Relations and ordering

Relations

Familiar Examples of relations such as

Ex: Relation of family

Father to Son

Mother to Son

Brother to Sister

Ex on arithmetic (Real no.s)

"greater than" "less than" "equality"

We also know the relation between the

Area of a square and its side

Area of a circle and its radius

A relation between two objects can be defined by listing the two objects as an ordered pair.

A set of all such ordered pairs, in each of which the 1st member has some definite relationship to the second, describes a particular relationship.

Def Binary relation

A set of order pairs defines a binary relation

We shall call a binary relation simply a relation.

Notation $(x, y) \in R$, where R is a relation

↳ x is in relation R to y

x is related to y by R

x R y related to y

In mathematics, relations are often denoted by special symbols rather than by capital letters.

Ex1 A familiar example is the relation "greater than" for real numbers. The relation is denoted by '>'

$$> = \{ (x, y) \mid x, y \text{ are real numbers and } x > y \}$$

Ex2 The relation of father to his child can be described by a set, say F, of ordered pairs in which the 1st member is the name of the father and second the name of his child. That is

$$F = \{ (x, y) \mid x \text{ is a father of } y \}$$

Relation A and B two sets $R \subseteq A \times B$.
↳ Relation
$(x, y) \in R$ then $x \in A$ and $y \in B$.

Ex3. Let R denote the set of real numbers. Then

$$Q = \{ (x^2, x) \mid x \in R \}$$

defines the relation of the squares of a real number.

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

$$D(S) = \{ x \mid (\exists y) \ (x, y) \in S \}$$

Def **Range**: The set R(S) of all objects y such that for some x, $(x, y) \in S$ is called the range of S that is

$$R(S) = \{ y \mid (\exists x \cdot (x, y) \in S) \}$$

The definition of relation permits any set of ordered pairs to define a relation. For example, the set S is given by

$$S = \{(2,4), (1,3), (\lambda,6), (\text{Toan}, \mu)\}$$

For relation S described above we have

$$D(S) = \{2, 1, \lambda, \text{Toan}\} \quad R(S) = \{4, 3, 6, \mu\}$$

Let X and Y be any two sets. A subset of the Cartesian product $X \times Y$ defines a relation. Say C.

We have $D(C) \subseteq X$ and $R(C) \subseteq Y$.

If $X = Y$ then C is called a relation in X (or on X).

Thus any relation in X is a subset of $X \times X$.

The set itself $(X \times X)$ defines a relation in X called Universal relation

While the empty set which is also a subset of $X \times X$. is called Void relation.

If R is the set of real numbers, then the elements of $R \times R$ can be represented by points in a plane

$$R_1 = \{(x,y) / (x,y) \in R \times R \wedge x * y \geq 1\}$$

$$R_2 = \{(x,y) / (x,y) \in R \times R \wedge x^2 + y^2 \leq 9\}$$

$$R_3 = \{(x,y) / (x,y) \in R \times R \wedge y^2 < x\}$$

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

$$R = \{(x,y) / x \in X \wedge y \in X \wedge (x-y) \text{ is an integral non zero multiple of } 2\}$$

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

$$S = \{(x,y) / x \in X \wedge y \in X \wedge (x-y) \text{ is an integral non zero multiple of } 3\}$$

$$= \{(1,4), (4,1)\}$$

(b) Find RUS and RNS.

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

$RNS = \phi$.

Properties of Binary Relations in a Set.

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

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

Ex. 1. The relation $\leq$ is reflexive in the set of real numbers
∵ for any x we have $x \leq x$.

Similarly

2. The relation of equality of sets is also reflexive
3. The relation $<$ is not reflexive in the set of real numbers.
4. The relation of inclusion is reflexive in the family of all subsets of Universal set.
5. The relation of proper inclusion is not reflexive in the family of subsets of a Universal set.

Def: Symmetric

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

Ex: 1. The relations $\leq$ and $<$ are not symmetric in the set of real numbers.

2. The relation equality $(=)$ is symmetric in R

3.

3 The Relation of Similarity in a Set of triangles in a plane is both reflexive and symmetric.

4 The relation of being brother is not symmetric in the set of all people

5 But the relation of being brother is symmetric in the set of all males

Def: Transitive

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

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

Ex. 1. The Relations $\leq$, $<$ and $=$ are transitive in R

2. The Relations $\subseteq$, $\subset$ and equality are also transitive in the family of subsets of Universal set.

3. The Relation of Similarity of triangles in a plane is transitive

4 The Relation of being brother is not transitive.

Def: Irreflexive: A relation R in a set X is irreflexive if for every $x \in X$, $(x, x) \notin R$.

Note: Any relation which is not reflexive is not necessarily irreflexive. and Vice Versa.

Ex: 1. The relation $<$ in the set of real numbers is irreflexive because for no x do we have $x < x$.

2. The relation of Proper inclusion in the set of all non empty subsets of a Universal set is irreflexive.

3. for a set $A = \{1,2,3\}$.

$S = \{(1,1), (1,2), (3,2), (2,3), (3,3)\}$ is not reflexive and not irreflexive

3 The Relation of Similarity in a Set of triangles in a plane is both Reflexive and Symmetric

4 The Relation of being brother is not Symmetric in the Set of all people

5 But the Relation of being brother is Symmetric in the Set of all males

Def: Transitive

A Relation R in a Set X is transitive if, for every x, y and z in X, whenever $x R y$ and $y R z$, then $x R z$. That is

R is transitive in $X \iff (x)(y)(z)\big((x \in X \wedge y \in X \wedge z \in X \wedge x R y \wedge y R z) \rightarrow x R z\big)$

Ex 1 The Relations $\leq$, $<$ and $=$ are transitive in R

2 The Relations $\subseteq$, $\subset$ and equality are also transitive in the family of Subsets of Universal Set

3 The Relation of Similarity of triangles in a plane is transitive

4 The Relation of being brother is not transitive

Def: Irreflexive: A Relation R in a Set X is irreflexive if for every $x \in X$, $(x, x) \notin R$.

Note: Any Relation which is not Reflexive is not necessarily irreflexive and Vice Versa

Ex: 1 The Relation $<$ in the Set of Real numbers is irreflexive because for no x in R we have $x < x$

2 The Relation of Proper inclusion in the Set of all non empty Subsets of a Universal Set is irreflexive.

3 For a Set $A = \{1, 2, 3\}$

$S = \{(1,1), (1,2), (3,2), (2,3), (3,3)\}$ is not Reflexive and not irreflexive

3 The Relation of Similarity in a Set of triangles in a plane is both reflexive and symmetric.

4 The relation of being brother is not symmetric in the set of all people

5 But the relation of being brother is symmetric in the set of all males

Def: Transitive

A Relation R in a Set X is transitive if, for every x, y and z in X, whenever xRy and yRz, then xRz, that is

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

Ex. 1 The Relations $\leq$, $<$ and $=$ are transitive in R

2. The Relations $\subseteq$, $\subset$ and equality are also transitive in the family of subsets of Universal set.

3. The Relation of similarity of triangles in a plane is transitive

4. The Relation of being brother is not transitive.

Def: Irreflexive: A Relation R in a Set X is irreflexive if for every $x \in X$, $(x, x) \notin R$.

Note: Any Relation which is not reflexive is not necessarily irreflexive. and Vice Versa.

Ex: 1. The relation $<$ in the Set of Real numbers is irreflexive because for no x do we have $x < x$.

2. The Relation of proper inclusion in the Set of all non empty subsets of a Universal Set is irreflexive.

3. For a Set $A = \{1,2,3\}$.

$S = \{(1,1), (1,2), (3,2), (2,3), (3,3)\}$ is not reflexive and not irreflexive

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

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

Ex. 1. Let R be the set of real numbers. The relations $\geq$ (greater than) and $\leq$ (less than) in R are both irreflexive, symmetric and transitive.

2. Let X be the set of all courses offered at a University and for $x \in X$ and $y \in X$, xRy if x is a prerequisite for y. The relation of being a prerequisite is irreflexive and transitive.

3. Let X be the set of all male Canadians and let xRy, where $x \in X$ and $y \in X$, denote the relation "x is a brother of y". The relation R is irreflexive and symmetric but not transitive.

4. Let X be the collection of the subsets of a Universal set. The relation of inclusion in X is reflexive, antisymmetric and transitive. ~~Also~~

5. The relation of proper inclusion in X is irreflexive antisymmetric and transitive.

Relation matrix and the Graph of a Relation

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. M_R, $M(R)$, Matrix of the Relation

Let $X = \{x_1, x_2, \ldots, x_m\}$, $Y = \{y_1, y_2, \ldots, y_n\}$ and R be the Relation from X to Y. As a special case, Consider $m = 3$, $n = 2$ and

$X = \{x_1, x_2, x_3\}$
$Y = \{y_1, y_2\}$

$$R = \{(x_1, y_1), (x_2, y_1), (x_3, y_2), (x_2, y_2)\} \quad \text{---(1)}$$

If $x_i R y_j$, then we enter a '1' in ith row and jth column

If $x_k \not R x_l$ then we enter a '0' in the kth row and jth column

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

where r_{ij} is the element in the ith row and jth column.

The matrix obtained in this way is called the Relation matrix

If X has 'm' elements and Y has 'n' elements, then the Relation matrix is an $m \times n$ matrix.

For the Relation R in eq(1)

	y_1	y_2
x_1	1	0
x_2	1	1
x_3	0	1

	y_1	y_2
x_1	1	0
x_2	1	1
x_3	0	1

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

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

The matrix of R

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

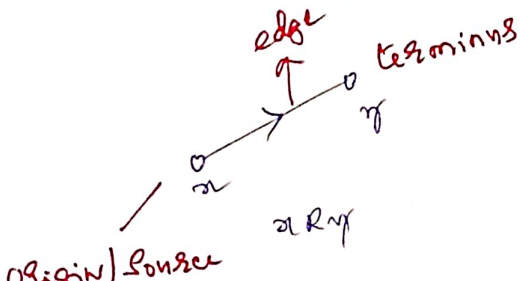
Digraph of a Relation

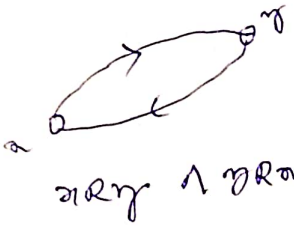
A Relation can also be represented by pictorially by drawing its graph. Here we use graphs only as a tool to represent Relations. Let R be a Relation in a set $X = \{x_1, \dots, x_m\}$.

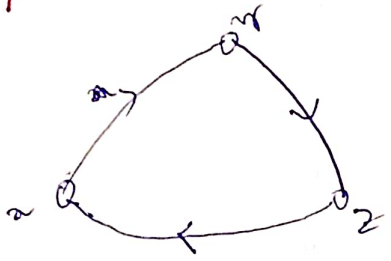
directed graph / digraph of R

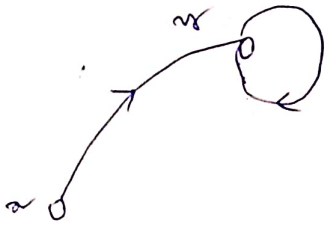
The elements of X are represented by points or circles called nodes / Bullets. The nodes corresponding to x_i and x_j are labeled x_i and x_j respectively. These nodes may also be called Vertices.

If $x_i R x_j$, that is if $(x_i, x_j) \in R$, then we connect nodes x_i and 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 (directed graph) of the Relation R. If $x_i R x_j$ and $x_j R x_i$, then we draw two arcs between x_i and x_j. For the sake of simplicity, we may replace the two arcs by one arc with arrows pointing in both directions. 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.







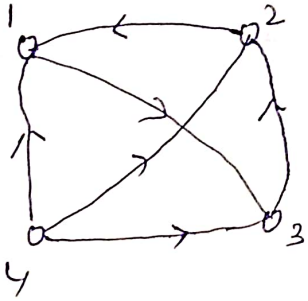


Isolated Vertex. A Vertex which is neither a source nor a terminus of any edge is called **isolated Vertex**

Example: Let $X = \{1, 2, 3, 4\}$ and $R = \{(x, y) \mid x > y\}$

Draw the graph of R and also its matrix

Sol: The relation $R = \{(4,1), (4,2), (4,3), (3,1), (3,2), (2,1)\}$



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

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

	B_0	B_1	B_2	B_3	B_4	B_5	B_6	B_7
B_0	0	1	1	1	1	1	1	1
B_1	0	0	0	1	0	1	0	1
B_2	0	0	0	1	0	0	1	1
B_3	0	0	0	0	0	0	0	1
B_4	0	0	0	0	0	0	1	1
B_5	0	0	0	0	0	0	0	1
B_6	0	0	0	0	0	0	0	0
B_7	0	0	0	0	0	0	0	0

The relations given in Example 1 and 2 are both transitive, antisymmetric, and irreflexive

From the graph of a Relation it is possible to observe some of its properties

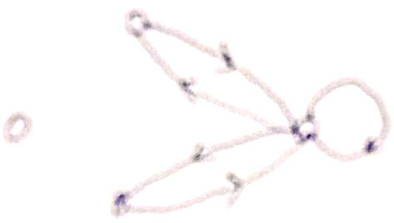
→ If a Relation is Reflexive, then there must be a loop at each node

→ If a Relation is Irreflexive, then there is no loop at any node

→ If a Relation is Symmetric and if one node is connected to another, then there must be a Relation also from the second node to first node

→ For each Symmetric Relation on Set A and Relation pairs should exist.

→ If a Relation is Transitive, the Relation is not in Triangle



Symmetric

anti Symmetric

Example

From the graph of a relation it is possible to observe some of its properties.

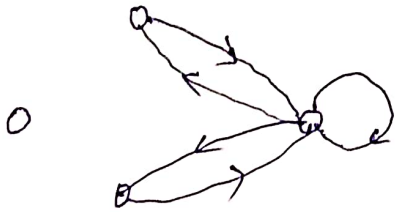
→ If a relation is reflexive, then there must be a loop at each node

→ If a relation is irreflexive, then there is no loop at any node

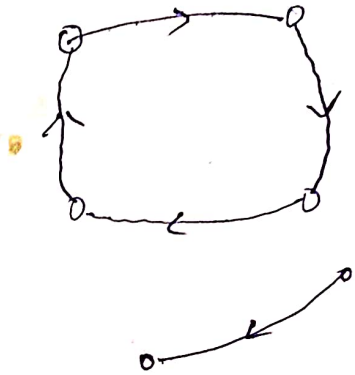
→ If a relation is symmetric and if one node is connected to another, then there must be a return arc from the second node to first node

→ For anti symmetric relations no such directed return path should exist.

→ If a relation is transitive, the situation is not so simple.



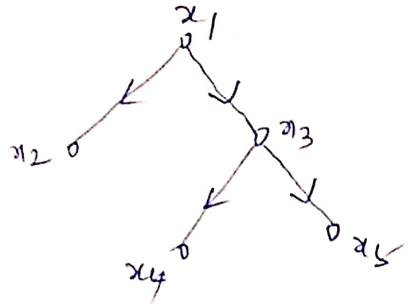
Symmetric



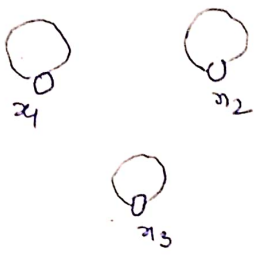
anti symmetric

Example.

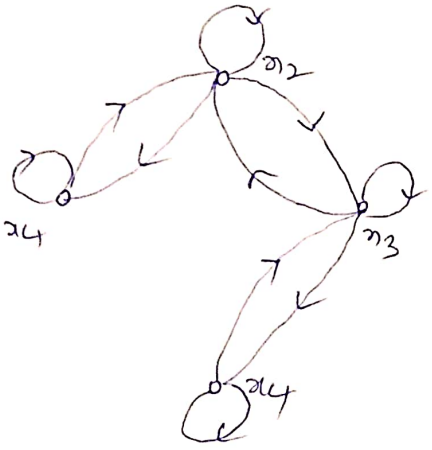
Ex Determine the properties of the relation given by graphs and also write the corresponding relation matrices



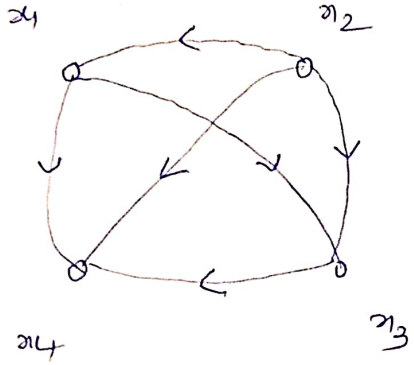
	x_1	x_2	x_3	x_4	x_5
x_1	0	1	0	0	1
x_2	0	0	0	0	0
x_3	0	0	0	1	1
x_4	0	0	0	0	0
x_5	0	0	0	0	0



	x_1	x_2	x_3
x_1	1	0	0
x_2	0	1	0
x_3	0	0	1



	x_1	x_2	x_3	x_4
x_1	1	1	0	1
x_2	1	1	1	0
x_3	0	1	1	0
x_4	1	0	0	1



	x_1	x_2	x_3	x_4
x_1	0	0	1	1
x_2	1	0	1	1
x_3	0	0	0	1
x_4	0	0	0	0

Equivalance Relations

Def: A relation R in a set X is called an equivalance relation if it is reflexive, symmetric and transitive.

If R is an equivalance relation in a set X. then $D(R)$. the domain of R is X itself.

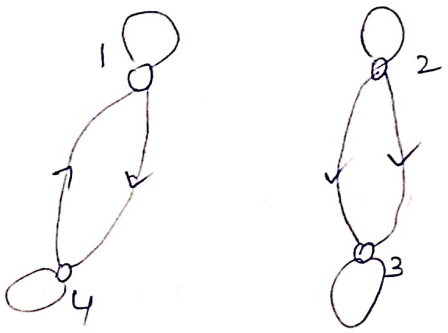
1. Equality of numbers on a set of real numbers
2. Equality of subsets of universal set-
3. Similarity of triangles on the set of triangles
4. Relation of lines being parallel on a set of lines in a plane
5. Relation of living in the same town on the set of persons living in Canada

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

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

Write the matrix of R and sketch its graph

Sol: It is clear that R is an equivalance relation



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

Ex $A = \{1, 2, 3, 4\}$ and $R = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,3), (3,3), (4,4)\}$ be a relation on A.

Verify that R is an equivalence relation

Sol We have to show that R is reflexive, symmetric, and transitive

First we note that all of $(1,1), (2,2), (3,3), (4,4)$ belongs to R

That is $(a,a) \in R$ for all $a \in A$

$\therefore$ R is reflexive

Next, we note the following

$(1,2), (2,1), (3,4), (4,3) \in R$ and

that is if whenever $(a,b) \in R$ then $(b,a) \in R$ for $a,b \in A$

Therefore R is symmetric relation. Lastly, we note that

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

$(4,3), (3,4), (4,4) \in R$.

That is, if whenever $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$.

for $a,b,c \in A$. Therefore R is transitive relation

Accordingly, R is an equivalence relation

Reflexive

Example: Let $X = \{1, 2, \ldots, 7\}$ and

$R = \{(x, y) / x - y \text{ is divisible by } 3\}$

1. For any $a \in X$, $a - a$ is divisible by 3. Hence R is reflexive
2. For any $a, b \in X$, if $a - b$ is divisible by 3:
   then $b - a$ is also divisible by 3'
   i.e. $aRb \Rightarrow bRa$, Thus R is symmetric
3. For $a, b, c \in X$, if aRb and bRc then both
   $a - b$ and $b - c$ are divisible by 3'
   So that $a - c = (a - b) + (b - c)$ is also divisible by 3'
   and hence aRc. Thus R is transitive
   $\therefore$ R is equivalance relation

Ex: $R = \{(x, y) / x - y \text{ is divisible by } m\}$
R is a equivalence relation.

Compatibility Relations

Def: A relation R in X is said to be a Compatibility relation if it is reflexive and symmetric.

Ex: Obviously all equivalance relations are Compatibility relations.

Let $X = \{$ ball, bed, dog, let, egg$\}$ and let the relation $R = \{(x, y) / x, y \in X$ and xRy if x and y contain some common letter$\}$

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

$R_2 = \{(1,1), (2,2), (1,2), (2,1)\}$ — not reflexive symmetric

$R_3 = \{(1,1), (2,2), (3,3), (1,2), (2,3)\}$ — not symmetric reflexive

Partition and Covering of a Set-

Def: Let S be a given set and $A = \{A_1, A_2, \dots, A_m\}$ where each A_i, $i = 1, 2, \dots, m$ is a subset of S and

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

then the set A is called Covering of S, and the sets $A_1, A_2, \dots, A_m$ are said to cover S.

The elements of A, which are subsets of S are mutually disjoint, then A is called a partition of S.

The sets $A_1, A_2, \dots, A_m$ are called the blocks of the partition

For example let $S = \{a, b, c\}$ and consider the following collections of subsets S.

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

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

The sets A and F are Coverings of S.

The sets C, D, and E are partitions of S.

(Of Course every partition is also Covering.)

The set B is neither a partition nor a Covering of S.

The partition D has only one blocks and E has three blocks.

Composition of Binary Relations

Def: Let R be a relation from X to Y.
S be a relation from Y to Z

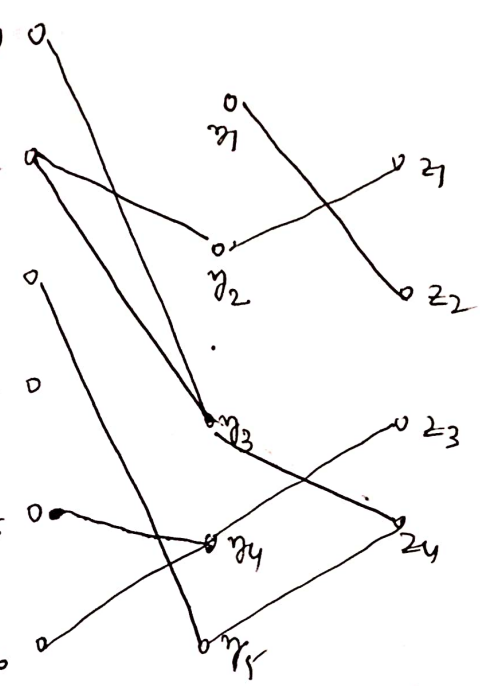
Then the relation written as $R \circ S$ is called a Composite relation of R and S. where

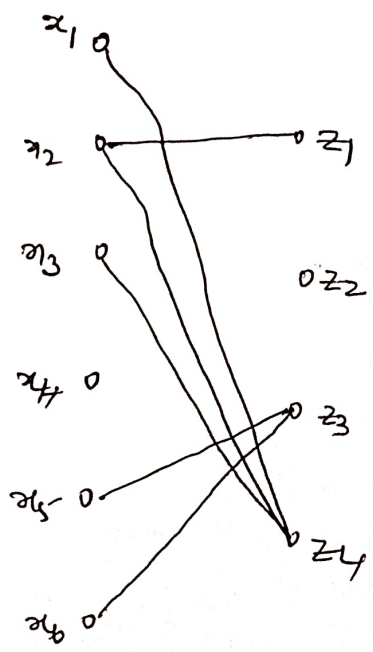
$$R \circ S = \{(x, z) \mid x \in X \wedge z \in Z \wedge (\exists y)(y \in Y \wedge (x, y) \in R \wedge (y, z) \in S)\}$$

The operation of obtaing $R \circ S$ from R and S called Composition Product of Relations.

Note: 1. $R \circ S$ is empty if the intersection of the range of R and domain of S is empty

2. For the relation $R \circ S$, the domain is a subset of X and the range is a subset of Z.





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

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

find $R \circ S$, $S \circ R$, $R \circ (S \circ R)$, $(R \circ S) \circ R$, $R \circ R$, $S \circ S$ and $R \circ R \circ R$.

Sol:

$R \circ S = \{(1,5), (3,2), (2,5)\}$

$S \circ R = \{(4,2), (3,2), (1,4)\} \neq R \circ S$.

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

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

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

$S \circ S = \{(4,5), (3,3), (1,1)\}$

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

Example: Let R and S be two relations on a set of +ve integers I:

$R = \{(x, 2x) \mid x \in I\}$, $S = \{(x, 7x) \mid x \in I\}$

find $R \circ S$, $R \circ R$, $R \circ R \circ R$ and $R \circ S \circ R$

$R \circ S = \{(x, 14x) \mid x \in I\} = S \circ R$.

$R \circ R = \{(x, 4x) \mid x \in I\}$

$R \circ R \circ R = \{(x, 8x) \mid x \in I\}$

$R \circ S \circ R = \{(x, 28x) \mid x \in I\}$

Ex: For the relations R and S given in above example over the set $\{1,2,3,4,5\}$ obtain the relation matrices for $R \circ S$ and $S \circ R$.

Solution

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

M_R $\qquad$ M_S $\qquad$ $M_{R \circ S}$

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

M_S $\qquad$ M_R $\qquad$ $M_{S \circ R}$

Def / Ex Given a relation $R : X \to Y$ then a relation

$\tilde{R} : Y \to X$ is called 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 $x \in X$ and $y \in Y$, that $x R y \iff y \tilde{R} x$

Note From this definition $\tilde{R}$ it follows that

$$\tilde{\tilde{R}} = R.$$

The relation matrix $M_{\tilde{R}}$ of $\tilde{R}$ can be obtained by simply interchanging the rows and columns of M_R. Such a matrix is called the transpose of M_R. Therefore

$$M_{\tilde{R}} = \text{transpose of } M_R.$$

R is a relation from X to $Y \Rightarrow \tilde{R}$ is a relation from Y to X.

S is a relation from Y to $Z \Rightarrow \tilde{S}$ is a relation from Z to Y.

$R \circ S$ is a relation from X to $Z \Rightarrow R \circ S$ is a relation from Z to X

$$\underline{R \circ S = \tilde{S} \circ \tilde{R}}$$

The same rule can be expressed in terms of the relation matrices by saying that the transpose of $M_{R \circ S}$ is same as the matrix $M_{\tilde{S} \circ \tilde{R}}$.

Ex: Given the relation matrices M_R and M_S. Find $M_{R\cup S}$, $M_{\tilde{R}}$, $M_{\tilde{S}}$, $M_{R\circ S}$ and S.T. $M_{R\circ S} = M_{\tilde{S}\circ\tilde{R}}$

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

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

$$M_{\tilde{S}} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \text{Transpose of } M_S$$

$$M_{R\cup S} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \qquad M_{R\circ S} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

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

Ex Prove that the relation "congruence modulo m" given by

$\equiv = \{ \langle x, y \rangle \mid x-y \text{ is divisible by } m \}$

$a \equiv b \pmod{n}$ iff $a-b$ is multiple of n

or equivalently, $(a-b) = kn$ for some $k \in \mathbb{Z}$

First we note that for every $a \in \mathbb{Z}$, $a-a = 0$ is a multiple of n.

That is $a \equiv a \pmod{n}$. or aRa, $\therefore R$ is Reflexive

Next, we note that - for all $a, b \in \mathbb{Z}$

$$aRb \Rightarrow a \equiv b \pmod{n}$$
$$\Rightarrow a - b \text{ is divisible by } n$$
$$\Rightarrow b - a \text{ is divisible by } n$$
$$\Rightarrow b \equiv a \pmod{n}$$
$$\Rightarrow bRa$$

$\therefore$ R is symmetric

Lastly, we note that - for $a, b, c \in \mathbb{Z}$

aRb and $bRc \Rightarrow a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$
$\Rightarrow a - b$ and $b - c$ are multiples of n
$\Rightarrow (a - b) + (b - c)$ is a multiple of n
$\Rightarrow \therefore a \equiv c \pmod{n}$
$\Rightarrow aRc$

$\therefore$ R is transitive.

This proves that R is an equivalence relation

Partial Ordering

Def A binary relation R in a set P is called Partial ordering or Partial order relation in P iff R is reflexive, antisymmetric and transitive.

It is conventional to denote a partial ordering by the symbol $\leq$. This symbol does not necessarily mean "less than or equal to". as is used for real numbers.

Since the relation of partial ordering is reflexive we shall hencefoth call it a relation on a set. say P.

If $\leq$ is a partial ordering on P, then the ordered pair $(P, \leq)$ is called partially ordered set or a poset.

Def: Let $(P, \leq)$ 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.

If R is a partial ordering on P, then it is easy to see that the converse of R, namely $\tilde{R}$, is also a partial ordering on P. If R is denoted by $\leq$ then $\tilde{R}$ is denoted by $\geq$. This means that - if $(P, \leq)$ is a partially ordered set, then $(P, \geq)$ is also a partially ordered set.

$(P, \geq)$ is called the dual of $(P, \leq)$

Partial ordering

Def A relation R on a set A is called partial ordering relation or partial order on A iff

(i) R is reflexive

(ii) R is antisymmetric

(iii) R is transitive, on A

A set A with partial ordering R defined on it is called partially ordered set or an ordered set or a poset. and it is denoted by the ordered pair (A, R).

Examples: The relation "~~less than or~~ less than or equal to" (or $\leq$, $\star$) on the set of Real numbers R, is a partial ordering on R. because, this relation is reflexive, antisymmetric, and transitive). Thus $(R, \leq)$ is a poset.

Ex The relation "is greater than or equal to". denoted by $\geq$, is also a partial ordering on R. that is $(Z, \geq)$ is also a poset.

Ex The "divisibility relation" on the set Z^+ defined by a divides b. (denoted by a/b) for all $a, b \in Z^+$ is a partial order on Z^+.

Sol. for any $a \in Z^+$, the statement 'a divides a' is true

Thus aRa $((a,a) \in R)$ for all $a \in Z^+$.

Hence R is reflexive.

for any $a, b \in \mathbb{Z}^+$, 'a divides b' need not imply that "b divides a" (for instance, 3 divides 6 but 6 does not divides 3)

Thus aRb does not always imply bRa. Hence R is not symmetric

Further 'a divides b' and 'b divides a' imply that $a = b$.

Thus aRb and bRa imply $a = b$. Therefore R is antisymmetric

Lastly, we note that for any $a, b, c \in \mathbb{Z}^+$

"a divides b" and "b divides c" imply that "a divides c".

Thus aRb and bRa imply aRc. Hence R is transitive.

Ex: The "subset-relation" $\subseteq$ defined on the power set of A a set S is partial order on S.

Ex: The relations "is less than" and "is greater than" are not partial order over $\mathbb{Z}$; because these are not reflexive

Ex: The relation "Congruent modulo n" defined on the set of all integers $\mathbb{Z}$ is also not a partial order because this relation is not antisymmetric.

[Note that $a \equiv b \pmod n$ and $b \equiv a \pmod n$ do not always imply that $a = b$. For example $2 \equiv 8 \pmod 3$ and $8 \equiv 2 \pmod 3$ But $2 \neq 8$].

Total order

Let R be a partial order on A. Then R is called a total order (or a linear order) on A if for all $x, y \in A$ either xRy or yRx. In this case, the poset (A, R) is called a totally ordered set (or linearly ordered set) or a chain.

Ex: The partial order relation "less than or equal to" is a total order on the set R.

Because, for any $x, y \in R$, we have $x \leq y$ or $y \leq x$.

Thus $(R, \leq)$ is a totally ordered set.

Ex: The divisibility relation on the set $A = \{1, 2, 4, 8\}$ This relation is a total order on A.

Ex: The same relation is not a total order on the set $A = \{1, 2, 4, 6, 8\}$ although it is a partial order on A. (observe that neither 4 divides 6 nor 6 divides 4)

Ex: The subset relation is also not a total order on the power set of an arbitrary set S although it is a partial order, because for any two subsets S_1 and S_2 of S, neither $S_1 \subseteq S_2$ nor $S_2 \subseteq S_1$ can be true.

for example if $S = \{1, 2, 3\}$ $S_1 = \{1, 2\}$ and $S_2 = \{1, 3\}$ then $S_1 \subseteq S_2$ and $S_2 \subseteq S$. but $S_1 \not\subseteq S_2$ and $S_2 \not\subseteq S_1$

from the definition of a total order and examples given above it is clear that every total order is a partial order, but not every partial order is a total order

Hasse Diagram

Since a partial order is a relation on a set- we can think of the diagraph of partial order if the set is finite. Since a partial order is reflexive, at every vertex in the digraph of partial order, we need not exhibit such loops explicitly: they will be automatically understood (by convention)

If, in the diagraph of partial order, there is an edge from a vertex a to a vertex b and there is an edge from the vertex b to a vertex c, then there should be an edge from a to c. (because of transitivity) As such, we need not exhibit an edge from a to c explicitly: it will be automatically understood (by convention)

To simplify the format of the digraph of a partial order, we represent the vertices by dots (bullets) and draw the digraph in such a way that all edges point upward. With this convention, we need not put arrows in the edges

The digraph of a partial order drawn by adopting the conventions indicated in the above paragraph is called a poset diagram or the Hasse diagram for the partial order

Example : Let $A = \{1,2,3,4\}$ and

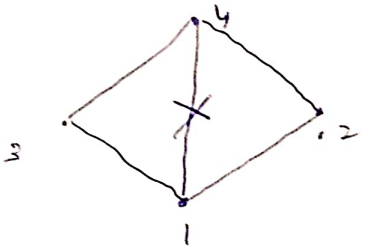
$R = \{(1,1), (1,2), (2,2), (2,4), (1,3), (3,3), (3,4), (1,4), (4,4)\}$

Verify that R is a partial order on R. Also, write down the Hasse diagram for R

Sol We observe that the given relation R is reflexive and transitive. Further, R does not contain ordered pairs of the form (a,b) and (b,a) with $b \neq a$. Therefore, R is anti-symmetric. As such, R is partial order on A.

The Hasse diagram for R must exhibit the relationships between the elements of A as defined by R; if $(a,b) \in R$ there must be an upward edge from a to b.

By examining the ordered pairs contained in R we find that the Hasse diagram of R is as shown below.



Example: Let $X = \{2, 3, 6, 12, 24, 36\}$ and the relation $\leq$ be such that $x \leq y$ if x divides y. Draw the Hasse diagram of $(X, \leq)$

$2 \xrightarrow{2,} 6, 12, 24, 36 \rightarrow (2,2), (2,6), (2,12), (2,24), (2,36)$.

$3 \rightarrow 3, 6, 12, 24, 36 \rightarrow (3,3), (3,12), (3,24), (3,36)$

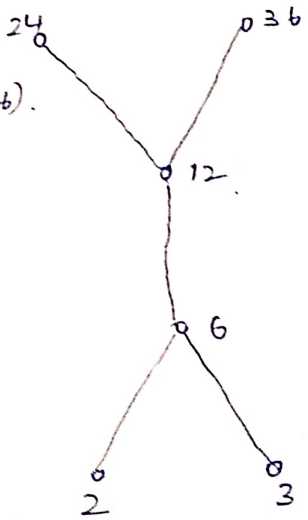
$6 \rightarrow 6, 12, 24, 36 \rightarrow (6,6), (6,12), (6,24), (6,36)$

$12 \rightarrow 12, 24, 36 \rightarrow (12,12), (12,24), (12,36)$.

$24 \rightarrow (24,24)$

$36 \rightarrow (36,36)$.

$R = \{(2,2), (2,6), (2,12), (2,24), (2,36), (3,3), (3,12), (3,24), (3,36), (6,6), (6,12), (6,36), (12,12), (12,24), (12,36), (24,24), (36,36)\}$



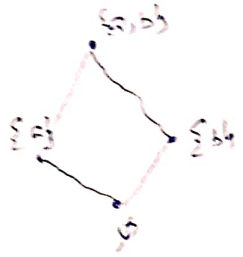
R is partially ordered set.
∵ R is reflexive, antisymmetric, transitive

Example: Let A be a given finite set and $\mathcal{P}(A)$ its power set. Let $\subseteq$ be the inclusion relation on the elements of $\mathcal{P}(A)$. Draw the Hasse diagram of $(\mathcal{P}(A), \subseteq)$ for

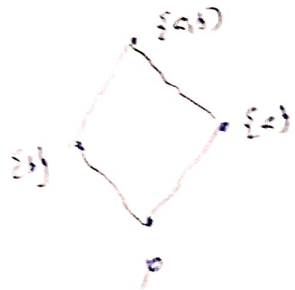
(a) $A = \{a\}$ b) $A = \{a, b\}$ c) $A = \{a, b, c\}$ d) $A = \{a, b, c, d\}$

$A = \{a\}$ $\phi \subseteq A$. $R = \{(\phi, \phi), (\phi, A), (A, A)\}$

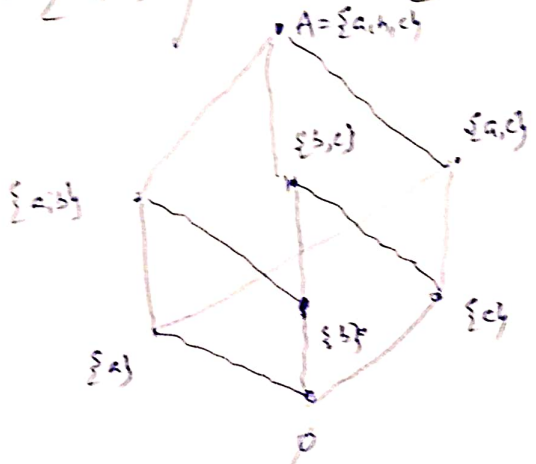
$A = \{a, b\}$ $\mathcal{P}(A) = \{\phi, \{a\}, \{b\}, A\}$

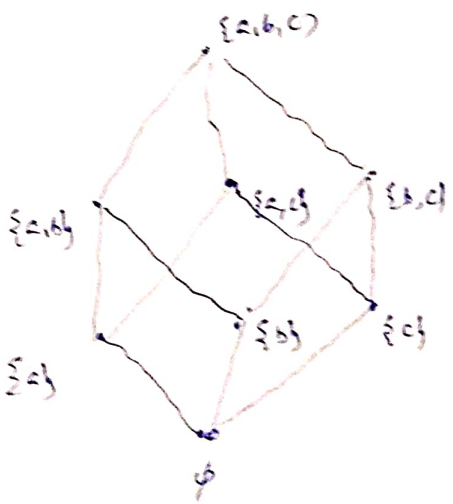


or



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





$R \to$ $\phi \longrightarrow \phi$ $\{(\phi, \phi)\}$

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

$\{b\} \to \phi, \{b\}, \{(\phi, \{b\}), (\{b\}, \{b\})\}$

$\{c\} \to \phi, \{c\}, \{(\phi, \{c\}), (\{a\}, \{c\})\}$

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

Example Let $S = \{1,2,3\}$ and $P(S)$, the power set of S. On $P(S)$, define the relation R by xRy if and only if $x \subseteq y$. Is this relation is a partial order on $P(S)$. Draw its Hasse diagram.

Sol For any set S, the $P(S)$ contains all subsets of S. We can prove that the subset relation $\subseteq$ is reflexive, antisymmetric and transitive on $P(S)$ for any set S. This relation is therefore a partial order on S. For any set S. For the given particular set $S=\{1,2,3\}$ also $\subseteq$ is a partial order.

For a given $S = \{1,2,3\}$, the subsets of S are

ϕ, $S_1 = \{1\}$, $S_2 = \{2\}$, $S_3 = \{3\}$, $S_4 = \{1,2\}$, $S_5 = \{2,3\}$

$S_6 = \{3,1\}$, and S

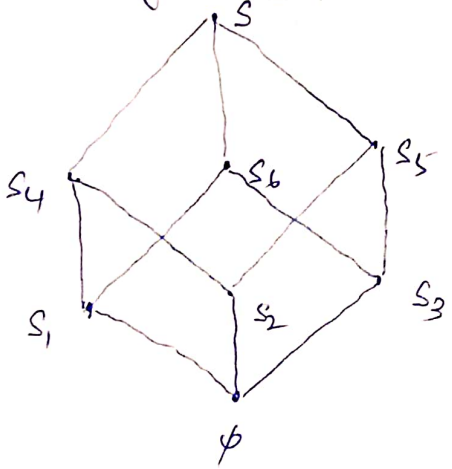
We check that

$\phi \subseteq S_i$, $i = 1,2,\ldots 6$ and $\phi \subseteq S$

$S_i \subseteq S$ and $S_i \subseteq S_i$, $i = 1,2,\ldots,6$.

$S_1 \subseteq S_4$, $S_1 \subseteq S_6$, $S_2 \subseteq S_4$, $S_2 \subseteq S_5$, $S_3 \subseteq S_5$; $S_3 \subseteq S_6$

The Hasse diagram for R must exhibit all these facts.



Ex Draw the Hasse Diagram representing the positive divisors of 36.

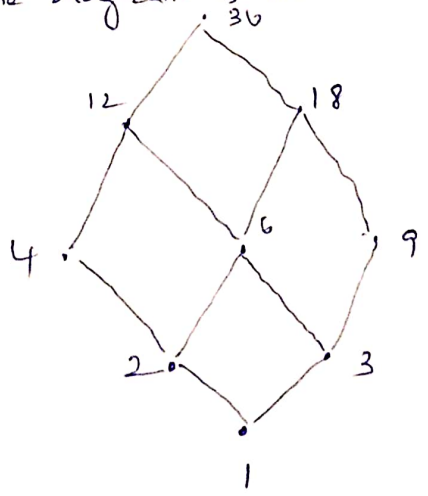
Sol The set of all +ve divisors of 36 is

$$D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

The relation R of divisibility (a R b if and only if a divides b) is a partial order on this set. Hasse diagram for this partial order is required here. We note that; under R

1 is related to all elements of D_{36}
2 is related to 2, 4, 6, 12, 18, 36
3 is related to 3, 6, 9, 12, 18, 36
4 is related to 4, 12, 36
6 is related to 6, 12, 18, 36
9 is related to 9, 18, 36
12 is related to 12 and 36
18 is related to 18 and 36
36 is related to 36

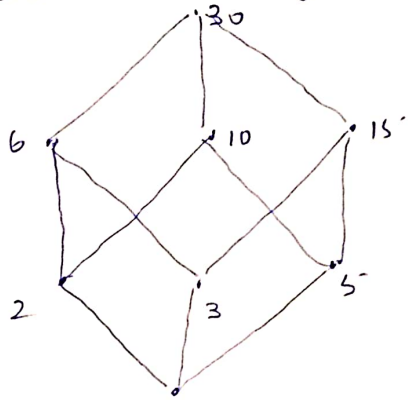
The Hasse diagram for R must exhibit all of the above facts. The diagram is as shown below



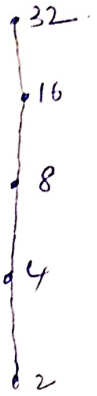
Ex: On the following cases, Consider the partial order of divisibility on the set A. Draw the Hasse diagram for the poset and determine whether the poset is totally ordered & not.

(i) $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ $A = \{2, 4, 8, 16, 32\}$

The Hasse diagram for the two cases are shown below.



case(i)



case(ii)

By examining the above Hasse diagrams, we find that the give relation is totally ordered in case(ii) but is not totally ordered in case(i)

Groups

Binary operation

Def Let S be a non empty set. If $f: S \times S \to S$ is a mapping, then f is called a binary operation or binary composition in S (or on S).

Thus 1. If a relation in S is such that every pair (distinct or equal) of elements of S taken in a definite order is associated with a unique element of S then it is called a binary operation in S

Otherwise the relation is not a binary operation in S and the relation is simply an operation in S.

2. We observe that - ~~Addition~~ (+)
multiplication ($\times$) or ($\cdot$)
Subtraction ($-$)
are binary operations in $\mathbb{R}$
and division ($\div$) is not a binary operation in $\mathbb{R}$
$\because$ division by 0 is not defined.

A binary operation will be denoted by means of a symbol such ~~that~~ as $*$, Δ, $+$, $\oplus$ etc. and the result of a binary operation on the elements, say $x_1, x_2 \in X$, is expressed by writing $x_1 * x_2$.

1. for $a,b \in S \Rightarrow a+b \in S \Rightarrow$ '+' is a binary operation in S
2. for $a,b \in S \Rightarrow a.b \in S \Rightarrow$ '.' is a binary operation in S
3. for $a,b \in S \Rightarrow a \circ b \in S \Rightarrow$ '$\circ$' is a binary operation in S
4. for $a,b \in S \Rightarrow a * b \in S \Rightarrow$ '$*$' is a binary operation in S.

This is called closure law

$a.b = a \circ b$ or $a * b = ab$ Notation

If $a,b \in S$ such that $a \circ b \notin S$ then '$\circ$' is not a binary operation in S. In this case we say that S is not closed under '$\circ$'.

Ex + is a binary operation in the set of natural numbers $\mathbb{N}$. as $a,b \in \mathbb{N} \Rightarrow a+b \in \mathbb{N}$.

— is not a binary operation in $\mathbb{N}$ as $a,b \in \mathbb{N}$ does not imply $a-b \in \mathbb{N}$.

Ex ...

Commutative law

Def: '$\circ$' is a binary operation in a set S. If for $a,b \in S$ $a \circ b = b \circ a$, then '$\circ$' is said to be Commutative in S. This is called Commutative law. Otherwise '$\circ$' is said to be not Commutative, in S

Associative law

Def '$\circ$' is a binary operation in a set 'S'. if for $a,b,c \in S$, $(a \circ b) \circ c = a \circ (b \circ c)$. then '$\circ$' is said to be associative in S. This is called associative law. Otherwise '$\circ$' is said to be not associative in S.

Note If '$\circ$' is associative in S, then we write

$$(a \circ b) \circ c = a \circ (b \circ c) = a \circ b \circ c.$$

Identity element

Def: Let S be a non-empty set and '$\circ$' is a binary operation on S.

(i) If $\exists$ an element $e_1 \in S$ such that $e_1 \circ a = a$ for $a \in S$ then e_1 is called a left identity of S w.r.t the operation '$\circ$'.

(ii) If there exists an element $e_2 \in S$ such that $a \circ e_2 = a$ for $a \in S$, then e_2 is called a right identity of S w.r.t the operation '$\circ$'.

(iii) If there exists an element $e \in S$ such that $e \circ a = a \circ e = a$ then e is both a left and right identity of S w.r.t '$\circ$' then e is called an identity of S.

Thus for $a \in S$, $e \circ a = a \circ e = a \Leftrightarrow e$ is an identity of S.

Invertable element

Def Let $(S, \circ)$ be an algebraic structure with the identity element e in S w.r.t '$\circ$'. An element $a \in S$ is said to be left invertable or left regular if there exists an element $x \in S$ such that $x \circ a = e$. x is called a left inverse of a w.r.t '$\circ$'.

An element $a \in S$ is said to be right invertable or right regular if there exists an element $y \in S$ such that $a \circ y = e$. y is called a right inverse of a w.r.t '$\circ$'

An element x which is both left inverse and right inverse of a is called an inverse of a and a is said to invertable or regular.

Identity element

Def: Let S be a non-empty set and '$\circ$' is a binary operation on S.

(i) If $\exists$ an element $e_1 \in S$ such that $e_1 \circ a = a$ for $a \in S$ then e_1 is called a left identity of S w.r.t the operation '$\circ$'.

(ii) If there exists an element $e_2 \in S$ such that $a \circ e_2 = a$ for $a \in S$, then e_2 is called a right identity of S w.r.t the operation '$\circ$'.

(iii) If there exists an element $e \in S$ such that $e \circ a = a \circ e = a$ then e is both a left and right identity of S w.r.t '$\circ$' then e is called an identity of S.

Thus for $a \in S$, $e \circ a = a \circ e = a \Leftrightarrow e$ is an identity of S.

Invertable element

Def Let $(S, \circ)$ be an algebraic structure with the identity element e in S w.r.t '$\circ$'. An element $a \in S$ is said to be left invertable or left regular if there exists an element $x \in S$ such that $x \circ a = e$. x is called a left inverse of a w.r.t '$\circ$'.

An element $a \in S$ is said to be right invertable or right regular if there exists an element $y \in S$ such that $a \circ y = e$. y is called a right inverse of a w.r.t '$\circ$'

An element a which is both left inverse and right inverse of a is called an inverse of a and a is said to invertable or regular.

Algebraic Structure

Def: A nonempty set G equipped with one or more binary operations is called an algebraic structure or an algebraic system.

If 'o' is a binary operation on G, then the algebraic structure is written as (G, o).

↳ Groupid Groupoid or quasigroup.

eg: $(N, +)$, $(Q, -)$, $(R, +, \cdot)$ → Algebraic structures. and $(N, +)$, $(Q, -)$ are groupoids or quasigroup.

Semigroup:

An algebraic system $(S, *)$ is called a semigroup if the binary operation 'o' is associative in S.

Ex. $(N, +)$, $(R, +)$ → $(Z, +)$, $(P(S), \cup)$ → Semigroups

$(Q, -)$, → not a semigroup

for $5, \frac{3}{2}, 1 \in Q$ does not imply

$$\left(5 - \frac{3}{2}\right) - 1 = 5 - \left(\frac{3}{2} - 1\right).$$

Ex Q is a set of rational numbers. 'o' is a binary operation defined on Q such that $a \circ b = a - b + ab$. for $a, b \in Q$.

(Q, o) is not a semigroup

for $a, b, c \in Q$, $(a \circ b) \circ c = (a \circ b) - c + (a \circ b)c$

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

$$= a - b + ab - c + ac - bc + abc$$

$$a \circ (b \circ c) = a - (b \circ c) + a(b \circ c)$$

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

$$= a - b + c + bc + ab - ac + abc.$$

and $(a \circ b) \circ c \neq a \circ (b \circ c)$

Ex: Q is a set of rational numbers, '0' is a binary operation defined on Q such that- $\forall a, b \in Q$

$a \circ b = a + b - ab$. $(Q, \circ)$ is a semigroup

Monoid

Def A semigroup $(S, \circ)$ with identity element w.r.t '$\circ$' is known as a monoid. i.e.

$(S, \circ)$ is a monoid if S is a nonempty set and '$\circ$' is a binary operation on S such that- '$\circ$' is associative and there exists an identity element w.r.t '$\circ$'

Eg 1: $(\mathbb{Z}, +)$ is a monoid and the identity is 0

Eg 2: $(\mathbb{Z}, \cdot)$ is monoid and identity element is 1

Eg 3: S is the set of all 2×2 matrices such that- each element in S are rational numbers.

then matrix addition (+) is a binary operation on S and $(S, +)$ is a monoid. and O_2 = null matrix is identity element in S.

Matrix multiplication (·) is a binary operation on S.

then $(S, \cdot)$ is a monoid and I_2 (Unit matrix) is the identity matrix. is the identity element.

Group

Def: If G is a nonempty set and 'o' is a binary operation defined on G such that the following three laws are satisfied then (G, o) is a group.

G_1: Associative law: for $a, b, c \in G$, $(a o b) o c = a o (b o c)$

G_2: Identity law: $\exists\, e \in G$ such that for any $a \in G$

$$a o e = a = e o a.$$

'e' is called an identity element in G

G_3: Inverse law: for every $a \in G$ there exists an element $b \in G$ such that $a o b = b o a = e$. 'b' is called an inverse of 'a'. $(b = \bar{a}')$

Ex $(Z, +), (Q, +), (R, +), (C, +) \rightarrow$ groups

Abelian or Commutative group

Def: A group $(G, *)$ in which the operation $*$ is commutative is called an abelian group.

Finite and Infinite groups

The order of the group $(G, *)$, denoted by $|G|$, is the number of elements of G, when G is finite.

Ex

Ex 1 The set of rational numbers excluding zero is an abelian group under multiplication

Ex 2 Let I be the set of integers. The algebra $(I, +)$ is an abelian group

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

Permutation group

We shall consider the set of all permutations of the elements of a finite set and define a binary operation on this. We shall consider those sets of permutations which form a group under this operation. Such groups are called permutation groups

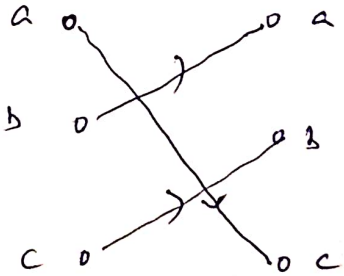
Let $S = \{a, b, c\}$ be a set and let p denote a permutation of the elements of S. That is $p: S \to S$ is a bijective mapping. There are two convenient ways of describing the permutation p.

Suppose that $p(a) = c \quad p(b) = a$ and $p(c) = b$

then we may represent p as

$$p = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

$$p = \begin{pmatrix} a & c & b \\ c & b & a \end{pmatrix} = \begin{pmatrix} b & a & c \\ a & c & b \end{pmatrix}$$



Ex: Consider the $3! = 6$ permutations of the elements of the set $\{1, 2, 3\}$. Let us denote the set of all permutations by $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$. The elements $P_1, \ldots, P_6$ are described by the following.

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

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

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

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

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

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

$$P_3 \diamond P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \diamond \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_4.$$

$\diamond$	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_2	P_6	P_1	P_5	P_4	P_2
P_4	P_4	P_5	P_6	P_3	P_6	P_1
P_5	P_6	P_3	P_4	P_2	P_1	P_5

Cyclic group

A group $(G, *)$ is said to be cyclic if there exists 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 called generator of the group G.

A cyclic group is abelian, because $p, q \in G$,

$p = a^r \quad q = a^s$ for some $r, s \in I$. and

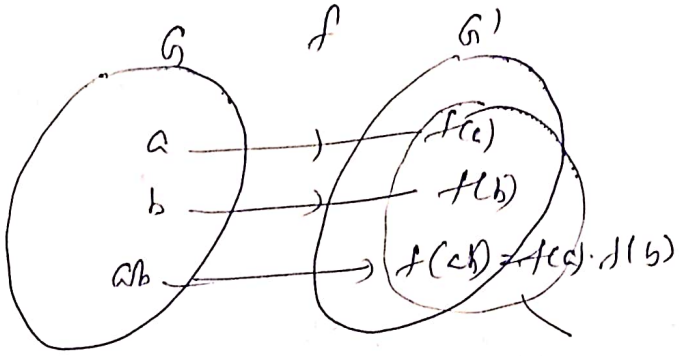
$$p * q = a^r * a^s = a^{r+s} = a^{s+r} = a^s * a^r = q * p$$

Homomorphism of Groups

Def Let G, G' be two groups and f, a mapping from G to G', if for $a, b \in G$

$$f(a.b) = f(a).f(b)$$

$f \rightarrow$ called homomorphism



Homomorphic Image

epimorphism — f is onto

A homomorphism of a group G into itself is called Endomorphism

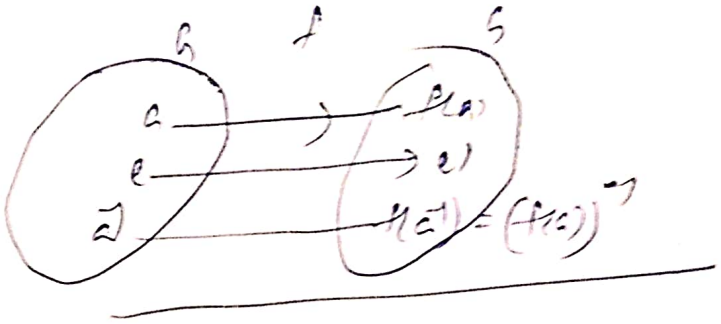
$f: G \rightarrow G$:

Endomorphism.

Monomorphism — A homomorphism — 1-1 — Monomorphism

Isomorphism : A homomorphism 1-1 and onto

Automorphism : Isomorphism



Cosets and Lagrange's Theorem

Def Let $(H, *)$ be a subgroup of $(G, *)$ for any $a \in G$ the set aH defined by $aH = \{ah / h \in H\}$

↳ left coset

$Ha = \{ha / h \in H\}$

↳ Right Coset of H

Lagrange's theorem The order of a subgroup of a finite group divides the order of the group

Normal Subgroup : A subgroup $(H, *)$ of $(G, *)$ is called a normal subgroup if for any $a \in G$ $aH = Ha$

Algebraic System with Two binary operations

Def An algebraic system $(S, +, \cdot)$ is called a ring if the binary operation $+$ and $\cdot$ on S satisfy the following three properties

(1) $(S, +)$ is an abelian group

(2) $(S, \cdot)$ is a semigroup

(3) The operation $\cdot$ distributive over $+$

That is for any $a, b, c \in S$

$a \cdot (b + c) = a \cdot b + a \cdot c$ and

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

$(\mathbb{Z}, +, \times)$ → Ring

$(\mathbb{R}, +, \times)$ → Ring

If $(S, \cdot)$ is commutative then the ring $(S, +, \cdot)$ is called commutative ring

If $(S, \cdot) \rightarrow$ monoid —

$(S, +, \cdot)$ is called a ring with identity elt.

Zero divisors

For any $a, b \in S$ such that $a \neq 0$ and $b \neq 0$, $a \cdot b = 0$ and the a, b are called zero divisors.

$(ab = 0 \Rightarrow a = 0 \text{ or } b = 0)$

A commutative ring $(S, +, \cdot)$ with identity and without zero divisors is called an integral domain

Def A commutative ring $(S, +, \cdot)$ which has more than one element such that every non zero elt of S has a multiplicative inverse in S then S is called a field.

$(\mathbb{Q}, +, \cdot)$