Discrete Mathematics - Unit II 202 pages

ShriRajkamal Browsing & X
The Best service centre
Gobi- 04285-2233444,22344: 223306.

# Relations and Functions

**Relation:** The word "Relation" suggests some familiar examples of relations such as the relation of father to son, mother to son, brother to sister etc. Familiar relations in arithmetic are, "greater than", "less than," or equality of two real numbers.

A relation between two objects, called binary relation. It can be defined by listing the two objects as an ordered pair. A set of all such ordered pairs, in each of which the first member has some definite relationship to the second.

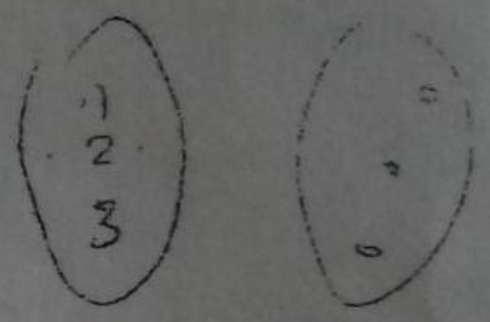
**Definition:**

Any set of ordered pairs defines a binary relation.

We shall call a binary relation simply a relation. It is sometimes convenient to express the fact that a particular ordered pair say $\langle x, y \rangle \in R$ where R is a relation, by writing $xRy$ which may be read as "$x$ is in relation R to $y$."

**Ex:**

1. $> = \{\langle x, y \rangle \mid x, y$ are real numbers and $x > y\}$
2. $F = \{\langle x, y \rangle \mid x$ is the father of $y\}$.
3. $S = \{\langle 2, 4 \rangle, \langle 1, 3 \rangle, \langle 7, 6 \rangle, \langle$ John, Mary $\rangle\}$.
4. Let R denote the set of real numbers. Then
   a. $Q = \{\langle x^2, x \rangle \mid x \in R\}$




**Definition: Domain**

Let S be a binary relation. The set D(S) of all objects x such that for some y, $\langle x,y \rangle \in S$ is called the domain of S.

(ie) $D(S) = \{x \mid (\exists y)(\langle x,y \rangle \in S)\}$.

**Range:**

The set R(S) of all objects y such that for some x, $\langle x,y \rangle \in S$ is called the range of S

(ie) $R(S) = \{y \mid (\exists x)(\langle x,y \rangle \in S\}$.

In Eg: ③, $D(S) = \{2, 1, 9, John\}$ & $R(S) = \{4, 3, 6, 4\}$;

**Universal & Void relation:**

Let X & Y be any two sets. A subset of the cartesian product $X \times Y$ defines a relation C. For any relation C, we have $D(C) \subseteq X$ and $R(C) \subseteq Y$, and the relation C is said to be from X to Y.

If $X = Y$, then C is said to be relation from X to X. In this case, C is called a relation in X. Thus any relation in X is a subset of $X \times X$. The set $X \times X$ itself defines a relation in X and is called a **universal relation** in X.

The emptyset which is also a subset of $X \times X$ is called a **Void relation** in X.

If R and S denote two relations, then R∩S defines a relation such that,

$x\,(R \cap S)\,y \Leftrightarrow xRy \wedge xSy$

Now, R∪S is a relation, i.e.

$x(R \cup S)y \Leftrightarrow xRy \vee xSy$

$x(R - S)y \Leftrightarrow xRy \wedge x \not S y$

$x(\sim R)y \Leftrightarrow x \not R y$.

Ex:1

(a) Let $X = \{1,2,3,4\}$.

If $R = \{\langle x,y\rangle \mid x \in X \wedge y \in X \wedge ((x-y)$ is an integral multiple of $2)\}$.

$= \{\langle 1,3\rangle, \langle 3,1\rangle, \langle 2,4\rangle, \langle 4,2\rangle\}$

$S = \{\langle x,y\rangle \mid x \in X \wedge y \in X \wedge ((x-y)$ is an integral nonzero multiple of $3)\}$

$= \{\langle 1,4\rangle, \langle 4,1\rangle\}$

Find R∪S and R∩S.

(b) If $X = \{1,2,3,\ldots\}$, what is R∩S for R and S as defined in (a)?

Soln:

(a) $R \cup S = \{\langle 1,3\rangle, \langle 3,1\rangle, \langle 2,4\rangle, \langle 4,2\rangle, \langle 1,4\rangle, \langle 4,1\rangle\}$

$R \cap S = \phi$.

b) $R \cap S = \{\langle x,y\rangle \mid x \in X \wedge y \in X \wedge ((x-y)$ is a nonzero multiple of $6)\}$.

## ⑧ [Properties of Binary relations in a set

**Defn: reflexive**

A binary relation R in a set X is reflexive if for every $x \in X$, $xRx$, that is $\langle x,x\rangle \in R$ (or)

R is reflexive in X $\Leftrightarrow (x)(x \in X \rightarrow xRx)$

**Defn:**

A relation R in a set X is symmetric if for every x and y in X, whenever $xRy$; then $yRx$

That is,

R is symmetric in X $\Leftrightarrow (x)(y)(x \in X \wedge y \in X \wedge xRy \rightarrow yRx)$.

**Defn:**

A relation R in a set X is transitive if for every x, y and z in X, whenever $xRy$ & $yRz$, then $xRz$. That is,

R is transitive in X $\Leftrightarrow (x)(y)(z)(x \in X \wedge y \in X \wedge z \in X \wedge xRy \wedge yRz \rightarrow xRz)$

**Defn:**

A relation R in a set X is irreflexive if for every $x \in X$ $\langle x,x\rangle \notin R$.

**Defn:**

A relation R in a set X is antisymmetric if, for every x & y in x, whenever $xRy$ & $yRx$, then $x=y$. Symbolically, R is antisymmetric in x iff,

$(x)(y)(x \in X \wedge y \in X \wedge xRy \wedge yRx \rightarrow x=y)$

## Relation Matrix and the Graph of a Relation

**Defn:**

A relation R from a finite set X to a finite set Y can also be represented by a matrix called the relation matrix of R.

Let $X = \{x_1, x_2, \ldots, x_m\}$, $Y = \{y_1, y_2, \ldots, y_n\}$ and R be a reln from X to Y.

If $x_i R y_j$, then we enter a 1 in the $i^{th}$ row & $j^{th}$ column. If $x_k \not R\, x_l$, then we enter a zero in the $k^{th}$ row & $l^{th}$ column.

Take $m=3$ & $n=2$. and R gn by,

$R = \{\langle x_1, y_1\rangle, \langle x_2, y_1\rangle, \langle x_3, y_2\rangle, \langle x_2, y_2\rangle\}$ → (1)

$$r_{ij} = \begin{cases} 1 & \text{if } x_i R y_i \\ 0 & \text{if } x_i \not R\, y_i \end{cases}$$

where $r_{ij}$ is the elt in the $i^{th}$ row and $j^{th}$ column.

If X has m elements and Y has n elements, the relation matrix is an m x n matrix.

Then the rein matrix for (1) is,

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

Table

| | $y_1$ | $y_2$ |
|---|---|---|
| $x_1$ | 1 | 0 |
| $x_2$ | 1 | 1 |
| $x_3$ | 0 | 1 |

QP

1) $f: A \to B$ and $g: B \to C$ be two mapping then P.T a) if f, g is 1-1 gof 1-1

b) if f is onto g is onto gof is onto.

## Graph of a Relation.

A reln can also be represented pictorially by drawing its graph.

Let R be a relation in a set $X = \{x_1, x_2, \ldots, x_m\}$. The elements of X are represented by points or circles called nodes.

The nodes corresponding to $x_i$ and $x_j$ are labeled $x_i$ & $x_j$ respectively. These nodes may also be called vertices. If $x_i R x_j$, (ie) if $\langle x_i, x_j \rangle \in R$ then we connect nodes $x_i$ & $x_j$ by means of an arc and put an arrow on the arc in the direction from $x_i$ to $x_j$.

When all the nodes corresponding to the ordered pairs in R are connected by arcs with proper arrows, we get a graph of the relation R. Defn:

If $x_i R x_i$, we get an arc which starts from node $x_i$ and returns to node $x_i$ such an arc is called a loop.

## Properties of a Graph:

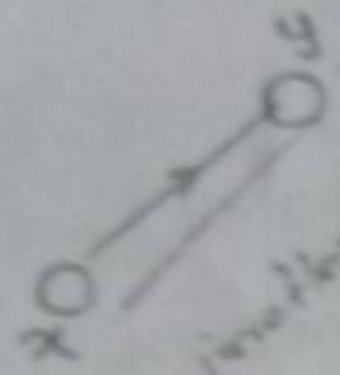
* If a relation is reflexive, then there must be a loop at each node.
* If the relation is irreflexive, then there is no loop at any node.
# If a reln is symmetric and if one node is connected to other, then there must be a return arc from the second node to the

- first.

* For antisymmetric, no such direct return path should exist.

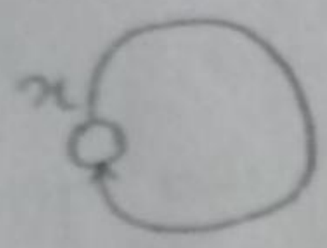
* If a relation is transitive, the situation is not so simple. Its graph must have loops.

Eg: Graphs of relations:

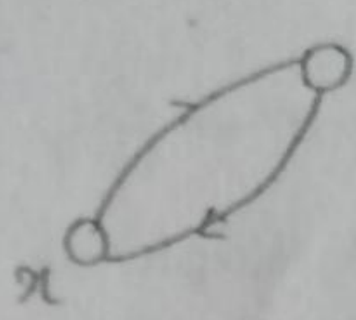



irreflexive

xRy

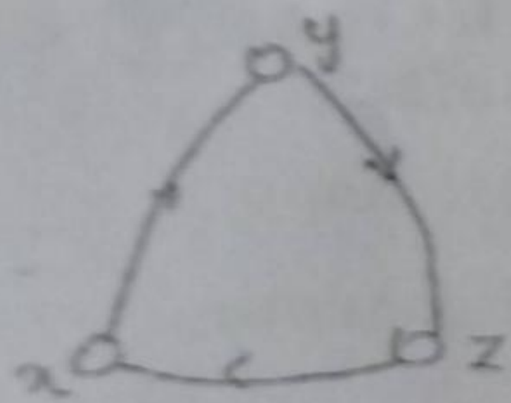



xRx reflexive



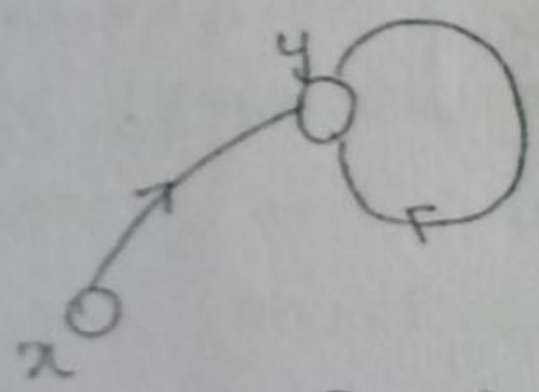

Symmetric.

xRy ∧ yRx.




transitive

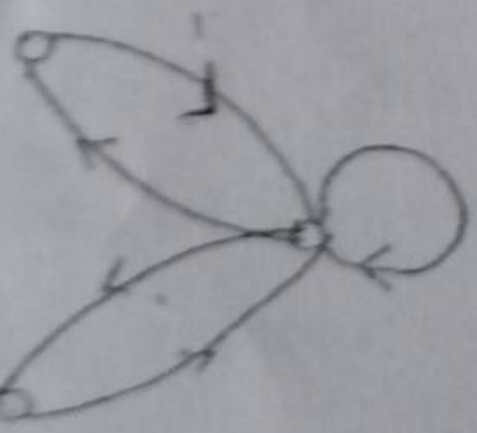
xRy ∧ yRz ∧ zRx

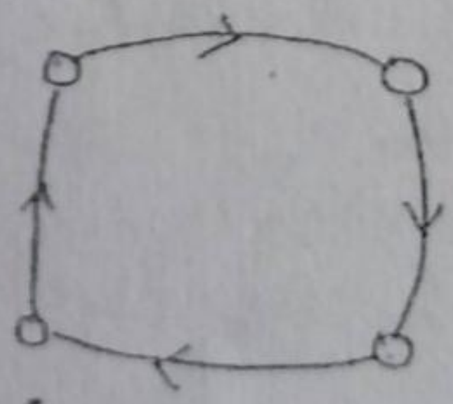



xRy ∧ yRy.

Symmetric

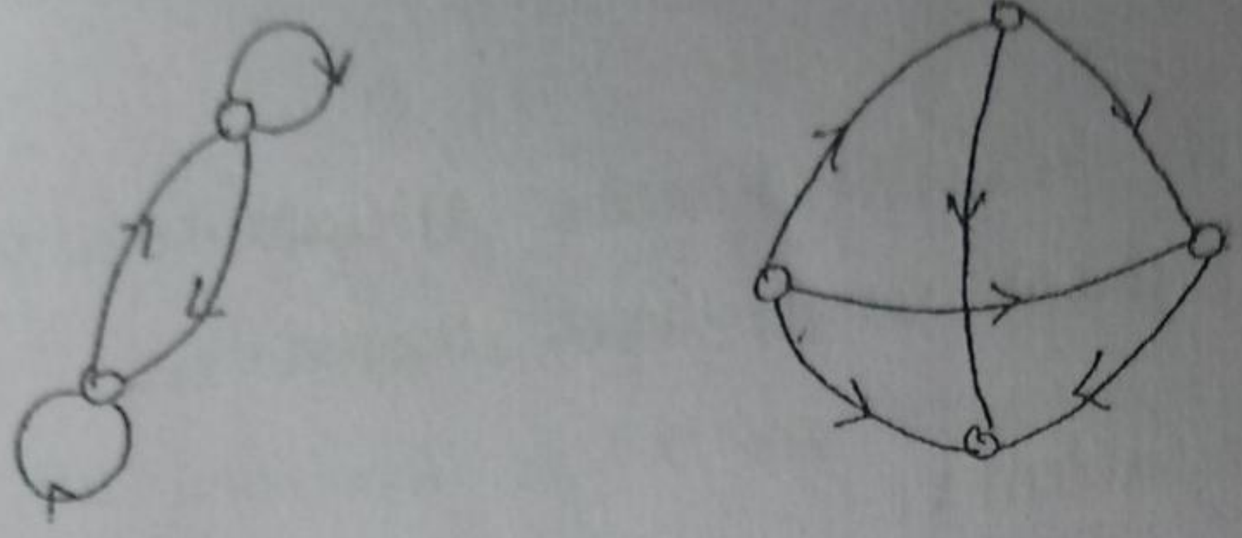
Antisymmetric





no loop

## Transitive relations:



**Ex:1**

Let $X = \{1,2,3,4\}$ and $R = \{\langle x,y\rangle \mid x > y\}$.

Q.1 Draw the graph of R and also give its matrix.

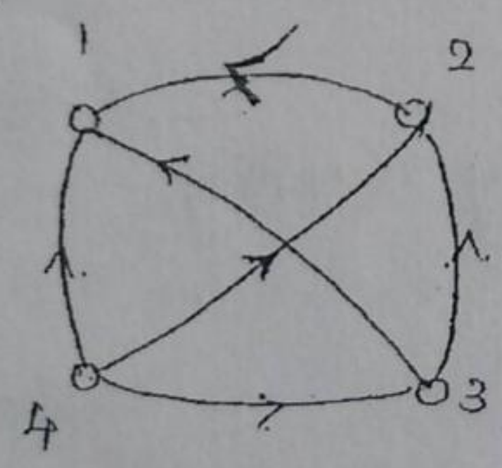
Soln:

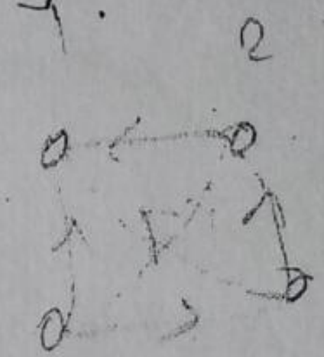
The graph & the corresponding relation matrix for the relation

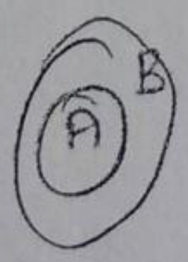
$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

$R = \{\langle 2,1\rangle, \langle 3,2\rangle, \langle 3,1\rangle, \langle 4,1\rangle, \langle 4,2\rangle, \langle 4,3\rangle\}$.

<4,1> <4,3> <4,2>
<3,2> <3,1>
<2,1>




$A \subset B$ contained in

A is a subset of B

3. when $A \neq B$

$A \subset B \Rightarrow B$ is a proper subset

**Ex:2**

Let $A = \{a,b,c\}$ and denote the subsets of A by $B_0, \ldots, B_7$. Thus $B_0 = \phi$, $B_1 = \{c\}$, $B_2 = \{b\}$, $B_3 = \{b,c\}$, $B_4 = \{a\}$, $B_5 = \{a,c\}$, $B_6 = \{a,b\}$ and $B_7 = \{a,b,c\}$. If R is the relation proper inclusion on the subsets $B_0, \ldots B_7$. Then give the matrix of a relation.

$A \subset B$ = $A \subseteq B$ but $A \neq B$.

$A = \{1,2,5\}$
$B = \{1,2\}$
$B \subseteq A$

Soln:

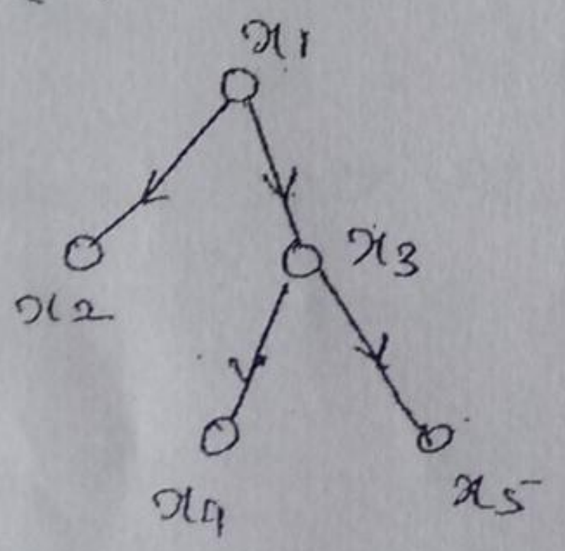
$A = \{a,b,c\}$

| | $\phi$ | $\{c\}$ | $\{b\}$ | $\{b,c\}$ | $\{a\}$ | $\{a,c\}$ | $\{a,b\}$ | $\{a,b,c\}$ |
|---|---|---|---|---|---|---|---|---|
| | $B_0$ | $B_1$ | $B_2$ | $B_3$ | $B_4$ | $B_5$ | $B_6$ | $B_7$ |
| $\phi$ $B_0$ | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\{c\}$ $B_1$ | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| $\{b\}$ $B_2$ | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| $\{b,c\}$ $B_3$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| $\{a\}$ $B_4$ | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| $\{a,c\}$ $B_5$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| $\{a,b\}$ $B_6$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| $\{a,b,c\}$ $B_7$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

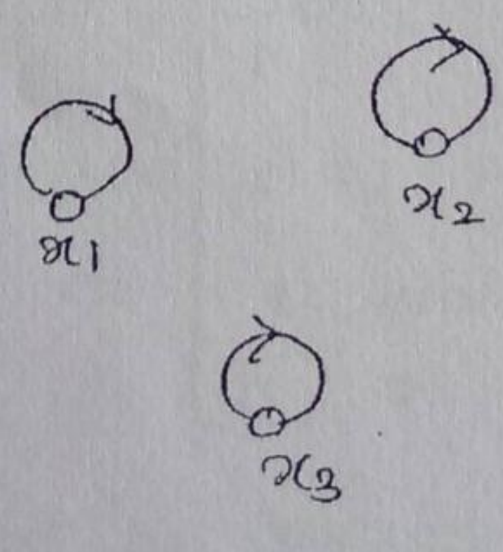
Ex:3

Determine the properties of a relations given by the graphs and also write the corresponding relation matrices.

(a)

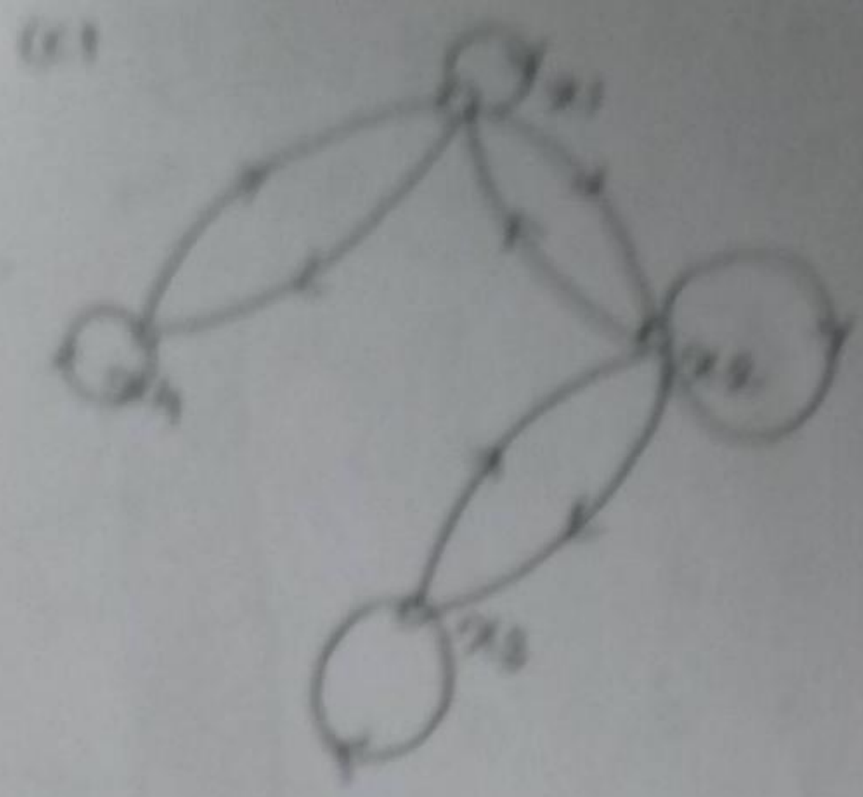



(b)

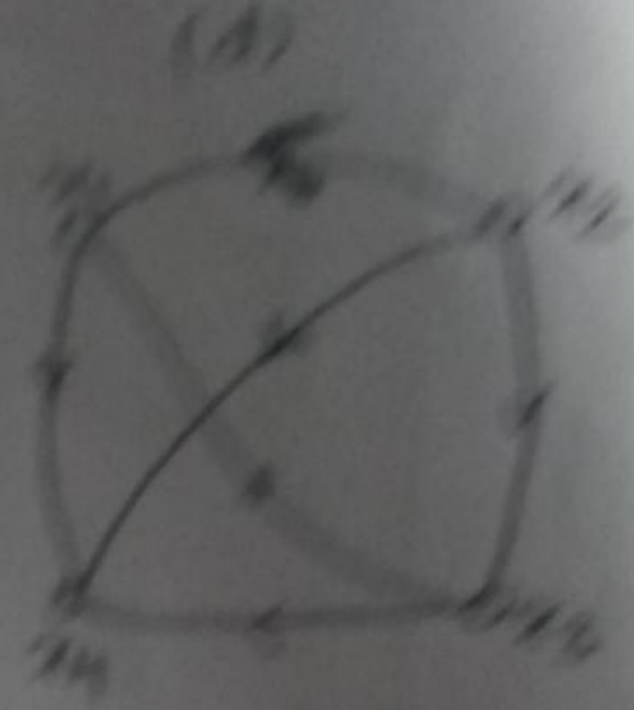



Eg

QP P.T the functions $F: R \to R$ gives $f(x) = \sin x$ is neither one to one or onto.



(a)



(b)

Soln:

The relation given by the graph in (a) is not symmetric but (b) is reflexive. (c) It is not reflexive & symmetric while in (d) it is transitive. The matrix representations are

(a)
$$\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{array}\begin{array}{c} \begin{array}{ccccc} x_1 & x_2 & x_3 & x_4 & x_5 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

(b)
$$\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \end{array}\begin{array}{c} \begin{array}{ccc} x_1 & x_2 & x_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

(c)
$$\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{array}\begin{array}{c} \begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

(d)
$$\begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{array}\begin{array}{c} \begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \end{array} \\ \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

$x_1 R x_3$

$x_1 R x_4$

$x_2 R x_1$

$x_2 R x_3$

$x_2 R x_4$

$x_3 R x_4$

Q1

## Equivalence Relns

Defn:

A reln R in a set X is called an equivalence reln, if it is reflexive, symmetric & transitive.

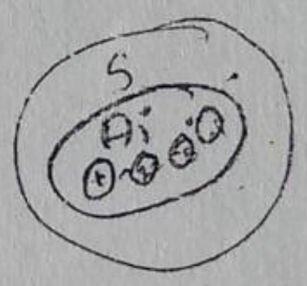
Note:

If R is an equi|: reln in a set X. Then D(R), the domain of R, is X itself. ∴ R will be called a reln on X. The following are some examples of Equi|:

Examplations.

(1) Equality of numbers on a set of real no's.
(2) Equality of subsets of a universal set.
(3) Similarity of triangles on the set of Δ'les.
(4) Reln of lines being parallel on a set of lines in a plane.
(5) Reln of living in the sametown on the set of persons living in canada.
(6) Reln of statements being equivalent in the set of statements.

## Partition and Covering of a set:




Defn:

Let S be a given set and $A = \{A_1, A_2, \ldots A_m\}$ where each $A_i$, $i = 1, \ldots, m$ is a subset of S and

$$\bigcup_{i=1}^{m} A_i = S.$$

Then the set A is called a covering of S, and the sets $A_1, A_2, \ldots, A_m$ are said to cover S.

The elements of A, which are the subsets of S, are mutually disjoint, then A is called a partition of S, and the sets $A_1, A_2, \ldots A_m$ → blocks of the partition.

Ex. let $S = \{a,b,c\}$

The subsets of S are.

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

$D = \{\{a,b,c\}\}$ $E = \{\{a\}, \{b\}, \{c\}\}$ $F = \{\{a\},$

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

F are

A, is called a covering of S.

C, D, & E are partitions of S.

Ex:1

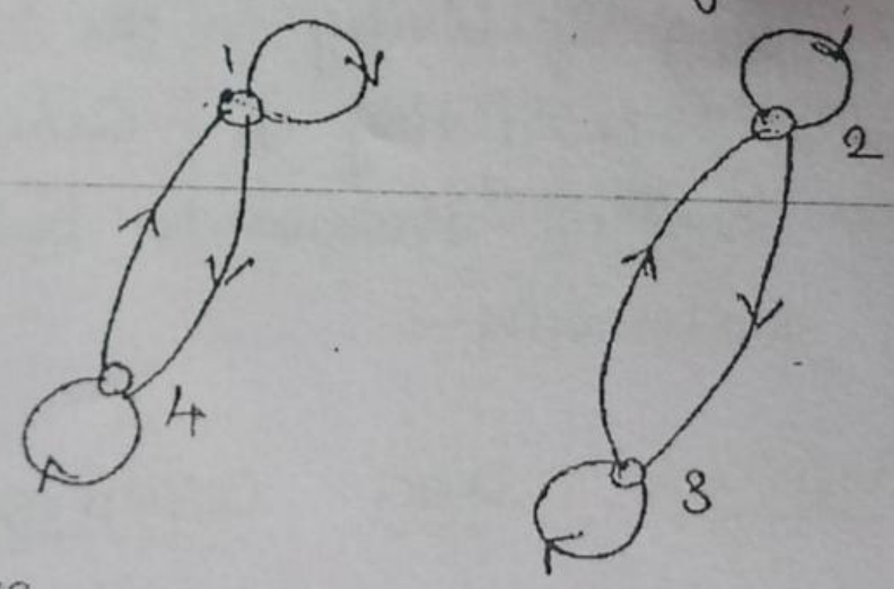
Let $X = \{1,2,3,4\}$ and

$R = \{\langle 1,1\rangle, \langle 1,4\rangle, \langle 4,1\rangle, \langle 4,4\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 3,2\rangle$

$\langle 3,3\rangle\}$ Write the matrix of R & sketch the graph.

Soln:

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \end{array}$$




2. ∵ It is reflexive, symmetric & transitive.

∴ It is an Equivalence Rel^n.

Q.P ② Let $X = \{1, \ldots 7\}$ $R = \{\langle x,y\rangle \mid x-y$ is divisible by $3\}$.

S.T R is an equivalence Rln and draw the graph of R.

Soln:

It is possible to prove the statement without using the graph of the Reln in the following manner.

- **Reflexive:**

For any $a \in X$, $a-a$ is divisible by 3.

Hence $aRa$.

(ie) R is reflexive.

**Symmetric:**

For any $a, b \in X$, if $a-b$ is divisible by 3, then $b-a$ is also divisible by 3.

(ie) $aRb \Rightarrow bRa$. Thus R is symmetric.

**Transitive:**

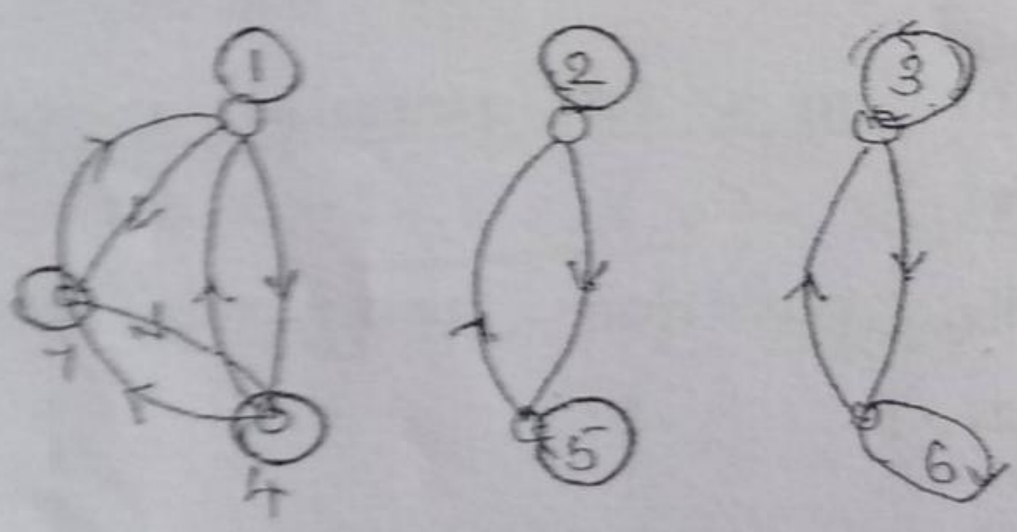
For any $a, b, c \in X$ if $aRb$ and $bRc$ then both $a-b$ & $b-c$ are divisible by 3.

So that $a-c = (a-b) + (b-c)$ is also divisible by 3.

Hence $aRc$. Thus R is transitive.

Let $X = \{1, 2, 3, 4, 5, 6, 7\}$ $\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle, \langle 4,4\rangle, \langle 5,5\rangle, \langle 6,6\rangle, \langle 7,7\rangle$.

& $R = \{\{\langle 1,4\rangle, \langle 1,7\rangle, \langle 2,5\rangle, \langle 3,6\rangle, \langle 4,1\rangle, \langle 4,7\rangle, \langle 5,2\rangle, \langle 6,3\rangle \langle 7,4\rangle, \langle 7,1\rangle\}\}$.




**R- equivalence class:**

Let R be an equivalence on a set X.

For any $x \in X$, then set $[x]_R \subseteq X$ gn by.

$[x]_R = \{y \mid y \in X \wedge xRy\}$ is called an R-equi
Class generated by $x \in X$.

Note:

Sometimes $[x]_R$ is also written as $x/R$.

Properties:

(i) Reflexive:

For any elt $x \in X$, we have $xRx$ beca
R is reflexive $\therefore x \in [x]_R$.

(ii) Symmetric:

Let $y \in X$ be any other elt $\ni: xRy$
so that $y \in [x]_R$ because of the symmetry of
R, $yRx$ and $x \in [y]_R$

(iii) Transitive:

Assume that there is atleast one elt
$y \in [x]_R$ and also $z \in [y]_R$
(ie) $xRy \;\&\; yRz \Rightarrow xRz$.

Note:

2f (i) Every equi rein on a set generated a unique partition of the set.)

(ii) The blocks of the partition corresponds to the R equivalent class.)

Ex: 1

Let Z be the set of integers and let R be the rein called "congruence modulo 3", defined by
$R = \{\langle x, y\rangle \mid x \in Z \wedge y \in Z \wedge (x-y)$ is divisible by $3\}$

Determine the equivalence classes generated by the elts of Z.

Soln: The equivalence classes are,

$x \equiv y \pmod 3$

$\frac{x-y}{3}$

$x - y = \text{mod } 3$

$\frac{x-y}{3}$

$[0]_R = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

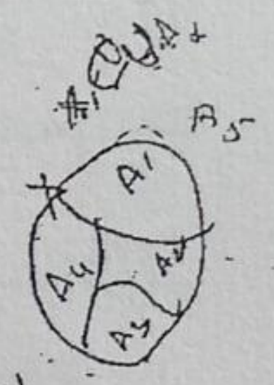
$[1]_R = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$

$[2]_R = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$

$Z/R = \{[0]_R, [1]_R, [2]_R\}$

Ex:2 Let S be the set of all statement fns in n variables and let R be the relⁿ gn by,

$R = \{ \langle x y \rangle / x \in S \wedge y \in S \wedge x \Leftrightarrow y \}$.




Discuss the equivalence classes generated by the elts of S.

Soln:

The no/: of possible distinct truth tables for statement fns which depend upon n statement variables is $2^{2^n} \cdot 2^{2^n}$.

Thus there are $2^{2^n}$ R-equivalence classes generated by the elements of S.

$\langle a,a\rangle \langle b,b\rangle \langle c,c\rangle \langle d,d\rangle \langle e,e\rangle$

$\langle a,b\rangle \langle b,a\rangle \langle d,e\rangle \langle e,d\rangle$

Ex:3 Q.P

Let $X = \{a, b, c, d, e\}$ & let $C = \{\{a,b\}, \{c\}, \{d,e\}\}$

S.T the partition C defines an equivalence relⁿ on X.

Soln:

$R = \{\langle a,a\rangle, \langle b,b\rangle, \langle a,b\rangle, \langle b,a\rangle, \langle c,c\rangle, \langle d,d\rangle, \langle e,e\rangle, \langle d,e\rangle, \langle e,d\rangle\}$.

$\langle a,a\rangle \langle b,b\rangle \langle c,c\rangle \langle d,d\rangle \langle e,e\rangle$ satisfies reflexive

$\langle a,b\rangle \langle b,a\rangle \langle d,e\rangle \langle e,d\rangle$ " symmetric

$\langle a,b\rangle \langle b,a\rangle \langle a,a\rangle$ transitive

$\langle d,e\rangle \langle e,d\rangle \langle d,d\rangle$ "

$\therefore R_{15}$ is equivalence rel.

## Compatibility Relation:

A relⁿ R in $x$ is said to be a compatibility relⁿ if it reflexive & symmetric.

## Composition of binary relⁿ's:

Let R be a relⁿ from X to Y and S be relⁿ from Y to Z. then the relⁿ written as RoS is called a composite relⁿ of R & S where,

$$RoS = \{ \langle x,z \rangle \mid x \in X \wedge z \in Z \wedge (\exists y) (y \in Y \wedge \langle x,y \rangle \in R \wedge \langle y,z \rangle \in S \}.$$

The operation of obtaining RoS from R&S is called composition of relⁿ.

## Note:

1, RoS is empty if the intersection of the range of R and the domain of S is empty.

2, From the graphs of R & S we can easily construct the graph of RoS.

## Theorem:

To show that the composition of relⁿ is associative.

(ie) To show that $(RoS)oP = Ro(SoP)$.

**Proof:** Let R be a relⁿ from x to y, S be a relⁿ from y to z. and P be a relⁿ from z to w

Then RoS is a relⁿ from x to z.

$\therefore (RoS)oP$ which is a relⁿ from x to w.

Hence R is also

• Let us assume that $(R \circ S) \circ P$ is non-empty and let $\langle x, y \rangle \in R$, $\langle y, z \rangle \in S$ & $\langle z, w \rangle \in P$,

this assumption means that $\langle x, z \rangle \in R \circ S$ and $\langle x, w \rangle \in (R \circ S) \circ P$. $\longrightarrow$ (1)

Also ordered pair $\langle y, w \rangle \in (S \circ P)$ & ~~$\langle x, w \rangle \in$~~ $\langle x, w \rangle \in R \circ (S \circ P)$, which shows that, $\longrightarrow$ (2)

(1) & (2) $(R \circ S) \circ P = R \circ (S \circ P)$.

$\langle x, y \rangle \in R$

$\langle y, w \rangle \in (S \circ P)$

$\langle x, w \rangle$

∴ The operation of composition on relations is associative.

So that, $(R \circ S) \circ P = R \circ (S \circ P) = R \circ S \circ P$.

Problems: Q.P(1)

Def $R = \{\langle 1,2 \rangle, \langle 3,4 \rangle, \langle 2,2 \rangle\}$ and $S = \{\langle 4,2 \rangle, \langle 2,5 \rangle, \langle 3,1 \rangle, \langle 1,3 \rangle\}$. Find $R \circ S$, $S \circ R$, $R \circ (S \circ R)$, $(R \circ S) \circ R$, $R \circ R$, $S \circ S$, & $R \circ R \circ R$.

Soln:

Q.(a) $R \circ S = \{\langle 1,5 \rangle, \langle 3,2 \rangle, \langle 2,5 \rangle\}$

$S \circ R = \{\langle 4,2 \rangle, \langle 3,2 \rangle, \langle 1,4 \rangle\} \neq R \circ S$

$(R \circ S) \circ R = \{\langle 3,7 \rangle\}$

$R \circ (S \circ R) = \{\langle 3,2 \rangle\} = (R \circ S) \circ R$.

$R \circ R = \{\langle 1,2 \rangle, \langle 2,2 \rangle\}$

$S \circ S = \{\langle 4,5 \rangle, \langle 3,3 \rangle, \langle 1,1 \rangle\}$.

$R \circ R \circ R = \{\langle 1,2 \rangle, \langle 2,2 \rangle\}$.

Q.P Ex:2. Let R & S be two relns on a set of positive integers I

$R = \{\langle x, 2x\rangle \mid x \in I\}$ $S = \{\langle x, 7x\rangle \mid x \in I\}$

Find RoS, RoR, RoRoR, and RoSoR,

Soln:

$RoS = \{\langle x, 14x\rangle \mid x \in I\} = SoR.$

$RoR = \{\langle x, 4x\rangle \mid x \in I\}$

$RoRoR = \{\langle x, 8x\rangle \mid x \in I\}.$

$RoSoR = \{\langle x, 28x\rangle \mid x \in I\}.$

Ex:3

Q.P For the reln R & S gn in Ex 1, over the set $\{1, 2, \ldots 5\}$ obtain the relm matrices for RoS, & SoR.

Soln:

$M_R$

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array}\begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

$M_S$

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array}\begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

$M_{RoS}$

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array}\begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

$M_e$ $M_R$ $M_{SoR}$

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

## Converse

Defn: Q.P

Gn a rel$^n$ R from X to Y, a rel$^n$ $\tilde{R}$ from Y to X is called the converse of R; where the ordered pairs of $\tilde{R}$ are obtained by interchanging the members in each of the ordered pairs of R.

This means, for $x \in X$, & $y \in Y$ that $x R y \Leftrightarrow y \tilde{R} x$.

Note:

1. $\tilde{\tilde{R}} = R$.
2. The rel$^n$ matrix $M_{\tilde{R}}$ of $\tilde{R}$ can be obtained by simply interchanging the rows & columns of $M_R$ such a matrix is called the transpose of $M_R$.

$\therefore M_{\tilde{R}}$ = Transpose of $M_R$.

3. The graph of $\tilde{R}$ is also obtained from that of R by simply reversing the arrows of an each arc.

To find $\tilde{R}$:

Problems: Q.P

Ex:1

1. Given the rel$^n$ matrices $M_R$ & $M_S$, find $M_{R \circ S}$, $M_{\tilde{R}}$, $M_{\tilde{S}}$, $M_{\tilde{R} \circ \tilde{S}}$ and s.t $M_{\tilde{R} \circ \tilde{S}} = M_{\tilde{S} \circ \tilde{R}}$.

Soln:

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

$\langle 1,1 \rangle$ $\langle 1,4 \rangle$ $\langle 2,3 \rangle$ $\langle 2,5 \rangle$ $\langle 3,2 \rangle$ $\langle 3,4 \rangle$

Soln:

$$M_{\tilde{R}} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \text{transpose of } M_R.$$

$\langle 1,1 \rangle$ $\langle 1,4 \rangle$ $\langle 1,1 \rangle$ $\langle 1,4 \rangle$ $\langle 2,3 \rangle$ $\langle 2,5 \rangle$ $\langle 3,2 \rangle$ $\langle 3,4 \rangle$ $\langle 3,3 \rangle$

$M_R' = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ : transpose of $M_R$.

$M_{R \circ S} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$ $\quad M_{R \tilde{\circ} S} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

$M_{\tilde{S} \circ \tilde{R}} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} = M_{R \tilde{\circ} S}$.

Note:

1. $\tilde{\tilde{R}} = R$
2. $R = S \Leftrightarrow \tilde{R} = \tilde{S}$
3. $R \subseteq S \Leftrightarrow \tilde{R} \subseteq \tilde{S}$
4. $R \tilde{\cup} S = \tilde{R} \cup \tilde{S}$
5. $R \tilde{\cap} S = \tilde{R} \cap \tilde{S}$

Transitive closure:

Let $X$ be a finite set & $R$ be a relⁿ in $X$. The relⁿ $R^+ = R \cup R^2 \cup R^3 \cup \ldots$ in $X$ is called the transitive closure of $R$ in $X$.

$R = \{\langle a,b\rangle, \langle a,c\rangle, \langle c,b\rangle\}$

Ex: $R \circ R = R^2 = \{\langle a,b\rangle\}$

$R^2 \circ R = R^3 = \phi$

$R^4 = \phi$

⋮

Q.1 (B) Partial Ordering:

A binary relⁿ $R$ in a set $P$ is called a partial order relⁿ or a partial ordering in $P$ iff $R$ is reflexive, antisymmetric and transitive.

Partial ordering is denoted by the symbol "$\leq$".

Poset:

If $\leq$ is a partial ordering on P, the ordered pair $\langle P, \leq \rangle$ is called a partial ordered set or poset.

Simple Ordering & chain:-

Defn: Let $\langle P, \leq \rangle$ be a partially ordered set. If for every $x, y \in P$ we have either $x \leq y \vee y \leq x$, then $\leq$ is called a simple ordering or linear ordering on P, and $(P, \leq)$ is called a totally ordered or simply ordered set or a chain.

Note:

1. If $R$ is denoted by $\leq$, then $\tilde{R}$ is denoted by $\geq$.
2. If $\langle P, \leq \rangle$ is a partially ordered set, then $\langle P, \geq \rangle$ is also a partially ordered set.
   $\langle P, \geq \rangle$ is called the dual of $\langle P, \leq \rangle$.

LessThan or EqualTo, GreaterThan or EqualTo:

Let R be the set of real no's. The relation "less than or equal to", or $\leq$, is a partial ordering on R.

The converse of this rein, "greaterthan or equal to" or $\geq$, is also a partial ordering on R.

Inclusion:

Let $e(A) = 2^A = X$ be the powerset of A, that is X is the set of subsets of A. The rein of inclusion ($\subseteq$) on X is a partial ordering.

The rein $\subseteq$ is a relation called proper inclusion ($\subset$) which is irreflexive, antisymmetric & transitive.

As a special case,

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

$X = e(A) = \{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$

The elements of the poset $\subseteq$

Note that: $\{\{a\}$ & $\{b,c\}\}$, $\{\{a,b\}, \{a,c\}\}$ are incomparable.

Divides and Integral Multiple:

If a & b are +ve integers, then we say "a divides b" written as $a|b$, iff there is an integer c such that $ac = b$. alternatively, we say that "b is an integral multiple of a".

The rel'n divides is a partial order relation, Let X be the set of +ve integers. The relations "divides" and "integral multiple of" are partial orderings on X and each is the converse of the other.

As a special case,

Let $X = \{2, 3, 6, 8\}$ and let $\leq$ be the rel'n "divides" on X. Then,

(i) $\leq = \{\langle 2,2\rangle, \langle 3,3\rangle, \langle 6,6\rangle, \langle 8,8\rangle, \langle 2,6\rangle, \langle 2,8\rangle, \langle 3,6\rangle\}$

The rel'n "integral multiple of", written as $\geq$ is given by

$\geq = \{\langle 2,2\rangle, \langle 3,3\rangle, \langle 6,6\rangle, \langle 8,8\rangle, \langle 8,2\rangle, \langle 6,2\rangle, \langle 6,3\rangle\}$

Lexicographic Ordering:

An example of simple or Total ordering is the lexicographic ordering.

Let R be the set of real nos. & let $P = R \times R$. The rel'n $\geq$ on R is assumed to be the usual rel'n "greater than or equal to". For any two ordered pairs $\langle x_1, y_1\rangle$ & $\langle x_2, y_2\rangle$ in P, we define the total ordering rel'n $\leq$ as follows:

- $\langle x_1, y_1 \rangle \leq \langle x_2, y_2 \rangle \Leftrightarrow x_1 < x_2 \vee ((x_1 = x_2) \wedge (y_1 \geq y_2))$

It is clear that if $\langle x_1, y_1 \rangle \nleq \langle x_2, y_2 \rangle$ then we must have $\langle x_2, y_2 \rangle \leq \langle x_1, y_1 \rangle$, so that $\leq$ is a Total ordering on P.

The partial ordering $\leq$ is called the lexicographic ordering.

Note:

- If $x$ may not be related to $y$. Then we say that $x$ & $y$ are incomparable.
- $\langle P, \geq \rangle$ is called the dual of $\langle P, \leq \rangle$.
- The relⁿ "$<$" is defined for every $x, y \in P$ as.

$$x < y \Leftrightarrow x \leq y \wedge x \neq y.$$

The relⁿ "$>$" is defined for every $x, y \in P$ as

$$x > y \Leftrightarrow x \geq y \wedge x \neq y.$$

- The relⁿ $<$ and $>$ are anti-symmetric & transitive. In addition these relations are irreflexive.

Partially ordered Set: Representation & Associated Terminology

Defn: In a partially ordered set $\langle P, \leq \rangle$, an elt $y \in P$ is said to cover an elt $x \in P$ if $x < y$ & if there does not exist any element $z \in P$ s: $x \leq z$ & $z \leq y$: that is

$$y \text{ covers } x \Leftrightarrow (x < y \wedge (x \leq z \leq y \Rightarrow x = z \vee z = y)).$$

## Hasse Diagram:

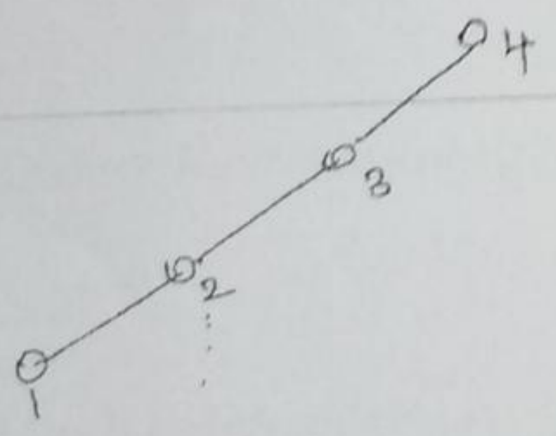
A partial ordering $\leq$ on a set P can be represented by means of a diagram known as a Hasse diagram (or) a partially ordered set diagram of $\langle P, \leq \rangle$.

In such a diagram, each elt is represented by a small circle or a dot. The circle for $x \in P$ is drawn below the circle for $y \in P$ if $x < y$, and a line is drawn blw $x$ & $y$ if $y$ covers $x$.

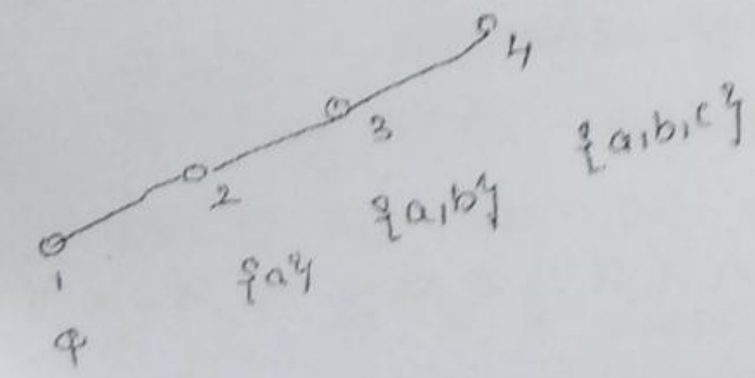
If $x < y$ but $y$ does not cover $x$, then $x$ & $y$ are not connected directly by a single line.

Eg: 1. Let $P = \{1, 2, 3, 4\}$, the Hasse diagram is shown below. The H.D of $\langle P, \leq \rangle$

-1




2. Let $P = \{\phi, \{a\}, \{a,b\}, \{a,b,c\}\}$. The Hasse diagram of $\langle P, \subseteq \rangle$



# Discrete Maths
## Unit-II

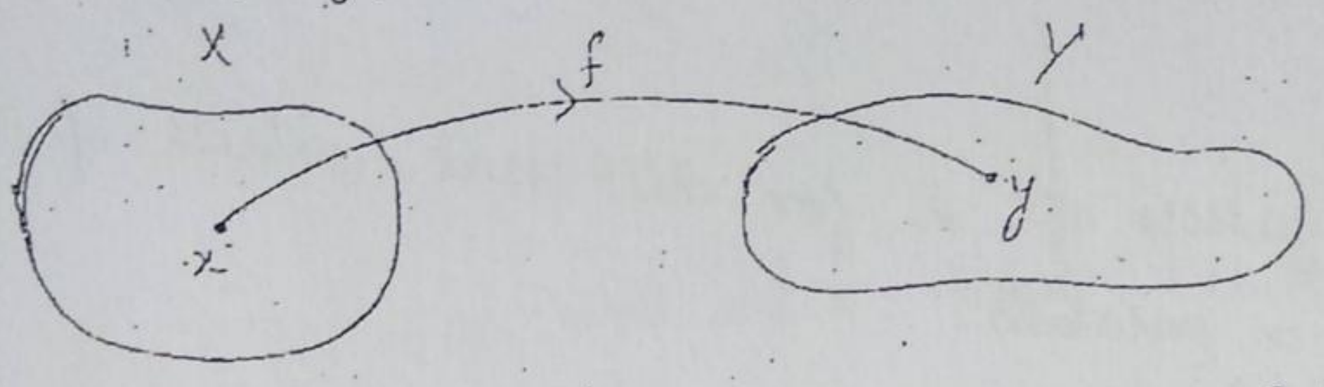


**Functions:**

**Defn: Function:**

Let x and y be any two sets. A relation f from set $X \to Y$ is called a function if $\forall x \in X$ there is a unique $y \in Y$ such that

$\langle x, y \rangle \in f$.




Terms such as "transformation", "mapping", "correspondence" and "operation" are used as synonyms for "fn."

The notations $f: X \to y$ (or) $x \xrightarrow{f} y$ are used to express f as from x to y.

For a function $f: X \to y$ if $\langle x, y \rangle \in f$ then

$x \to$ argument $y \to$ image of x under f.

We can also write $y = f(x)$ to define a fn. f.

We denote the range of f by $R_f$ by $f(X)$.

The domain of f is denoted by $D_f = X$.

The range of f, $R_f$ is a subset of y i.e. $R_f \subseteq y$.

The set y is called co-domain of f.

**Ex**

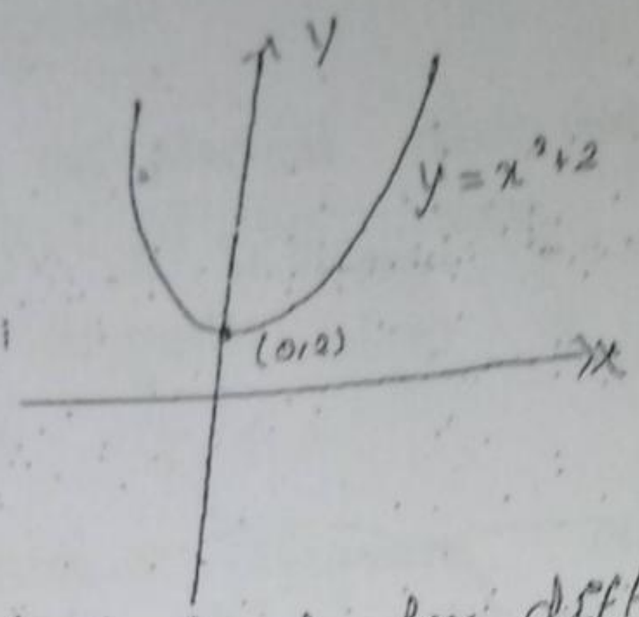
Let $X = \{1, 5, P, Jack\}$ $Y = \{2, 5, 7, q, Jill\}$

$f = \{\langle 1, 2 \rangle, \langle 5, 7 \rangle, \langle P, q \rangle, \langle Jack, q \rangle\}$ // obviously

$D_f = X$, $R_f = \{2, 7, q\}$, and // $f(1) = 2$, $f(5) = 7$,

$f(P) = q$, $f(Jack) = q$

Ex : 2 Let $x = y = R$ $f(x) = x^2 + 2$




The values of f for different values of $x \in R$ are lie on a parabola.

Ex : 3 : Let $x = y = R$

and let $f = \{ \langle x, x^2 \rangle / x \in R \}$

$g = \{ \langle x^2, x \rangle / x \in R \}$

The fn. $f : x \to y$ but g is not a function because the uniqueness condition is violated.

i, for any real no. a,

$\langle a^2, a \rangle$ & $\langle a^2, -a \rangle$ are both in g.

Ex : 4 : Let P be the set of all positive integers and

$\sigma : P \to P$ be such that

$\sigma(n) = n + 1$ where $n \in P$.

The fn. $\sigma$ is called peano's successor fn.

Let f & g be defined by

$f = \{ \langle x, \lfloor x \rfloor \rangle / x \in R \wedge \lfloor x \rfloor =$ the greatest integer less than or equal to $x \}$.

$g = \{ \langle x, \lceil x \rceil \rangle / x \in R \wedge \lceil x \rceil =$ the least integer greater than or equal to $x \}$.

the fn. $f(x) = \lfloor x \rfloor$ is called floor of x.

the fn. $f(x) = \lceil x \rceil$ is called ceiling of x.

Ex 1: $f(3.75) = \lfloor 3.75 \rfloor = 3$.

$f(4) = \lfloor 4 \rfloor = 4$.

$f(-3.75) = \lfloor -3.75 \rfloor = -4$.

$g(3.75) = \lceil 3.75 \rceil = 4$

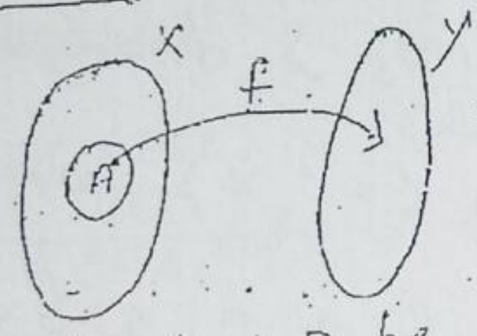
$g(4) = \lceil 4 \rceil = 4$

$g(-3.75) = \lceil -3.75 \rceil = -3$.

**Def 2:**

If $f: X \to Y$ and $A \subseteq X$. then $f \cap (A \times Y)$ is the function from $A \to Y$ is called restriction of $f$ to $A$. and written as "$f/A$".

If $g$ is restriction of $f$, then $f$ is called the extension of $g$.




Ex: Let $f: R \to R$ be given by

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

If $N$ is the set of all natural numbers $\{1, 2, 3, \ldots\}$ then $N \subseteq R$.

Then $f/N = \{\langle 1,1\rangle, \langle 2,4\rangle, \langle 3,9\rangle, \ldots\}$

Ex: Let $X = \{a, b, c\}$, $Y = \{0, 1\}$

Then $X \times Y = \{\langle a,0\rangle, \langle b,0\rangle, \langle c,0\rangle, \langle a,1\rangle, \langle b,1\rangle, \langle c,1\rangle\}$

How then are $2^6$ possible subsets of $X \times Y$ of these subsets only the following $2^3$ subsets define fns from $X$ to $Y$.

$f_0 = \{\langle a,0\rangle, \langle b,0\rangle, \langle c,0\rangle\}$

$f_1 = \{\langle a,0\rangle, \langle b,0\rangle, \langle c,1\rangle\}$

$f_2 = \{\langle a,0\rangle, \langle b,1\rangle, \langle c,0\rangle\}$

Problems:

1. For the semigroup $\langle N, \times \rangle$ let T be the set of multiples of a positive integer m; Then $\langle T, \times \rangle$ is a subsemigroup of $\langle N, \times \rangle$.

2. For the semigroup $\langle N, + \rangle$, the set E of all the even nonnegative integers is a subsemigroup $\langle E, + \rangle$ of $\langle N, + \rangle$.

3. Let X be a nonempty set and $X^X$ be the set of all mappings from X to X. Let $\circ$ denote the operation of composition of these mapping
ie, for $f, g \in X^X$, $f \circ g$ given by

$$f \circ g(x) = f(g(x)) \quad \forall x \in X \text{ in } X^X,$$

The algebra $\langle X^X, \circ \rangle$ is a monoid.

The semigroup $\langle \{0, 1\}, * \rangle$ is a subsemigroup of $\langle S, * \rangle$ but not a submonoid.

Theorem: 3.2.8

For any commutative monoid $\langle M, * \rangle$, the set of idempotent elements of M forms a submonoid.

proof:

Since the identity element $e \in M$ is idempotent $e \in S$, where S is the set of idempotents of M

Let $a, b \in S$. So that

$$a * a = a \quad \text{and} \quad b * b = b.$$

Now, $(a * b) * (a * b) = (a * b) * (b * a)$ ($\langle M, * \rangle$ is commutative)

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

Hence $a * b \in S$ and $\langle S, * \rangle$ is a submonoid.

## Direct Product :

Let $\langle S, * \rangle$ and $\langle T, \Delta \rangle$ be two semigroups. The direct product of $\langle S, * \rangle$ and $\langle T, \Delta \rangle$ is the algebraic system $\langle S \times T, \circ \rangle$ in which the operation $\circ$ on $S \times T$ is defined by,

$$\langle s_1, t_1 \rangle \circ \langle s_2, t_2 \rangle = \langle s_1 * s_2, t_1 \Delta t_2 \rangle \text{ for any } \langle s_1, t_1 \rangle \text{ and } \langle s_2, t_2 \rangle \in S \times T.$$

## Note

1. If $\langle S, * \rangle$ and $\langle T, \Delta \rangle$ are both commutative semigroups then their direct-product is also commutative.

2. If $\langle S, * \rangle$ and $\langle T, \Delta \rangle$ are monoids with $e_S$ & $e_T$ as their identity elements respectively, then their direct product $\langle S \times T, \circ \rangle$ is also a monoid with $\langle e_S, e_T \rangle$ as the identity element, because

$$\langle e_S, e_T \rangle \circ \langle s, t \rangle = \langle e_S * s, e_T \Delta t \rangle = \langle s, t \rangle$$

$$\langle s, t \rangle \circ \langle e_S, e_T \rangle = \langle s * e_S, t \Delta e_T \rangle = \langle s, t \rangle.$$

3. If $z_S$ and $z_T$ all any zeros of $\langle S, * \rangle$ and $\langle T, \Delta \rangle$ respectively. then $\langle z_S, z_T \rangle$ is a zero of $\langle S \times T, \circ \rangle$.

Ily if $s \in S$ and $t \in T$ have inverses, then $\langle s^{-1}, t^{-1} \rangle$ is the inverse of $\langle s, t \rangle$

## Group :

A group $\langle G, * \rangle$ is an algebraic system in which the binary operation $*$ on $G$ satisfies three conditions.

1. For all $x, y, z \in G$.

$$x * (y * z) = (x * y) * z \quad [\text{Associative}$$

2. There exists an $e \in G$ such that for any $x \in G$

$$x * e = e * x = x \quad [\text{Identity}$$

## permutation:

Any one-to-one mapping of a set of S onto S is called a permutation of S

**Theorem: 3.5.1**

Every row or column in the composition table of a group $\langle G, * \rangle$ is a permutation of the elements of G.

**Proof:** As a first step we shall show that no row or column in the composition table can have an element of G more than once.

Let us assume, to the contrary, that the row corresponding to an element $a \in G$ has two entries which are both k.

Assume that, $a * b_1 = a * b_2 = k$, $b_1, b_2 \in K$ and $b_1 \neq b_2$.

From the cancellation property we have $b_1 = b_2$.

which is contradiction.

As a next step of our proof, we show that every element of G appears in each row & column of the table of the composition.

For this step, again consider the row corresponding to the element $a \in G$, and let b be any element of G.

Since $b = a * (a^{-1} * b)$, b must appear in the row corresponding to the element $a \in G$.

The same argument applies to every column of the table as well.

From the above result and the fact that no two rows or columns are identical. It follows that every row of the composition table is obtained by a permutation of the elements of G and that each row is a distinct permutation.

The same result applies to the columns of the composition table.

| * | e | a |
|---|---|---|
| e | e | a |
| a | a | e |

Defn:

The order of a group $\langle G, * \rangle$, denoted by $|G|$ is the number of elements of G, when G is finite.

Abelian group:

A Group $\langle G, * \rangle$ in which the operation $*$ is commutative is called an abelian group.

Ex:1

Let I be the set of Integers. The algebraic $\langle I, + \rangle$ is an abelian group.

Ex:2

The set of rational numbers excluding zero is an abelian group under multiplication.

Note:

Consider the set of all permutations of the elements of the finite set and define a binary operation on them.

$$P_3 \diamond P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \diamond \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \diamond \begin{pmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$= P_4.$$

Note that $\langle S_3, \diamond \rangle$ is not an abelian group. It is of order 6. The degree of this permutation group is 3, because $S_3$ consists of permutations of a set of 3 elements.

The set $S_n$ of all permutations of n-elements is a permutation group $\langle S_n, \diamond \rangle$ also called the symmetric group the group $\langle S_n, \diamond \rangle$ is of order n! and degree n.

Cyclic group:

A group $\langle G, * \rangle$ is said to be cyclic if there exist an element $a \in G$ such that every element of G can be written as some power of a, that is $a^n$ for some integer n. In such a case, a cyclic group is said to be generated by a, or a is a generator of the group G.

A cyclic group is abelian, because for any $p, q \in G$ $p = a^r$ and $q = a^s$ for some $r, s \in I$ and

$$p * q = a^r * a^s = a^{r+s} = a^{s+r} = a^s * a^r = q * p.$$

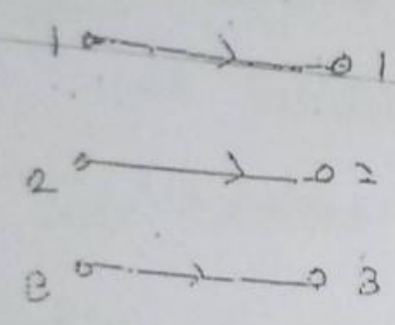
Consider the $3! = 6$ permutations of the elements of the set $\{1, 2, 3\}$.

Let us denote the set of all permutations by $S_3 = \{P_1, P_2, \ldots, P_6\}$. The elements $P_1, P_2, \ldots, P_6$ are described as follows.

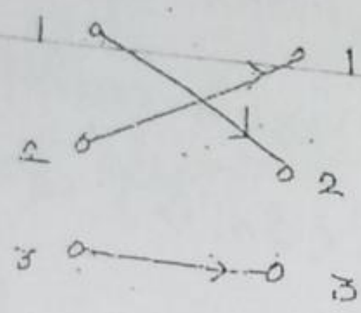
$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

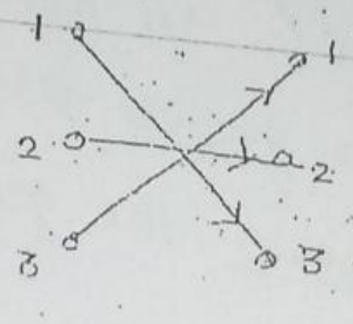
$P_1$



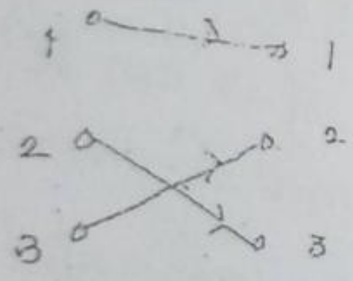
$P_2$



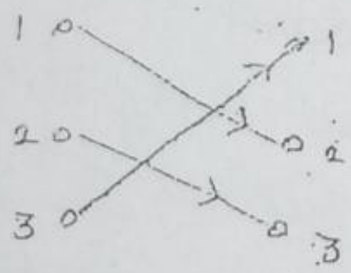
$P_3$



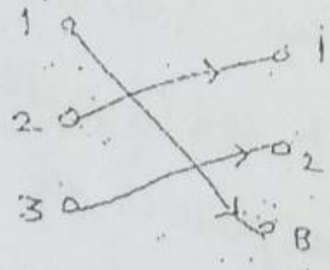
$P_4$



$P_5$



$P_6$



The composition of permutations on $S_3$ is given by

| ◇ | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | $P_6$ |
|---|---|---|---|---|---|---|
| $P_1$ | $P_1$ | $P_2$ | $P_3$ | $P_4$ | $P_5$ | $P_6$ |
| $P_2$ | $P_2$ | $P_1$ | $P_5$ | $P_6$ | $P_3$ | $P_4$ |
| $P_3$ | $P_3$ | $P_6$ | $P_1$ | $P_5$ | $P_4$ | $P_2$ |
| $P_4$ | $P_4$ | $P_5$ | $P_6$ | $P_1$ | $P_2$ | $P_3$ |
| $P_5$ | $P_5$ | $P_4$ | $P_2$ | $P_3$ | $P_6$ | $P_1$ |
| $P_6$ | $P_6$ | $P_3$ | $P_4$ | $P_2$ | $P_1$ | $P_5$ |

Theorem 3.5.2

Let $\langle G, * \rangle$ be a finite cyclic group generated by an element $a \in G$. If $G$ is of order $n$, that is $|G| = n$, then $a^n = e$, so that $G = \{a, a^2, a^3, \ldots, a^n = e\}$ furthermore, $n$ is the least +ve integer for which $a^n = e$.

Proof

Let us assume that for every +ve integer $m < n$, $a^m = e$.

Since, $G$ is a cyclic group, any element of $G$ can be written as $a^k$ for some $k \in I$.

From Euclid's algorithm, we can write $k = mq + r$, where $q$ is some integer and $0 \leq r < m$.

This means $a^k = a^{mq+r}$

$= (a^m)^q * a^r$.

$= a^r$.

So that every element of $G$ can be expressed as $a^r$ for some $0 \leq r < m$.

Thus implying that $G$ has atmost $m$ distinct elements, that is $|G| = m < n$ which is a contradiction.

Hence, $a^m = e$ for $m < n$ is not possible.

Next, we show that the elements $a, a^2, a^3, \ldots, a^n$ are all distinct, where $a^n = e$.

Assume to the contrary that $a^i = a^j$ for $i < j \leq n$.

This means that $a^{j-i} = e$ where $j - i < n$, which is again a contradiction.

## Subgroup and homomorphisms

### Subgroup

Let $\langle G, * \rangle$ be a group and $S \subseteq G$ be such that $S$ satisfies the following conditions.

1. $e \in S$, where $e$ is the identity of $\langle G, * \rangle$.
2. For any $a \in S$, $a^{-1} \in S$.
3. For any $a, b \in S$, $a * b \in S$

Then $\langle S, * \rangle$ is called a subgroup of $\langle G, * \rangle$

Note:

1. $\langle S, * \rangle$ itself is a group with the same identity element as that of $\langle G, * \rangle$
2. For any group $\langle G, * \rangle$ naturally $\langle \{e\}, * \rangle$ and $\langle G, * \rangle$ are trivial subgroups of $\langle G, * \rangle$. All other subgroups of $\langle G, * \rangle$ are called proper subgroups.
3. Let $\langle G, * \rangle$ be a group and let $a$ be any element of $G$. Obviously $G$ must contain all the integral powers of $a$, that is $a^r \in G$ for $r \in I$. This means that the cyclic groups generated by $a$ must be a subgroups of $\langle G, * \rangle$

Theorem: 3.5.3

A subset $S \neq \phi$ of $G$ is a subgroup of $\langle G, * \rangle$ iff for any pair of elements $a, b \in S$, $a * b^{-1} \in S$.

Proof:

Assuming that $S$ is a subgroup, it is clear that if $a, b \in S$ then $b^{-1} \in S$ and $a * b^{-1} \in S$

To prove the converse, let us assume that $a, b \in S$ and $a * b^{-1} \in S$, for any pair $a, b$

Taking $b=a$, $a*a^{-1}=e \in S$.

From $e, a, b \in S$, we have $e*a^{-1}=a^{-1} \in S$

Similarly $b^{-1} \in S$.

Finally because $a$ and $b^{-1}$ are in $S$, we have

$$a*b \in S.$$

Hence $\langle S, * \rangle$ is a subgroup of $\langle G, * \rangle$.

Group Homomorphism:

Let $\langle G, * \rangle$ and $\langle H, \Delta \rangle$ be two groups. A mapping $g: G \to H$ is called a group homomorphism from $\langle G, * \rangle$ to $\langle H, \Delta \rangle$ if for any $a, b \in G$

$$g(a*b) = g(a) \Delta g(b).$$

Note:

1. If $e_G$ and $e_H$ are the identities of $\langle G, * \rangle$ and $\langle H, \Delta \rangle$ respectively, then $g(e_G) = e_H$.

   Also for any $a \in G$

   $$g(a^{-1}) = [g(a)]^{-1}$$

2. If $\langle S, * \rangle$ is a subgroup of $\langle G, * \rangle$ and $g(S)$ denotes the image set of $S$ under the homomorphism $g$, then $\langle g(S), \Delta \rangle$ is a subgroup of $\langle H, \Delta \rangle$.

3. A group homomorphism $g$ is called a monomorphism, epimorphism or isomorphism depending upon whether $g$ is one-to-one, onto or one-to-one and onto respectively.

4. A homomorphism from a group $\langle G, * \rangle$ to $\langle G, * \rangle$ is called an endomorphism, while an isomorphism of $\langle G, * \rangle$ to $\langle G, * \rangle$ is called an automorphism.

Defn:
Let $g$ be a group homomorphism from $\langle G, * \rangle$ to $\langle H, \Delta \rangle$. The set of elements of $G$ which are mapped into $e_H$, the identity of $H$, is called the kernal of the homomorphism $g$ and denoted by $\ker(g)$.

Theorem: 3.5.4

The kernal of a homomorphism $g$ from a group $\langle G, * \rangle$ to $\langle H, \Delta \rangle$ is a subgroup of $\langle G, * \rangle$.

Navaneetakrishnan

Proof:

Since $g(e_G) = e_H$, $e_G \in \ker(g)$

Also if $a, b \in \ker(g)$, that is $g(a) = g(b) = e_H$, then so that $a * b \in \ker(g)$

Finally if $a \in \ker(g)$, then $g(a^{-1}) = [g(a)]^{-1} = e_H^{-1} = e_H$

Hence $a^{-1} \in \ker(g)$ and $\ker(g)$ is a subgroups of $\langle G, * \rangle$.

Cayley's Theorem:

V.B.C

Theorem: 3.5.5

(Every finite group of order $n$) is isomorphic to a permutation group of degree $n$.

Proof:

Let $\langle G, * \rangle$ be a group of order $n$.

We know that, (Every row & column in the composition table of $\langle G, * \rangle$ represents a permutation of the elements of $G$)

Corresponding to an element $a \in G$, we denote by $P_a$ the permutation given by the column under $a$ in the composition table, Thus,

$P_a(c) = c * a$ for any $c \in G$.

for every element we can define permutations of the elements of G.

Let the set of permutations be denoted by P.

obviously P has n-elements

We shall now show that $\langle P, \diamond \rangle$ is a group, where $\diamond$ denote the right composition of the permutations of P. $(P, \diamond)$

Note that, since $e \in G$, $p_e \in P$ and

$$p_e \diamond p_a = p_a \diamond p_e = p_a \quad \text{for any } a \in G.$$

Also for any $a \in G$,

$$p_a^{-1} \diamond p_a = p_e.$$

Also for $a, b \in G$,

$$p_a \diamond p_b = p_{a*b} \rightarrow (1)$$

eqn (1) shows that for any element $c \in G$,

$$p_a(c) = c * a$$

so that $(p_a \diamond p_b)(c) = (c*a)*b = c*(a*b)$

$$= p_{a*b}(c)$$

Hence, $(P, \diamond)$ is a group

The last step is sufficient to gaurantee that $\langle P, \diamond \rangle$ is a group; because it shows that $\langle P, \diamond \rangle$ is isomorphic to $\langle G, * \rangle$.

Consider a mapping $f: G \rightarrow P$ given by $f(a) = p_a$ for any $a \in G$.

Consider a mapping $f: G \rightarrow P$ given by $f(a) = p_a$ for any $a \in G$.

Naturally, f is 1-1, onto according to Thm 3.5.1 (1) can be written as

$$f(a*b) = f(a) \diamond f(b)$$

$\therefore$ f is an isomorphism.

45 43.

## Cosets and Lagrange's Theorem:

**Defn:**

Let $\langle H, * \rangle$ be a subgroup of $\langle G, * \rangle$. For any $a \in G$ the set $aH$ defined by

$$aH = \{a * h / h \in H\}$$

is called the left coset of $H$ in $G$ determined by the element $a \in G$. The element $a$ is called the representative element of the left coset $aH$.

**Theorem: 3.5.6**

Let $\langle H, * \rangle$ be a subgroup of $\langle G, * \rangle$. The set of left cosets of $H$ in $G$ form a partition of $G$. Every element of $G$ belongs to one and only one left coset of $H$ in $G$.

**Proof:**

First let us p.T every element of $G$ appear in atleast one left coset.

Let $aH = \{a * h / h \in H\}$ is a left coset of $H$ in $G$.

for $a \in G$, $e \in H \Rightarrow a * e \in aH$

Every element of $G$ appears atleast one left coset.

We know that the left coset or right coset of $H$ in $G$ are either identical or disjoint.

Each element of $G$ appears in exactly one and only one left coset of $G$.

Since the union of disjoint coset of $H$ in $G$ are equal to $G$.

$\therefore$ The set of left coset form a partition of $G$.

Left coset theorem:

Let $\langle G, * \rangle$ be a group and $\langle H, * \rangle$ be a subgroups of $\langle G, * \rangle$. We shall define an equivalence relation with respect to the subgroup $\langle H, * \rangle$ a left coset relation modulo H denoted by the symbol $\equiv$, such that, for $a, b \in G$

$a \equiv b$ or more precisely $a \equiv b \pmod{H}$ If $b^{-1} * a \in H$.

To show that this relation is an equivalence relation.

(i) Reflexive:

Since H is a subset of G, $e_G \in H$

For any $a \in G$, $a^{-1} * a = e_G \in H$

$\therefore a \equiv a \pmod{H}$

$\therefore aH$ is reflexive.

(ii) Symmetric

If $b^{-1} * a \in H$;

Then $(b^{-1} * a)^{-1} = a^{-1} * b \in H$.

$\Rightarrow$ If $a \equiv b \pmod{H}$ then $b \equiv a \pmod{H}$.

$\therefore aH$ is symmetric.

(iii) Transitive

If $b^{-1} * a \in H$ & $c^{-1} * b \in H$ i, $a \equiv b \pmod{H}$ &

Then $c^{-1} * a = (c^{-1} * b) * (b^{-1} * a) \in H$. $b \equiv c \pmod{H}$.

$= c^{-1} * e * a \in H$.

$= c^{-1} * a \in H$.

$\Rightarrow a \equiv c \pmod{H}$.

$\therefore aH$ is transitive.

416.45

Note:

We shall denote the equivalence class containing $a$ by $[a]$ i.e., $[a] = \{x \in G / x \equiv a \pmod{H}\}$

$= \{x \in G / a^{-1} * x \in H\}$

$= \{a * h / h \in H\}$

Normal subgroups:

A subgroup $\langle H, * \rangle$ of $\langle G, * \rangle$ is called a normal subgroup if for any $a \in G$, $aH = Ha$ (or)

A subgroup $\langle H, * \rangle$ of a group $\langle G, * \rangle$ is said to be a normal subgroups of $G$ if for $H \in G$ for $x \in H$, $xhx^{-1} \in H$ (or) $xHx^{-1} \in H$.

Note:

1. A subgroup $A$ of a group is normal iff $xhx^{-1} = H \ \forall x \in G$.
2. $aH = Ha$ does not necessarily mean that $a * h = h * a$. for any $h \in H$. It means that $a * h = h_1 * a$ for some $h, h_1 \in H$.
3. If $A$ is a normal subgroups then both left & right cosets of $H$ in $G$ are equal.

Theorem:

A subgroup $H$ of $G$ is normal iff each left coset of $H$ in $G$ is equal to the right coset of $H$ in $G$.

Proof:

Let $H$ be a normal subgroup of $G$, then

$xHx^{-1} = H$ for all $x \in G$.

$(xHx^{-1})x = Hx$.

$xHe = Hx$.

$xH = Hx$. for every $x \in G$.

Each left coset of $H$ in $G$ is equal to the right coset of $H$ in $G$

$$xH = Hx \quad \forall x \in G.$$

$$(xH)x^{-1} = Hxx^{-1}$$

$$xHx^{-1} = He$$

$$xHx^{-1} = H.$$

$\therefore$ H is a normal subgroups of G.

**Theorem: 3.58**

Let $\langle G, * \rangle$ and $\langle H, \Delta \rangle$ be groups and $g: G \to H$ be a homomorphism, then the kernal of g is a normal subgroup.

**proof:**

W.K.T $K = \ker(g) = \{a / a \in G \text{ and } g(a) = e_H\}$ is a subgroup of $\langle G, * \rangle$.

now, for any $a \in G$, and $k \in K$

$$g(a^{-1} * k * a) = g(a^{-1}) \Delta g(k) \Delta g(a).$$

$$= g(a^{-1}) \Delta e_H \Delta g(a).$$

$$= [g(a)]^{-1} \Delta g(a).$$

$$= e_H.$$

Hence $a^{-1} * k * a \in K$, which shows that K is a normal subgroup.