let q : "I will study CS".

$P \rightarrow Q$: "If I will study DM, then I will study CS"

$P \wedge Q$: "I will study DM and I will study CS."

$(P \rightarrow (P \wedge Q))$: - "If I will study DM then I will study CS."

Module 1
completed

Example of Destructive Dilemma:-

let p : "I will study DM"

q : "I will study CS"

r : "I will study PS".

s : "I will study Biochemistry".

$P \rightarrow Q$: "If I will study DM then I will study CS"

$r \rightarrow s$: "If I will study PS then I will study Biochemistry"

$\neg Q \vee \neg S$: "I will not study CS or I will not study Biochemistry"

$\therefore$ "Therefore I will not study DM or I will not study PS"

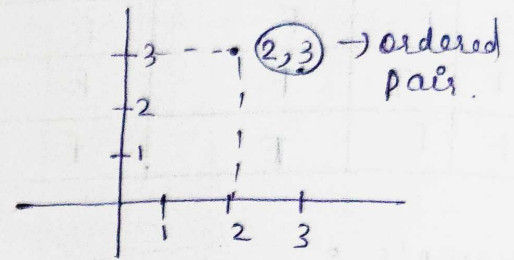
• Cartesian product of 2 sets :-

→ Let A & B be two sets, then, cartesian product of A & B is denoted as $A \times B$

→ It is defined as,

$$A \times B = \{ (x, y) : x \in A \text{ and } y \in B \}$$

↓
ordered pair



① Remark :-

Ordered pair -

$(a, b) \rightarrow$ 2nd element
↓
(y-coordinate)

1st
Element
(x-coordinate)

② Remark :- In general $(a, b) \neq (b, a)$

but,

$$(a, b) = (b, a) \text{ if } \boxed{a = b}$$

1Q Example :-

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

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

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

Cardinality.
↓

no of elements
Present in a set.

$$|A| = n(A)$$

2Q Example :- $A = \{1, 2, 3\}$

$$B = \{1, 2\}$$

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

$(1, 2) \neq (2, 1)$

$(1, 1) \neq (1, 1)$ It is same
so can be written
in this way.

Remark :-

$$\text{If } |A| = m$$

$$|B| = n$$

Then $|A \times B| = mn$

$$\Rightarrow \boxed{|A \times B| = |A| \cdot |B| = mn}$$

Example :- If $|A| = 2$
 $|B| = 3$

Then $|A \times B| = 6$

Relation :- let A & B be two sets

Cartesian product.

A relation from A to B is a subset of $A \times B$, i.e. $R \subseteq A \times B$

→ Suppose R is a relation from A to B then R is a set of ordered pairs (a, b) where $a \in A$ and $b \in B$.

→ Every such ordered pair is written as :- $a R b$ → read as " a is related to b by R ".

→ If $(a, b) \notin R$ then " a is not related to b by R " and is written as $a \not R b$

(Ex) :- $A = \{a, b, c\}$
 $B = \{1, 2\}$

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

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

$$R_2 = \{(a, 2), (b, 1), (b, 2), (c, 1)\}$$

$$R_3 = \{(2, a), (b, 1), (b, 2)\}$$

$$R_4 = \{(a, 2), (a, 1)\}$$

$$R_5 = \{(a, 3), (2, b)\}$$

$$R_6 = \{(a, 1), (b, 1), (a, 2), (b, 2), (c, 1), (c, 2)\}$$

→ $R_1 \subseteq A \times B \therefore R_1$ is a relation from A to B .

→ $R_2 \subseteq A \times B$

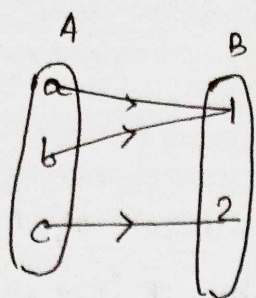
→ R_3 is not a relation from $A \times B$. bcz $(2, a) \notin A \times B$.

→ R_4 is a relation from $A \times B$

→ R_5 is not a relation from $A \times B \rightarrow$ so it is known as empty relation

→ R_6 is a relation from $A \times B$. $\phi \rightarrow$ universal set

Arrow Diagram :-



$$R : A \rightarrow B$$

R is a relation from A to B .

Types of relation :-

- (1) Empty relation
 - (2) universal relation
 - (3) ~~one-one relation~~ Binary relation
 - (4) composite relation
 - (5) one-one relation
 - (6) one-many relation
 - (7) many-one relation
 - (8) many-many relation
 - (9) Reflexive relation
 - (10) Symmetric relation
 - (11) Transitive relation
 - (12) Equivalence relation
 - (13) Anti-symmetric relation
 - (14) partial-ordering relation
 - (15) congruence modulo relation
- Suppose,
 $R = \{(a, 1), (b, 2), (c, 3)\}$
 $\downarrow$ $\downarrow$
 domain range.

Equivalence relation

D-1 :- 27/02/24

Reflexive Relation :-

$$\forall a \in A \Rightarrow (a, a) \in R.$$

Example :- $A = \{a, b, c\}$.

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

$$R_1 = \{(a, a), (c, c)\} \rightarrow R_1 \text{ is not reflexive}$$

(10) Symmetric Relation :-

For $a, b \in A$, $(a, b) \in R \Rightarrow (b, a) \in R$.

Example :-

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

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

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

$\hookrightarrow$ Symmetric.

(11) Transitive relation :-

For $a, b, c \in A$, $\boxed{(a,b) \in R \text{ and } (b,c) \in R \Rightarrow (a,c) \in R}$.

EX :-

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

$$R = \{(1,2), (2,1), (1,1)\} \rightarrow \text{this is Transitive.}$$

(13) Anti-symmetric Relation

$\rightarrow$ A relation R on a set A , is said to be anti-symmetric relation if $\boxed{(a,b) \in R \text{ and } (b,a) \in R \Rightarrow a = b}$

Example :-

① $R = \{(m, y) \in \mathbb{R}^2 ; m \leq y\}$ is anti-symmetric relation on R .

Justify -

Since we know that,

$$m < y \text{ and } y < m.$$

$$\text{Then } \underline{m = y}.$$

$$\{ \Rightarrow (m, y) \in R \text{ \& } (y, m) \in R \Rightarrow m = y \}.$$

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

Example 2 -

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

$$(1,2) \in R, (2,1) \in R \Rightarrow 1 \neq 2$$

(12) Equivalence relation :-

→ A relation on a set A is said to be equivalence if which satisfies all the three relation :-
(i) Reflexive
(ii) Symmetric
(iii) Transitive.

Example :-

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

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

All three relations are present.

• Remark :- Equality is an equivalence relation on any set which is the smallest equivalence relation.

(ii) Identity relation is also an equivalence relation.

(iii) If $R = A \times A$ then universal relation is an equivalence relation on set A which is the largest equivalence relation.

(15) Congruence modulo relation :-

→ If $(a, b) \in \mathbb{Z}$ and m be a positive integer then a is congruent to b , modulo m if $(a - b)$ is divisible by m i.e. m divides $(a - b)$.

→ Symbolically representation : $m \mid (a - b)$

→ Congruence modulo relation is denoted as $a \equiv b \pmod{m}$

→ If $a \equiv b \pmod{m}$.

$$\boxed{\Rightarrow m \mid (a - b)} \text{ read as } m \text{ divides } (a - b)$$

or

$(a - b)$ is divisible by m .

→ In other way, it is defined as $\underbrace{a - b}_{\text{Imp}} = \underbrace{mk}_{\text{Imp}}$ where $k \in \mathbb{Z}$.

Example

$$27 \equiv 7 \pmod{10}$$

$$\Rightarrow (27 - 7) = 20 \text{ is divisible by } 10,$$

Ex:- $1 \equiv 9 \pmod{4}$

$$1 - 9 = -8$$

now -8 is divisible by 4

Remark:

$$(1) a \equiv b \pmod{m}$$

$$(2) b \equiv a \pmod{m}$$

$$(3) a \not\equiv b \pmod{m}$$

Read as 'a is congruent to b mod m'.

Important

→ The relation congruence modulo m is an equivalent relation in the set of integers.

Proof this -

Ans (i) Reflexive - By definition of reflexive relation we have
 (a, a) element $\in R \forall a \in A$.

So, $a - a = 0$ which is divisible by m .

$$\Rightarrow a - a = n \cdot 0, 0 \in \mathbb{Z}$$

$$\Rightarrow a \equiv a \pmod{n} \quad a - b = nk, k \in \mathbb{Z}.$$

$$\Rightarrow a \equiv b \pmod{n}.$$

$\therefore$ The ^{congruence} relation is reflexive.

(ii) Symmetric - According to definition,

$$a, b \in A$$

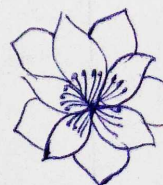
$$(a, b) \in R \Rightarrow a \equiv b \pmod{n}$$

$$\Rightarrow n \mid (a - b) \Rightarrow n \mid -(b - a)$$

$$\therefore a R b \Rightarrow b R a$$

$$\Rightarrow n \mid (b - a).$$

The congruence relation is symmetric $\Rightarrow b \equiv a \pmod{n}.$



(iii) Transitive -

$$a, b, c \in \mathbb{Z}$$

$$\text{if } (a, b) \in R \Rightarrow a \equiv b \pmod{n}.$$

$$\Rightarrow n \mid (a-b).$$

$$\Rightarrow \boxed{a-b = nk_1} \text{ where } k_1 \in \mathbb{Z}. \quad \textcircled{1}$$

$$\text{let } (b, c) \in R \Rightarrow b \equiv c \pmod{n}$$

$$\Rightarrow n \mid (b-c)$$

$$\Rightarrow \boxed{b-c = nk_2} \text{ where } k_2 \in \mathbb{Z}. \quad \textcircled{2}$$

Adding eqn $\textcircled{1}$ & $\textcircled{2}$

$$(a-b) = nk_1$$

$$+ (b-c) = nk_2$$

$$(a-b) + (b-c) = nk_1 + nk_2$$

$$a - \cancel{b} + \cancel{b} - c = nk_1 + nk_2$$

$$\Rightarrow \boxed{a-c = n(k_1+k_2)} \text{ — where } k_1 \& k_2 \in \mathbb{Z} \text{ so, } (k_1+k_2) \text{ is also element of } \mathbb{Z}$$

$$\Rightarrow \boxed{a-c = nk} \text{ where}$$

$$\Rightarrow n \mid (a-c) \quad \boxed{k = k_1+k_2 \in \mathbb{Z}}$$

$$\Rightarrow \boxed{a \equiv b \pmod{n}} \therefore \text{The congruence relation } \mathcal{R} \text{ is Transitive.}$$

Thus, for $n > 1$, congruence modulo n is an equivalence relation on set of integers ($\mathbb{Z}$)

HENCE PROVED

• Equivalence class / congruence class :-

∩

→ congruence class :-

The equivalence classes of congruence mod n are called congruence classes.

→ The congruence class of mod n of an integer n is the set of all integers ^{to} which a is congruent mod n .

Equivalence class :- It is denoted as $[ai]$ where $i = 1, 2, 3, \dots, n$.

(Q) Find equivalence classes of 4? on set $\mathbb{Z}$.

Ans If a no is divisible by 4, then remainders are, 0, 1, 2, 3

$$[0]_4 = \{ \dots, -12, -8, -4, 0, 4, 8, 12, \dots \}$$

$$[1]_4 = \{ \dots, -7, -3, 1, 5, 9, 13, \dots \}$$

$$[2]_4 = \{ \dots, -10, -6, -2, 2, 6, 10, 14, \dots \}$$

$$[3]_4 = \{ \dots, -9, -5, -1, 3, 7, 11, 15, \dots \}$$

$$\therefore [0]_4 \cup [1]_4 \cup [2]_4 \cup [3]_4$$

$$= \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$$

$$= \mathbb{Z} \rightarrow \text{all integers}$$

↓

Ans

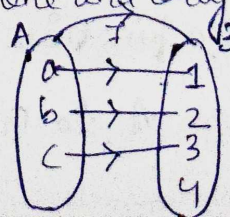
FUNCTION

• function :- A relation 'f' from A to B is said to be a function if it satisfies the following conditions :-

(i) domain $f = A$.

(ii) Each domain has one and only one image in set B.

Example :-



⇒ Arrow diagram.

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

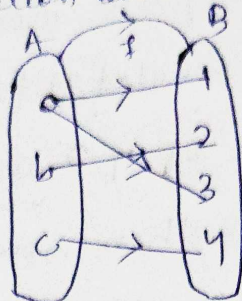
$$(i) \text{ domain } f = \{a, b, c\} = A$$

(ii) Each element has one and only image in set B.

• Remark :-

→ Every function is a relation but every relation need not be a function.

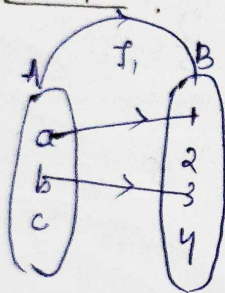
Example



$\therefore f_1$ is a relation but not function.

Dt :- 9/08/24

(1)



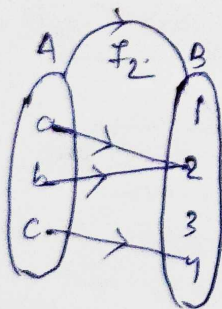
1 is the image of a

3 is the image of b.

$$\text{dom } f_1 = \{a, b\} \neq A$$

$\therefore f_1$ is a relation but not a function.

(2)

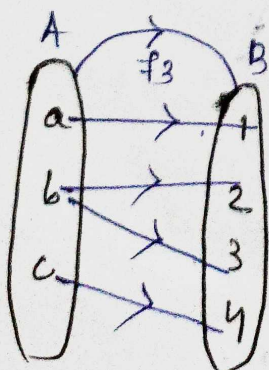


$$(i) \text{ dom } f_2 = \{a, b, c\}$$

(ii) $\therefore f_2$ is a function.

Remark -

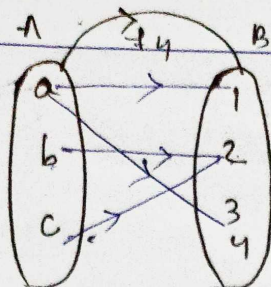
Every function is a relation but every relation need not be a function.



$$(i) \text{ domain } f_3 = \{a, b, c\}$$

(ii) $\therefore f_3$ is not a function but it is a relation from A to B.

(4)



$$\therefore \text{dom } f = \{a, b, c\}$$

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

f is not a function but a relation.

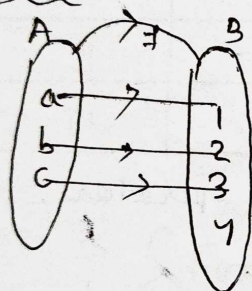
Types of Function :-

- (1) One-one function / Injective function / Injection function.
- (2) Many one function.
- (3) Surjective function (onto function) / Surjection
- (4) Bijective function (one-one and onto function) // Bijection.

(1) One-one function or Injective function :-

$\rightarrow$ A function $f: A \rightarrow B$ is said to be injective if $f(x) = f(y) \Rightarrow x = y$.

Example -



$\rightarrow$ one-one function.

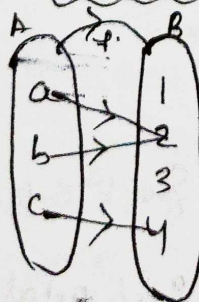
$$\therefore f = \{(a, 1), (b, 2), (c, 3)\}$$

1 is the image of a.

2 is the image of b.

3 is the image of c.

(2) Manyone function :-

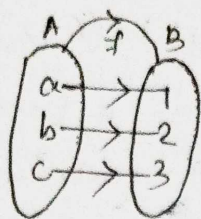


$\rightarrow$ manyone function.

(3) Surjective Function :-

$\rightarrow$ A function $f: A \rightarrow B$ is said to be surjective if all element of set B are the image of atleast one element of set A.
(Range of ~~func~~ set B = codomain)

Example -



→ onto function.

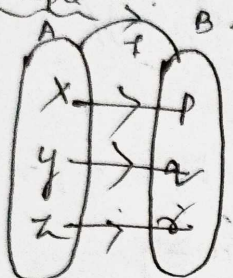
→ It is also an example of Bijective function.

(4)

Bijective Function :-

→ A function is said to be $f: A \rightarrow B$ Bijective if it is one-one and onto function.

Example -



Bijective function.

Binary relation -

Bi means 2.

$$2 \times 4 = 8$$

$$4 - 2 = 2$$

$$2 + 4 = 6$$

$$4 \div 2 = 2$$

These are Binary operators.

$$2 * 4 = \underline{2}$$

$$2 \circ 4 = \underline{\quad}$$

$$2 \square 4 = \underline{\quad}$$

$$2 \Delta 4 = \underline{12}$$

$$f: A \rightarrow B$$

$$f: R \rightarrow R \text{ if } \boxed{a * b = \frac{ab}{4}} \text{ where } \{a, b \in R\}.$$

To prove associative law of Binary operation / Relation :-

$$\text{i.e. } \boxed{a * (b * c) = (a * b) * c}$$

where, $a, b, c \in R$.

$R: R \rightarrow R$ where

$$a * b = \frac{ab}{4} \rightarrow \text{Binary relation}$$

LHS

$$\begin{aligned} a * (b * c) \\ = a * \frac{bc}{4} \\ = \frac{abc}{\frac{4}{4}} = \frac{abc}{16} \end{aligned}$$

RHS

$$\begin{aligned} (a * b) * c \\ = \left(\frac{ab}{4} \right) * c \\ = \frac{\frac{ab}{4}c}{\frac{4}{4}} = \frac{abc}{16} \end{aligned}$$

Hence
LHS = RHS
Hence
proved

For this we have to draw a table.

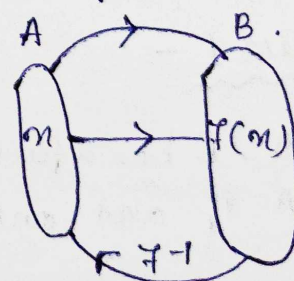
Δ	1	2	3	4	5
1	3	5	7	9	11
2	5	8	11	14	17
3	7	11	15	19	23
4	9	14	19	24	29
5	11	17	23	29	35

$$\{ \text{Formula :- } x \Delta y = x + y + xy \}$$

Dt :- 11/03/24.

- Invertible Functions :- A function $f: A \rightarrow B$ is invertible if its relation f^{-1} is also a function from the range of f into A .

$$\begin{aligned} \text{i.e. if } f: A \rightarrow B \\ \text{Then } f^{-1}: B \rightarrow A \end{aligned}$$



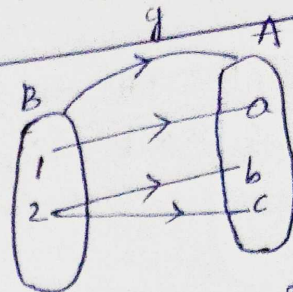
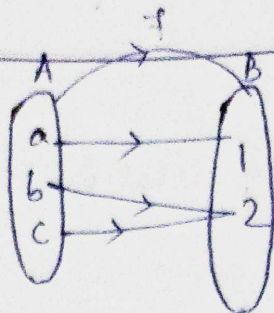
f^{-1} is possible
when it is
bijective

Ex :- Let $A = \{a, b, c\}$

$$B = \{1, 2\}$$

$$f: \{(a, 1), (b, 2), (c, 2)\}$$

$$g: \{(1, a), (2, b), (2, c)\}$$



$\Rightarrow g$ is not a function.

Example -

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

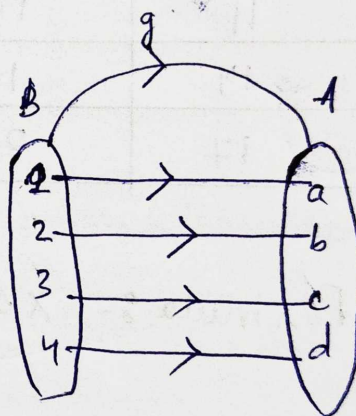
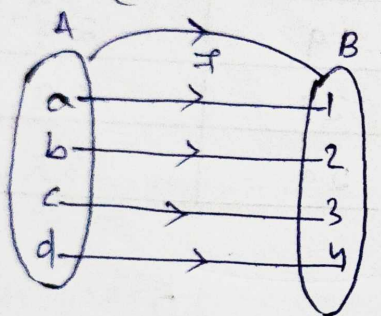
$B = \{1, 2, 3, 4\}$

$f: A \rightarrow B$

$f = \{(a, 1), (b, 2), (c, 3), (d, 4)\}$

$g: B \rightarrow A$

$g = \{(1, a), (2, b), (3, c), (4, d)\}$



$\therefore g$ is the inverse of f .

It is denoted as $\boxed{g = f^{-1}}$.

Theorem 1 -

$\rightarrow$ Let $f: A \rightarrow B$ be a function. Then f^{-1} is a function from range of f to A if and only if f is (one to one & onto) or bijective.

Theorem 2 -

$\rightarrow$ Let f be one-one and onto, function from A to B . Then,

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

Theorem-3 -

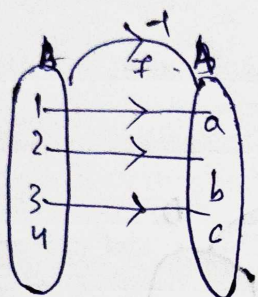
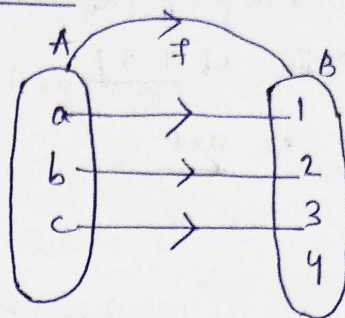
→ Let f be one to one function from A into B . Then f^{-1} is a function from B into A if and only if f is onto.

Example -

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

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

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



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

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

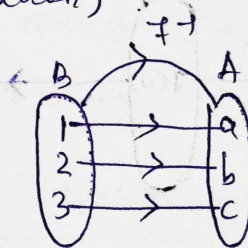
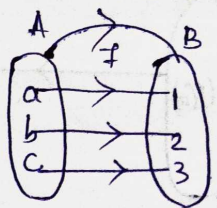
$$f = \{(a, 1), (b, 2), (c, 3)\}$$

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

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

f^{-1} is not a function

(f^{-1} is a relation)



Theorem:-

→ The inverse of an one-one and onto function is one to one and onto function (Bijective).

Compositions of Functions:-

Let A, B, C are 3 sets

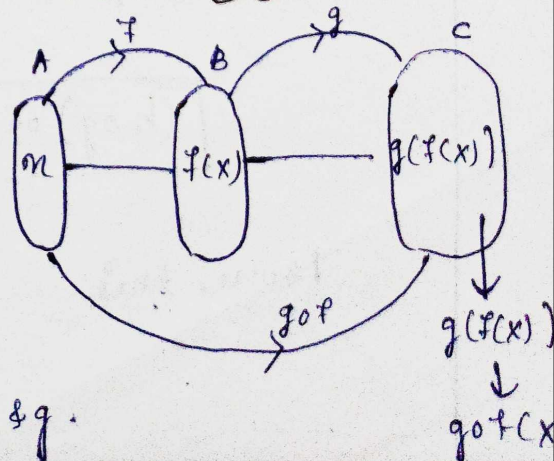
Let $f: A \rightarrow B$ and $g: B \rightarrow C$, then

$$g \circ f: A \rightarrow C$$

→ composite function.

∴ $g \circ f$ is the composite function of f & g .

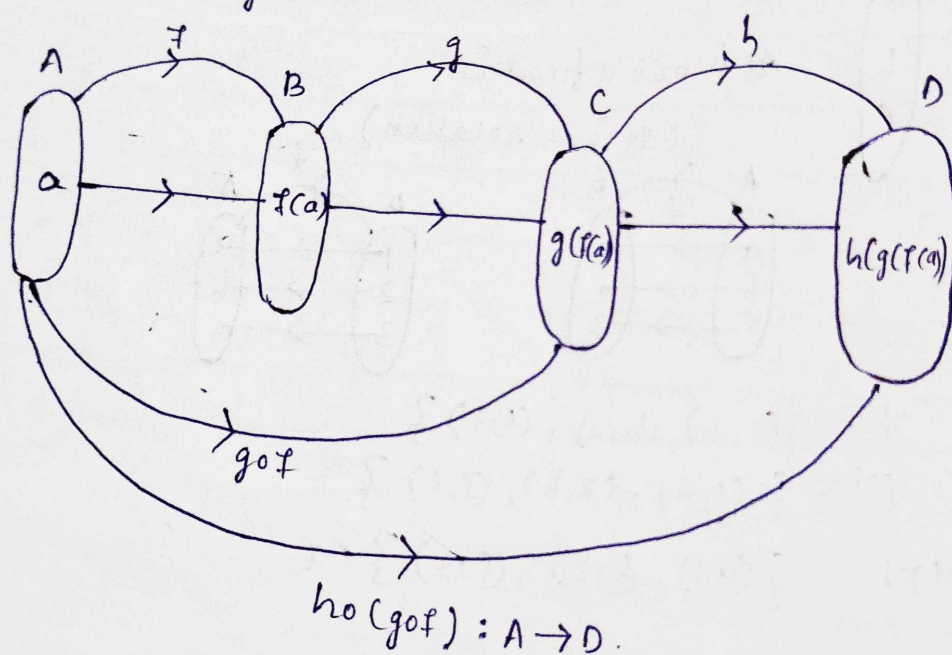
Arrow diagram -



- Definition - $f: A \rightarrow B$
 → let f is a function from A to B and $g: B \rightarrow C$. then the function $g \circ f: A \rightarrow C$ defined by $(g \circ f)(a) = g(f(a))$ where, $a \in A$ is called the composition of f & g .
 → It is denoted as $g \circ f$

• Remark -

let $F: A \rightarrow B$, $g: B \rightarrow C$, $h: C \rightarrow D$
 then $g \circ f: A \rightarrow C$
 $h \circ (g \circ f): A \rightarrow D$.



• Associative law of composition of Functions :-

let $f: A \rightarrow B$, $g: B \rightarrow C$ and $h: C \rightarrow D$.

then,

$$(h \circ g) \circ f = h \circ (g \circ f)$$

Prove this

Proof - let $x \in A$.

$$\begin{aligned}\text{L.H.S} - ((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) \\ &= h(g(f(x))) \\ &= h \circ g f(x)\end{aligned}$$

$$\begin{aligned}\text{R.H.S} - h \circ (g \circ f)(x) &= h \circ (g(f(x))) \\ &= h(g(f(x))) \\ &= h \circ g f(x)\end{aligned}$$

$$\therefore \text{L.H.S} = \text{R.H.S}$$

Hence proved.

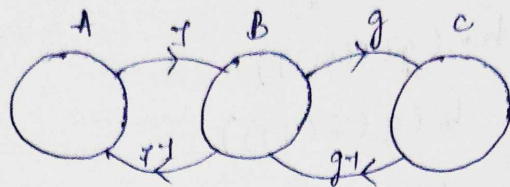
Remark - We can write $h \circ g \circ f$: From A to D without any parenthesis

DT :- 12/03/24

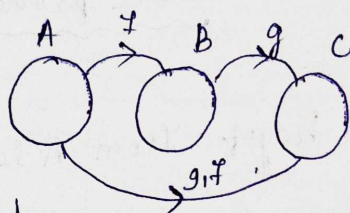
Prob-1 - VVIMPP

Let f be a function $f: A \rightarrow B$ and $g: B \rightarrow C$ be both one-to-one and onto function. Then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof -



As f and g both one-to-one and onto. So $g \circ f$ is also one-to-one and onto function from A to C.



$\therefore (g \circ f)^{-1}$ exists and onto mappings from C to A.

Let c be any element of 'C'

We have to show that

$$(g \circ f)^{-1}(c) = (f^{-1} \circ g^{-1})(c)$$

We have to prove this one,

$$\text{Let } (g \circ f)^{-1}(c) = a.$$

$$\Rightarrow (g \circ f)(a) = c \quad \text{--- (i)}$$

$$\Rightarrow f(f^{-1}(g^{-1}(c))) = c$$

$$\Rightarrow f(a) = g^{-1}(c)$$

$\therefore g^{-1}$ is invertible.

$$\Rightarrow a = f^{-1}(g^{-1}(c))$$

$$\Rightarrow a = (f^{-1} \circ g^{-1})(c) \quad \text{--- (ii)}$$

Since it is invertible.

From eqn (i) and (ii), we have,

$$(g \circ f)^{-1}(c) = (f^{-1} \circ g^{-1})(c) = a.$$

$$\Rightarrow (g \circ f)^{-1} = f^{-1} \circ g^{-1} \quad \text{Hence proved}$$

Closure of Relations :-

- Let R be the relation on set A , then R may or may not be some property ' P '. such as reflexivity, symmetric or transitivity.
- If there is a relation ' S ' with property ' P ' containing ' R ' such that ' S ' is a subset of every relation with ' P ' containing ' R '. Then ' S ' is called the closure of R with respect to P .

(i) Reflexive closure :- or w.r.t.

- The reflexive closure are represented as (R^r) of a relation R is the smallest reflexive relation that contains R as a subset.
- To find the reflexive closure, one has to know, what pairs have to be added to the relation to make it reflexive.

Thus, $R^r = R \cup I_A$

Suppose EX

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

$I_A = \text{Identity.}$
~~Main~~ element

$\cup I_A$?

$R^r = R \cup I_A =$

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

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

where, $I_A = \{(a, a); a \in A\}$.

which is the diagonal relation on Identity relation only.

(ii) Symmetric closure :-

- The symmetric closure that is $R^{(s)}$ is the smallest symmetric relation that contains R as a subset.
- A symmetric relation contains (x, y) if it contains (y, x) . since the inverse relation ~~is inverse~~ R^{-1} contains (y, x) if $(x, y) \in R$.
- A symmetric closure of a relation can be constructed by taking the union of R and R^{-1} . ($R \cup R^{-1}$)

$\therefore R^{(s)} = R \cup R^{-1}$ is the symmetric closure of R on set A

where, $R^{-1} = \{ (y, x) : \text{if } (x, y) \in R \text{ on set } A \}$.

EX:- If $R = \{ (1, 2), (4, 3), (2, 2), (2, 1), (3, 1) \}$

be a relation on $S = \{ 1, 2, 3, 4 \}$.

Find the symmetric closure.

Ans

Given that $S = \{ 1, 2, 3, 4 \}$

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

$R^{-1} = \{ (2, 1), (3, 4), (2, 2), (1, 2), (1, 3) \}$

$R \cup R^{-1} = \{ (1, 2), (4, 3), (2, 2), (2, 1), (3, 1), (3, 4), (1, 3) \}$

$\hookrightarrow R(S)$

It is a symmetric closure.

(iii) Transitivity Relation

The relation obtained by adding the list no of ordered pairs to ensure transitivity is called the transitive closure of the relation.

NOTE -

$\rightarrow$ It is denoted by $R(t)$

$\rightarrow$ Let R be a relation on set A . If A contains no of elements that is represented as,

R^m is represented as / all m pairs of elements.

So, A to relation,

It is defined as $R(t) = R \cup R^2 \cup R^3 \dots \cup R^m$.

• The matrix of a relation :-

→ let $A = \{a_1, a_2, a_3, \dots, a_n\} \rightarrow |A| = n$.

& $B = \{b_1, b_2, b_3, \dots, b_n\} \rightarrow |B| = n$.

are the finite sets containing m and n elements respectively and let R be a relation from A to B . ($R: A \rightarrow B$) then R can be represented by the $m \times n$ matrix.

ie -

$$M_R = [m_{ij}] \text{ where ,}$$

$$m_{ij} = \begin{cases} 1, & \text{if } (a_i, b_j) \in R. \\ 0, & \text{if } (a_i, b_j) \notin R. \end{cases}$$

The matrix M_R is called,

where $i = 1, 2, 3, \dots, m$

$j = 1, 2, 3, \dots, n$.

the Matrix of a relation

(Q) let R be the relation from set $A = \{1, 3, 4\}$ on itself. and defined by $R = \{(1, 1), (1, 3), (3, 3), (4, 4)\}$. Then the matrix R can be found as follows :-

Ans

let M_R be the Matrix of relation R , $R: A \rightarrow A$

$$A = \begin{matrix} & 1 & 3 & 4 \\ \begin{matrix} 1 \\ 3 \\ 4 \end{matrix} & \begin{matrix} | & | & | \\ \hline | & | & | \\ \hline | & | & | \end{matrix} \end{matrix}$$

Number of rows in M_R = Number of elements in $A = 3$.

Since the relation from the set A to itself, so the number of element or number of columns in M_R be 3.

So, M_R is 3×3 Matrix

We have the elements of A ,

$$\begin{matrix} a_1 = 1 & a_2 = 3 & a_3 = 4 \\ b_1 = 1 & b_2 = 3 & b_3 = 4 \end{matrix}$$

Since,

$1R1$, we have $m_{11} = 1$ as $(a_1, b_1) = (1, 1) = 1$.

$1R3$, we have $m_{12} = 1$ as $(a_1, b_2) = (1, 3) = 1$.

$3R3$, we have $m_{22} = 1$ as $(a_2, b_2) = (3, 3) = 1$.

$4R4$ $\Rightarrow$ we have $m_{33} = 1$ as $(a_3, b_3) = (4, 4) = 1$.

and all other elements of M_R are zeros -

M_R = The matrix of relation R that is defined in Matrix form

$$= \begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

(Q)

let $A = \{a_1, a_2, a_3\}$

$B = \{b_1, b_2, b_3, b_4\}$

which ordered pair are in the relation R represented by the matrix.

$$M_R = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} m_{11} & m_{12} & m_{13} & m_{14} \\ m_{21} & m_{22} & m_{23} & m_{24} \\ m_{31} & m_{32} & m_{33} & m_{34} \end{bmatrix}$$

Ans Since R contains of those ordered pairs (a_i, b_j) with $m_{ij} = 1$ so it follows that,

$$R = \left\{ (a_1, b_2), (a_1, b_3), (a_1, b_4), (a_2, b_1), (a_2, b_3), (a_2, b_4), (a_3, b_1), (a_3, b_3) \right\}$$

condition / properties -

If R and S are relations, on a set A using operations on boolean matrix, one can show,

① $M_{R \cup S} = M_R \vee M_S$ disjunction

② $M_{R \cap S} = M_R \wedge M_S$ conjunction

③ $M_{R^{-1}} = M_R^T$ or $M_{R^{-1}} = \text{Transp of Matrix } M_R$

- Reflexive relation on Matrix form

- If all the elements ~~of~~ in the main diagonal of the matrix representation of a relation are '1', then the relation is reflexive.
- Then the main diagonal elements of the matrix M_R is the set of all M_{ii}
- If all $M_{ii} = 1$, then the relation is reflexive.

EX :- $A = \{1, 2, 3\}$.

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

$M_R = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \rightarrow \text{Reflexive matrix.}$

Diagonal elements -

Dt: 18/03/24

- Symmetric relation on Matrix form :-

- If the representative matrix of a relation is symmetric w.r.t the main diagonal that is $m_{ij} = m_{ji} \forall$ values of i & j , then the relation is symmetric i.e. $M_R = M_R^T$.

EX :- $M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, M_R^T = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

$\therefore M_R = M_R^T$

Hence, M_R is the matrix of symmetric relation.

- Anti-symmetric relation on Matrix form :-

- A relation is anti-symmetric if and only if $M_{ij} = 1$

means that

$M_{ji} = 0$

Dt :- 18/03/24

$$M_R = \begin{bmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$\text{Here } M_{12} = 1$$

$$M_{22} = 1$$

$$M_{32} = 1$$

Transitive relation on matrix form :-

→ There is no simple way to test whether a relation R is a transitive.

→ A Relation R is transitive if and only if its matrix M_R has the properties if $M_{ij} = 1$ & $M_{jk} = 1$ then $M_{ik} = 1$.

→ This statement shows that,

$$(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R.$$

$$M_{ij} = 1, M_{jk} = 1 \Rightarrow M_{ik} = 1$$

Remark -

→ This statement simply means, R is transitive if, $M_R \cdot M_R$ has 1 in position (i, k) .

Thus, the transitivity of R means that,

$$M_R^2 = M_R \cdot M_R \text{ has a 1 in any position, then } M_R \text{ must have a 1 in the same position.}$$

Thus, R is transitive, if and only if,

$$M_R^2 + M_R = M_R$$

Ex - let $A = \{1, 2, 3, 4\}$

let R be a relation on A whose matrix is,

$$M_R = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Show that R is transitive

Ans Proof - $M_{R^2} = M_R \cdot M_R$.

$$M_{R^2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \rightarrow \text{next class}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Now we have to check,

$$M_{R^2} + M_R = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} = M_R$$

(if $M_{R^2} + M_R = M_R$. Then we can say that M_R is transitive).

closure of relation

R may or maynot have some property p such as reflexivity, symmetric or transitivity.

If there is a relation S with property p containing R such that S is a subset of every relation with p containing R . Then S is called closure of R . w.r.t to p .

condition - If R is reflexive, so R^S and R^T
① ② if R is symmetric, so R^S and R^T are.

WIMP Problem of closure - ③ if R is transitive, so, R^{ST} and R^{TS} are R^{ST} .

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

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

find the reflexive, symmetric and transitive closure of R using,

- (i) composition of ~~matrix~~ relation R
- (ii) composition of Matrix relation R .
- (iii) Graphical representation of R .

Ans The reflexive closure are denoted by R^{ST} is given by,

$$\begin{aligned} R^{ST} &= R \cup I_A \\ &= \{(1,2), (2,3), (3,1)\} \cup \{(1,1), (2,2), (3,3)\} \\ &= \{(1,1), (1,2), (2,2), (2,3), (3,1), (3,3)\} \end{aligned}$$

Dt: -28/03/24

→ continue 2

Symmetrical closure of relation R^0

→ It is defined as M_S .

$$M_S = M \vee M^T$$

$$= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \vee \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$\begin{cases} 0 \vee 0 = 0 \\ 0 \vee 1 = 1 \\ 1 \vee 1 = 1 \end{cases}$$

$$= \begin{bmatrix} 0 \vee 0 & 1 \vee 0 & 0 \vee 1 \\ 0 \vee 1 & 0 \vee 0 & 1 \vee 0 \\ 1 \vee 0 & 0 \vee 1 & 0 \vee 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

This is the symmetric form.

Transitive closure of relation R :-

$$\rightarrow M^T = M \vee M^2 \vee M^3$$

$$M^2 = M \odot M = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \odot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \begin{cases} 0 \cdot 0 = 0 \\ 1 \cdot 0 = 0 \\ 1 \cdot 1 = 1 \end{cases}$$

$$= \begin{bmatrix} 0+0+0 & 0+0+0 & 0+1+0 \\ 0+0+1 & 0+0+0 & 0+0+0 \\ 0+0+0 & 1+0+0 & 0+0+0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$M^3 = M^2 \odot M.$$

$$= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \odot \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$\begin{aligned} 0 \cdot 0 &= 0 \\ 0 \cdot 1 &= 0 \\ 1 \cdot 1 &= 1 \end{aligned}$$

$$= \begin{bmatrix} 0+0+1 & 0+0+0 & 0+0+0 \\ 0+0+0 & 1+0+0 & 0+0+0 \\ 0+0+0 & 0+0+0 & 0+1+0 \end{bmatrix}$$



then
this
↓

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$M^4 = M \vee M^2 \vee M^3.$$

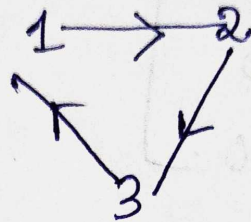
$$= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \vee \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 \vee 0 \vee 1 & 1 \vee 0 \vee 0 & 0 \vee 1 \vee 0 \\ 0 \vee 1 \vee 0 & 0 \vee 0 \vee 1 & 1 \vee 0 \vee 0 \\ 1 \vee 0 \vee 0 & 0 \vee 1 \vee 0 & 0 \vee 0 \vee 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

(iii) Graphical Representation :-

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



VVIMP

WARSHALL'S ALGORITHM

→ Warshall's algorithm which is a more efficient algorithm for computing transitive closure of a relation.

problem -

(Q) Let $A = \{1, 2, 3, 4, 5\}$

and $R = \{(1,1), (1,3), (1,5), (2,3), (2,4), (3,3), (3,5), (4,2), (4,4), (5,4)\}$

Find the transitive closure of R by .

WARSHALL'S ALGORITHM

Ans

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

$R = \{$

$M_R = \begin{matrix} & \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{matrix} & \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{matrix}$

We have to draw a table,

	In W_{k-1}		W_k has 1's in	W_k
k	pos of 1's in col k	pos of 1's in row k		
1	1	1, 3, 5	$(1,1), (1,3), (1,5)$	$\begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{matrix}$
2	4	3, 4	$(4,3), (4,4)$	

VVIMP

WARSHALL'S ALGORITHM

→ Warshall's algorithm which is a more efficient algorithm for computing transitive closure of a relation.

problem -

(Q) Let $A = \{1, 2, 3, 4, 5\}$

and $R = \{(1,1), (1,3), (1,5), (2,3), (2,4), (3,3), (3,5), (4,2), (4,4), (5,4)\}$

find the transitive closure of R by.

WARSHALL'S ALGORITHM

Ans

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

$R = \{$

$$M_R = \begin{matrix} & \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{matrix} & \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{matrix}$$

We have to draw a table,

k	In W_{k-1}		W_k has 1's in	W_k				
	pos of 1's in col k	pos of 1's in row k		1	2	3	4	5
1	1	1, 3, 5	$(1,1), (1,3), (1,5)$	1	0	1	0	1
2	4	3, 4	$(4,3), (4,4)$	0	0	1	1	0
3				0	0	1	0	1
4				0	1	0	1	0
5				0	0	0	1	0

Dt :- 04/04/24

2 4 (3,4) (4,3),(4,4)

	1	2	3	4	5
1	1	0	1	0	1
2	0	0	1	1	0
3	0	0	1	0	1
4	0	1	1	1	0
5	0	0	0	1	0

3 1,2,3,4 (3,5) (1,3)(1,5),(2,3),(2,5)
(3,3),(3,5),(4,3),(4,5)

	1	2	3	4	5
1	1	0	1	0	1
2	0	0	1	1	1
3	0	0	1	0	1
4	0	1	1	1	1
5	0	0	0	1	0

4 2,4,5 (2,3,4,5) (2,2)(2,3),(2,4),(2,5)
(4,2)(4,3),(4,4),(4,5)
(5,2)(5,3),(5,4),(5,5)

	1	2	3	4	5
1	1	0	1	0	1
2	0	1	1	1	1
3	0	0	1	0	1
4	0	1	1	1	1
5	0	1	1	1	1

5 1,2,3,4,5 (2,3,4,5) (1,2)(1,3),(1,4),(1,5)
(2,2)(2,3)(2,4)(2,5)
(3,2)(3,3)(3,4)(3,5)
(4,2)(4,3),(4,4),(4,5)
(5,2)(5,3),(5,4),(5,5)

	1	2	3	4	5
1	1	1	1	1	1
2	0	1	1	1	1
3	0	1	1	1	1
4	0	1	1	1	1
5	0	1	1	1	1

$\therefore R = \{ (1,1), (1,2), (1,3), (1,4), (1,5), (2,2), (2,3), (2,4), (2,5), (3,2), (3,3), (3,4), (3,5), (4,2), (4,3), (4,4), (4,5), (5,2), (5,3), (5,4), (5,5) \}$

Transitive closure.

• partial order relation and its application -

POSET $\rightarrow$ partial order set.

IMP

DOR

$\hookrightarrow$ def - A relation R on a set A is called a partial order relation if it satisfies the following 3 properties -

- (i) Relation R is reflexive i.e. $aRa, \forall a \in A$.
- (ii) Relation R is antisymmetric i.e. aRb , and $bRa \Rightarrow \boxed{a=b}$
- (iii) Relation R is transitive i.e. aRb and $bRc \Rightarrow aRc$.

$\therefore$ Then, POSET: (partial ordered set)

Defn - consider a relation R on a set S satisfying the following properties:-

- (i) Relation R is reflexive i.e. $nRn, \forall n \in S$.
- (ii) Relation R is antisymmetric i.e. $nRy \& yRn \Rightarrow \boxed{x=y}$
- (iii) Relation R is transitive i.e. $nRy \& yRz \Rightarrow xRz$.

Then R is called a partial ordered relation and the set ' S '. Together with partial order. is called partial order set or

POSET.

$\rightarrow$ It is denoted by $(S, \leq)$. $(S, \leq) \mapsto \text{POSET} \mapsto (S; R)$
 $\quad \quad \quad \times \quad \quad \quad$
 $(S, \leq)$

(1) The set N (natural number set) form a poset under the relation $\leq$ because:-

- (i) $n \leq n$ (Reflexive). $\rightarrow 1 \leq 1, 1 < 1$ or $1 = 1$
- (ii) $n \leq y$ and $y \leq n$, then we have $\boxed{n=y}$ (anti-symmetric),
 $n R y$ & $y R n \rightarrow 1 < 2, 2 \not< 1, 2 < 3$
 $\Rightarrow n = y$
- (iii) $n \leq y$ and $y \leq z$, then $n \leq z$ (Transitive) $\forall n, y, z \in N$.
 $\rightarrow 3, 1 \leq 2; 2 \leq 3$
 $\Rightarrow 1 \leq 3$.

• HASSE DIAGRAMS -

$\rightarrow$ Lattice.

$\rightarrow$ A graphical representation of a partial order relation which all arrowhead are understood to be pointing upper upward and is known as the HASSE diagram.

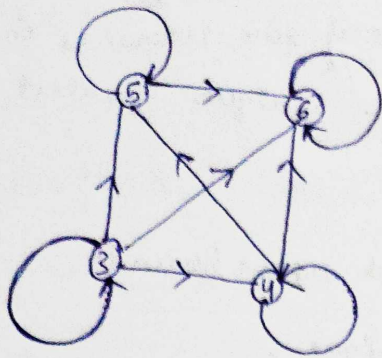
For Hasse diagram,

the following properties should be followed -

- ① Delete the reflexive edges from the figure as circular or loop.
- ② Delete the edges of transitive case i.e. $(a,b) \in R, (b,c) \in R \Rightarrow (a,c) \in R$.
 then the edges of arc $\rightarrow$ should be deleted in Transitive case.
- ③ Then the circles represented in diagram connected to dots in Hasse diagram without using Arrow head.

EX - $S = \{3, 4, 5, 6\}$, $\leq$, POSET $(S, \leq)$

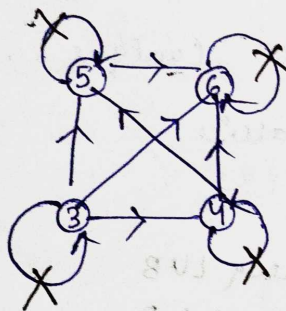
$R = \{(3, 4), (3, 5), (3, 6), (4, 5), (4, 6), (5, 6)\} \cup \{(3, 3), (4, 4), (5, 5), (6, 6)\}$



Digraph of relation R

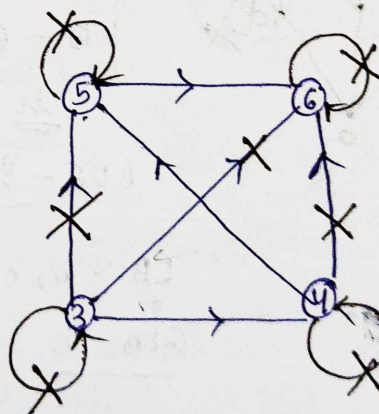
How to convert a digraph to a Hasse diagram

Reflexive -

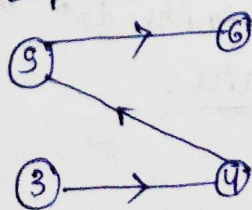


~~antisymmetric~~ -

Transitive -



So the graph will be like -



which is the required Hasse diagram of the given digraph.

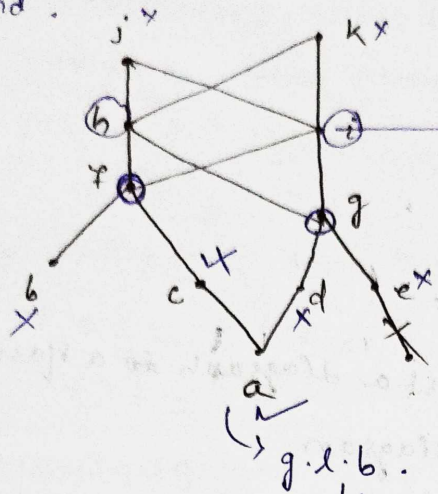
Dt :- 08/04/24

power set $\rightarrow$ The set of all subsets of a given set A is known as its power set.

Lattices

A POSET (P, R) is said to be a lattice if every two elements in the set L has an unique l.u.b of upper bound and unique greatest lower bound.

Ex:-

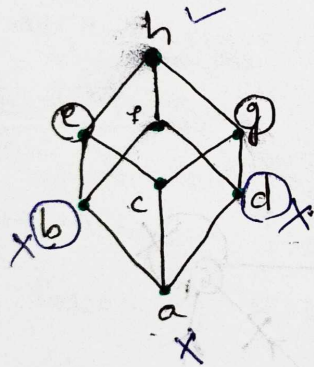


h & i are least upper bound.
 $\therefore$ It is not unique.

$\rightarrow$ greatest lower bound.
(unique).

$\therefore$ This Hasse diagram is not lattice.

Ex -



check LUB
g.l.b.

LUB - e & h as it is directly connected to

$\therefore$ h
LUB - h (unique)

LB = $b, c, d, \& a$.

GLB = c (unique)

$\therefore$ This Hasse diagram is lattice.

Prob-1 - let S be any non empty finite set and $P(S)$ be its power set so that, $(P(S), \subseteq)$ is lattice.

consider $P(S)$

power set.

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

(i) $\emptyset \in P(A)$

(ii) $\{a\} \in P(A)$

$$(iii) \{b\} \subset A$$

$$(iv) \{c\} \subset A$$

$$(v) \{a, b\} \subset A$$

$$(vi) \{b, c\} \subset A$$

$$(vii) \{c, a\} \subset A$$

$$(viii) \{a, b, c\} \subset A$$

Formula,

$$|A| = n$$

$$|P(A)| = 2^n$$

$$\hookrightarrow 2^3 = 8$$

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

Soln

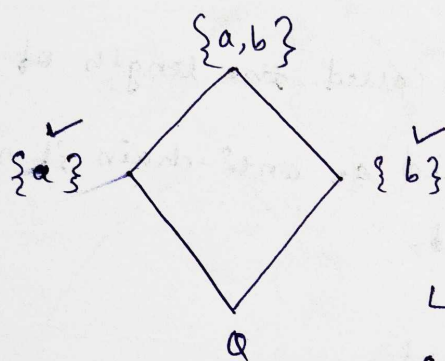
consider $S = \{a, b\}$

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

$$R = \{(\emptyset, \emptyset), (\emptyset, a), (\emptyset, b), (\emptyset, \{a, b\})\}$$

Its hasse diagram,

$$(P(S), \subseteq)$$



$$LUB = \{a, b\} \text{ unique.}$$

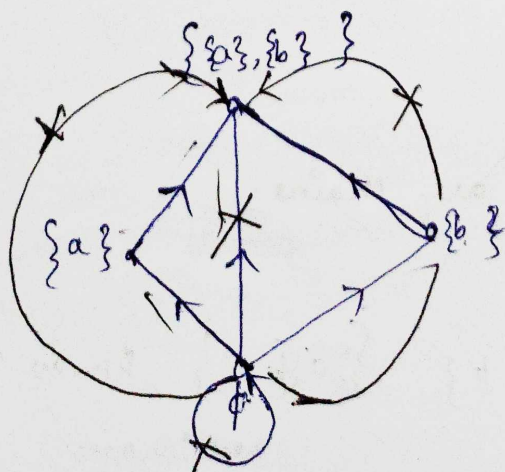
$$GLB = \emptyset \rightarrow \text{unique}$$

$\therefore$ This is the figure of lattice.

$$\{\emptyset\} \subset \{a, b\}$$

$$\{b\} \subset \{a, b\}$$

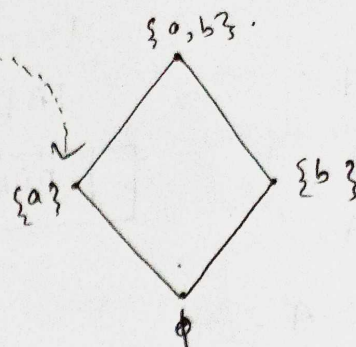
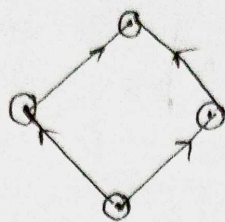
$$\{\{a\}, \{a, b\}\}, \{\{b\}, \{a, b\}\}, \{\{a, b\}, \{a, b\}\}$$



is a directed graph
or
digraph.

DI:- 09/04/24

Hasse diagram



• chains and Anti-chains -

• Chain :-

Let $(A, \leq)$ be a partially ordered set (POSET). A subset of A is called a chain if every 2 elements in the subset are related.

• length :-

The no of elements in a chain is called the length of the chain.

• Antichain :- A subset of A is called an anti-chain if no two distinct elements in the subset are related.

• * TOSET - Total order set.

→ A partially ordered set i.e. $(A, \leq)$ is called a TOSET or linearly ordered set.

→ also known as Linearly ordered set or LOS.

Example :-

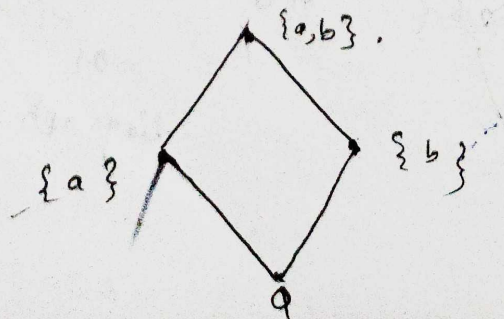
Let A is a set i.e. $A = \{a, b\}$.

$(A, \leq)$ be a POSET

Then $\{\phi, \{a\}, \{a, b\}\}$.

$\{\{a\}, \{a, b\}, \{\phi, \{a\}\}\}$ are chains.

Then,



$\{\{a\}, \{b\}\}$ is an example of an anti-chain

since $\{a\} \not\subseteq \{b\}$ so it is antichain.

$$2A4 \\ = 2 \text{ divides } 4$$

VVTMP for sem:-

(Q) Draw the Hasse diagram of following sets under partial order relation that is divides. and indicate those chains and anti-chains. and check TOSET with diagram of the following set,

$$A = \{1, 3, 9, 18\} \text{ and } B = \{3, 5, 30\}$$

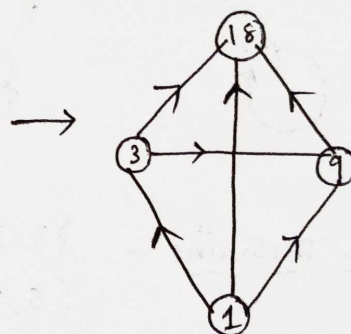
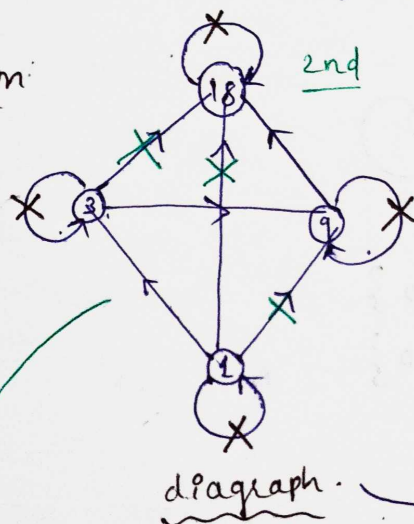
Ans

$$A = \{1, 3, 9, 18\}$$

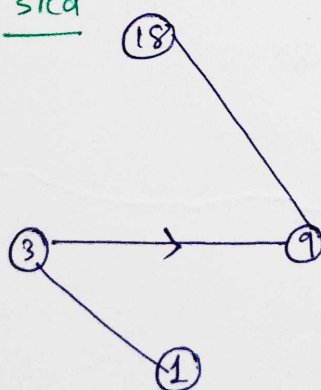
$$R = \{(1, 3), (1, 9), (1, 18), (3, 9), (3, 18), (9, 18), (1, 1), (3, 3), (9, 9), (18, 18)\}$$

Hasse diagram:

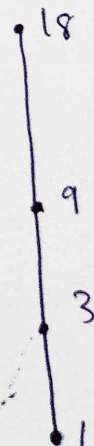
a



3rd



final Hasse diagram is



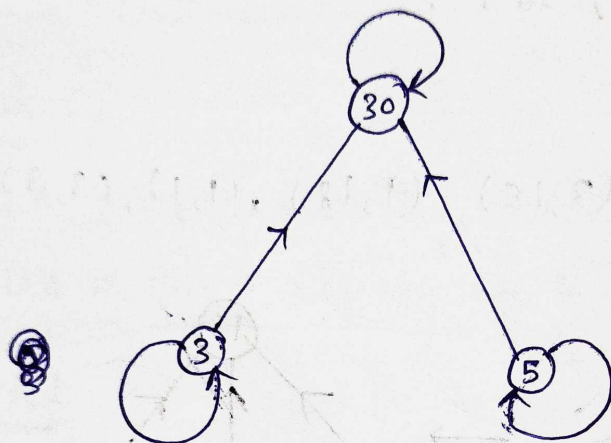
This poset is a ~~chain~~ chain because every 2 elements are related. Hence it is TOSET.

$$B = \{3, 5, 30\}$$

$$R = \{ \cancel{(3,5)}, \cancel{(3,30)}, \cancel{(5,30)}, 3,$$

$$R = \{ (3,3), (5,5), (30,30), (3,30), (5,30) \}$$

diagraph



There are 2 chains - $\{3, 30\}$
 $\{5, 30\}$

Antichain - $\{3, 5\}$.

Pigeonhole problem.

Formula

VRMP problem solving from pigeonhole.

If $(N+1)$ or more objects are placed into N boxes, then there is at least one box containing two or more objects.

Example -

→ If 6th colours are used to paint 37 homes, so that at least 7 home of them will be of same colour.

→ $[X] [x] [X] \rightarrow$ Greatest Integer Function,

→ Smallest integer function.

$$[x] - [2.59] = 2.$$

$$[2.59] = 3.$$

→ Smallest integer function.

$$\begin{array}{r} 6 \overline{) 37} \quad 6 \cdot 1 \\ \underline{36} \\ 20 \\ \underline{6} \\ 4 \end{array}$$

$$\left[\frac{37}{6} \right] = [6.1] = 7.$$

$$\text{or} \quad \left[\frac{37}{6} \right] = [6.1] = 7.$$

Generalized pigeonhole principle formula:-

If n pigeonhole are assigned by $(kn+1)$ or more pigeons. Then at least one pigeonhole is assigned by $(k+1)$ or more pigeons.

prob-1

find the minimum no of teachers in college to be sure that ⁴ both of them are born in the same month

n $n = 12$

$$k+1 = 4.$$

$$\Rightarrow k = 3$$

D.2.6 MODULE

1 lakh

2 - born same time

It will be assigned by $k_{n+1} = 3 \times 12 + 1$

$$= 36 + 1$$

$$= 37$$

$$\begin{array}{r} 12 \overline{) 37} \quad | \quad 3 \\ \underline{36} \\ 1 \end{array}$$

$$\rightarrow \left\lceil \frac{37}{12} \right\rceil = 4 \rightarrow \text{all born in same month}$$

1 lakh people.

NO - M-2

2 - born same time

$$24 \mid 1000000 \mid 4167.$$

$$\lceil x \rceil = \lceil x \rceil \text{ is } < \text{ or } = \text{ to } n$$

$$60 \mid 4167 \mid 69 \dots = 70. \quad \lceil 69 \rceil = \lceil 70 \rceil$$

$$60 \mid 70 \mid 1.$$

$$\left\lceil \frac{70}{60} \right\rceil = 2. \rightarrow \underline{\underline{\text{smallest}}}$$

Group :- A non empty set 'G' is called a group under binary operation '*' if it satisfies.

(iii) Identity property :-

(i) closure property :-

for $\forall a, b \in G$
 $\Rightarrow a * b \in G$

$a + 0 = a \rightarrow$ identity in addition
 $a * 1 = a \rightarrow$ identity in multiplication.

$a \in G, a * e = a$

$e =$ identity element $\in G$

(ii) Associate property :-

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

EX :- $(a + b) + c = a + (b + c)$

$$\Rightarrow (2 - 3) + 4 = 3$$

$$\Rightarrow 2 - (3 + 4)$$

$$= -5$$

(iv) Inverse property :-

$$(a_e)^G$$

EX :- $5 + (-5) = 0 = -5$ = additive Inverse of 5

$$5 * \frac{1}{5} = 1 = \frac{1}{5}$$
 = multiplicative Inverse of 5.

$$a * b = e \text{ (identity)}$$

$b =$ inverse of a .

EX :- Prove that set $\{1, -1, i, -i\}$ is a group under multiplication.

Ans

(i) closure

(ii) Associative

(iii) Identity element = 1

(iv) Inverse :-

	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

$$i = \sqrt{-1}$$

$$i^2 = -1$$

$$i^3 = i \cdot i^2$$

$$= i(-1)$$

$$= -i$$

Inverse of 1 = 1
 Inverse of -1 = -1
 Inverse of i = -i
 Inverse of -i = i

EX :- $\mathbb{Z}$ is not a group under multiplication.

$\mathbb{Z}$ = set of integers.

$$= \{-3, -2, -1, 0, 1, 2, 3, \dots\}$$

Inverse of $5 \in \mathbb{Z}$

$$\text{Inverse of } 5 = \frac{1}{5} \in \mathbb{Z}.$$

→ real no

EX :- A 2×2 matrix with real entities is a group under addition.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}_{2 \times 2}.$$

Ans

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}_{2 \times 2}$$

$$B = \begin{bmatrix} x & y \\ z & w \end{bmatrix}_{2 \times 2}$$

$$A+B = \begin{bmatrix} a+x & b+y \\ c+z & d+w \end{bmatrix}_{2 \times 2}$$

(i) closure ✓

(ii) Associative ✓

(iii) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}_{2 \times 2}$ is the identity.(iv) Inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}_{2 \times 2} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}_{2 \times 2}$ (v) $V(n)$ = Set of all the +ve integers less than n and relate.

$$V(10) = \{1, 3, 7, 9\}$$

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

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

$$V(8) = \{1, 3, 7\}$$

$$V(11) = \{1, \dots, 10, 11\}$$

• Congruence Module :-

→ Let a, b are any integers and x be a fixed integer a is called congruent to b module x or symbolically $a \equiv b \pmod{x}$. if :-

EX :- Prove that $V(10)$ is a group under multiplication module 10.

$$V(10) = \{1, 3, 7, 9\}$$

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

identity = 1

inverse of 1 = 1

inverse of 3 = 7

inverse of 7 = 3

inverse of 9 = 9

Set of all
 $\mathbb{Z}_n = \{ \text{Set of all non-negative integer less than } n \}$
 $= \{0, 1, 2, \dots, (n-1)\}$

$$\text{EX :- } \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

$$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

(Q) test that $\mathbb{Z}_4$ is a group under addition module 4 or not.
 $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

Ans

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

018-15/02/24

→ If $a * b = b * a$ (i.e commutative).
 then the group is called Abelian group.

$$2 + 3 = 3 + 2$$

$$2 * 3 = 3 * 2$$

• Subgroup :-

→ H be any subset of group G

→ H is called subgroup of G if it satisfies all group axioms.



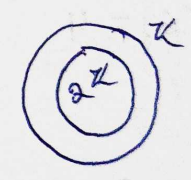
EX:- $(\mathbb{Z}, +) \rightarrow$ Set of integers under addition.

$G = (\mathbb{Z}, +)$ group.

$2\mathbb{Z} =$ set of ~~integers~~ Even numbers.

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

$$2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, 6, 8, \dots\}$$



(i) closure, $x \in 2\mathbb{Z}$, $y \in 2\mathbb{Z}$, $2 + 4 = 6 \in 2\mathbb{Z}$

(ii) Associative, $(2 + 4) + 6 = 2 + (4 + 6)$

(iii) Identity, $0 \in 2\mathbb{Z}$

(iv) Inverse of 4 = $-4 \in 2\mathbb{Z}$

$(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$

• Two step Theorem :-

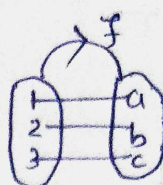
- (i) closure ✓
- (ii) Inverse ✓ Imp

→ A non empty subset H of group G is called subgroup if it is satisfied :-

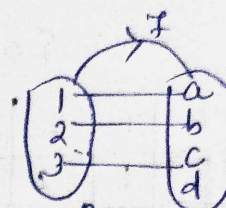
(i) closure — $a * b \in +1, a, b \in +1$

(ii) Inverse — $a \in H$
 $\Rightarrow a^{-1} \in +1$

Permutation group :-



one-one ✓
 onto ✓



one-one ✓
 onto ✗

→ permutation of set A is a function from A to A which is both 1-1 and onto.

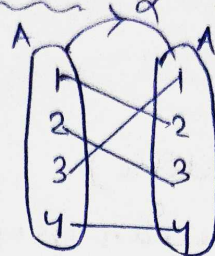
(Φ) $A = \{1, 2, 3, 4\}$

$$\alpha(1) = 2$$

$$\alpha(2) = 3$$

$$\alpha(3) = 1$$

$$\alpha(4) = 4$$



one-one ✓
 onto ✓

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ \alpha(1) & \alpha(2) & \alpha(3) & \alpha(4) \end{bmatrix}$$

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

So, it can be a permutation.

(Φ) $B = \{1, 2, 3, 4, 5, 6\}$

$$B(1) = 5$$

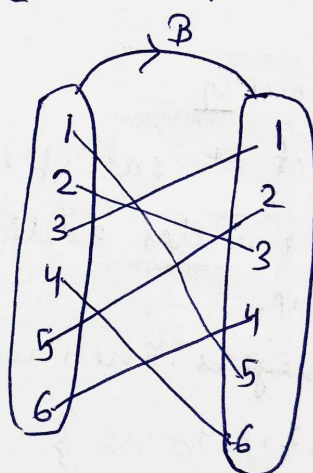
$$B(2) = 3$$

$$B(3) = 1$$

$$B(4) = 6$$

$$B(5) = 2$$

$$B(6) = 4$$



one-one ✓
 onto ✓

$$B = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ B(1) & B(2) & B(3) & B(4) & B(5) & B(6) \end{bmatrix}$$

$$B = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$$

So, it can be a permutation.

Composition of permutation :-

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \sigma(5) \end{bmatrix}$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \beta(1) & \beta(2) & \beta(3) & \beta(4) & \beta(5) \end{bmatrix}$$

$$\sigma(1) = 2$$

$$\sigma(2) = 4$$

$$\sigma(3) = 3$$

$$\sigma(4) = 5$$

$$\sigma(5) = 1$$

$$\beta(1) = 5$$

$$\beta(2) = 4$$

$$\beta(3) = 1$$

$$\beta(4) = 2$$

$$\beta(5) = 3$$

$$\begin{aligned} \sigma \beta(1) &= \sigma(\beta(1)) \\ &= \sigma(5) \\ &= 1 \end{aligned}$$

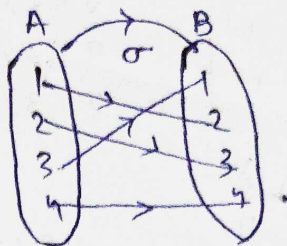
DE: 14/02/24

permutation group

A function $\sigma: A \rightarrow A$ is permutation if it is both one-one function and onto.

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

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$



$$\begin{aligned} \sigma(B(2)) &= \sigma(B(2)) \\ &= \sigma(4) \\ &= 4 \end{aligned}$$

$$\begin{aligned} \sigma(B(3)) &= \sigma(B(3)) \\ &= \sigma(1) \\ &= 2 \end{aligned}$$

$$\begin{aligned} \sigma(B(4)) &= \sigma(B(4)) \\ &= \sigma(2) \\ &= 3 \end{aligned}$$

$$\begin{aligned} \sigma(B(5)) &= \sigma(B(5)) \\ &= \sigma(3) \\ &= 1 \end{aligned}$$

$$\begin{aligned} B\sigma(1) &= B(\sigma(1)) \\ &= B(2) \\ &= 4 \end{aligned}$$

$$\begin{aligned} B\sigma(2) &= B(\sigma(2)) \\ &= B(3) \\ &= 1 \end{aligned}$$

$$\begin{aligned} B\sigma(3) &= B(\sigma(3)) \\ &= B(1) \\ &= 2 \end{aligned}$$

$$\begin{aligned} B\sigma(4) &= B(\sigma(4)) \\ &= B(4) \\ &= 4 \end{aligned}$$

$$\begin{aligned} B\sigma(5) &= B(\sigma(5)) \\ &= B(5) \\ &= 5 \end{aligned}$$

(Q)

$$\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

$$\begin{aligned} \alpha(1) &= 2 \\ \alpha(2) &= 3 \\ \alpha(3) &= 1 \end{aligned}$$

$$\alpha^2 = \alpha \alpha$$

$$\alpha^2(1) = \alpha(\alpha(1)) = \alpha(2) = 3$$

$$\alpha^2(2) = \alpha(\alpha(2)) = \alpha(3) = 1$$

$$\alpha^2(3) = \alpha(\alpha(3)) = \alpha(1) = 2$$

$$\alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

Composition is not commutative.

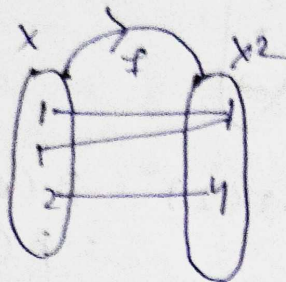
Identity permutation

$$\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$

$$\sigma(1) = 1$$

$$\sigma(2) = 2$$

$$\sigma(3) = 3$$



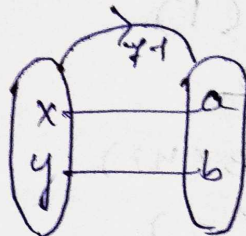
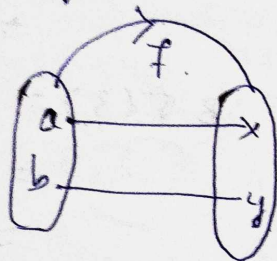
$$f(x) = x^2$$

$$\Rightarrow f(1) = 1^2 = 1$$

$$\Rightarrow f(2) = 2^2 = 4$$

Linear permutation

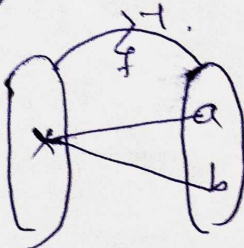
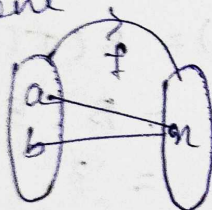
only possible when one-one & ~~only~~ onto.



} one-one

manyone

}



} one many.

$$\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

$$\alpha^{-1} = \begin{bmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix}$$

$$\beta^{-1} = \begin{bmatrix} 4 & 2 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{bmatrix}$$

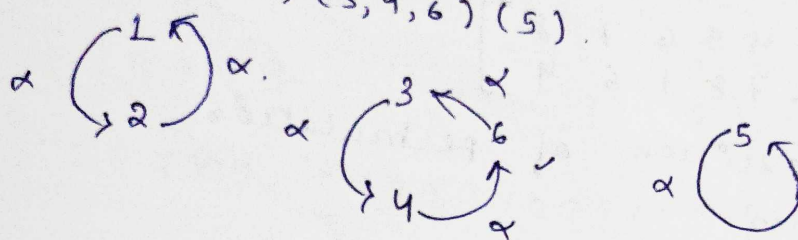
$$= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}$$

DE - 30/03/24.

Cyclic Notation -

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix} \rightarrow \text{Permutation to cycle.}$$

$$= (1, 2) (3, 4, 6) (5)$$



$$\sigma = (\widehat{2 \ 4 \ 3 \ 5}) (\widehat{1 \ 6}) (\widehat{8})$$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 4 & 5 & 3 & 2 & 1 & 7 & 8 \end{bmatrix} \rightarrow \text{cycle to permutation.}$$

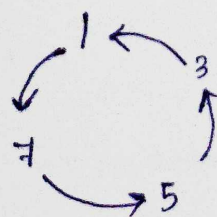
length of cycle -

→ No of elements/entries present in the cycle.

order of permutation -

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{bmatrix}$$

$$= (1 \ 7 \ 5 \ 3) \quad (2 \ 6 \ 4)$$



→ Every permutation can be written as product of cycles.

Order of permutation = LCM of lengths.

$$\text{Order of } \alpha = \text{LCM}(4, 3) = 12$$

Q find the order of $\alpha\beta$

where $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 3 & 2 & 7 & 6 & 1 & 5 \end{bmatrix}$

$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 2 & 7 & 8 & 1 & 6 & 4 \end{bmatrix}$

find the composition of permutation.

Ans

$\alpha\beta(1) = \alpha(3) = 3$

$\alpha\beta(2) = \alpha(5) = 7$

$\alpha\beta(3) = \alpha(2) = 4$

$\alpha\beta(4) = \alpha(7) = 1$

$\alpha\beta(5) = \alpha(8) = 5$

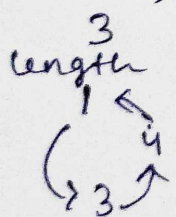
$\alpha\beta(6) = \alpha(1) = 8$

$\alpha\beta(7) = \alpha(6) = 6$

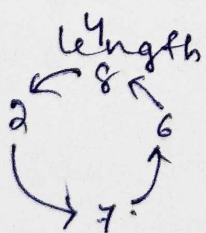
$\alpha\beta(8) = \alpha(4) = 2$

$\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 7 & 4 & 1 & 5 & 8 & 6 & 2 \end{bmatrix}$

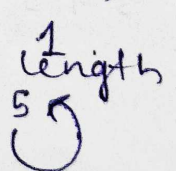
$(1\ 3\ 4)$



$(2\ 7\ 6\ 8)$



(5)



• 2 cycle / transposition -

A cycle of length 2 is called 2-cycle.

eg = $A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ \downarrow & & & \\ 2 & 1 & 4 & 3 \end{bmatrix}$

$= (1\ 2)(3\ 4)$

$$* (a_1 a_2 a_3) = (a_1 a_3) (a_1 a_2)$$

$$(a_1 a_2 a_3 a_4) = (a_1 a_4) (a_1 a_3) (a_1 a_2)$$

Ex

$$(1 2 3 4) = (1, 4) (13) (12).$$

$$(2 4 7 8 9) = (29) (28) (27) (24).$$

ϕ = Test alpha is even or odd ?
Imp

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 4 & 5 & 3 & 2 & 1 & 8 & 7 \end{bmatrix}$$

$$\text{Product of cycle} = (1 6) (2 4 3 5) (7 8)$$

connected to 2 cycles,

$$(1 6) (2 5) (2 3) (2 4) (7 8)$$

↓

add no of permutation cycles.

→ A permutation is even/odd if it can be written as product of even/odd no of 2 cycles.

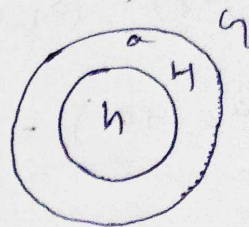
cosets -

→ let H be a subgroup of G and $a \in G$

Then $a * H = \{ a * h : h \in H \}$ is called left coset of H .

$H * a = \{ h * a : h \in H \}$ is called right coset of H .

for ex:-



$$G = \mathbb{Z} = \{ \dots -3, -2, -1, 0, 1, 2, 3 \dots \}$$

$$H = 3\mathbb{Z} = \{ \dots -9, -6, -3, 0, 3, 6, 9 \dots \}$$

$G = (G, +)$, $H = (H, +) \longrightarrow$ Group under Addition.

find all left cosets of H ,

$$\begin{aligned} 0 + H &= \{ \dots 0-9, 0-6, 0-3, 0+0, 0+3, \dots \} \\ &= \{ \dots -9, -6, -3, 0, 3, 6, \dots \} \end{aligned}$$

$$\begin{aligned} 1 + H &= \{ \dots 1-9, 1-6, 1-3, 1+0, 1+3, 1+6, \dots \} \\ &= \{ \dots -8, -5, -2, 1, 4, 7, \dots \} \end{aligned}$$

$$\begin{aligned} 2 + H &= \{ \dots 2-9, 2-6, 2-3, 2+0, 2+3, 2+6, \dots \} \\ &= \{ \dots -7, -4, -1, 2, 5, 8, \dots \} \end{aligned}$$

$$\begin{aligned} 3 + H &= \{ \dots 3-9, 3-6, 3-3, 3+0, 3+3, 3+6, \dots \} \\ &= \{ \dots -6, -3, 0, 3, 6, 9, \dots \} \end{aligned}$$

this is same as " $0 + H$ "

it can be written,
$$\left. \begin{aligned} 4 + H &= 1 + H \\ 5 + H &= 2 + H \end{aligned} \right\}$$

So,

There are only 3 distinct cosets,

$$\dots -6 + H = -3 + H = 0 + H = 3 + H = 6 + H \dots$$

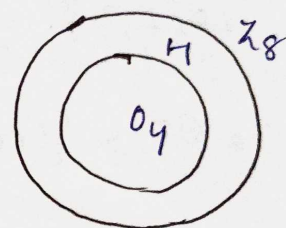
$$\dots = -2 + H = -1 + H = 1 + H = 4 + H = 7 + H \dots$$

$$\dots = -1 + H = 2 + H = 5 + H = 8 + H \dots$$

(Q) find all the cosets of $H = \{0, 4\}$ in the group $G = (\mathbb{Z}_8, +)$ modulo 8.

$$\mathbb{Z}_n = \{0, 1, 2, \dots, (n-1)\}$$

$$\mathbb{Z}_8 = \{0, 1, 2, \dots, 7\}$$



Ans

$$0 + H = \{0+0, 0+4\} = \{0, 4\} \checkmark$$

$$1 + H = \{1+0, 1+4\} = \{1, 5\} \checkmark$$

$$2 + H = \{2+0, 2+4\} = \{2, 6\} \checkmark$$

$$3 + H = \{3+0, 3+4\} = \{3, 7\} \checkmark$$

$$4 + H = \{4+0, 4+4\} = \{4, 8\} = \{4, 0\} \checkmark$$

$$5 + H = \{5+0, 5+4\} = \{5, 9\} = \{5, 1\} \checkmark$$

$$6 + H = \{6+0, 6+4\} = \{6, 10\} = \{6, 2\} \checkmark$$

$$7 + H = \{7+0, 7+4\} = \{7, 11\} = \{7, 3\} \checkmark$$

We have to divide 8 in every element.

As element 8 is not present.

There are 4 cosets.

code, error detection

↳ DP scr

Dt :- 02/04/24

External direct product -

$$G_1 = \{2, 3\}$$

$$G_2 = \{4, 5, 7\}$$

$$G_1 \oplus G_2 = \{(2, 4), (2, 5), (2, 7), (3, 4), (3, 5), (3, 7)\}$$

Q $Z_2 \oplus Z_3$

$$Z_n = \{0, 1, \dots, (n-1)\}$$

$$Z_2 = \{0, 1\}$$

$$Z_3 = \{0, 1, 2\}$$

$$Z_2 \oplus Z_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$$

$$\begin{array}{r} 10 \overline{) 10118} \\ \underline{20} \\ 1 \end{array}$$

Q Find $(3, 7) \cdot (7, 9)$ in $U(8) \oplus U(10)$.

$U(n) =$ ^(+ve) numbers less than n and relatively prime to n .

Ans $U_8 = \{1, 3, 5, 7\}$

$$U_{10} = \{1, 3, 7, 9\}$$

Two numbers are relatively prime if $\gcd = 1$

$$\gcd(8, 1) = 1 \checkmark$$

$$\gcd(8, 2) = 2 \times$$

$$\gcd(8, 3) = 1 \checkmark$$

$$\begin{array}{l} (3 \cdot 7) \cdot (7 \cdot 9) \\ = (21, 63) \end{array} \begin{array}{l} \xrightarrow{U(10)} \\ \xrightarrow{U(8)} \end{array}$$

$$= (21 \pmod{8}, 63 \pmod{10})$$

$$= (5, 3)$$

Suppose

$$\begin{array}{l} (7 \cdot 3) \cdot (3 \cdot 3) \\ = (21, 9) \end{array} \begin{array}{l} \xrightarrow{U(10)} \\ \xrightarrow{U(8)} \end{array}$$

$$= (21 \pmod{8}, 9 \pmod{10})$$

$$= (5, 9)$$

$$\begin{aligned}
 & (3 \cdot 9) \cdot (9 \cdot 9) \\
 & = (27, 81) \xrightarrow{UC(10)} \\
 & \quad \quad \quad \xrightarrow{UC(8)} \\
 & = (27 \pmod{8}, 81 \pmod{10}) \\
 & = (3, 1)
 \end{aligned}$$

$$\begin{array}{r}
 2 \ 12 \ 1 \\
 \underline{2} \\
 0
 \end{array}
 \quad
 \begin{array}{r}
 3 \ 12 \ 1 \\
 \underline{3} \\
 0
 \end{array}$$

Q) find $2(1,1)$, $3(1,1)$, $4(1,1)$ & $5(1,1)$ in $\mathbb{Z}_2 \oplus \mathbb{Z}_3$.

$$\mathbb{Z}_2 = \{0, 1\}$$

$$\mathbb{Z}_3 = \{0, 1, 2\}$$

$$\begin{aligned}
 4(1,1) &= (4, 4) \\
 &= (4 \pmod{2}, 4 \pmod{3}) \\
 &= (0, 1)
 \end{aligned}$$

Group Homomorphism -

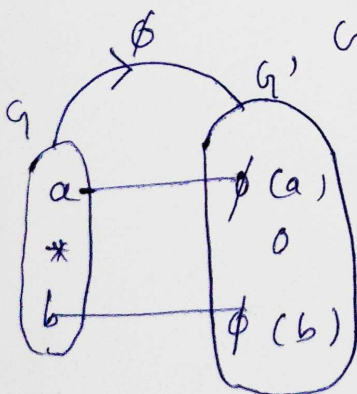
→ A function ϕ from group G is called Homomorphism, if,

$$\phi(a * b) = \phi(a) \cdot \phi(b).$$

$$\forall a, b \in G.$$

$$G = (G, *)$$

$$G' = (G', \cdot)$$



$$2(1,1) = (2, 2)$$

$$= (2 \pmod{2}, 2 \pmod{3})$$

$$= (0, 2) \Rightarrow \text{not possible.}$$

$$3(1,1) = (3, 3)$$

$$= (3 \pmod{2}, 3 \pmod{3})$$

$$= (1, 0)$$

$$5(1,1) = (5, 5)$$

$$= (5 \pmod{2}, 5 \pmod{3})$$

$$= (1, 2)$$

Example -

$$\phi : G \rightarrow G'$$

$$G = (G, +)$$

$$G' = (G, \cdot).$$

$$\phi(x) = 2^x.$$

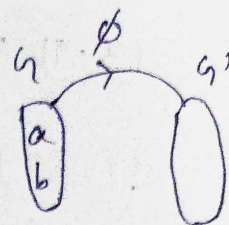
Test ϕ is homomorphism or not.

let $a, b \in G$.

$$\phi(a) = 2^a$$

$$\phi(b) = 2^b$$

$$\boxed{\phi(a+b) = \phi(a) \cdot \phi(b)}$$



$$\underline{\phi(a+b)} = 2^{a+b} = 2^a \cdot 2^b = \phi(a) \cdot \phi(b).$$

(Φ) $\phi : G \rightarrow G', \phi(x) = 10x$

$$\boxed{\phi(a+b) = \phi(a) - \phi(b)}$$

$$\begin{aligned} \phi(a+b) &= \phi(a) - \phi(b) \\ &= 10a - 10b. \end{aligned}$$

$$\phi(a) = 10a$$

$$\phi(b) = 10b.$$

$$\phi(a+b) = 10(a+b).$$

$$= 10a + 10b$$

$$\boxed{= \phi(a) + \phi(b)}$$

$$G = (G, +)$$

$$G' = (G, -)$$

