UNIT-2
Set Theory

Set:A set is collection of well defined objects.

In the above definition the words set and collection for all practical purposes are Synonymous. We have really used the word set to define itself.
Each of the objects in the set is called a member of an element of the set. The objects themselves can be almost anything. Books, cities, numbers, animals, flowers, etc. Elements of a set are usually denoted by lower-case letters. While sets are denoted by capital letters of English larguage.

The symbol $\in$ indicates the membership in a set.
If "a is an element of the set A", then we write $a \in A$.
The symbol $\in$ is read "is a member of " or "is an element of ".
The symbol $\notin$ is used to indicate that an object is not in the given set.
The symbol $\notin$ is read "is not a member of " or "is not an element of ".
If x is not an element of the set A then we write $x \notin A$.

Subset*:*

A set A is a subset of the set B if and only if every element of A is also an element of B. We also say that A is contained in B, and use the notation $A \subseteq B$.

Proper Subset*:*

A set A is called proper subset of the set B. If (*i*) A is subset of B and (*ii*) B is not a subset A i.e., A is said to be a proper subset of B if every element of A belongs to the set B, but there is atleast one element of B, which is not in A. If A is a proper subset of B, then we denote it by $A \subset B$.

Super set: If A is subset of B, then B is called a superset of A.

Null set: The set with no elements is called an empty set or null set. A Null set is designated by the symbol ϕ. The null set is a subset of every set, i.e., If A is any set then $\phi \subset A$.

Universal set:
In many discussions all the sets are considered to be subsets of one particular set. This set is called the universal set for that discussion. The Universal set is often designated by the script letter μ. Universal set in not unique and it may change from one discussion to another.

Power set:
The set of all subsets of a set A is called the power set of A.
The power set of A is denoted by $P(A)$. If A has n elements in it, then $P(A)$ has 2^n elements:

Disjoint sets:
Two sets are said to be disjoint if they have no element in common.

Union of two sets:
The union of two sets A and B is the set whose elements are all of the elements in A or in B or in both. The union of sets A and B denoted by $A \cup B$ is read as "A union B".

Intersection of two sets:
The intersection of two sets A and B is the set whose elements are all of the elements common to both A and B. The intersection of the sets of "A" and "B" is denoted by $A \bigcap B$ and is read as "A intersection B"

Difference of sets:
If A and B are subsets of the universal set U, then the relative complement of B in $A$is the set of all elements in A which are not in A. It is denoted by $A - B$ thus: $A - B = \{x \mid x \in A \text{ and } x \notin B\}$

Complement of a set:
If U is a universal set containing the set A, then $U - A$ is called the complement of A. It is denoted by A^1 . Thus $A^1 = \{x: x \notin A\}$

Inclusion-Exclusion Principle:

The inclusion–exclusion principle is a counting technique which generalizes the familiar method of obtaining the number of elements in the unionof two finite sets; symbolically expressed as

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

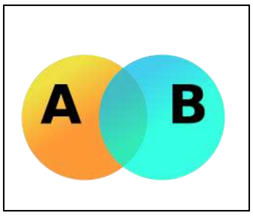


Fig.Venn diagram showing the union of sets A and B

where A and B are two finite sets and $|S|$ indicates the cardinality of a set S (which may be considered as the number of elements of the set, if the set is finite). The formula expresses the fact that the sum of the sizes of the two sets may be too large since some elements may be counted twice. The double-counted elements are those in the intersection of the two sets and the count is corrected by subtracting the size of the intersection.

The principle is more clearly seen in the case of three sets, which for the sets A, B and C is given by

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

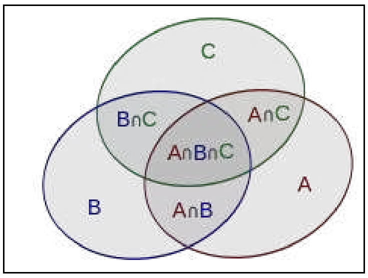


Fig.Inclusion–exclusion illustrated by a Venn diagram for three sets

This formula can be verified by counting how many times each region in the Venn diagram figure is included in the right-hand side of the formula. In this case, when removing the contributions of over-counted elements, the number of elements in the mutual intersection of the three sets has been subtracted too often, so must be added back in to get the correct total.

In general, Let A1, · · · , Ap be finite subsets of a set U. Then,

$$\left|A_1 \cup A_2 \cup \ldots \cup A_p\right| = \sum_{1 \le i \le p} |A_i| - \sum_{1 \le i_1 < i_2 \le p} \left|A_{i_1} \cap A_{i_2}\right| +$$

$$\sum_{1 \le i_1 < i_2 < i_3 \le p} \left|A_{i_1} \cap A_{i_2} \cap A_{i_3}\right| - \ldots + (-1)^{p-1} \left|A_1 \cap A_2 \cap \cdots \cap A_p\right|,$$

Example: How many natural numbers $n \le 1000$ are not divisible by any of 2, 3?

Ans: Let $A_2 = \{n \in N \mid n \le 1000, 2|n\}$ and $A_3 = \{n \in N \mid n \le 1000, 3|n\}$.
Then, $|A_2 \cup A_3| = |A_2| + |A_3| - |A_2 \cap A_3| = 500 + 333 - 166 = 667$.
So, the required answer is $1000 - 667 = 333$.

Example: How many integers between 1 and 10000 are divisible by none of 2, 3, 5, 7?

Ans: For $i \in \{2, 3, 5, 7\}$, let $A_i = \{n \in N \mid n \le 10000, i|n\}$.
Therefore, the required answer is $10000 - |A_2 \cup A_3 \cup A_5 \cup A_7| = 2285$.

Relations

Definition: Any set of ordered pairs defines a *binary relation*.

We shall call a binary relation simply a relation. Binary relations represent relationships between elements of two sets. If R is a relation, a particular ordered pair, say $(x, y) \in R$ can be written as xRy and can be read as "x is in relation R to y".

Example: Give an example of a relation.
Solution: The relation "greater than" for real numbers is denoted by '$>$'. If x and y are any two real numbers such that $x > y$, then we say that $(x, y) \in >$. Thus the relation $>$ is $\{ \} >= (x, y) : x$ and y are real numbers and $x > y$
Example: Define a relation between two sets $A = \{5, 6, 7\}$ and $B = \{x, y\}$.

Solution: If $A = \{5, 6, 7\}$ and $B = \{x, y\}$, then the subset $R = \{(5, x), (5, y), (6, x), (6, y)\}$ is a relation from A to B.

Definition: Let S be any relation. The *domain* of the relation S is defined as the set of all first elements of the ordered pairs that belong to S and is denoted by $D(S)$.

$$D(S) = \{ x : (x, y) \in S, \text{ for some } y \}$$

The *range* of the relation S is defined as the set of all second elements of the ordered pairs that belong to S and is denoted by $R(S)$.

$$R(S) = \{ y : (x, y) \in S, \text{ for some } x\}$$

Example: $A = \{2, 3, 4\}$ and $B = \{3, 4, 5, 6, 7\}$. Define a relation from A to B by $(a, b) \in R$ if a divides b.
Solution: We obtain $R = \{(2, 4), (2, 6), (3, 3), (3, 6), (4, 4)\}$.

Domain of $R = \{2, 3, 4\}$ and range of $R = \{3, 4, 6\}$.

Properties of Binary Relations in a Set

A relation R on a set X is said to be

- Reflexive relation if xRx or $(x, x) \in R, \ \forall x \in X$
- Symmetric relation if xRy then $yRx, \ \forall x, y \in X$
- Transitive relation if xRy and yRz then $xRz, \ \forall x, y, z \in X$
- Irreflexive relation if $x \not R x$ or $(x, x) \notin R, \ \forall x \in X$
- Antisymmetric relation if for every x and y in X, whenever xRy and yRx, then $x = y$.

Examples: (i). If $R_1 = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 3)\}$ be a relation on $A = \{1, 2, 3\}$, then R_1 is a reflexive relation, since for every $x \in A, (x, x) \in R_1$.

(ii). If $R_2 = \{(1, 1), (1, 2), (2, 3), (3, 3)\}$ be a relation on $A = \{1, 2, 3\}$, then R_2 is not a reflexive relation, since for every $2 \in A, (2, 2) \notin R_2$.

(iii). If $R_3 = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 1), (3, 1)\}$ be a relation on $A = \{1, 2, 3\}$, then R_3 is a symmetric relation.

(iv). If $R_4 = \{(1, 2), (2, 2), (2, 3)\}$ on $A = \{1, 2, 3\}$ is an antisymmetric.

Example: Given $S = \{1, 2, ..., 10\}$ and a relation R on S, where $R = \{(x, y) | x + y = 10\}$.
What are the properties of the relation R?

Solution: Given that

$S = \{1, 2, ..., 10\}$

- $= \{(x, y) | x + y = 10\}$
- $= \{(1, 9), (9, 1), (2, 8), (8, 2), (3, 7), (7, 3), (4, 6), (6, 4), (5, 5)\}$.

(i). For any $x \in S$ and $(x, x) \notin R$. Here, $1 \in S$ but $(1, 1) \notin R$.

$\Rightarrow$ the relation R is not reflexive. It is also not irreflexive, since $(5, 5) \in R$.

(ii). $(1, 9) \in R \Rightarrow (9, 1) \in R$

$(2, 8) \in R \Rightarrow (8, 2) \in R$.....

$\Rightarrow$ the relation is symmetric, but it is not antisymmetric. (iii). $(1, 9) \in R$ and $(9, 1) \in R$

$\Rightarrow (1, 1) \notin R$

$\Rightarrow$ The relation R is not transitive. Hence, R is symmetric.

Relation Matrix and the Graph of a Relation

Relation Matrix: A relation R from a finite set X to a finite set Y can be repre-sented by a matrix is called the *relation matrix* of R.

Let $X = \{x_1, x_2, ..., x_m\}$ and $Y = \{y_1, y_2, ..., y_n\}$ be finite sets containing m and n elements, respectively, and R be the relation from A to B. Then R can be represented by an $m \times n$ matrix $M_R = [r_{ij}]$, which is defined as follows:

$$r_{ij} = \begin{cases} 1, & \text{if } (x_i, y_j) \in R \\ 0, & \text{if } (x_i, y_j) \notin R \end{cases}$$

Example. Let $A = \{1, 2, 3, 4\}$ and $B = \{b_1, b_2, b_3\}$. Consider the relation $R = \{(1, b_2), (1, b_3), (3, b_2), (4, b_1), (4, b_3)\}$. Determine the matrix of the relation.

Solution: $A = \{1, 2, 3, 4\}$, $B = \{b_1, b_2, b_3\}$.

Relation $R = \{(1, b_2), (1, b_3), (3, b_2), (4, b_1), (4, b_3)\}$.

Matrix of the relation R is written as

That is $M_R = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$

Example: Let $A = \{1, 2, 3, 4\}$. Find the relation R on A determined by the matrix

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

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

Properties of a relation in a set:

(i). If a relation is reflexive, then all the diagonal entries must be 1.

(ii). If a relation is symmetric, then the relation matrix is symmetric, i.e., $r_{ij} = r_{ji}$ for every i and j.

(iii). If a relation is antisymmetric, then its matrix is such that if $r_{ij} = 1$ then $r_{ji} = 0$ for $i \neq j$.

Graph of a Relation: A relation can also be represented pictorially by drawing its *graph*. Let R be a relation in a set $X = \{x_1, x_2, ..., x_m\}$. The elements of X are represented by points or circles called *nodes*. These nodes are called *vertices*. If $(x_i, x_j) \in R$, then we connect the 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 . This is called an *edge*. If all the nodes corresponding to the ordered pairs in R are connected by arcs with proper arrows, then we get a graph of the relation R.

Note: (i). If x_iRx_j and $x_j\ Rx_i$, then we draw two arcs between x_i and x_j with arrows pointing in both directions.

(ii). If x_iRx_i, then we get an arc which starts from node x_i and returns to node x_i. This arc is called a *loop*.

Properties of relations:

(i). If a relation is reflexive, then there must be a loop at each node. On the other hand, if the relation is irreflexive, then there is no loop at any node.

(ii). 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 the first.

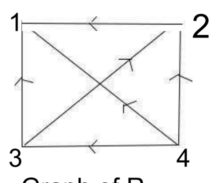
(iii). For antisymmetric relations, no such direct return path should exist.

(iv). If a relation is transitive, the situation is not so simple.

Example: Let $X = \{1, 2, 3, 4\}$ and $R=\{(x, y)|\ x > y\}$. Draw the graph of R and also give its matrix.

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

The graph of R and the matrix of R are



Graph of R

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

Partition and Covering of a Set

Let S be a given set and $A = \{A_1, A_2, \cdots, A_m\}$ where each A_i, $i = 1, 2, \cdots, m$ 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 $A_1, A_2, \cdots, A_m$ are said to *cover* S. If, in addition, the elements of A, which are subsets of S, are mutually disjoint, then A is called a *partition* of S, and the sets $A_1, A_2, \cdots, A_m$ are called the *blocks* of the partition.

Example: Let $S = \{a, b, c\}$ and consider the following collections of subsets of S. $A = \{\{a, b\}, \{b, c\}\}$, $B = \{\{a\}, \{a, c\}\}$, $C = \{\{a\}, \{b, c\}\}$, $D = \{\{a, b, c\}\}$, $E = \{\{a\}, \{b\}, \{c\}\}$, and $F = \{\{a\}, \{a, b\}, \{a, c\}\}$. Which of the above sets are covering?

Solution: The sets A, C, D, E, F are covering of S. But, the set B is not covering of S, since their union is not S.

Example: Let $S = \{a, b, c\}$ and consider the following collections of subsets of S. $A = \{\{a, b\}, \{b, c\}\}$, $B = \{\{a\}, \{b, c\}\}$, $C = \{\{a, b, c\}\}$, $D = \{\{a\}, \{b\}, \{c\}\}$, and $E= \{\{a\}, \{a, c\}\}$.
Which of the above sets are covering?

Solution: The sets B, C and D are partitions of S and also they are covering. Hence, every partition is a covering.

The set A is a covering, but it is not a partition of a set, since the sets $\{a, b\}$ and $\{b, c\}$ are not disjoint. Hence, every covering need not be a partition.

The set E is not partition, since the union of the subsets is not S. The partition C has one block and the partition D has three blocks.

Example: List of all ordered partitions $S = \{a, b, c, d\}$ of type (1, 2, 2).

Solution:

$(\{a\}, \{b\}, \{c, d\})$,	$(\{b\}, \{a\}, \{c, d\})$
$(\{a\}, \{c\}, \{b, d\})$,	$(\{c\}, \{a\}, \{b, d\})$
$(\{a\}, \{d\}, \{b, c\})$,	$(\{d\}, \{a\}, \{b, c\})$
$(\{b\}, \{c\}, \{a, d\})$,	$(\{c\}, \{b\}, \{a, d\})$
$(\{b\}, \{d\}, \{a, c\})$,	$(\{d\}, \{b\}, \{a, c\})$
$(\{c\}, \{d\}, \{a, b\})$,	$(\{d\}, \{c\}, \{a, b\})$.

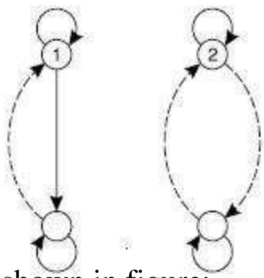
Equivalence Relations

A relation R in a set X is called an *equivalence relation* if it is reflexive, symmetric and transitive. The following are some examples of equivalence relations:

1. Equality of numbers on a set of real numbers.
2. Equality of subsets of a universal set.

Example: Let $X = \{1, 2, 3, 4\}$ and $R == \{(1, 1), (1, 4), (4, 1), (4, 4), (2, 2), (2, 3), (3, 2), (3, 3)\}$.
Prove that R is an equivalence relation.

$$M_R = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 01 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$



The corresponding graph of R is shown in figure:
Clearly, the relation R is reflexive, symmetric and transitive. Hence, R is an equivalence relation.
Example: Let $X = \{1, 2, 3, ..., 7\}$ and $R =(x, y)|\ x - y$ is divisible by 3. Show that R is an equivalence relation.

Solution: (i). For any $x \in X$, $x - x = 0$ is divisible by 3.

$\therefore xRx$

$\Rightarrow R$ is reflexive.

(ii). For any $x, y \in X$, if xRy, then $x - y$ is divisible by 3.

$\Rightarrow -(x - y)$ is divisible by 3.

$\Rightarrow y - x$ is divisible by 3.

$\Rightarrow yRx$

Thus, the relation R is symmetric.

(iii). For any $x, y, z \in X$, let xRy and yRz.

$\Rightarrow (x - y) + (y - z)$ is divisible by 3

$\Rightarrow x - z$ is divisible by 3

$\Rightarrow xRz$

Hence, the relation R is transitive.
Thus, the relation R is an equivalence relation.

Congruence Relation: Let I denote the set of all positive integers, and let m be apositive integer.
For $x \in I$ and $y \in I$, define R as $R = \{(x, y)|\ x - y$ is divisible by m $\}$
The statement "$x - y$ is divisible by m" is equivalent to the statement that both x and y have the same remainder when each is divided by m.
In this case, denote R by $\equiv$ and to write xRy as $x \equiv y \pmod{m}$, which is read as "x equals to y modulo m". The relation $\equiv$ is called a *congruence relation*.
Example: $83 \equiv 13 (\text{mod } 5)$, since 83-13=70 is divisible by 5.
Example: Prove that the relation "congruence modulo m" over the set of positive integers is an equivalence relation.

Solution: Let N be the set of all positive integers and m be a positive integer. We define the relation "congruence modulo m" on N as follows:

Let $x, y \in N$. $x \equiv y \pmod{m}$ if and only if $x - y$ is divisible by m.

Let $x, y, z \in N$. Then

(i). $x - x = 0.m$

$\Rightarrow x \equiv x \pmod{m}$ for all $x \in N$

(ii). Let $x \equiv y \pmod{m}$. Then, $x - y$ is divisible by m.

$\Rightarrow -(x - y) = y - x$ is divisible by m.

i.e., $y \equiv x \pmod{m}$

$\therefore$ The relation $\equiv$ is symmetric.

$\Rightarrow x - y$ and $y - z$ are divisible by m. Now $(x - y) + (y - z)$ is divisible by m. i.e., $x - z$ is divisible by m.

$\Rightarrow x \equiv z \pmod{m}$

$\therefore$ The relation $\equiv$ is transitive.

Since the relation $\equiv$ is reflexive, symmetric and transitive, the relation *congruence modulo m* is an equivalence relation.

Example: Let R denote a relation on the set of ordered pairs of positive integers such that $(x,y)R(u, v)$ iff $xv = yu$. Show that R is an equivalence relation.

Solution: Let R denote a relation on the set of ordered pairs of positive integers.

Let x, y, u and v be positive integers. Given $(x, y)R(u, v)$ if and only if $xv = yu$.

(i). Since $xy = yx$ is true for all positive integers

$\Rightarrow (x, y)R(x, y)$, for all ordered pairs (x, y) of positive integers.

$\therefore$ The relation R is reflexive. (ii). Let $(x, y)R(u, v)$

$\Rightarrow xv = yu \Rightarrow yu$

$= xv \Rightarrow uy = vx$

$\Rightarrow (u, v)R(x, y)$

$\therefore$ The relation R is symmetric.

(iii). Let x, y, u, v, m and n be positive integers

Let $(x, y)R(u, v)$ and $(u, v)R(m, n)$

$\Rightarrow xv = yu$ and $un = vm$

$\Rightarrow xvun = yuvm$

$\Rightarrow xn = ym$, by canceling uv

$\Rightarrow (x, y)R(m, n)$

$\therefore$ The relation R is transitive.

Since R is reflexive, symmetric and transitive, hence the relation R is an equivalence relation.

Compatibility Relations

Definition: A relation R in X is said to be a *compatibility relation* if it is reflexive and symmetric. Clearly, all equivalence relations are compatibility relations. A compatibility relation is sometimes denoted by $\approx$.

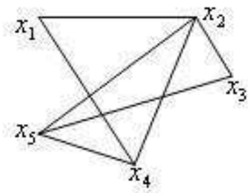
Example: Let $X = \{$ball, bed, dog, let, egg$\}$, and let the relation R be given by

$R = \{(x, y) \mid x, y \in X \wedge xRy$ if x and y contain some common letter$\}$.

Then R is a compatibility relation, and x, y are called compatible if xRy.

Note: ball$\approx$bed, bed$\approx$egg. But ball$\not\approx$egg. Thus $\approx$ is not transitive.

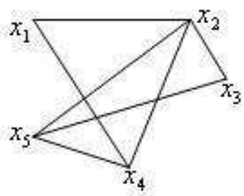
Denoting "ball" by x_1, "bed" by x_2, "dog" by x_3, "let" by x_4, and "egg" by x_5, the graph of $\approx$ is given as follows:



Maximal Compatibility Block:

Let X be a set and $\approx$ a compatibility relation on X. A subset $A \subseteq X$ is called a *maximal compatibility block* if any element of A is compatible to every other element of A and no element of $X - A$ is compatible to all the elements of A.

Example: The subsets $\{x_1, x_2, x_4\}$, $\{x_2, x_3, x_5\}$, $\{x_2, x_4, x_5\}$, $\{x_1, x_4, x_5\}$ are maximal compatibility blocks.

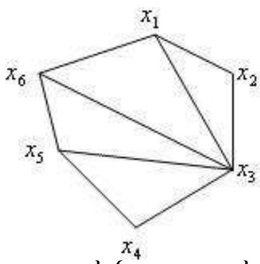


Example: Let the compatibility relation on a set $\{x_1, x_2, ..., x_6\}$ be given by the matrix:

$$\begin{array}{cccccc}
x_2 & 1 & & & & \\
x_3 & 1 & 1 & & & \\
x_4 & 0 & 0 & 1 & & \\
x_5 & 0 & 0 & 1 & 1 & \\
x_6 & 1 & 0 & 1 & 0 & 1 \\
 & x_1 & x_2 & x_3 & x_4 & x_5
\end{array}$$

Draw the graph and find the maximal compatibility blocks of the relation.

Solution:



The maximal compatibility blocks are $\{x_1, x_2, x_3\}$,$\{x_1, x_3, x_6\}$,$\{x_3, x_5, x_6\}$,$\{x_3, x_4, x_5\}$.

Composition of Binary Relations

Let R be a relation from X to Y and S be a relation from Y to Z. Then a relation written as $R \circ S$ is called a *composite relation* of R and S where $R \circ S = \{(x, z) \mid x \in X, z \in Z,$ and there exists $y \in Y$ with $(x, y) \in R$ and $(y, z) \in S\}$.

Theorem: If R is relation from A to B, S is a relation from B to C and T is a relation from C to D then $T \circ (S \circ R) = (T \circ S) \circ R$

Example: Let $R = \{(1, 2), (3, 4), (2, 2)\}$ and $S = \{(4, 2), (2, 5), (3, 1), (1, 3)\}$. Find $R \circ S$, $S \circ R$, $R \circ (S \circ R)$, $(R \circ S) \circ R$, $R \circ R$, $S \circ S$, and $(R \circ R) \circ R$.

Solution: Given $R = \{(1, 2), (3, 4), (2, 2)\}$ and $S = \{(4, 2), (2, 5), (3, 1), (1, 3)\}$.

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

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

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

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

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

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

Example: Let $A = \{a, b, c\}$, and R and S be relations on A whose matrices are as given below:

$$M_R = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \text{ and } M_S = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Find the composite relations $R \circ S$, $S \circ R$, $R \circ R$, $S \circ S$ and their matrices.

Solution:

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

$S = \{(a, a), (b, b), (b, c), (c, a), (c, c)\}$. From these, we find that

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

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

$R \circ R = R^2 = \{(a, a), (a, c), (a, b), (b, a), (b, c), (b, b), (c, a), (c, b), (c, c)\}$ $S \circ S = S^2 = \{(a, a), (b, b), (b, c), (b, a), (c, a), (c, c)\}$.

The matrices of the above composite relations are as given below:

$$M_{RO\,S} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix};\ M_{SO\,R} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix};\ M_{RO\,R} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix};$$

$$M_{SO\,S} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Transitive Closure

Let X be any finite set and R be a relation in X. The relation $R^{+} = R \cup R^{2} \cup R^{3} \cup \cdots \cup R^{n}$ in X is called the *transitive closure* of R in X.

Example: Let the relation $R = \{(1, 2), (2, 3), (3, 3)\}$ on the set $\{1, 2, 3\}$. What is the transitive closure of R?

Solution: Given that $R = \{(1, 2), (2, 3), (3, 3)\}$.

The transitive closure of R is $R^{+} = R \cup R^{2} \cup R^{3} \cup \cdots =$

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

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

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

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

$R^{+} = R \cup R^{2} \cup R^{3} \cup R^{4} \cup \ldots$

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

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

Therefore $R^{+} = \{(1, 2), (1, 3), (2, 3), (3, 3)\}$.

Example: Let $X = \{1, 2, 3, 4\}$ and $R = \{(1, 2), (2, 3), (3, 4)\}$ be a relation on X. Find R^{+}.

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

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

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

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

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

Partial Ordering

A binary relation R in a set P is called a *partial order relation* or a *partial ordering* in P iff R is reflexive, antisymmetric, and transitive. i.e.,

- aRa for all $a \in P$
- aRb and $bRa \Rightarrow a = b$
- aRb and $bRc \Rightarrow aRc$

A set P together with a partial ordering R is called a *partial ordered set* or *poset*. The relation R is often denoted by the symbol $\leq$ which is different from the usual less than equal to symbol. Thus, if $\leq$ is a partial order in P , then the ordered pair $(P, \leq)$ is called a poset.

Example: Show that the relation "greater than or equal to" is a partial ordering on the set of integers.

Solution: Let Z be the set of all integers and the relation $R = {'}\geq{'}$

(i). Since $a \geq a$ for every integer a, the relation ${'}\geq{'}$ is reflexive.

(ii). Let a and b be any two integers.

Let aRb and $bRa \Rightarrow a \geq b$ and $b \geq a$

$\Rightarrow a = b$

$\therefore$ The relation ${'}\geq{'}$ is antisymmetric. (iii).

Let a, b and c be any three integers.

Let aRb and $bRc \Rightarrow a \geq b$ and $b \geq c$

$\Rightarrow a \geq c$

$\therefore$ The relation '$\geq$' is transitive.

Since the relation '$\geq$' is reflexive, antisymmetric and transitive, '$\geq$' is partial ordering on the set of integers. Therefore, $(Z, \geq)$ is a poset.

Example: Show that the inclusion $\subseteq$ is a partial ordering on the set power set of a set S.

Solution: Since (i). $A \subseteq A$ for all $A \subseteq S$, $\subseteq$ is reflexive.

(ii). $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$, $\subseteq$ is antisymmetric.

(iii). $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$, $\subseteq$ is transitive.

Thus, the relation $\subseteq$ is a partial ordering on the power set of S.

Example: Show that the divisibility relation '/' is a partial ordering on the set of positive integers.

Solution: Let Z^+ be the set of positive integers.

Since (i). a/a for all $a \in Z^+$, / is reflexive.

(ii). a/b and $b/a \Rightarrow a = b$, / is antisymmetric.

(iii). a/b and $b/c \Rightarrow a/c$, / is transitive.

It follows that / is a partial ordering on Z^+ and $(Z^+, /)$ is a poset.

Note: On the set of all integers, the above relation is not a partial order as a and $-a$ both divide each other, but $a = -a$. i.e., the relation is not antisymmetric. Definition: 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*.

Note: It is not necessary to have $x \leq y$ or $y \leq x$ for every x and y in a poset P . In fact, x may not be related to y, in which case we say that x and y are incomparable. Examples:

(i). The poset $(Z, \leq)$ is a totally ordered.

Since $a \leq b$ or $b \leq a$ whenever a and b are integers.

(ii). The divisibility relation / is a partial ordering on the set of positive integers.

Therefore $(Z^+, /)$ is a poset and it is not a totally ordered, since it contain elements that are incomparable, such as 5 and 7, 3 and 5.

Definition: In a poset $(P, \leq)$, an element $y \in P$ is said to *cover* an element $x \in P$ if $x < y$ and if there does not exist any element $z \in P$ such that $x \leq z$ and $z \leq y$; that is, y covers $x \Leftrightarrow (x < y \wedge (x \leq z \leq y \Rightarrow x = z \vee z = y))$.

Hasse Diagrams

A partial order $\leq$ on a set P can be represented by means of a diagram known as Hasse diagram of $(P, \leq)$. In such a diagram,

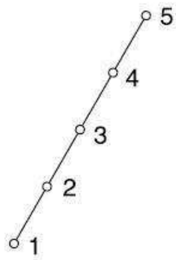
(i). Each element is represented by a small circle or dot.

(ii). The circle for $x \in P$ is drawn below the circle for $y \in P$ if $x < y$, and a line is drawn between x and y if y covers x.

(iii). If $x < y$ but y does not cover x, then x and y are not connected directly by a single line.

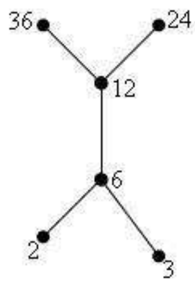
Note: For totally ordered set (P, $\leq$), the Hasse diagram consists of circles one below the other. The poset is called a chain.

Example: Let $P = \{1, 2, 3, 4, 5\}$ and $\leq$ be the relation "less than or equal to" then the Hasse diagram is:



It is a totally ordered set.

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, $\leq$). Solution: The Hasse diagram is is shown below:



It is not a total order set.

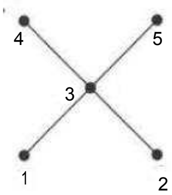
Example: Draw the Hasse diagram for the relation R on $A = \{1, 2, 3, 4, 5\}$ whose relation matrix given below:

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

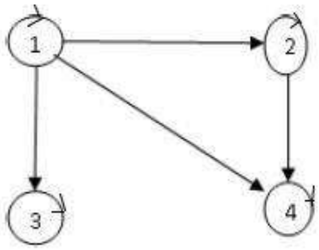
Solution:

$R = \{(1, 1), (1, 3), (1, 4), (1, 5), (2, 2), (2, 3), (2, 4), (2, 5), (3, 3), (3, 4), (3, 5), (4, 4), (5.5)\}$.

Hasse diagram for M_R is



Example: A partial order R on the set $A = \{1, 2, 3, 4\}$ is represented by the following digraph. Draw the Hasse diagram for R.

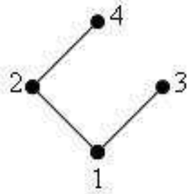


Solution: By examining the given digraph , we find that

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

We check that R is reflexive, transitive and antisymmetric. Therefore, R is partial order relation on A.

The hasse diagram of R is shown below:



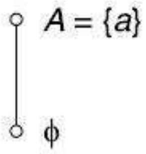
Example: Let A be a finite set and $\rho(A)$ be its power set. Let $\subseteq$ be the inclusion relation on the elements of $\rho(A)$. Draw the Hasse diagram of $\rho(A)$, $\subseteq$) for

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

Solution: (i). Let $A = \{a\}$

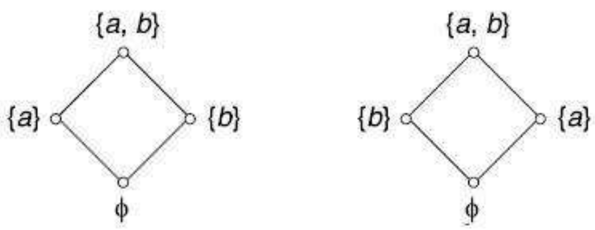
$\rho(A) = \{\phi, a\}$

Hasse diagram of $(\rho(A), \subseteq)$ is shown in Fig:



(ii). Let $A = \{a, b\}$. $\rho(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$.

The Hasse diagram for $(\rho(A), \subseteq)$ is shown in fig:

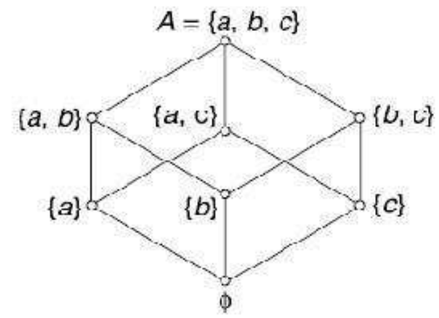


Example: Draw the Hasse diagram for the partial ordering $\subseteq$ on the power set $P(S)$ where $S = \{a, b, c\}$.

Solution: $S = \{a, b, c\}$.

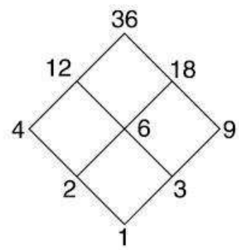
$P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Hasse diagram for the partial ordered set is shown in fig:



Example: Draw the Hasse diagram representing the positive divisions of 36 (i.e., D_{36}).

Solution: We have $D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ if and only a divides b. The Hasse diagram for R is shown in Fig.



Minimal and Maximal elements(members): Let $(P, \leq)$ denote a partially or-dered set. An element $y \in P$ is called a *minimal member* of P relative to $\leq$ if for no $x \in P$, is $x < y$.

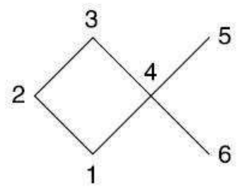
Similarly an element $y \in P$ is called a maximal member of P relative to the partial ordering $\leq$ if for no $x \in P$, is $y < x$.

Note:

(i). The minimal and maximal members of a partially ordered set need not unique.

(ii). Maximal and minimal elements are easily calculated from the Hasse diagram. They are the *'top'* and *'bottom'* elements in the diagram.

Example:



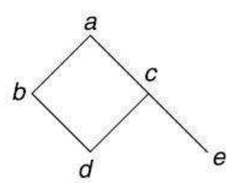
In the Hasse diagram, there are two maximal elements and two minimal elements.

The elements 3, 5 are maximal and the elements 1 and 6 are minimal.

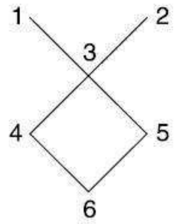
Example: Let $A = \{a, b, c, d, e\}$ and let the partial order on A in the natural way.

The element a is maximal.

The elements d and e are minimal.



Upper and Lower Bounds: Let $(P, \leq)$ be a partially ordered set and let $A \subseteq P$. Any element $x \in P$ is called an *upper bound* for A if for all $a \in A$, $a \leq x$. Similarly, any element $x \in P$ is called a *lower bound* for A if for all $a \in A$, $x \leq a$. Example: $A = \{1, 2, 3, ..., 6\}$ be ordered as pictured in figure.

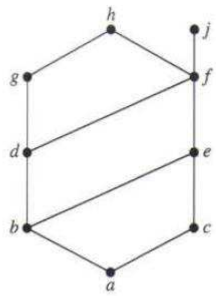


If $B = \{4, 5\}$ then the upper bounds of B are 1, 2, 3. The lower bound of B is 6.

Least Upper Bound and Greatest Lower Bound:

Let $(P, \leq)$ be a partial ordered set and let $A \subseteq P$. An element $x \in P$ is a *least upper bound* or *supremum* for A if x is an upper bound for A and $x \leq y$ where y is any upper bound for A. Similarly, the *the greatest lower bound* or *in mum* for A is an element $x \in P$ such that x is a lower bound and $y \leq x$ for all lower bounds y.

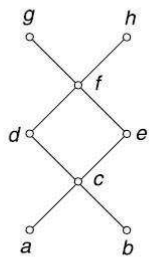
Example: Find the great lower bound and the least upper bound of $\{b, d, g\}$, if they exist in the poset shown in fig:



Solution: The upper bounds of $\{b, d, g\}$ are g and h. Since $g < h$, g is the least upper bound. The lower bounds of $\{b, d, g\}$ are a and b. Since $a < b$, b is the greatest lower bound.

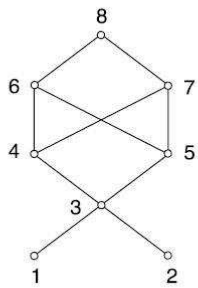
Example: Let $A = \{a, b, c, d, e, f, g, h\}$ denote a partially ordered set whose Hasse diagram is shown in Fig:

If $B = \{c, d, e\}$ then f, g, h are upper bounds of B. The element f is least upper bound.



Example: Consider the poset $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ whose Hasse diagram is shown in Fig and let $B = \{3, 4, 5\}$

The elements 1, 2, 3 are lower bounds of B. 3 is greatest lower bound.



Functions

A function is a special case of relation.

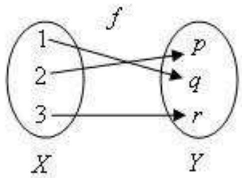
Definition: Let X and Y be any two sets. A relation f from X to Y is called a function if for every $x \in X$, there is a unique element $y \in Y$ such that $(x, y) \in f$. Note: The definition of function requires that a relation must satisfies two additional conditions in order to qualify as a function. These conditions are as follows:

(i) For every $x \in X$ must be related to some $y \in Y$, i.e., the domain of f must be X and nor merely a subset of X.

(ii). Uniqueness, i.e., $(x, y) \in f$ and $(x, z) \in f \Rightarrow y = z$.

The notation $f : X \to Y$, means f is a function from X to Y .

Example: Let $X = \{1, 2, 3\}$, $Y = \{p, q, r\}$ and $f = \{(1, p), (2, q), (3, r)\}$ then $f(1) = p, f(2) = q, f(3) = r$. Clearly f is a function from X to Y .



Domain and Range of a Function: If $f : X \to Y$ is a function, then X is called the Domain of f and the set Y is called the codomain of f. The range of f is defined as the set of all images under f.
It is denoted by $f(X) = \{y|$ for some x in $X, f(x) = y\}$ and is called the image of X in Y . The Range f is also denoted by R_f .

Example: If the function f is defined by $f(x)=x^2 + 1$ on the set $\{-2, -1, 0, 1, 2\}$, find the range of f.

Solution: $f(-2) = (-2)^2 + 1 = 5$

$f(-1) = (-1)^2 + 1 = 2$

$f(0) = 0 + 1 = 1$

$f(1) = 1 + 1 = 2$

$f(2) = 4 + 1 = 5$

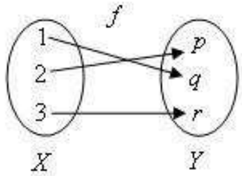
Therefore, the range of $f = \{1, 2, 5\}$.

Types of Functions

One-to-one(Injection): A mapping $f : X \to Y$ is called *one-to-one* if distinct elements of X are mapped into distinct elements of Y , i.e., f is one-to-one if

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

or equivalently $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ for $x_1, x_2 \in X$.



Example: $f : R \rightarrow R$ defined by $f(x) = 3x,\ \forall x \in R$ is one-one, since

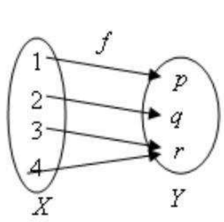
$$f(x_1) = f(x_2) \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2,\ \forall x_1, x_2 \in R.$$

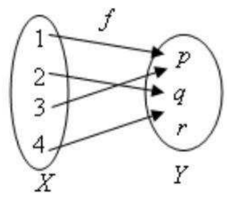
Example: Determine whether $f : Z \rightarrow Z$ given by $f(x) = x^2$, $x \in Z$ is a one-to-One function.

Solution: The function $f : Z \rightarrow Z$ given by $f(x) = x^2$, $x \in Z$ is not a one-to-one function. This is because both 3 and -3 have 9 as their image, which is against the definition of a one-to-one function.

Onto(Surjection): A mapping $f : X \rightarrow Y$ is called *onto* if the range set $R_f = Y$.

If $f : X \rightarrow Y$ is onto, then each element of Y is f-image of atleast one element of X.
i.e., $\{f(x) : x \in X\} = Y$.
If f is not onto, then it is said to be *into*.

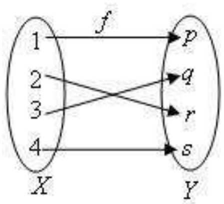




Surjective Not Surjective

Example: $f : R \rightarrow R$, given by $f(x) = 2x,\ \forall x \in R$ is onto.

Bijection or One-to-One, Onto: A mapping $f : X \rightarrow Y$ is called *one-to-one, onto* or *bijective* if it is both one-to-one and onto. Such a mapping is also called a one-to-one correspondence between X and Y .



Example: Show that a mapping $f : R \rightarrow R$ defined by $f(x) = 2x + 1$ for $x \in R$ is a bijective map from R to R.

Solution: Let $f : R \rightarrow R$ defined by $f(x) = 2x + 1$ for $x \in R$. We need to prove that f is a bijective map, i.e., it is enough to prove that f is one-one and onto.

- Proof of f being one-to-one
  Let x and y be any two elements in R such that $f(x) = f(y)$
  $\Rightarrow 2x + 1 = 2y + 1$
  $\Rightarrow x = y$
  Thus, $f(x) = f(y) \Rightarrow x = y$
  This implies that f is one-to-one.

- Proof of f being onto
  Let y be any element in the codomain R

  $\Rightarrow f(x) = y$

  $\Rightarrow 2x + 1 = y$

  $\Rightarrow x = (y-1)/2$

Clearly, $x = (y-1)/2 \in R$

Thus, every element in the codomain has pre-image in the domain.
This implies that f is onto
Hence, f is a bijective map.

Identity function: Let X be any set and f be a function such that $f : X \rightarrow X$ is defined by $f(x) = x$ for all $x \in X$. Then, f is called the identity function or identity transformation on X. It can be denoted by I or I_X.

Note: The identity function is both one-to-one and onto.

Let $I_X(x) = I_X(y)$

$\Rightarrow x = y$

$\Rightarrow I_X$ is one-to-one

I_X is onto since $x = I_X(x)$ for all x.

Composition of Functions

Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ be two functions. Then the composition of f and g denoted by $g \circ f$, is the function from X to Z defined as

$$(g \circ f)(x) = g(f(x)), \text{ for all } x \in X.$$

Note. In the above definition it is assumed that the range of the function f is a subset of Y (the Domain of g), i.e., $R_f \subseteq D_g$. $g \circ f$ is called the left composition g with f.

Example: Let $X = \{1, 2, 3\}$, $Y = \{p, q\}$ and $Z = \{a, b\}$. Also let $f : X \rightarrow Y$ be f $= \{(1, p), (2, q), (3, q)\}$ and $g : Y \rightarrow Z$ be given by $g = \{(p, b), (q, b)\}$. Find $g \circ f$. Solution: $g \circ f = \{(1, b), (2, b), (3, b)$.

Example: Let $X = \{1, 2, 3\}$ and f, g, h and s be the functions from X to X given by

$$f = \{(1, 2), (2, 3), (3, 1)\} \qquad g = \{(1, 2), (2, 1), (3, 3)\}$$
$$h = \{(1, 1), (2, 2), (3, 1)\} \qquad s = \{(1, 1), (2, 2), (3, 3)\}$$

Find $f \circ f$; $g \circ f$; $f \circ h \circ g$; $s \circ g$; $g \circ s$; $s \circ s$; and $f \circ s$.

Solution:

$$f \circ g = \{(1, 3), (2, 2), (3, 1)\}$$
$$g \circ f = \{(1, 1), (2, 3), (3, 2)\} \neq f \circ g$$
$$f \circ h \circ g = f \circ (h \circ g) = f \circ \{(1, 2), (2, 1), (3, 1)\}$$
$$= \{(1, 3), (2, 2), (3, 2)\}$$
$$s \circ g = \{(1, 2), (2, 1), (3, 3)\} = g$$
$$g \circ s = \{(1, 2), (2, 1), (3, 3)\}$$
$$\therefore s \circ g = g \circ s = g$$
$$s \circ s = \{(1, 1), (2, 2), (3, 3)\} = s$$
$$f \circ s = \{(1, 2), (2, 3), (3, 1)\}$$

Thus, s ∘ s = s, f ∘ g ≠ g ∘ f, s ∘ g = g ∘ s = g and h ∘ s = s ∘ h = h.

Example: Let $f(x) = x + 2$, $g(x) = x - 2$ and $h(x) = 3x$ for $x \in R$, where R is the set of real numbers. Find $g \circ f$; $f \circ g$; $f \circ f$; $g \circ g$; $f \circ h$; $h \circ g$; $h \circ f$; and $f \circ h \circ g$.

Solution: $f : R \rightarrow R$ is defined by $f(x) = x + 2$

f: $R \rightarrow R$ is defined by $g(x) = x - 2$

$h : R \rightarrow R$ is defined by $h(x) = 3x$

- $g \circ f : R \rightarrow R$

  Let $x \in R$. Thus, we can write

  $(g \circ f)(x) = g(f(x)) = g(x + 2) = x + 2 - 2 = x$

  $\therefore (g \circ f)(x) = \{(x, x)| \ x \in R\}$
- $(f \circ g)(x) = f(g(x)) = f(x - 2) = (x - 2) + 2 = x$

  $\therefore f \circ g = \{(x, x)| \ x \in R\}$
- $(f \circ f)(x) = f(f(x)) = f(x + 2) = x + 2 + 2 = x + 4$

  $\therefore f \circ f = \{(x, x + 4)| \ x \in R\}$
- $(g \circ g)(x) = g(g(x)) = g(x - 2) = x - 2 - 2 = x - 4$

  $\Rightarrow g \circ g = \{(x, x - 4)| \ x \in R\}$
- $(f \circ h)(x) = f(h(x)) = f(3x) = 3x + 2$

  $\therefore f \circ h = \{(x, 3x + 2)| \ x \in R\}$
- $(h \circ g)(x) = h(g(x)) = h(x - 2) = 3(x - 2) = 3x - 6$

  $\therefore h \circ g = \{(x, 3x - 6)| \ x \in R\}$
- $(h \circ f)(x) = h(f(x)) = h(x + 2) = 3(x + 2) = 3x + 6$ $h \circ f =$ $\{(x, 3x + 6)| \ x \in R\}$
- $(f \circ h \circ g)(x) = [f \circ (h \circ g)](x)$

  $f(h \circ g(x)) = f(3x - 6) = 3x - 6 + 2 = 3x - 4$

  $\therefore f \circ h \circ g = \{(x, 3x - 4)| \ x \in R\}$.

Example: What is composition of functions? Let f and g be functions from R to R, where R is a set of real numbers defined by $f(x) = x^2 + 3x + 1$ and $g(x) = 2x - 3$. Find the composition of functions: i) $f \circ f$ ii) $f \circ g$ iii) $g \circ f$.

Inverse Functions

A function $f : X \rightarrow Y$ is aid to be *invertible* of its inverse function f^{-1} is also function from the range of f into X.

Theorem: A function $f : X \rightarrow Y$ is invertible $\Leftrightarrow f$ is one-to-one and onto.

Example: Let $X = \{a, b, c, d\}$ and $Y = \{1, 2, 3, 4\}$ and let $f : X \rightarrow Y$ be given by f = $\{(a, 1), (b, 2), (c, 2), (d, 3)\}$. Is f^{-1} a function?

Solution: $f^{-1} = \{(1, a), (2, b), (2, c), (3, d)\}$. Here, 2 has two distinct images b and c.

Therefore, f^{-1} is not a function.

Example: Let R be the set of real numbers and $f : R \rightarrow R$ be given by $f = \{(x, x^2) | x \in R\}$. Is f^{-1} a function?

Solution: The inverse of the given function is defined as $f^{-1} = \{(x^2, x) | x \in R\}$.
Therefore, it is not a function.

Theorem: If $f : X \rightarrow Y$ and $g : Y \rightarrow X$ be such that $g \circ f = I_X$ and $f \circ g = I_y$, then f and g are both invertible. Furthermore, $f^{-1} = g$ and $g^{-1} = f$.

Example: Let $X = \{1, 2, 3, 4\}$ and f and g be functions from X to X given by $f = \{(1, 4), (2, 1), (3, 2), (4, 3)\}$ and $g = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$. Prove that f and g are inverses of each other.

Solution: We check that

$$(g \circ f)(1) = g(f(1)) = g(4) = 1 = I_X(1), \quad (f \circ g)(1) = f(g(1)) = f(2) = 1 = I_X(1).$$

$$(g \circ f)(2) = g(f(2)) = g(1) = 2 = I_X(2), \quad (f \circ g)(2) = f(g(2)) = f(3) = 2 = I_X(2).$$

$$(g \circ f)(3) = g(f(3)) = g(2) = 3 = I_X(3), \quad (f \circ g)(3) = f(g(3)) = f(4) = 3 = I_X(3).$$

$$(g \circ f)(4) = g(f(4)) = g(3) = 4 = I_X(4), \quad (f \circ g)(4) = f(g(4)) = f(1) = 4 = I_X(4).$$

Thus, for all $x \in X$, $(g \circ f)(x) = I_X(x)$ and $(f \circ g)(x) = I_X(x)$. Therefore g is inverse of f and f is inverse of g.

Example: Show that the functions $f(x) = x^3$ and $g(x) = x^{1/3}$ for $x \in R$ are inverses of one another.

Solution: $f : R \rightarrow R$ is defined by $f(x) = x^3$; f: $R \rightarrow R$ is defined by $g(x) = x^{1/3}$

$$(f \circ g)(x) = f(g(x)) = f(x^{1/3}) = x^{3(1/3)} = x = I_X(x)$$

i.e., $(f \circ g)(x) = I_X(x)$

and $(g \circ f)(x) = g(f(x)) = g(x^3) = x^{3(1/3)} = x = I_X(x)$

i.e., $(g \circ f)(x) = I_X(x)$

Thus, $f = g^{-1}$ or $g = f^{-1}$

i.e., f and g are inverses of one other.

***Example: $f : R \rightarrow R$ is defined by $f(x) = ax + b$, for $a, b \in R$ and $a \neq 0$. Show that f is invertible and find the inverse of f.

(i) First we shall show that f is one-to-one

Let $x_1, x_2 \in R$ such that $f(x_1) = f(x_2)$

$\Rightarrow ax_1 + b = ax_2 + b$

$\Rightarrow ax_1 = ax_2$

$\Rightarrow x_1 = x_2$

$\therefore f$ is one-to-one.

- To show that f is onto.

  Let $y \in R$(codomain) such that $y = f(x)$ for some $x \in R$.

  $\Rightarrow y = ax + b$

  $\Rightarrow ax = y - b$

  $\Rightarrow x = (y-b)/a$

Given $y \in R$(codomain), there exists an element $x = (y-b)/a \in R$ ~~such~~ that $f(x) = y$.

$\therefore f$ is onto

$\Rightarrow f$ is invertible and $f^{-1}(x) = (x-b)/a$

Example: Let $f : R \to R$ be given by $f(x) = x^3 - 2$. Find f^{-1}.

(i) First we shall show that f is one-to-one

Let $x_1, x_2 \in R$ such that $f(x_1) = f(x_2)$

$\Rightarrow x^3_1 - 2 = x^3_2 -$

$2 \Rightarrow x^3_1 = x^3_2$

$\Rightarrow x_1 = x_2$

$\therefore f$ is one-to-one.

- To show that f is onto.

  $\Rightarrow y = x^3 - 2$

  $\Rightarrow x^3 = y+2$

  $\Rightarrow x = \sqrt[3]{y+2}$

Given $y \in R$(codomain), there exists an element $x = \sqrt[3]{y+2} \in R$ such that $f(x) = y$.

$\therefore f$ is onto

$\Rightarrow f$ is invertible and $f^{-1}(x) = \sqrt[3]{x+2}$

Floor and Ceiling functions:

Let x be a real number, then the least integer that is not less than x is called the CEILING of x.

The CEILING of x is denoted by $\lceil x \rceil$.

Examples: $\lceil 2.15 \rceil = 3, \lceil \sqrt{5} \rceil = 3, \lceil -7.4 \rceil = -7, \lceil -2 \rceil = -2$

Let x be any real number, then the greatest integer that does not exceed x is called the Floor of x.

The FLOOR of x is denoted by $\lfloor x \rfloor$.

Examples: $\lfloor 5.14 \rfloor = 5, \lfloor \sqrt{5} \rfloor = 2, \lfloor -7.6 \rfloor = -8, \lfloor 6 \rfloor = 6, \lfloor -3 \rfloor = -3$

Example: Let f and g abe functions from the positive real numbers to positive real numbers defined by $f(x) = \lfloor 2x \rfloor$, $g(x) = x^2$. Calculate $f \circ g$ and $g \circ f$.

Solution: $f \circ g(x) = f(g(x)) = f(x^2) = \lfloor 2x^2 \rfloor$

$g \circ f(x) = g(f(x)) = g(\lfloor 2x \rfloor) = (\lfloor 2x \rfloor)^2$

Recursive Function

Total function: Any function $f : N^n \to N$ is called *total* if it is defined for every n-tuple in N^n.

Example: $f(x, y) = x + y$, which is defined for all $x, y \in N$ and hence it is a total function.

Partial function: If $f : D \to N$ where $D \subseteq N^n$, then f is called a *partial function*.

Example: $g(x, y) = x - y$, which is defined for only $x, y \in N$ which satisfy $x \geq y$.

Hence $g(x, y)$ is partial.

Initial functions:

The initial functions over the set of natural numbers is given by

- ***Zero function*** Z: $Z(x) = 0$, for all x.
- ***Successor function*** S: $S(x) = x + 1$, for all x.
- ***Projection function*** U_i^n: $U_i^n(x_1, x_2, ..., x_n) = x_i$ for all n tuples $(x_1, x_2, ..., x_n)$, $1 \leq i \leq n$.

Projection function is also called *generalized identity function*.

For example, $U_1^1(x) = x$ for every $x \in N$ is the identity function.

$U_1^2(x, y) = x$, $U_1^3(2, 6, 9) = 2$, $U_2^3(2, 6, 9) = 6$, $U_3^3(2, 6, 9) = 9$.

Composition of functions of more than one variable:

The operation of composition will be used to generate the other function.

Let $f_1(x, y)$, $f_2(x, y)$ and $g(x, y)$ be any three functions. Then the composition of g with f_1 and f_2 is defined as a function $h(x, y)$ given by

$$h(x, y) = g(f_1(x, y), f_2(x, y)).$$

In general, let $f_1, f_2, ..., f_n$ each be partial function of m variables and g be a partial function of n variables. Then the composition of g with $f_1, f_2, ..., f_n$ produces a partial function h given by

$$h(x_1, x_2, ..., x_m) = g(f_1(x_1, x_2, ..., x_m), ..., f_n(x_1, x_2, ...x_m)).$$

Note: The function h is total iff $f_1, f_2, ..., f_n$ and g are total.

Example: Let $f_1(x, y) = x + y$, $f_2(x, y) = xy + y^2$ and $g(x, y) = xy$. Then

$$\begin{aligned} h(x, y) &= g(f_1(x, y), f_2(x, y)) \\ &= g(x + y, xy + y^2 \\ &= (x + y)(xy + y^2) \end{aligned}$$

Recursion: The following operation which defines a function $f(x_1, x_2, ..., x_n, y)$ of $n + 1$ variables by using other functions $g(x_1, x_2, .., x_n)$ and $h(x_1, x_2, ..., x_n, y, z)$ of n and $n + 2$ variables, respectively, is called *recursion*.

$$f(x_1, x_2, ..., x_n, 0) = g(x_1, x_2, ..., x_n)$$

$$f(x_1, x_2, ..., x_n, y + 1) = h(x_1, x_2, ..., x_n, y, f(x_1, x_2, ..., x_n, y))$$

where y is the inductive variable.

Primitive Recursive: A function f is said to be *Primitive recursive* iff it can be obtained from the initial functions by a finite number of operations of composition and recursion.

*****Example:** Show that the function $f(x, y) = x + y$ is primitive recursive. Hence compute the value of $f(2, 4)$.

Solution: Given that $f(x, y) = x + y$.

Here, $f(x, y)$ is a function of two variables. If we want f to be defined by recursion, we need a function g of single variable and a function h of three variables. Now,

$$\begin{aligned} f(x, y + 1) &= x + (y + 1) \\ &= (x + y) + 1 \\ &= f(x, y) + 1. \end{aligned}$$

Also, $f(x, 0) = x$.
We define $f(x, 0)$ as

$$\begin{aligned} f(x, 0) = x &= U_1^1(x) \\ &= S(f(x, y)) \\ &= S(U_3^3(x, y, f(x, y))) \end{aligned}$$

If we take $g(x) = U_1^1(x)$ and $h(x, y, z) = S(U_3^3(x, y, z))$, we get $f(x, 0) = g(x)$ and $f(x, y + 1) = h(x, y, z)$.
Thus, f is obtained from the initial functions U_1^1, U_3^3, and S by applying composition once and recursion once.
Hence f is primitive recursive.
Here,

$$\begin{aligned} f(2, 0) &= 2 \\ f(2, 4) &= S(f(2, 3)) \\ &= S(S(f(2, 2))) \\ &= S(S(S(f(2, 1)))) \\ &= S(S(S(S(f(2, 0))))) \\ &= S(S(S(S(2))))) \\ &= S(S(S(3))) \\ &= S(S(4)) \\ &= S(5) \\ &= 6 \end{aligned}$$

Example: Show that $f(x, y) = x * y$ is primitive recursion.

Solution: Given that $f(x, y) = x * y$.

Here, $f(x, y)$ is a function of two variables. If we want f to be defined by recursion, we need a function g of single variable and a function h of three variables. Now, $f(x, 0) = 0$ and

$$f(x, y + 1) = x * (y + 1) = x * y$$

- $f(x, y) + x$

We can write

$$f(x, 0) = 0 = Z(x) \text{ and}$$
$$f(x, y + 1) = f_1(U_3^3(x, y, f(x, y)), U_1^3(x, y, f(x, y)))$$

where $f_1(x, y) = x + y$, which is primitive recursive. By taking $g(x) = Z(x) = 0$ and h defined by $h(x, y, z) = f_1(U_3^3(x, y, z), U_1^3(x, y, z)) = f(x, y + 1)$, we see that f defined by recursion. Since g and h are primitive recursive, f is primitive recursive. Example: Show that $f(x, y) = x^y$ is primitive recursive function. Solution: Note that $x^0 = 1$ for $x \neq 0$ and we put $x^0 = 0$ for $x = 0$.
Also, $x^{y+1} = x^y * x$

Here $f(x, y) = x^y$ is defined as

$$f(x, 0) = 1 = S(0) = S(Z(x))$$

$f(x, y + 1) = x * f(x, y)$

- $U_1^3(x, y, f(x, y)) * U_3^3(x, y, f(x, y))$

$h(x, y, f(x, y) = f_1(U_1^3(x, y, f(x, y)), U_3^3(x, y, f(x, y)))$ where $f_1(x, y) = x * y$, which is primitive recursive.

$\therefore f(x, y)$ is a primitive recursive function.

Example: Consider the following recursive function definition: If $x < y$ then $f(x, y) = 0$, if $y \leq x$ then $f(x, y) = f(x - y, y) + 1$. Find the value of $f(4, 7)$, $f(19, 6)$.

Solution: Given $f(x, y) = \begin{cases} 0; x < y \\ f(x-y, y)+1 \; ; y \leq x \end{cases}$

$$
\begin{aligned}
f(4, 7) &= 0 \qquad [\because 4 < 7] \\
f(19, 6) &= f(19 - 6, 6) + 1 \\
&= f(13, 6) + 1 \\
f(13, 6) &= f(13 - 6, 6) + 1 \\
&= f(7, 6) + 1 \\
f(7, 6) &= f(7 - 6, 6) + 1 \\
&= f(1, 6) + 1 \\
&= 0 + 1 \\
&= 1 \\
f(13, 6) &= f(7, 6) + 1 \\
&= 1 + 1 \\
&= 2 \\
f(19, 6) &= 2 + 1 \\
&= 3
\end{aligned}
$$

Example: Consider the following recursive function definition: If $x < y$ then $f(x, y) = 0$, if $y \leq x$ then $f(x, y) = f(x - y, y) + 1$. Find the value of $f(86, 17)$

Permutation Functions

Definition: A *permutation* is a one-one mapping of a non-empty set onto itself.

Let $S = \{a_1, a_2, ..., a_n\}$ be a finite set and p is a permutation on S, we list the elements of S and the corresponding functional values of $p(a_1), p(a_2), ..., p(a_n)$ in the following form:

$$\begin{pmatrix} a_1 & a_2 & . & . & . & a_n \\ p(a_1) & p(a_2) & . & . & . & p(a_n) \end{pmatrix}$$

If $p : S \rightarrow S$ is a bijection, then the number of elements in the given set is called the *degree* of its permutation.

Note: For a set with three elements, we have 3! permutations.

Example: Let $S = \{1, 2, 3\}$. The permutations of S are as follows:

$P_1=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$; $P_2=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$; $P_3=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$; $P_4=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$; $P_5=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$; $P_6=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Example: Let $S = \{1, 2, 3, 4\}$ and $p : S \rightarrow S$ be given by $f(1) = 2$, $f(2) = 1$, $f(3) = 4$, $f(4) = 3$. Write this in permutation notation.

Solution: The function can be written in permutation notation as given below:

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

Identity Permutation: If each element of a permutation be replaced by itself, then such a permutation is called the *identity permutation.*

Example: Let $S = \{a_1, a_2, , a_n\}$.then I=$\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ a_1 & a_2 & \dots & a_n\end{pmatrix}$ is the identity permutation on S.

Equality of Permutations: Two permutations f and g of degree n are said to be equal if and only if $f(a) = g(a)$ for all $a \in S$.

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

$$f=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix};g=\begin{pmatrix}4 & 1 & 3 & 2\\ 4 & 3 & 2 & 1\end{pmatrix}$$

We have $f(1) = g(1) = 3$

$f(2) = g(2) = 1$

$f(3) = g(3) = 2$

$f(4) = g(4) = 4$

i.e., $f(a) = g(a)$ for all $a \in S$.

Product of Permutations: (or Composition of Permutations)

Let S={a,b,…h}and let $\begin{pmatrix}a & b & \dots & h\\ f(a) & f(b) & \dots & f(h)\end{pmatrix}$,g=$\begin{pmatrix}a & b & \dots & h\\ g(a) & g(b) & \dots & g(h)\end{pmatrix}$

We define the composite of f and g as follows:

$$f\circ g=\begin{pmatrix}a & b & \dots & h\\ f(a) & f(b) & \dots & f(h)\end{pmatrix}\text{o}\begin{pmatrix}a & b & \dots & h\\ g(a) & g(b) & \dots & g(h)\end{pmatrix}$$

$$=\begin{pmatrix}a & b & \dots & h\\ f(g(a)) & f(g(b)) & \dots & f(g(h))\end{pmatrix}$$

Clearly, $f\circ g$ is a permutation.

Example: Let $S = \{1, 2, 3, 4\}$ and let $f=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$ and $g=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}$ Find $f\circ g$ and $g\circ f$ in the permutation from.

Solution: $f\circ g=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 4 & 1\end{pmatrix}$;$g\circ f=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$

Note: The product of two permutations of degree n need not be commutative.

Inverse of a Permutation:

If f is a permutation on $S = \{a_1, a_2, , a_n\}$ such that $f=\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ b_1 & b_2 & \dots. & b_n\end{pmatrix}$

then there exists a permutation called the inverse f, denoted f^{-1} such that $f\circ f^{-1}=f^{-1}\circ f=I$ (the identity permutation on S)

where $f^{-1} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$

Example: If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, then find f^{-1}, and show that $f \circ f^{-1} = f^{-1} \circ f = I$

Solution: $f^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$

$$f \circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \text{o} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Similarly, $f^{-1} \circ f = I. \Rightarrow f \circ f^{-1} = f^{-1} \circ f = I.$

Cyclic Permutation: Let $S = \{a_1, a_2, ..., a_n\}$ be a finite set of n symbols. A permutation f defined on S is said to be *cyclic permutation* if f is defined such that

$$f(a_1) = a_2, f(a_2) = a_3, ..., f(a_{n-1}) = a_n \text{ and } f(a_n) = a_1.$$

Example: Let $S = \{1, 2, 3, 4\}$.

Then $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ =(1 4)(2 3) is a cyclic permutation.

Disjoint Cyclic Permutations: Let $S = \{a_1, a_2, ..., a_n\}$. If f and g are two cycles on S such that they have no common elements, then f and g are said to be disjoint cycles.

Example: Let $S = \{1, 2, 3, 4, 5, 6\}$.

If $f = (1\ 4\ 5)$ and $g = (2\ 3\ 6)$ then f and g are disjoint cyclic permutations on S.

Note: The product of two disjoint cycles is commutative.

Example: Consider the permutation $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 \end{pmatrix}$

The above permutation f can be written as $f = (1\ 2\ 3\ 4\ 5)(6\ 7)$. Which is a product of two disjoint cycles.

Transposition: A cyclic of length 2 is called a *transposition*.

Note: Every cyclic permutation is the product of transpositions.

Example: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$ =(1 2 4)(3 5) = (1 4)(1 2)(3 5).

Inverse of a Cyclic Permutation: To find the inverse of any cyclic permutation, we write its elements in the reverse order.

For example, $(1\ 2\ 3\ 4)^{-1} = (4\ 3\ 2\ 1)$.

Even and Odd Permutations: A permutation *f* is said to be an *even permutation* if *f* can be expressed as the product of even number of transpositions.

A permutation *f* is said to be an *odd permutation* if *f* is expressed as the product of odd number of transpositions.

Note:

(i) An identity permutation is considered as an even permutation.

(ii) A transposition is always odd.

(iii). The product of an even and an odd permutation is odd. Similarly the product of an odd permutation and even permutations is odd.

Example: Determine whether the following permutations are even or odd permutations.

(i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$

(ii) $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 7 & 8 & 6 & 1 & 4 & 3 \end{pmatrix}$

(iii) $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$

Solution: (i). For $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} = (1\ 2\ 4) = (1\ 4)(1\ 2)$

$\Rightarrow f$ is an even permutation

(ii). For $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 7 & 8 & 6 & 1 & 4 & 3 \end{pmatrix}$

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

$\Rightarrow$ g is an even permutation.

(iii) h= $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix} = (1\ 4\ 2\ 3) = (1\ 3)(1\ 2)(1\ 4)$

Product of three transpositions

$\Rightarrow h$ is an odd permutation.

Lattices

In this section, we introduce lattices which have important applications in the theory and design of computers.

Definition: A lattice is a partially ordered set $(L, \leq)$ in which every pair of elements $a, b \in L$ has a greatest lower bound and a least upper bound.

Example: Let Z^+ denote the set of all positive integers and let R denote the relation 'division' in Z^+, such that for any two elements $a, b \in Z^+$, aRb, if a divides b. Then (Z^+, R) is a lattice in which the join of a and b is the least common multiple of a and b, i.e.

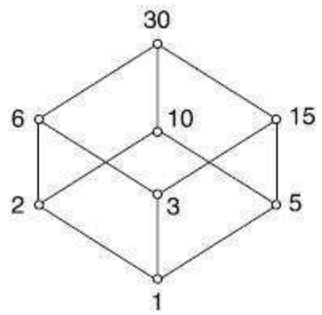
$$a \vee b = a \oplus b = \text{LCM of } a \text{ and } b,$$

and the meet of a and b, i.e. $a * b$ is the greatest common divisor (GCD) of a and b i.e.,

$$a \wedge b = a * b = \text{GCD of } a \text{ and } b.$$

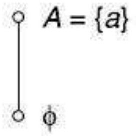
We can also write $a+b = a \vee b = a \oplus b$=LCM of a and b and $a.b = a \wedge b = a * b$=GCD of a and b.

Example: Let n be a positive integer and S_n be the set of all divisors of n If $n = 30$, $S_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$. Let R denote the relation division as defined in Example 1. Then (S_{30}, R) is a Lattice see Fig:

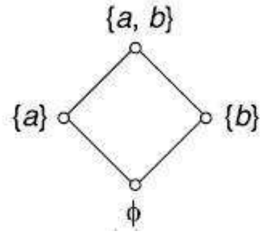


Example: Let A be any set and $P(A)$ be its power set. The poset $P(A), \subseteq)$ is a lattice in which the meet and join are the same as the operations $\cap$ and $\cup$ on sets respectively.

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



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



Some Properties of Lattice

Let $(L, \leq)$ be a lattice and $*$ and $\oplus$ denote the two binary operation meet and join on $(L, \leq)$. Then for any $a, b, c \in L$, we have

(L1): $a * a = a$, $(L1)'$: $a \oplus a = a$ (Idempotent laws)

$(L2)$: $b * a = b * a$, $(L2)'$: $a \oplus b = b + a$ (Commutative laws)

$(L3)$: $(a * b) * c = a * (b * c)$, $(L3)'$: $(a \oplus b) \oplus c = a \oplus (b + c)$ (Associative laws)

$(L4)$: $a * (a + b) = a$, $(L4)'$: $a \oplus (a * b) = a$ (Absorption laws).

The above properties $(L1)$ to $(L4)$ can be proved easily by using definitions of meet and join. We can apply the principle of duality and obtain $(L1)'$ to $(L4)'$.

Theorem: Let $(L, \leq)$ be a lattice in which $*$ and $\oplus$ denote the operations of meet and join respectively. For any $a, \in L$, $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.

Proof: We shall first prove that $a \leq b \Leftrightarrow a * b = b$.

In order to do this, let us assume that $a \leq b$. Also, we know that $a \leq a$.

Therefore $a \leq a * b$. From the definition of $a * b$, we have $a * b \leq a$.

Hence $a \leq b \Rightarrow a * b = a$.

Next, assume that $a * b = a$; but it is only possible if $a \leq b$, that is, $a * b = a \Rightarrow a \leq b$.

Combining these two results, we get the required equivalence.

It is possible to show that $a \leq b \Leftrightarrow a \oplus b = b$ in a similar manner.

Alternatively, from $a * b = a$, we have

$$b \oplus (a * b) = b \oplus a = a \oplus b$$

but $b \oplus (a * b) = b$

Hence $a \oplus b = b$ follows from $a * b = a$.

By repeating similar steps, we can show that $a * b = a$ follows from $a \oplus b = b$.

Therefore $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.

Theorem: Let $(L, \leq)$ be a lattice. Then $b \leq c \Rightarrow \begin{cases} a * b \leq a * c \\ \mathrm{a} \oplus \mathrm{b} \leq \mathrm{a} \oplus \mathrm{c} \end{cases}$

Proof: By above theorem $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.

To show that $a * b \leq a * c$, we shall show that $(a * b) * (a * c) = a * b$

$$\begin{aligned}(a * b) * (a * c) &= a * (b * a) * c \\ &= a * (a * b) * c \\ &= (a * a) * (b * c) \\ &= a * (b * c) \\ &= a * b\end{aligned}$$

$\therefore$ If $\mathrm{b} \leq \mathrm{c}$ then $\mathrm{a} * \mathrm{b} \leq \mathrm{a} * \mathrm{c}$. Next, let $b \leq c \Rightarrow b \oplus c = c$.

To show that $a \oplus b \leq a \oplus c$. It sufficient to show that $(a \oplus b) \oplus (a \oplus c) = a \oplus c$.

Consider,$(a \oplus b) \oplus (a \oplus c) = a \oplus (b \oplus a) \oplus c$

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

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

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

$= a \oplus b$

$\therefore$ If $b \leq c$ then $a \oplus b \leq a \oplus c$.

Note: The above properties of a Lattice are called properties of Isotonicity.

Lattice as an algebraic system:

We now define lattice as an algebraic system, so that we can apply many concepts associated with algebraic systems to lattices.

Definition: A lattice is an algebraic system $(L, *, \oplus)$ with two binary operation '$*$'and '$\oplus$' on L which are both commutative and associative and satisfy absorption laws.

Bounded Lattice:

A bounded lattice is an algebraic structure $(L,\wedge,\vee,0,1)$ sucha that $(L,\wedge,\vee)$ is a lattice, and the constants $0,1\in L$ satisfy the following:

1. for all $x\in L$, $x\wedge 1=x$ and $x\vee 1=1$
2. for all $x\in L$, $x\wedge 0=0$ and $x\vee 0=x$.

The element 1 is called the upper bound, or top of L and the element 0 is called the lower bound or bottom of L.

Distributive lattice:

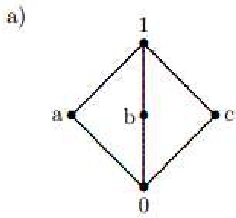
A lattice $(L,\vee,\wedge)$ is **distributive** if the following additional identity holds for all x, y, and z in L:

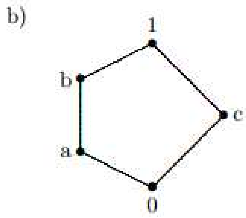
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

Viewing lattices as partially ordered sets, this says that the meet peration preserves nonempty finite joins. It is a basic fact of lattice theory that the above condition is equivalent to its dual

$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ for all x, y, and z in L.

Example: Show that the following simple but significant lattices are not distributive.



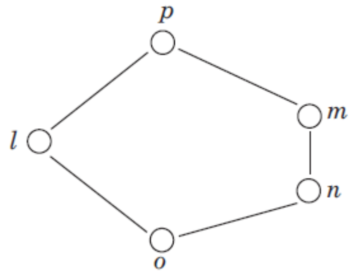


Solution a) To see that the diamond lattice is not distributive, use the middle elements of the lattice: $a \wedge (b \vee c) = a \wedge 1 = a$, but $(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$, and $a \neq 0$.

Similarly, the other distributive law fails for these three elements.

b) The pentagon lattice is also not distributive

Example: Show that lattice is not a distributive lattice.



Sol. A lattice is distributive if all of its elements follow distributive property so let we verify the distributive property between the elements n, l and m.

GLB(n, LUB(l, m)) = GLB(n, p) [$\therefore$ LUB(l, m) = p]

= n (LHS)

also LUB(GLB(n, l), GLB(n, m)) = LUB(o, n); [$\therefore$ GLB(n, l) = o and GLB(n, m) = n]

= n (RHS)

so LHS = RHS.

But GLB(m, LUB(l, n)) = GLB(m, p) [$\therefore$ LUB(l, n) = p]

= m (LHS)

also LUB(GLB(m, l), GLB(m, n)) = LUB(o, n); [$\therefore$ GLB(m, l) = o and GLB(m, n) = n]

= n (RHS)

Thus, LHS $\neq$ RHS hence distributive property doesn't hold by the lattice so lattice is not distributive.

Example: Consider the poset (X, $\leq$) where X = {1, 2, 3, 5, 30} and the partial ordered relation $\leq$ is defined as i.e. if x and y $\in$X then x $\leq$ y means 'x divides y'. Then show that poset (I+, $\leq$) is a lattice.

Sol. Since GLB(x, y) = $x \wedge y$ = $lcm(x, y)$

and LUB(x, y) = $x \vee y$ = $gcd(x, y)$

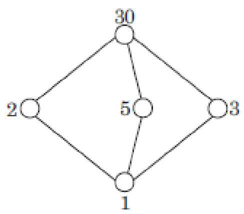
Now we can construct the operation table I and table II for GLB and LUB respectively and the Hasse diagram is shown in Fig.

Table I

LUB	1	2	3	5	30
1	1	2	3	5	30
2	2	2	30	30	30
3	3	30	3	30	30
5	5	30	30	5	30
30	30	30	30	30	30

Table II

GLB	1	2	3	5	30
1	1	1	1	1	1
2	1	2	1	1	2
3	1	1	3	1	3
5	1	1	1	5	5
30	1	2	3	5	30



Test for distributive lattice, i.e.,

GLB(x, LUB(y, z)) = LUB(GLB(x, y), GLB(x, z))

Assume x = 2, y = 3 and z = 5, then

*RHS:*GLB(2, LUB(3, 5)) = GLB(2, 30) = 2

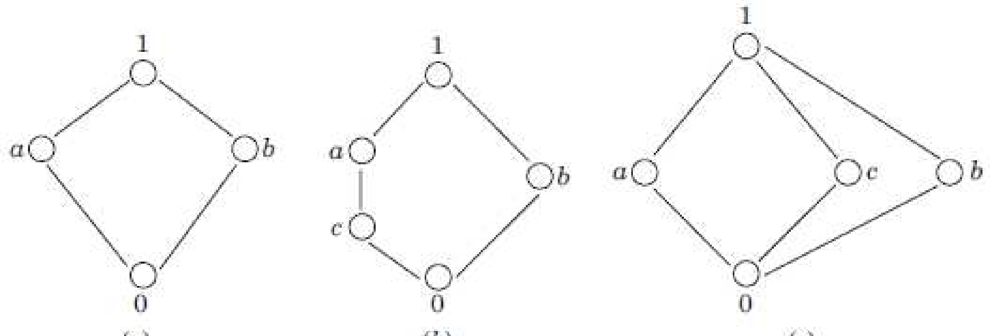
LHS: LUB(GLB(2, 3), GLB(2, 5)) = LUB(1, 1) = 1

Since*RHS* $\neq$ *LHS*, hence lattice is not a distributive lattice.

Complemented lattice:

A complemented lattice is a bounded lattice (with least element 0 and greatest element 1), in which every element a has a complement, i.e. an element b satisfying a ∨ b = 1 and a ∧ b = 0. Complements need not be unique.

Example: Lattices shown in Fig (a), (b) and (c) are complemented lattices.



(a) (b) (c)

Sol.

For the lattice (*a*) GLB(*a*, *b*) = 0 and LUB(*x*, *y*) = 1. So, the complement *a* is *b* and vise versa. Hence, a complement lattice.

For the lattice (*b*) GLB(*a*, *b*) = 0 and GLB(*c*, *b*) = 0 and LUB(*a*, *b*) = 1 and LUB(*c*, *b*) = 1; so both *a* and *c* are complement of *b*.
Hence, a complement lattice.

In the lattice (*c*) GLB(*a*, *c*) = 0 and LUB(*a*, *c*) = 1; GLB(*a*, *b*) = 0 and LUB(*a*, *b*) = 1. So, complement of *a* are *b* and *c*.
Similarly complement of *c* are *a* and *b* also *a* and *c* are complement of *b*.
Hence lattice is a complement lattice.

Previous Questions

1. a) Let R be the Relation R= {(x,y)/ x divides y)} . Draw the Hasse diagram?
   b) Explain in brief about lattice?
   c) Define Relation? List out the Operations on Relations
2. Define Relation? List out the Properties of Binary operations?
3. Let the Relation R be R={(1,2) ,(2,3),(3,3)} on the set A= {1,2,3}. What is the Transitive Closure of R?
4. Explain in brief about Inversive and Recursive functions with examples?
5. Prove that (S, ≤) is a Lattice, where S= {1,2,5,10} and ≤ is for divisibility. Prove that it is also a Distributive Lattice?
6. Prove that (S,≤) is a Lattice, where S= {1,2,3,6} and ≤ is for divisibility. Prove that it is also a Distributive Lattice?
7. Let A be a given finite set and P(A) its power set. Let ⊆ be the inclusion relation on the elements of P(A). Draw Hasse diagrams of (P(A), ⊆) for A={a}; A={a,b}; A={a,b,c} and A={a,b.c.d}.
8. Let Fx be the set of all one-to-one onto mappings from X onto X, where X={1,2,3}. Find all the elements of Fx and find the inverse of each element.
9. Show that the function f(x) = x+y is primitive recursive.
10. Let X={2,3,6,12,24,36) and a relation ≤' be such that x≤ _if x divides y. Draw the Hasse diagram of (x,≤).
11. If A={1,2,3,4} and P={{1,2},{3},{4}} is a partition of A, find the equivalence relation

determined by P.

12. Let X={1,2,3} and f, g, h and s be functions from X to X given by f={<1,2>, <2,3>, <3,1>} g={<1,2>, <2,1>, <3,3>} h={<1,1>, <2,2>, <3,1>} and s={<1,1>, <2,2>, <3,3>}. Find fog, fohog, gos, fos.
13. 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.
14. Let X = {a,b,c,d,e} and let C = {{a,b},{c},{d,e}}. Show that the partition C defines an equivalence relation on X.
15. Show that the function f(x)= $\begin{cases} x/2; & when\ x is even \\ (x-1)/2; & when\ x is\ odd \end{cases}$ is primitive recursive.
16. If A={1,2,3,4} and R,S are relations on A defined by R={(1,2),(1,3),(2,4),(4,4)} S={(1,1),(1,2),(1,3),(1,4),(2,3),(2,4)} find R o S, S o R, R^2, S^2, write down there matrices.
17. Determine the number of positive integers n where 1≤n≤2000 and n is not divisible by2,3 or 5 but is divisible by 7.
18. Determine the number of positive integers n where 1≤n≤100 and n is not divisible by2,3 or 5.
19. Which elements of the poset /({2,4,5,10,12,20,25},/) are maximal and which are minimal?
20. Let X={(1,2,3} and f,g,h and s be functions from X to X given by f={(1,2),(2,3),(3,1)}, g={(1,2),(2,1),(3,3)}, h={(1,1),(2,2),(3,1) and s={(1,1),(2,2),(3,3)}.

<u>Multiple choice questions</u>

1. A _______ is an ordered collection of objects.
   a) Relation b) Function c) Set d) Proposition
   Answer: c
2. The set O of odd positive integers less than 10 can be expressed by ___________ .
   a) {1, 2, 3} b) {1, 3, 5, 7, 9} c) {1, 2, 5, 9} d) {1, 5, 7, 9, 11}
   Answer: b
3. Power set of empty set has exactly _____ subset.
   a) One b) Two c) Zero d) Three
   Answer: a
4. What is the Cartesian product of A = {1, 2} and B = {a, b}?
   a) {(1, a), (1, b), (2, a), (b, b)} b) {(1, 1), (2, 2), (a, a), (b, b)}
   c) {(1, a), (2, a), (1, b), (2, b)} d) {(1, 1), (a, a), (2, a), (1, b)}
   Answer: c
5. The Cartesian Product B x A is equal to the Cartesian product A x B. Is it True or False?
   a) True b) False
   Answer: b
6. What is the cardinality of the set of odd positive integers less than 10?
   a) 10 b) 5 c) 3 d) 20
   Answer: b
7. Which of the following two sets are equal?
   a) A = {1, 2} and B = {1} b) A = {1, 2} and B = {1, 2, 3}
   c) A = {1, 2, 3} and B = {2, 1, 3} d) A = {1, 2, 4} and B = {1, 2, 3}
   Answer: c
8. The set of positive integers is _________.
   a) Infinite b) Finite c) Subset d) Empty
   Answer: a

9. What is the Cardinality of the Power set of the set {0, 1, 2}.

a) 8 b) 6 c) 7 d) 9

Answer: a

10. The members of the set S = {x | x is the square of an integer and x < 100} is-----

a) {0, 2, 4, 5, 9, 58, 49, 56, 99, 12} b) {0, 1, 4, 9, 16, 25, 36, 49, 64, 81}

c) {1, 4, 9, 16, 25, 36, 64, 81, 85, 99} d) {0, 1, 4, 9, 16, 25, 36, 49, 64, 121}

Answer: b

11. Let R be the relation on the set of people consisting of (a,b) where aa is the parent of b. Let S be the relation on the set of people consisting of (a,b) where a and b are siblings. What are S∘R and R∘S?

A) (a,b) where a is a parent of b and b has a sibling; (a,b) where a is the aunt or uncle of b.
B) (a,b) where a is the parent of b and a has a sibling; (a,b) where a is the aunt or uncle of b.
C) (a,b) where a is the sibling of b's parents; (a,b) where aa is b's niece or nephew.
D) (a,b) where a is the parent of b; (a,b) where a is the aunt or uncle of b.

12. On the set of all integers, let (x,y)∈R(x,y)∈R *iff* xy≥1xy≥1. Is relation R reflexive, symmetric, antisymmetric, transitive?

A) Yes, No, No, Yes B) No, Yes, No, Yes

C) No, No, No, Yes D) No, Yes, Yes, Yes E) No, No, Yes, No

13. Let R be a non-empty relation on a collection of sets defined by ARB if and only if A∩ B = ØThen (pick the TRUE statement)

A.R is relexive and transitive B.R is symmetric and not transitive

C.R is an equivalence relation D.R is not relexive and not symmetric

Option: B

14. Consider the divides relation, m | n, on the set A = {2, 3, 4, 5, 6, 7, 8, 9, 10}. The cardinality of the covering relation for this partial order relation (i.e., the number of edges in the Hasse diagram) is

(a) 4 (b) 6 (c) 5 (d) 8 (e) 7

Ans:e

15. Consider the divides relation, m | n, on the set A = {2, 3, 4, 5, 6, 7, 8, 9, 10}. Which of the following permutations of A is not a topological sort of this partial order relation?

(a) 7,2,3,6,9,5,4,10,8 (b) 2,3,7,6,9,5,4,10,8

(c) 2,6,3,9,5,7,4,10,8 (d) 3,7,2,9,5,4,10,8,6

(e) 3,2,6,9,5,7,4,10,8

Ans:c

16. Let A = {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} and consider the divides relation on A. Let C denote the length of the maximal chain, M the number of maximal elements, and m the number of minimal elements. Which is true?

(a) C = 3, M = 8, m = 6 *(b) C = 4, M = 8, m = 6*

(c) C = 3, M = 6, m = 6 *(d) C = 4, M = 6, m = 4*

(e) C = 3, M = 6, m = 4

Ans:a

17. What is the smallest N > 0 such that any set of N nonnegative integers must have two distinct integers whose sum or difference is divisible by 1000?

(a) 502 (b) 520 (c) 5002 (d) 5020 (e) 52002

Ans:a

18. Let R and S be binary relations on a set A. Suppose that R is reflexive, symmetric, and transitive and that S is symmetric, and transitive but is not reflexive. Which statement is always true for any such R and S?

(a) R ∪ S is symmetric but not reflexive and not transitive.
(b) R ∪ S is symmetric but not reflexive.
(c) R ∪ S is transitive and symmetric but not reflexive

(d) R ∪ S is reflexive and symmetric. (e) R ∪ S is symmetric but not transitive.
Ans:d

19. Let R be a relation on a set A. Is the transitive closure of R always equal to the transitive closure of R^2? Prove or disprove.
    Solution: Suppose A = {1, 2, 3} and R = {(1, 2),(2, 3)}. Then R2 = {(1, 3)}.
    Transitive closure of R is R∗ = {(1, 2),(2, 3),(1, 3)}.
    Transitive closure of R^2 is {(1, 3)}.
    They are not always equal.
20. Suppose R1 and R2 are transitive relations on a set A. Is the relation R1 ∪ R2 necessariy a transitive relation? Justify your answer.
    Solution: No. {(1, 2)} and {(2, 3)} are each transitive relations, but their union {(1, 2),(2, 3)} is not transitive.
21. Let D_{30} = {1, 2, 3, 4, 5, 6, 10, 15, 30} and relation I be partial ordering on D_{30}. The all lower bounds of 10 and 15 respectively are
    A.1,3 B.1,5 C.1,3,5 D.None of these Option: B
22. Hasse diagrams are drawn for
    A.partially ordered sets B.lattices C.boolean Algebra D.none of these
    Option: D
23. A self-complemented, distributive lattice is called
    A.Boolean algebra B.Modular lattice C.Complete lattice D.Self dual lattice
    Option: A
24. Let D30 = {1, 2, 3, 5, 6, 10, 15, 30} and relation I be a partial ordering on D30. The lub of 10 and 15 respectively is
    A.30 B.15 C.10 D.6 Option: A
25: Let X = {2, 3, 6, 12, 24}, and ≤ be the partial order defined by X ≤ Y if X divides Y. Number of edges in the Hasse diagram of (X, ≤) is
    A.3 B.4 C.5 D.None of these
    Option: B
26. Principle of duality is defined as
    A.≤ is replaced by ≥ B.LUB becomes GLB
    C.all properties are unaltered when ≤ is replaced by ≥
    D.all properties are unaltered when ≤ is replaced by ≥ other than 0 and 1 element.
    Option: D
27. Different partially ordered sets may be represented by the same Hasse diagram if they are
    A.same B.lattices with same order C.isomorphic D.order-isomorphic
    Option: D
28. The absorption law is defined as
    A.a * (a * b) = b B.a * (a ⊕ b) = b C.a * (a * b) = a ⊕ bD.a * (a ⊕ b) = a
    Option: D
29. A partial order is deined on the set S = {x, a_1, a_2, a_3,...... a_n, y} as x ≤ a i for all i and a_i ≤ y for all i, where n ≥ 1. Number of total orders on the set S which contain partial order ≤ is
    A.1 B.n C.n + 2 D.n ! Option: D
30. Let L be a set with a relation R which is transitive, antisymmetric and reflexive and for any two elements a, b ∈ L. Let least upper bound lub (a, b) and the greatest lower bound glb (a, b) exist. Which of the following is/are TRUE ?
    A.L is a Poset B.L is a boolean algebra C.L is a lattice D.none of these
    Option: C