Discrete Mathematics

B.E. Semester-III
C.E and I.T Branches

MANOJ R. PATEL
Assistant Professor in Mathematics
Science and Humanites Department
LDRP Institute of Technology and Research
Gandhinagar

VIJAY K. PATEL
Assistant Professor in Mathematics
Science and Humanites Department
LDRP Institute of Technology and Research
Gandhinagar

LDRP Institute of Technology and Research
Sector-15, Near KH-5 Circle, Gandhinagar -382015

Constituent College of

Kadi Sarva Vishwavidyalaya

Gandhinagar

Contents

Chapter 1

Preliminaries Of Set Theory

1.1 Introduction

It will not be execrating if one says that the invention of computers revolutionised the human life. The new concept of industries and management imerged. From space flight to daily human activities are now governed by computers. A new branch of knowledge computer science covering all aspects related to computers came into existence in a natural way. To obtain maximum benefits from computers, one must be familiar with basics course here. In fact new branches known as Discrete Mathematics, Graph Theory,.... came into existence.

1.2 Basic Definitions

1.2.1 Set

A set is a collection of objects called elements that are distinct. Sets are denoted by capital letters $A, B, C, \cdots$ and it's elements are denoted by lower case letters $a, b, c, \cdots$

- $\Longrightarrow$ If $'a'$ is an element of set A then we write $a \in A$ and read as a belongs to A.
- $\Longrightarrow$ If $'a'$ is not an element of set A then we write $a \notin A$ and read as a belongs to A.

There are following three ways of defining a set.

(I) Listing Or Rouster Method :

A set can be describe by listing all it's elements within braces and separating by commas.
For examples

1. $\{1, 2, 3, 4, 5\}$ the set of first five natural numbers.
2. $\{1, i, -1, -i\}$ the set of fourth roots of unity.
3. $\{a, e, i, o, u\}$ the set of English vowel.

Some time it is not possible to list all the members then the set is described by listing it's few elements at the beginning followed by dots

For examples

1. $\{1, 2, 3, \cdots\}$ the set of natural numbers.
2. $\{0, \pm 1, \pm 2, \pm 3, \cdots\}$ the set of integers numbers.

(II) Set Builder Method :

In this method the set is define by specifying the property possessed by each elements. It's general form is $\{x : \mathbb{P}(x)\}$ which is read as "set of elements x such that it has property $P(x)$ " the symbol " : " & "/" stand for such that .
For examples

1. The set of English vowel, $\{ x : x$ is a vowel of English alphabet.$\}$
2. The set of fourth root of unity $\{ x \mid x^4 = 1\}$
3. The set of squares of natural numbers $\{ x \mid x = n^2 \text{where}' n' \text{is a natural numbers } \}$

(III) Recurrence Relation Method :

A set can be define by a recursive formula. One or more elements are given along with a rule by which the rest of the elements of the set can be generated.
For examples

1. If A is the set of first 10 natural numbers then it can be described as
   $A = \{ n_{i+1} = n_i + 1, i = 1, 2, 3, \cdots, 9$ where $n_1 = 1\}$

1.2.2 Types Of Sets

(I) Finite And Infinite Set :

A set containing finite numbers of elements is called a finite set and a set that contains infinitely many elements is called an infinite set.
For examples

1. The set of days in a week is finite set
2. The set of Natural, Integers, Rational, Real numbers are infinite sets.

(II) Null Set Or Empty Set :

A set that contains no elements is call a null set or an empty set. It is denoted by ϕ
For examples

1. $\phi = \{ x \mid x \neq x\}$
2. $\phi = \{ x \mid x \in \mathbb{N}\text{and } x + 1 = 0\}$
3. $\phi = \{ x \mid x\mathbb{N} \;\&x^2 + 1 = 0\}$
4. The set of prime numbers between 31 and 37

(III) Singleton Set :

A set that contains only one elements is called singleton set.
For examples

1. $A = \{ 0\}$
2. $B = \{ x \mid x \in \ \mathbb{N}\text{and } 10 < x < 12\}$
3. $C = \{ x \mid 2x = 10\text{where } x\text{positive integer}\}$

(IV) Universal Set :

It is a special set in which ever set A under discussion is a subset of U,where U is universal set.Thus $A \subseteq U$ for every set A.

(V) Equality of sets :

Two sets A and B are said to be equal if they have same elements and written as $A = B$. Mathematically: $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$,that is $x \in A \Leftrightarrow x \in B$

(VI) Subset :

Let A and B be any two nonempty sets the set $A$is called a subset of B if every elements of A is an element of B and denoted by $A \subset B$. Mathematically: $A \subseteq B$ if $x \in A \Rightarrow x \in B$

(VII) Proper Subset :

The set A is called a proper subset of B if every element of A is an element of B and there is at least one element in B that is not in A
For examples

1. $A = \{ 1, 2, 3\}$ and $B = \{1, 2, 3, 4, 5\}$ then $A \subset B$
2. The set of natural numbers $\mathbb{N}$ is a proper sub set of integers. $\Longrightarrow \mathbb{N} \subset \mathbb{Z}$

(VII) Power Set :

If A is any set then the set of all it's subset is called the power set of A and denoted by $\mathcal{P}(A)$.
For examples

1. $A = \{ 1, 2, 3\}$ then $\mathcal{P}(A) = \{ \phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3, 4, 5\}\}$

(VIII) Cardinality Of a Set :

The number of distinct elements contained in finite set A is called the cardinality or the cardinal number of the set. The cardinality of set is denoted by $n(A)$, $card(A)$, $|A|$

1.3 Set Operation

1. Union of two sets $\Longrightarrow A \cup B = \{ x \mid x \in A \text{ or } x \in B\}$
2. Intersection of two sets $\Longrightarrow A \cap B = \{ x \mid x \in A \text{ and } x \in B\}$
3. Difference of two sets $\Longrightarrow A - B = \{ x \mid x \in A \text{ and } x \notin B\}$
4. Complement of sets $\Longrightarrow A' = \{ x \mid x \in U \text{ or } x \in A\}$

Law Of Sets

(I) Idempotent Laws
$A \cup A = A$ & $A \cap A = A$

(II) Commutative Laws
$A \cup B = B \cup A$ & $A \cap B = B \cap A$

(III) Associative Laws
$(I) A \cup (B \cup C) = (A \cup B) \cup C$
$(II) A \cap (B \cap C) = (A \cap B) \cap C$

(IV) Distributive Laws
$(I) A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$(II) A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(V) DeMorgen's Laws
$(A \cup B)' = A' \cap B'$ & $(A \cap B)' = A' \cup B'$

1.4 The Inclusion And Exclusion Principal

Where two or more task are performed simultaneously, then the usual sum and product rules cannot be used. In the case of two tasks, if we add the number of ways in which each task is performed, then the number of ways to perform both the tasks is counted twice. In order to correct this double counting and find the number of ways of doing either of the tasks, the number of ways of performing each task is added that is Inclusion and the number of ways of performing both the tasks is subtracted from this sum that is Exclusion. This method of counting is called the principal of Inclusion and Exclusion. Let A and B be two finite sets consisting of p and q elements. An element from the set A can be selected in p ways similarly an element from the set B can be selected in q ways. The number of ways to selected an element from A or B is $(p+q)$ minus the number of ways to select an element that is in both A and B, say r. Thus the number of ways in which an element is selected from A or B is $p+q-r$

$$n(A \cup B) = p + q - r = n(A) + n(B) - n(A \cap B)$$

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

Remark. If $n(A \cap B) = \phi$ then we have the sum rules *i.e* $(A \cup B) = n(A) + n(B)$

1.4.1 Example. Find the number of positive integers $\leq$ 200 and divisible by 2 or 5.
Solution:
Here we want to find number of positive integer ≤ 200, which is divisible by 2 or 5, for that let $A = \{x \ / \ x \in \mathbb{N} \ \& \ x \leq 200$ &divisible by 2$\}$, $B = \{x \ / \ x \in \mathbb{N} \ \& \ x \leq 200$ &divisible by 5$\}$ and $A \cap B = \{x \ / \ x \in \mathbb{N} \ \& \ x \leq 200$ &divisible by 2 and 5$\}$

$$\therefore A = \{2, 4, 6, 8, \cdots, 200\} \Rightarrow n(A) = 100$$
$$\therefore B = \{5, 10, 15, \cdots, 200\} \Rightarrow n(B) = 40$$
$$\therefore A \cap B = \{10, 20, 30, \cdots, 200\} \Rightarrow n(A \cap B) = 20$$

Hence by Inclusion and Exclusion Principal

$$\begin{aligned} n(A \cup B) &= n(A) + n(B) - n(A \cap B) \\ &= 100 + 40 - 20 \\ n(A \cup B) &= 120. \end{aligned}$$

1.4.2 Example. Let S be the set of all integers from 100 to 999 which are neither divisible by 3 nor divisible by 5 then find number of elements in S.
Solution:
Here given set S contain the integer from 100 to 999 then $n(S) = 900$
Now first we want to find number of element of S which is divisible by 3 or 5, for that let $A = \{x \ / \ 100 \leq x \leq 999$ &divisible by 3$\}$, $B = \{x \ / \ 100 \leq x \leq 999$ &divisible by 5$\}$ and $A \cap B = \{x \ / \ 100 \leq x \leq 999$ &divisible by 3 and 5$\}$

$$\therefore n(A) = \frac{900}{3} = 300, \ n(B) = \frac{900}{5} = 180 \text{ and } n(A \cap B) = n(B) = \frac{900}{15} = 60$$

Hence by Inclusion and Exclusion Principal

$$\begin{aligned} n(A \cup B) &= n(A) + n(B) - n(A \cap B) \\ &= 300 + 180 - 60 \\ n(A \cup B) &= 420. \end{aligned}$$

Now the number of element in S neither divisible by 3 nor 5 is = 900-420= 480

1.5 Cartesian Product Set

In Cartesian product two sets can be combined to obtain another set. The cartesian product of sets A and B is the set denoted by $A \times B$ and defined by

$$A \times B = \{(a, b)/a \in A \ \& \ b \in B\}$$

More generally

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, a_3, \cdots, a_n)/a_i \in A_i \text{ and } i = 1, 2, 3, \cdots, n\}$$

1.6 Relation

1.6.1 Basic Definition

1.6.2 Relation

For given non empty set A and B a sub set R of $A \times B$ is called relation from A to B. If only two sets are involved then R is known as Binary Relation from A to B

- $\Longrightarrow$ If $(x, y) \in R$ then we say that element x of A is related to element y of B by relation R and it is denoted by xRy
- $\Longrightarrow$ If $(a, b) \notin R$ then we say that element a of A is not related to element b of B by relation R and it is denoted by $a \not R b$

1.6.3 Domain And Range Of Relation

For a relation R from A to B the set $D(R) = \{ x \in A | (x, y) \in R\}$ is called the domain of relation R. It is also denoted by $dom(R)$ while the set $R(R) = \{ y \in B/(x, y) \in R\}$ is called the range of relation R. It is also denoted by $range(D)$.

1.6.1 Example. Let $A = \{3, 5, 7\}$ and $B = \{3, 6, 10, 14, 15\}$. Define relation R from A to B by $R = \{(a, b) | a \text{ divides } b\}$.

Solution: Here given sets are $A = \{3, 5, 7\}$ and $B = \{3, 6, 10, 14, 15\}$, we want to find relation $R = \{(a, b)|a \text{ divides } b\}$, for that

$$R = \{(3, 3), (3, 6), (3, 15), (5, 10), (5, 15), (7, 14)\}$$

■

1.6.2 Example. Let $A = \{1, 2, 3, 4\}$ and $B = \{1, 2, 3, 4\}$ then find $A \times B$ and few relation from A to B.

Solution: Here given sets are $A = \{1, 2, 3, 4\}$ and $B = \{1, 2, 3, 4\}$ and we want to find $A \times B$ and few relation, for that

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

Now we find the few relation as follow

1. The set $R_1 = \{(x, y)|x = y\}$ is relation.

$$R_1 = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$$

2. The set $R_2 = \{(x, y)|x > y\}$ is relation.

$$R_2 = \{(2, 1), (3, 1), (4, 1), (3, 2), (4, 2), (4, 3)\}$$

3. The set $R_3 = \{(x, y)|x < y\}$ is relation.

$$R_3 = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$$

■

1.7 Properties of a Relation

(I) Reflexive Relation

Suppose A be a non empty set and R is a relation on set A. If for, $\forall a \in A$, aRa then R is said to be reflexive relation.
e.g.

1. Let $\mathbb{R}$ be the set of real numbers. Define a relation " $\leq$ " (R) on $\mathbb{R}$.
   $R = \left\{(a, b)/a \leq b, \ i.e\ b - a \text{ is non negative }, \ \forall a, b \in \mathbb{R}\right\}$
   So " $\leq$ " is reflexive relation on A.
2. $A = \{1, 2, 3\}$ and $R = \{(1, 1), (2, 2), (3, 3), (1, 3)\}$. So R is reflexive relation on A

(II) Symmetric Relation

Suppose A is non empty set and R is relation of set A. If $xRy \implies yRx$ then relation R is said to be a symmetric relation.
e.g

1. $\forall\ a, b \in \mathbb{R},\ a = b \implies b = a$. So " = " is a symmetric relation on $\mathbb{R}$.
2. $2 \leq 3$ but $3 \not\leq 2 \implies$ " $\leq$ " is not a symmetric relation on R.

(III) Asymmetric

A relation R is said to be an asymmetric relation if $aRb \implies b \not R a$
e.g $2 < 3$ and $3 \not< 2$ is asymmetric relation and similarly " $>$ " is also asymmetric.

(IV) Antisymmetric Relation

A relation R is said to be an anti-symmetric relation on set A if $a, b \in A$ with aRb and $bRa \implies a = b$.

Or

A relation R is said to be an anti-symmetric relation on set A. If $a \neq b$ with aRb then $b \not R a$.
e.g

(i) " $\leq$ " is anti-symmetric on $\mathbb{R}$. If $a \leq b$ and $b \leq a$ then $a = b$

(ii) " $\geq$ ", " = ", " $\subset$ " are also anti-symmetric.

(iii) let $A = \{5, 6\}$ and $R = \{(5,5), (5,6), (6,5), (6,6)\}$ is relation on set A. Here R is not anti-symmetric relation on set A because $(5,6)$ & $(6,5)\ \in R$ but $5 \neq 6$.

(V) Irreflexive

A relation R on a set A is said to be an irreflexive relation if $a \not R a$ for any $a \in A$.
e.g

(i) $\forall a \in \mathbb{R},\ a \not< a$ so " $<$ " is irreflexive on $\mathbb{R}$ but " $\leq$ " is not irreflexive.

(VI) Transitive Relation

Suppose A is non-empty set and R is relation on set A and if $\forall\ a, b, c \in A$ with $aRb,\ bRc \implies aRc$ then R is said to be transitive relation on set A.

e.g (1) let $\leq$ is relation on $\mathbb{R}$ with $a \leq b,$ and bRc

$$\begin{aligned} a \leq b,\ \&\ b \leq c &\implies aRb,\ \&\ bRc \\ &\implies (b-a) \text{ and} (c-b) \text{ are non negative} \\ &\implies (b-a) + (c-b) \text{ are non negative} \\ &\implies (c-a) \text{ is non negative} \\ &\implies a \leq c. \end{aligned}$$

$\implies$ " $\leq$ " is Transitive relation on $\mathbb{R}$

(2) " $\subset$ " is Transitive relation on $\mathbb{R}$

(VII) Equivalence Relation

Suppose A is non-empty set and R be the relation on set A. If relation R is reflexive, symmetric and transitive then this relation R is called Equivalence Relation on set A.
$\implies$ Equivalence Relation is denoted by symbol " $\sim$ ".

1.7.1 Example. A relation is define on set $\mathbb{Z}$ is $R = \Big\{(x, y) / \ x - y \ \text{ divided by } \ 5\Big\}$ then check that R is equivalence relation.

Solution:
Here given set A is integer set $\mathbb{Z}$ and relation $R = \Big\{(x,y)/\ x-y \ \text{ divided by } \ 5\Big\}$. Now we want to check that R is equivalence relation for that we check reflexive, symmetric and transitive as follow.

(I) Reflexive

$\forall x \in A = \mathbb{Z}$ then we have xRx, because $(x-x) = 0$ is divided by 5.

(II) Symmetric

For, $\forall x, y \in A = \mathbb{Z}$

$$\begin{aligned} \text{Suppose } xRy &\implies (x-y) \text{ is divided by } 5 \\ &\implies -(y-x) \text{ is divided by } 5 \\ &\implies (y-x) \text{ is divided by } 5 \\ &\implies yRx \end{aligned}$$

$\therefore R$ is symmetric

(III) Transitive

For, $x, y, z \in A = \mathbb{Z}$

$$\begin{aligned} \text{Suppose } xRy,\ \&\ yRz &\implies xRy,\ \&\ yRz \\ &\implies (x-y) \text{ is divided by } 5 \text{ and} (y-z) \text{ is divided by } 5 \\ &\implies (x-y)+(y-z) \text{ is divided by } 5 \\ &\implies (x-z) \text{ is divided by } 5 \\ &\implies xRz. \end{aligned}$$

$\therefore$ "R" is Transitive relation on $\mathbb{Z}$

$\therefore$ R is equivalence relation on the set $A = \mathbb{Z}$.

1.8 Partially Ordered Relation

A relation R on a non empty set X. If relation R has following three properties then relation R is called Partial order relation.

(i) Relation R is reflexive. *i.e* xRx, for every $x \in X$

(ii) Relation R is antisymmetric. *i.e* whenever xRy and yRx then $x = y$

(iii) Relation R is transitive. if xRy and yRz then xRz

$\implies$ Partially Ordered Relation is denoted by " $\leq$ "

1.9 Composition Relation

Let R be a relation from a set A into a set B and let S be a relation from set B into a set C The composition of R and S, denoted by $S \circ R$, is the relation from A into C, define by, for all $a \in A,\ c \in C,\ a(S \circ R)c$ if there exist some $b \in B$ such that aRb and bSc.

1.10 Pictorial Representation of Relation

The pictorial representation of relation is called graph of the relation. A relation can also be represented in tabular form by a matrix or by an arrow diagram.

1.11 Matrix Representation of Relation

Let $A = \{x_1, x_2, x_3, \cdots, x_n\}$ and $y_1, y_2, y_3, \cdots, y_n$ are ordered set and R be the relation from A to B can be expressed by $n \times m$ matrix $[R_{ij}]_{n\times m}$ by $R_{ij} = \begin{cases} 1 & \text{if } x_i R y_j \\ 0 & \text{if } x_i \not R y_j \end{cases}$ is called the matrix representation of relation R. It is denoted by M_R.

1.11.1 Example. Let $A = \{1, 2, 3, 4\}$ be the finite set and $R = \{(1,1), (1,2), (1,3), (1,4), (2,4), (3,2), (4,$ be the relation on A, then find matrix relation M_R.

Solution: Here given set $A = \{1, 2, 3, 4\}$ and relation $R = \{(1,1), (1,2), (1,3), (1,4), (2,4), (3,2), (4,3)\}$, for matrix relation we write matrix as follow

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

■

Theorem 1.11.2. *Let A, B and C be finite sets. Let R be a relation from A into B and S be a relation from B into C. Then*

$$M_{S\circ R} = M_R \odot M_S$$

i.e., the matrix $M_{S\circ R}$ of the relation $S \circ R$ is same as the matrix of the Boolean product of M_R and M_S.

Remark: Before defining Boolean product we note following operation $* \,\&\, +$

(i) $a+b = \begin{cases} 1 & \text{if } a=1, \text{ or } b=1, \text{ or } (a=1 \text{ and } b=1) \\ 0 & \text{otherwise} \end{cases}$

(ii) $a*b = \begin{cases} 1 & \text{if } a=1 \text{ and } b=1 \\ 0 & \text{otherwise} \end{cases}$

1.11.3 Example. Let $M_R = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ and $M_S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \end{bmatrix}$ be the two matrix relation on relation sets R and S respectively then find $M_{S\circ R}$.

Solution: Here given matrix relation are $M_R = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ and $M_S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \end{bmatrix}$ and we want to find $M_{S\circ R}$, for that, by above theorem we write

$$\begin{aligned} M_{S\circ R} &= M_R \odot M_S \\ &= \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \odot \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} (1*1)+(1*0)+(0*0)+(1*1) & (1*0)+(1*1)+(0*0)+(1*1) \\ (0*1)+(0*0)+(1*0)+(1*1) & (0*0)+(0*1)+(1*0)+(1*1) \\ (0*1)+(0*0)+(1*0)+(0*1) & (0*0)+(0*1)+(1*0)+(0*1) \end{bmatrix} \\ &= \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 0 \end{bmatrix} \end{aligned}$$

■

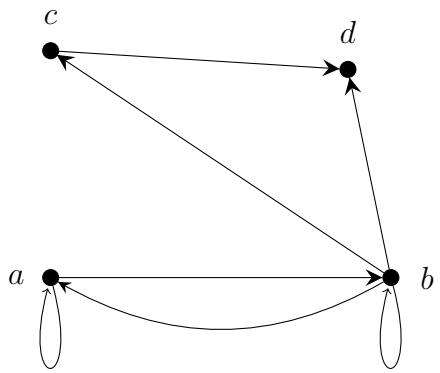
Theorem 1.11.4. *Let A be a finite set and R be a relation on A. Let M_{R^n} be the matrix of the relation R^n. Then for all $n \geq 1$*

$$M_{R^n} = \underbrace{M_R \odot M_R \odot \cdots M_R}_{n \text{ times}}$$

1.12 Directed Graph of Relation

Let R be a relation on a finite set A. We can describe R pictorially as follows: For each element of A, we draw a small or big dot and label the dot by the corresponding element of A.

We next draw an arrow from a dot labeled, say a, to another dot labeled, say b, if aRb. The resulting pictorial representation of relation R is called the directed graph representation of the relation R. In the directed graph representation of R, each dot is called vertex and an arrow form labeled vertex to vertex is called directed edge. This representation also known as directed graph, or digraph.
i.e. Let $A = \{a, b, c, d\}$. Let R be the relation defined by $R = \{(a, a), (a, b), (b, b), (b, c), (b, a), (b, d), (c, d)\}$ Let us construct a digraph of the relation as follow



1.12.1 In-degree and Out-degree of Vertices

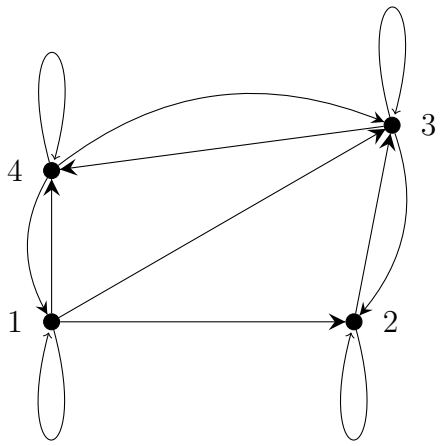
Let R be a relation on a set A whose elements are called vertices. If $a \in A$, then the number of edges terminating at a is called the in-degree of the vertex a. The out degree of vertex a is the number of edges leaving the vertex a.

1.12.1 Example. Let $A = \{1, 2, 3, 4\}$ be a given set and the relation R on A be given by, $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 3), (3, 3), (2, 2), (3, 2), (3, 4), (4, 4), (4, 1), (4, 3)\}$ find the matrix for relation R, draw its diagraph and also find in-degree and out-degree.

Solution: Here given relation is $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 3), (3, 3), (2, 2), (3, 2), (3, 4), (4, 4), (4, 1)$ we want to find matrix representation of relation and diagraph, for that

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

and the corresponding diagraph is as follows:



Now, In-degree and out-degree as follow:

Vertices	1	2	3	4
In-degree	2	3	4	3
Out-degree	4	2	3	3

■

1.13 Function

Let A and B be sets and $f : A \longrightarrow B$ be a function. The set A is referred to as the domain of the function and the set B is called the codomain of f. The set

$$f(A) = \{f(x) \mid x \in A\}$$

is a subset of the codomain B. The set $f(A)$ is called the range of the function f, or the image of the set A under the function f, denoted by $Im(f)$ or $I(f)$.

1.13.1 Bijective Function

Let A and B be sets and $f : A \longrightarrow B$. Then

(i) f is called one-one (or injective or injection) if for all $x,\ y \in A$, $x \neq y \Longrightarrow f(x) \neq f(y)$.
i.e., images of distinct elements of the domain are distinct.

(ii) f is called onto B (or surjective or surjection) if for every $y \in B$ there exists at least one $x \in A$ such that $f(a) = b$
i.e., $Im(f) = B$

(iii) f is called one to one correspondence (or bijective or bijection) if f is both one-one and onto.

1.13.1 Example. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be define by $f(x) = 9x + 5$. Then check that f is one-one and onto.

Solution: Here given function is $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be define by $f(x) = 9x + 5$ and we want to check that given function is one-one and onto, for that, let $x_1,\ x_2 \in \mathbb{Z}$. Now

$$\begin{aligned} f(x_1) &= f(x_2) \\ 9x_1 + 5 &= 9x_2 + 5 \\ 9x_1 &= 9x_2 \\ x_1 &= x_2 \end{aligned}$$

Hence f is one-one function. However, f is not onto $\mathbb{Z}$. Indeed, here, $4 \in \mathbb{Z}$ has no preimage under f. For

$$\begin{aligned} &\text{if } f(x) = 4 \text{ for some } x \in \mathbb{Z} \\ &9x + 5 = 4 \\ &9x = -1 \\ &x = -\frac{1}{9} \notin \mathbb{Z}. \end{aligned}$$

Hence f is not onto $\mathbb{Z}$. Observe that if we consider $f : \mathbb{R} \longrightarrow \mathbb{R}$ by defining $f(x) = 9x + 5$, for all $x \in \mathbb{R}$ then f becomes example of a function which is both one-one and onto $\mathbb{R}$ and hence bijective function. ■

1.13.2 Example. Prove that $f : \mathbb{R} \longrightarrow \mathbb{R}$ define by $f(x) = ax + b,\quad a \neq 0$ is bijective function.

Solution: Here we want to prove that $f : \mathbb{R} \longrightarrow \mathbb{R}$ define by $f(x) = ax + b,\quad a \neq 0$ is bijective function, for that we prove f is one-one and onto. Let $x_1,\ x_2 \in \mathbb{R}$. Now

$$\begin{aligned} f(x_1) &= f(x_2) \\ ax_1 + b &= ax_2 + b \\ ax_1 &= ax_2 \\ x_1 &= x_2 \end{aligned}$$

Hence f is one-one function. For onto, we prove for every $y \in \mathbb{R}$, there exist $x \in \mathbb{R}$ such that $f(x) = y$, for that

$$y = ax + b \iff x = \frac{y - b}{a}$$

Now we write

$$\begin{aligned} f(x) &= f\left(\frac{y-b}{a}\right) \\ &= a\left(\frac{y-b}{a}\right) + b \\ &= y - b + b \\ &= y \end{aligned}$$

Hence given function is one-one and onto, so f is bijective. ■

1.13.2 Composite Function

Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$ be function. The composition of f and g, written $f \circ g$, is the function from A to C define as

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

1.13.3 Example. If $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^3$ and $g : \mathbb{R} \longrightarrow \mathbb{R}$, $g(x) = x^5$ then prove $gof = fog$

Solution: Here given functions are $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^3$ and $g : \mathbb{R} \longrightarrow \mathbb{R}$, $g(x) = x^5$ and we want to prove that $gof = fog$, for that

(i) Here $gof : \mathbb{R} \longrightarrow \mathbb{R}$, $(gof)(x) = g(f(x)) = g(x^3) = (x^3)^5 = x^{15}$

(ii) Here $fog : \mathbb{R} \longrightarrow \mathbb{R}$, $(fog)(x) = f(g(x)) = f(x^5) = (x^5)^3 = x^{15}$

Hence proved the given result. ■

1.13.3 Inverse of a Function

If $f : A \longrightarrow B$ is a function and if there exist a function $g : B \longrightarrow A$ such that $gof = I_A$ and $fog = I_B$ we say $g : B \longrightarrow A$ is inverse function of $f : A \longrightarrow B$ and denote g by f^{-1}

> **Remark:** If $f : A \longrightarrow B$ is one-one and onto function then f has inverse.

1.13.4 Example. Let $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = ax + b$, $a \neq 0$ then find the inverse of f.

Solution: Here given function is $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = ax + b$, $a \neq 0$ and we want to find the inverse of f, for that first we check that given function is one-one and onto. Let $x_1,\ x_2 \in \mathbb{R}$. Now

$$\begin{aligned} f(x_1) &= f(x_2) \\ ax_1 + b &= ax_2 + b \\ ax_1 &= ax_2 \\ x_1 &= x_2 \end{aligned}$$

Hence f is one-one function. For onto, we prove for every $y \in \mathbb{R}$, there exist $x \in \mathbb{R}$ such that $f(x) = y$, for that

$$y = ax + b \iff x = \frac{y - b}{a}$$

Now we write

$$\begin{aligned} f(x) &= f\left(\frac{y-b}{a}\right) \\ &= a\left(\frac{y-b}{a}\right) + b \\ &= y - b + b \\ &= y \end{aligned}$$

Hence given function is one-one and onto, so f is bijective.

$$\therefore\ f^{-1} : \mathbb{R} \longrightarrow \mathbb{R},\ f^{-1}(x) = \frac{x-b}{a}$$

■

Chapter 2

Lattice

2.1 Partially Ordered Relation

A relation R on a non empty set X. If relation R has following three properties then relation R is called Partial order relation.

(i) Relation R is reflexive. *i.e* xRx, for every $x \in X$

(ii) Relation R is antisymmetric. *i.e* whenever xRy and yRx then $x = y$

(iii) Relation R is transitive. if xRy and yRz then xRz

$\Longrightarrow$ Partially Ordered Relation is denoted by " $\leq$ "

2.2 Partially Ordered Sets (POSET)

A relation define on non-empty set X is partially ordered relation then this set is called partially ordered set.
$\Longrightarrow$ Poset are denoted by $\langle X, \leq \rangle$

2.2.1 Example. Show that $\langle \mathbb{N}, < \rangle$ is not Poset
Solution:
$\forall a \in \mathbb{N}$, $a < a$ always not true. So reflexive property not satisfy for relation " $<$ " $\therefore$ $\langle \mathbb{N}, < \rangle$ is not Poset.

2.2.2 Example. Show that $\langle \mathbb{N}, \leq \rangle$ is Poset. where relation " $\leq$ " is smaller or equal.
Solution:
Here given that sets $\mathbb{N}$ and relation " $\leq$ ". Now foe Poset we check following properties

(i) **Reflexive:**
$\forall\ a \in \mathbb{N}$ we write $a \leq a \implies$ " $\leq$ " is reflexive.

(ii) **Anti symmetric:**
$\forall\ a, b \in \mathbb{N}$, suppose $a \leq b$ and $b \leq a$ then always possible $a = b \implies$ " $\leq$ " is antisymmetric.

(iii) **Transitive:**
$\forall\ a, b, c \in \mathbb{N}$, suppose $a \leq b$ and $b \leq c$ then we write $a \leq c \implies$ " $\leq$ " is transitive.

from (1),(2) and (3) relation " $\leq$ " is partially ordered relation. Hence we proved that $\langle \mathbb{N}, \leq \rangle$ is Poset.

2.2.3 Example. Suppose A is any non empty set and $P(A)$ is set of all subset of A then show that $\langle P(A), \leq \rangle$ is Partially ordered relation where " $\leq$ " means " $\subseteq$ "
Solution:
Here given set is all the subset of A which is $P(A)$ and relation " $\leq$ " means " $\subseteq$ "
Now foe Poset we check following properties

(i) **Reflexive:**
$\forall\ A_1 \in P(A)$ we write $A_1 \subseteq A_1 \implies$ " $\subseteq$ is reflexive.

(ii) **Anti symmetric:**
$\forall\ A_1, A_2 \in P(A)$, suppose $A_1 \subseteq A_2$ and $A_2 \subseteq A_1$ then always possible $A_1 = A_2 \implies$ " $\subseteq$ is antisymmetric.

(iii) **Transitive:**
$\forall\ A_1, A_2, A_3 \in P(A)$, If $A_1 \subseteq A_2$ and $A_2 \subseteq A_3$ then for subset of power set is possible $A_1 \subseteq A_3 \implies$ " $\subseteq$ " is transitive.

from (1),(2) and (3) relation " $\leq$ " is partially ordered relation. Hence we proved that $\langle P(A), \leq \rangle$ is Poset.

2.2.4 Example. Under the divisibility relation (aRb means, a divides b that is $a \mid b$) show that set of natural number $\mathbb{N}$ is Poset.
Solution:
Here given that sets $\mathbb{N}$ and relation "$a \mid b$"
Now foe Poset we check following properties

(i) **Reflexive:**
The relation is reflexive as every natural numbers is divisor of it self $\forall\ a \in \mathbb{N}$ we write $a \mid a \implies$ " $\leq$ " is reflexive.

(ii) **Anti symmetric:**
The relation is antisymmetric as $\forall\ a, b \in \mathbb{N}$, suppose $a \mid b$ and $b \mid a$ then always possible $a = b \implies$ " $\leq$ " is antisymmetric.

(iii) **Transitive:**
The relation is transitive as $\forall\ a, b, c \in \mathbb{N}$,

$$\begin{aligned} \text{suppose } a \mid b \text{ and } b \mid c &\implies b = k_1 a \ \&\ c = k_2 b \text{ where } k_1, k_2 \in \mathbb{Z} \\ &\implies c = k_1 k_2 a \\ &\implies c = ka \text{ take } k_1 k_2 = k \\ &\implies a \mid c \end{aligned}$$

then we get $a \leq c \implies$ " $\leq$ " is transitive.

from (1),(2) and (3) relation " $\leq$ " is partially ordered set.

Remark . The relation of divisibility over the set of integers $\mathbb{Z}$ is not a Poset because for antisymmetric we know that $-5 \mid 5$ and $5 \mid -5$ but $-5 \neq 5$.

2.3 Linearly Ordered Set or Totally Ordered Set or Chain

Let $\langle X, \leq \rangle$ be Poset. If every pair of element of X is comparable that is, if for every $a, b \in X$ there exists $a \leq b$ or $b \leq a$ then the set X is called Linearly ordered or Totally ordered set or Chain.
i.e $\implies$ The set of natural number $\mathbb{N}$, the set of integers $\mathbb{Z}$ and the set of real number $\mathbb{R}$ with relation "less or equal to"$(\leq)$ are totally ordered set.

2.3.1 Example. Let $\mathbb{N}$ be set with divisibility relation then find whether the following subset of $\mathbb{N}$ are totally ordered.

(i) {2,4,8,16} (ii) {2,4,8,10} (iii) {3,6,9,12,13} (iv) {1}

Solution:
(I) here we have each pair like $(2,4),(2,8),(2,16),(4,8),(4,16),(8,16)$ is comparable with respect to divisibility relation so given set is totally ordered.
(II) The pair $(4,10)$ and $(8,10)$ are not comparable with given relation because under given relation in the pair (4,10), 4 does not divide 10 similarly for (8,10). So this set is not totally ordered.
(III) The pair (3,13),(6,13),(9,13),(12,13) are not comparable with the given relation. So given set is not totally ordered.
(IV) The subset $\{1\}$ is totally ordered as the set containing a single element is always totally ordered.

2.3.2 Example. Prove that $\langle \{1, 2, 2^2, 2^3, \cdots\}, D \rangle$ are Poset and chain.
Solution:
Here given set $A = \{1, 2, 2^2, 2^3, \cdots\}$ and relation "D"(" $\mid$ ") is divisibility. Now first we prove that A is Poset,for that we check following properties

(i) **Reflexive:**
$\forall\, a \in A$ we write $a \mid a \implies$ "D" is reflexive.

(ii) **Anti symmetric:**
Here we have $2^r, 2^s \in A$,with $r < s$ then it is clear that $2^r D 2^s$ but $2^s \not D 2^r$ and if possible then $2^r = 2^s \implies$ "D" is antisymmetric.

(iii) **Transitive:**
Here we take $\forall\, 2^r, 2^s, 2^t \in A$,

$$\begin{aligned} \text{suppose } 2^r \mid 2^s \text{ and } 2^s \mid 2^t &\implies 2^s = k_1 2^r \;\&\; 2^t = k_2 2^s \text{ where } k_1, k_2 \in \mathbb{Z} \\ &\implies 2^t = k_1 k_2 2^r \\ &\implies 2^t = k 2^r \text{ take} k_1 k_2 = k \\ &\implies 2^r \mid 2^t \end{aligned}$$

then we get $2^r D 2^t \implies$ "D" is transitive.

from (1),(2) and (3) the set $\langle \{1, 2, 2^2, 2^3, \cdots\}, D \rangle$ is partially ordered set
For chain we proved only comparable property

(4) Comparable

Let $x, y \in A$ with $x \neq 1$ & $y \neq 1$
Now let $x = 2^r$ & $y = 2^s$ for some $r, s \in \mathbb{N}$, we have either $r \leq s$ or $r > s$ that is $2^r D 2^s$ or $2^s D 2^r$ that is xDy or yDx, so for any element $x, y \in A$ that are comparable. Hence given set is chain.

Exercise

(i) $\langle \mathbb{N}, \leq \rangle$ is chain.

(ii) $\langle \mathbb{N}, D \rangle$ is poset but not chain.

(iii) $\langle \{1, 2, 5, 6\}, D \rangle$ is not chain.

(iv) $\langle \{1, 3, 6, 9\}, D \rangle$ is not chain.

(v) $\langle \{\phi, \{a\}, \{b\}, \{a, b\}\}, \subseteq \rangle$ is not a chain.

2.4 Primal and Dual for poset

If $\langle X, R \rangle$ or $(\langle X, \leq \rangle)$ is poset then $\langle X, \widetilde{R} \rangle$ or $(\langle X, \geq \rangle)$ is also poset which called the dual of $\langle X, R \rangle$ or $(\langle X, \leq \rangle)$. The poset $\langle X, \leq \rangle$ is called the primal of $\langle X, \geq \rangle$

2.5 Cover Of An Element Of Poset

Let $\langle X, R \rangle$ be any poset and $a, b \in X$ with aRb then b covers a if there is no $c \in X$ such that aRc and cRb where $c \neq a,\ c \neq b$.
$\underset{e.g}{\Longrightarrow}$ Also we say that element b is an immediate successor of a.

(i) In poset $\langle \mathbb{N}, \leq \rangle$ if $a = 2$ and $b = 3$ then we say that b covers a but if $a = 2$ and $b = 4$ then b is not covers a.

(ii) In poset $\langle \mathbb{N}, D \rangle$ if $a = 2$ and $b = 4$ then we say that b covers a but if $a = 2$ and $b = 12$ then b is not covers a as 6,4 are in between a and b.

(iii) Let poset $\langle \{2, 4, 6, 8, 10, 12\}, D \rangle$ then find cover of each element.
$\Longrightarrow$

cover of $2 = 4, 6, 10$
cover of $4 = 8, 12$
cover of $6 = 12$
cover of $8 = -$
cover of $10 = -$
cover of $12 = -$

***Remark*.** (i) S_n = Divisor of n
S_6 = Divisor of 6 =$\{1, 2, 3, 6\}$
S_{18} = Divisor of 18 =$\{1, 2, 3, 6, 9, 18\}$

(ii) $\langle S_n, D \rangle$ is also poset.

Note:

b covers $a \iff$ (1) aRb
(2) $a \neq b$
(3) aRx & $xRb \implies a = x$ or $x = b$

2.6 Hasse Diagram

Let X be a finite set and $\langle X, \leq \rangle$ is a poset. The Hasse diagram of a poset is a diagrammatical (Geometrical) representation of a poset in plane by following properties.

(i) Every element of X marked (expressed) by small circle ($\circ$) or dot($\bullet$) in the plane.

(ii) If $a, b \in X$ and b cover a ($a \leq b$) then the dot($\bullet$) of a is placed at below the dot($\bullet$) of b and this dot joined by a line segment.

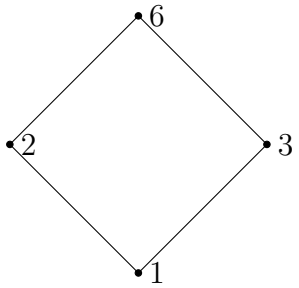
(iii) If aRb and there is no element c in X such that aRc & cRb then the position of dot($\bullet$)of a is just below the position of dot($\bullet$)of b.

(iv) If aRb but $c \in X$ such that aRc & cRb then dot of a is not joined dot of b by a single line.

The diagram obtained for all the points of X is called the Hasse Diagram of a poset $\langle X, \leq \rangle$

2.6.1 Example. Draw the Hasse diagram of the following poset.
(I) $\langle S_6, D \rangle$

Here we have $S_6 = \{1, 2, 3, 6\}$
cover of $1 = 2, 3$
cover of $2 = 6$
cover of $3 = 6$
cover of $6 = -$



(II) $\langle S_8, D \rangle$

Here we have $S_8 = \{1, 2, 4, 8\}$

cover of $1 = 2$

cover of $2 = 4$

cover of $4 = 8$

cover of $8 = -$

(III) $\langle S_{12}, D \rangle$

Here we have $S_{12} = \{1, 2, 3, 4, 6, 12\}$

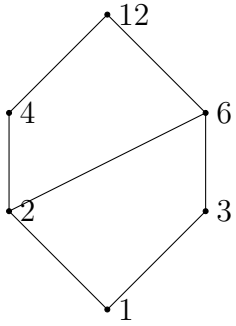
cover of $1 = 2, 3$

cover of $2 = 4, 6$

cover of $4 = 12$

cover of $6 = 12$

cover of $12 = -$



(IV) $\langle S_{36}, D \rangle$

Here we have $S_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36, \}$

cover of $1 = 2, 3$

cover of $2 = 4, 6$

cover of $3 = 6, 9$

cover of $4 = 12$

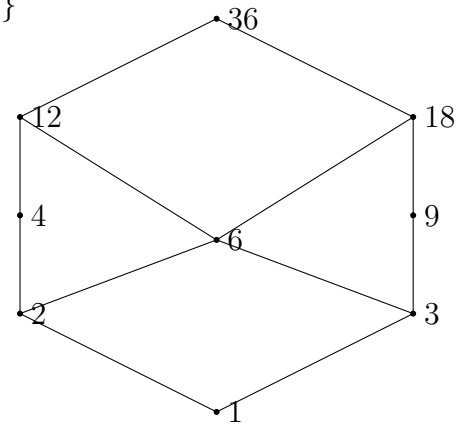
cover of $6 = 12, 18$

cover of $9 = 18$

cover of $12 = 36$

cover of $18 = 36$

cover of $36 = -$



(v) $\langle P(A), \subseteq \rangle$ **;** $A = \{a, b\}$

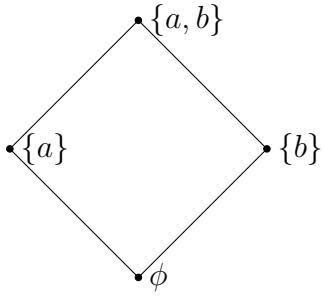
Here we have $P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$

cover of $\phi = \{a\}, \{b\}$

cover of $\{a\} = \{a, b\}$

cover of $\{b\} = \{a, b\}$

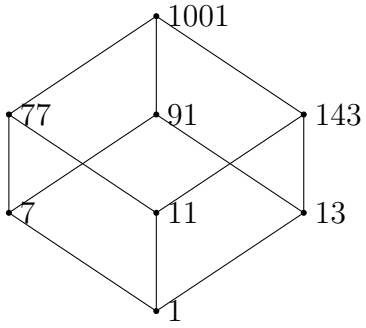
cover of $\{a, b\} = -$



(VI) $\langle S_{1001}, D \rangle$

Here we have $S_{1001} = \{1, 7, 11, 13, 77, 91, 143, 1001\}$

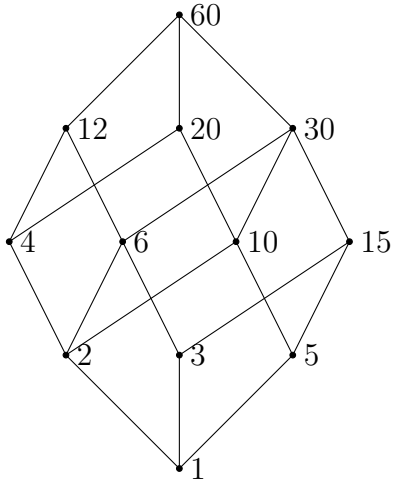
cover of $1 = 7, 11, 13$
cover of $7 = 77, 91$
cover of $11 = 77, 143$
cover of $13 = 91, 143$
cover of $77 = 1001$
cover of $91 = 1001$
cover of $143 = 1001$
cover of $1001 = -$

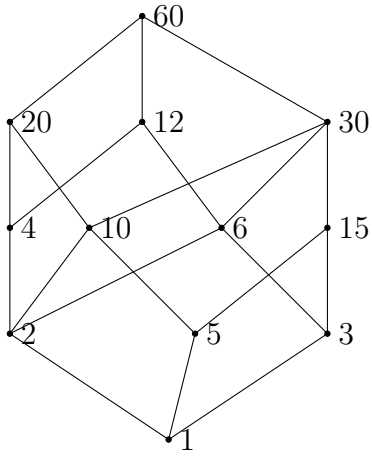


(VII) $\langle S_{60}, D \rangle$

Here we have $S_{60} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$

cover of $1 = 2, 3, 5$
cover of $2 = 4, 6, 10$
cover of $3 = 6, 15$
cover of $4 = 12, 20$
cover of $5 = 10, 15$
cover of $6 = 12, 30$
cover of $10 = 20, 30$
cover of $12 = 60$
cover of $15 = 30$
cover of $20 = 60$
cover of $30 = 60$
cover of $60 = -$





2.7 Lower and Upper Bounds

2.7.1 Lower Bound

Let $\langle X, \leq \rangle$ be a poset and $A \subset X$, if there exists $x \in X$ such that $x \leq a$, $\forall\ a \in A$ then x is called lower bound of the set A.

Greatest Lower Bound

Let $\langle X, \leq \rangle$ be a poset and $A \subset X$, if there exists $y \in X$ such that

(i) y is lower bound of A.

(ii) For any lower bound x of A $x \leq y$ then y is called greatest lower bound of set A.

$\Longrightarrow$ Some time Greatest lower bound is denote by *glb*.
e.g $\Longrightarrow$ $\langle S_6, D \rangle$ $\Longrightarrow$ Here $A = S_6 = \{1, 2, 3, 6\} \subset \mathbb{N} = X$, Then from the given set we get element $1 \in \mathbb{N}$ which is $1Da$, $\forall\ a \in S_6$, so 1 is greatest lower bound of S_6

2.7.2 Upper Bound

Let $\langle X, \leq \rangle$ be a poset and $A \subset X$, if there exists $x \in X$ such that $a \leq x$, $\forall\ a \in A$ then x is called upper bound of the set A.

Least Upper Bound

Let $\langle X, \leq \rangle$ be a poset and $A \subset X$, if there exists $y \in X$ such that

(i) y is upper bound of A.

(ii) For any upper bound x of A $y \leq x$ then y is called least upper bound of set A.

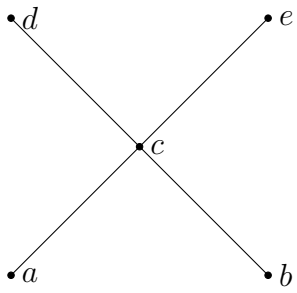
$\Longrightarrow$ Some time Least upper bound is denote by lub. $e.g \Longrightarrow \langle S_6, D \rangle \Longrightarrow$ Here $A = S_6 = \{1, 2, 3, 6\} \subset \mathbb{N} = X$, Then from the given set we get element $6 \in \mathbb{N}$ which is $aD6$, $\forall\ a \in S_6$, so 6 is least upper bound of S_6

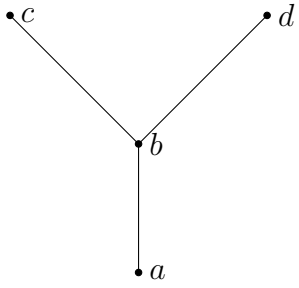
2.8 Well Ordered Set

Let $\langle X, \leq \rangle$ be a poset then X is called a well ordered set if every non empty subset A of X has a least element.

2.9 Lattice

Let $\langle L, \leq \rangle$ be a poset for any pair of elements $x, y \in L$ if $glb\{x, y\}$ as well as $lub\{x, y\}$ exist in L then $\langle L, \leq \rangle$ is said to be a lattice.





2.9.1 Lattice as a Poset

Let $\langle L, \leq \rangle$ be a Poset for any (every) pair of elements $x, y \in L$ has greatest lower bound and least upper bound in L then $\langle L, \leq \rangle$ is said to be a lattice

Remark . (i) The greatest lower bound of a subset $\{x, y\} \subseteq L$ will be denoted by $x * y$. It is customary to call $glb\{x, y\} = x * y$ the meet or product of $x$and y . Also another symbol such as $\wedge$, $\cdot$
i.e $glb\{x, y\} = x \wedge y = x \cdot y = x * y = x \cap y = gcd\{x, y\}$, read as a meet

(ii) The least upper bound of a subset $\{x, y\} \subseteq L$ will be denoted by $x \oplus y$. It is customary to call $lub\{x, y\} = x \oplus y$ the join or sum of $x$and y . Also another symbol such as $\vee$, $+$ *i.e.* $lub\{x, y\} = x \vee y = x + y = x \oplus y = x \cup y = lcm\{x, y\}$, read as Join.

2.9.1 Example. Show that $\langle \{2, 3, 6\}, D \rangle$ is not lattice
Solution:
Here for lattice we check *glb* and *lub* for pair of element of $\{2, 3, 6\} \subset \mathbb{N}$ under divisible relation
for that $glb\{2, 3\} = 1 \in \mathbb{N}$ but $1 \notin \{2, 3, 6\}$. So *glb* of pair $\{2, 3\}$ does not exist in $\{2, 3, 6\}$
$\therefore \{2, 3, 6\}$ is not lattice for relation D.

2.9.2 Example. Show that $\langle S_6, D \rangle$ is a lattice.
Solution:
we know that here given set $S_6 = \{1, 2, 3, 6\}$ is a poset. Now for lattice we check *glb* and *lub* of pair of element S_6 as follow.

$glb\{1, 2\} = gcd\{1, 2\} = 1$ $\quad$ $lub\{1, 2\} = lcm\{1, 2\} = 2$
$glb\{1, 3\} = 1$ $\quad$ $lub\{1, 3\} = 3$
$glb\{1, 6\} = 1$ $\quad$ $lub\{1, 6\} = 6$
$glb\{2, 3\} = 1$ $\quad$ $lub\{2, 3\} = 6$
$glb\{2, 6\} = 2$ $\quad$ $lub\{2, 6\} = 6$
$glb\{3, 6\} = 3$ $\quad$ $lub\{3, 6\} = 6$

$\therefore$ we have $glb\{a, b\} \in S_6$ and $lub\{a, b\} \in S_6$ $\forall a, b \in S_6$
$\therefore \langle S_6, D \rangle$ is lattice.

2.9.3 Example. Prove that $\langle P(A), \leq \rangle$ is lattice for $A\{a, b\}$
Solution:
Here given set $A\{a, b\}$ then $P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$. Also we know that $\langle P(A), \leq \rangle$ is poset.Now we prepare table as follow

$glb\{x, y\} = x \cap y$	ϕ	$\{a\}$	$\{b\}$	$\{a, b\}$
ϕ	ϕ	ϕ	ϕ	ϕ
$\{a\}$	ϕ	$\{a\}$	ϕ	$\{a\}$
$\{b\}$	ϕ	ϕ	$\{b\}$	$\{b\}$
$\{a, b\}$	ϕ	$\{a\}$	$\{b\}$	$\{a, b\}$

$lub\{x, y\} = x \cup y$	ϕ	$\{a\}$	$\{b\}$	$\{a, b\}$
ϕ	ϕ	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a, b\}$	$\{a, b\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	$\{b\}$	$\{a, b\}$
$\{a, b\}$	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$	$\{a, b\}$

From the table we have
$lub\{x, y\} = x \cup y \in P(A)$, $\forall x, y \in P(A)$ and $glb\{x, y\} = x \cap y \in P(A)$, $\forall x, y \in P(A)$
$\therefore$ given set $\langle P(A), \leq \rangle$ is lattice.

2.9.4 Example. Show that $\langle S_{1001}, D \rangle$ is lattice.
Solution:
Here we know that $\langle S_n, D \rangle$ is a poset $\forall n \in \mathbb{N}$, so $S_{1001} = \{1, 7, 11, 13, 77, 91, 143, 1001\}$ is poset. Now fore lattice.
let $x, y \in S_{1001}$ then $lub\{x, y\} = lcm\{x, y\} = x * y$ and $glb\{x, y\} = gcd\{x, y\} = x \oplus y$. Now we prepare table as follow

$x * y$	1	7	11	13	77	91	143	1001
1	1	1	1	1	1	1	1	1
7	1	7	1	1	7	1	1	7
11	1	1	11	1	11	1	13	11
13	1	1	1	13	1	7	11	13
77	1	7	11	1	77	7	11	77
91	1	1	1	7	7	91	13	91
143	1	1	13	11	11	13	143	143
1001	1	7	11	13	77	91	143	1001

$x \oplus y$	1	7	11	13	77	91	143	1001
1	1	7	11	13	77	91	143	1001
7	7	7	77	91	77	91	1001	1001
11	11	77	11	143	77	1001	143	1001
13	13	91	143	13	1001	91	143	1001
77	77	77	77	1001	77	1001	1001	1001
91	91	91	1001	1001	1001	91	1001	1001
143	143	1001	143	143	1001	1001	143	1001
1001	1001	1001	1001	1001	1001	1001	1001	1001

From the table $\forall x, y \ \in S_{1001}$ we have $x * y \in S_{1001}$ and $x \oplus y \in S_{1001}$
$\therefore \ \langle S_{1001}, D \rangle$ is a lattice.

Remark . Every Chain is a lattice.

2.10 Meet $(*)$ and Join $(\oplus)$

Suppose $\langle X, \leq \rangle$ any poset and $x, y \in X$ then *glb* of x and y is denoted by $x * y$ where $x * y$ is read as meet of x and y. and similarly *lub* of x and y is denoted by $x \oplus y$ where $x \oplus y$ is read as join of x and y.

2.10.1 Properties of Meet and Join

Theorem 2.10.1. *Let $\langle L, \leq \rangle$ be a lattice then $\forall a, b \in L$*

(i) $a * b \ \leq a$ *and* $a * b \leq b$

(ii) $a \leq a \oplus b$ *and* $b \leq a \oplus b$

(iii) $a * b \leq a \oplus b$

Proof. Here given that $\langle L, \leq \rangle$. let $\forall a, b \in L$

(1) $a * b \ = \ glb\{a, b\}$
$= \ a * b$ is a lower bound of {a,b}
$\implies a * b \ \leq a$ and $a * b \leq b$

(2) $a \oplus b = lub\{a, b\}$
$= a \oplus b$ is a upper bound of {a,b}
$\Longrightarrow a \leq a \oplus b$ and $b \leq a \oplus b$

(3) we know that $a * b \leq a$ and $a \leq a \oplus b \Longrightarrow \ a * b \leq a \oplus b$ □

Theorem 2.10.2. *Let* $\langle L, \leq \rangle$ *be a lattice and* $a, b, c \in L$ *then*

	Meet	***Join***
(1) Idempotent	*(1)* $a * a = a$	*(1)* $a \oplus a = a, \quad \forall a \in L$
(2) Commutativity	*(2)* $a * b = b * a$	*(2)* $a \oplus b = b \oplus a, \quad \forall a, b \in L$
(3) Associativity	*(3)* $a * (b * c) = (a * b) * c$	*(3)* $a \oplus (b \oplus c) = (a \oplus b) \oplus c, \quad \forall a, b, c \in L$
(4) Absorption	*(4)* $a * (a \oplus b) = a$	(4) $a \oplus (a * b) = a, \quad \forall a, b \in L$

Proof.

Meet (1) Idempotent $a * a = glb\{a, a\}$
$= glb\{a\}$
$a * a = a$

Join (1) Idempotent $a \oplus a = lub\{a, a\}$
$= lub\{a\}$
$a \oplus a = a$

Meet (2) Commutativity $a * b = glb\{a, b\}$
$= glb\{b, a\}$
$a * b = b * a$

Join (2) Commutativity $a \oplus b = lub\{a, b\}$
$= lub\{b, a\}$
$a \oplus b = b \oplus a$

Meet (3) Associativity let $x = a * (b * c)$, & $y = (a * b) * c$
Now $x = a * (b * c)$
$\Rightarrow x = glb\{a, b * c\}$
$\Rightarrow x \leq a,\ x \leq glb\{b, c\}$
$\Rightarrow x \leq a,\ x \leq b,\ x \leq c$
$\Rightarrow x$ is a lower bound of $\{a, b\}$ and c
$\Rightarrow x$ is a lower bound of $\{a * b, c\}$
$\Rightarrow x \leq (a * b) * c$
$\Rightarrow x \leq y$
similarly we get $y \leq x$
hence $x = y,\ i.e\ \ a * (b * c) = (a * b) * c$

Join (3) Associativity let $x = a \oplus (b \oplus c)$, & $y = (a \oplus b) \oplus c$
Now $x = a \oplus (b \oplus c)$
$\Rightarrow x = lub\{a, b \oplus c\}$
$\Rightarrow a \leq x,\ lub\{b, c\} \leq x$
$\Rightarrow a \leq x,\ b \leq x,\ c \leq x$
$\Rightarrow x$ is an upper bound of $\{a, b\}$ and c
$\Rightarrow x$ is an upper bound of $\{a \oplus b, c\}$
$\Rightarrow (a \oplus b) \oplus c \leq x$
$\Rightarrow y \leq x$
similarly we get $x \leq y$
hence $x = y,\ i.e\ \ a \oplus (b \oplus c) = (a \oplus b) \oplus c$

Meet (4) Absorption let $x = a * (a \oplus b)$

$\Rightarrow x = glb\{a, a \oplus b\}$

$\Rightarrow x \leq a$

$\Rightarrow a * (a \oplus b) \leq a \; ---------- (1)$

Now since $< L, \leq >$ is Lattice. $\Rightarrow \; \leq$ is reflexive

$\Rightarrow a \leq a \; ---------- (2)$

also, $a \leq lub\ \{a, b\}$ for all $b \in L \Rightarrow a \leq a \oplus b \; ----------(3)$

from (2) and (3) a is a lower bound of $\{a, a \oplus b\}$

$\Rightarrow a \; \leq glb \; \{a, a \oplus b\}$

$\Rightarrow a \leq a * (a \oplus b) ----------(4)$

from (1) and (4) $\Rightarrow a = a * (a \oplus b)$

Join (4) Absorption let $x = a \oplus (a * b)$

$\Rightarrow x = lub\{a, a * b\}$

$\Rightarrow a \leq x$

$\Rightarrow a \leq a \oplus (a * b) \; ---------- (1)$

Now since $< L, \leq >$ is Lattice. $\Rightarrow \; \leq$ is reflexive

$\Rightarrow a \leq a \; ---------- (2)$

also, $glb\{a, b\} \leq a \; \{a, b\}$ for all $b \in L \Rightarrow a * b \leq a \; ----------(3)$

from (2) and (3) a is an upper bound of $\{a, a * b\}$

$\Rightarrow lub \; \{a, a * b\} \leq a$

$\Rightarrow a \oplus (a * b) \leq a ----------(4)$

from (1) and (4) $\Rightarrow a = a \oplus (a * b)$

□

Remark .

(i) All the lower bounds are related to *glb* and *lub* are related to all the upper bounds.

(ii) $a \oplus (b \oplus c) = lub\{a, b, c\}$

(iii) $a * \{b * c\} = glb\{a, b, c\}$

Theorem 2.10.3 (Stability Property). *Let a, b, c be three elements of a lattice $\langle L, \leq \rangle$ then*

(i) $a \leq b, \; a \leq c \Longrightarrow \; a \leq b * c, \; a \leq b \oplus c.$

(ii) $b \leq a, \; c \leq a \Longrightarrow b * c \leq a, \; b \oplus c \leq a.$

Proof.
(1) Let $a \leq b, a \leq c \Longrightarrow a * a \leq a * b,\ \&\ a * b \leq c * b$
$\Longrightarrow a \leq a * b,\ a * b \leq b * c$
$\Longrightarrow a \leq b * c.$
Let $a \leq b, a \leq c \Longrightarrow a \oplus a \leq a \oplus b,\ \&\ a \oplus b \leq c \oplus b$
$\Longrightarrow a \leq a \oplus b,\ a \oplus b \leq b \oplus c$
$\Longrightarrow a \leq b \oplus c.$

(2) Let $b \leq a, c \leq a \Longrightarrow b * c \leq a * c,\ \&\ a * c \leq a * a$
$\Longrightarrow b * c \leq a * c,\ a * c \leq a$
$\Longrightarrow b * c \leq a.$
Let $b \leq a, c \leq a \Longrightarrow b \oplus c \leq a \oplus c,\ \&\ a \oplus c \leq a \oplus a$
$\Longrightarrow b \oplus c \leq a \oplus c,\ a \oplus c \leq a$
$\Longrightarrow b \oplus c \leq a.$

□

Theorem 2.10.4.
Let $\langle L, \leq \rangle$ be a lattice then for $a, b \in L$, $a \leq b \iff a * b = a \iff a \oplus b = b$

Proof. Here we shall prove $a \leq b \Longrightarrow a * b = a \Longrightarrow a \oplus b = b \Longrightarrow a \leq b$
(1) let $a \leq b$ and here L is lattice, so L has reflexive then we write $a \leq a$ also our hypothesis is $a \leq b$
$\therefore a$ is lower bound of $\{a, b\}$
$\therefore a \leq glb\{a, b\}$
$\therefore a \leq a * b - - - - - - - - - - - - - - -(1)$
from the definition of $*$, $a * b \leq a - - - - - - - - - - - - -(2)$
Since $\leq$ is anti symmetric
from $eq^n(1)$ & $(2) \implies a = a * b.$
(2) Let $a * b = a$

Now $a \oplus b = (a * b) \oplus b\ \ (a * b = a)$
$= b \oplus (a * b)\ \ (\text{Commutativity})$
$= b \oplus (b * a)\ \ (\text{Commutativity})$
$= b\ \ (\text{Absorption})$
$a \oplus b = b$

(3) Let $a \oplus b = b$, from the definition of $\oplus$
$a \leq a \oplus b$
$a \leq b\ \ (\text{by } a \oplus b = b)$
From above three result we proved required result. □

Theorem 2.10.5 (Isotonicity Property). *Let $\langle L, \leq \rangle$ be a lattice and $b, c \in L$ then*

(i) If $b \leq c \implies a * b \leq a * c,\ \forall a \in L.$

(ii) If $b \leq c \implies a \oplus b \leq a \oplus c,\ \forall a \in L.$

Proof. **(1)** Let $b \leq c$

$$\begin{aligned}\text{Now, } (a*b)*(a*c) &= [(a*b)*a]*c \\ &= [a*(b*a)]*c \ \text{(Associative of } *) \\ &= [a*(a*b)]*c \ \text{(Commutative of } *) \\ &= [(a*a)*b]*c \ \text{(Associative of } *) \\ &= (a*b)*c \\ &= a*(b*c) \ \text{(Associative of } *) \\ &= a*b \ \text{(if } b \leq c \text{ then } b*c = b)\end{aligned}$$

Thus $(a*b)*(a*c) = a*b \implies$ *i.e.* $a*b \leq a*c$ (by $a \leq b \iff a*b = a$)

(2) Let $b \leq c$

$$\begin{aligned}\text{Now, } (a\oplus b)\oplus(a\oplus c) &= [(a\oplus b)\oplus a]\oplus c \\ &= [a\oplus(b\oplus a)]\oplus c \ \text{(Associative of } \oplus) \\ &= [a\oplus(a\oplus b)]\oplus c \ \text{(Commutative of } \oplus) \\ &= [(a\oplus a)\oplus b]\oplus c \ \text{(Associative of } \oplus) \\ &= (a\oplus b)\oplus c \\ &= a\oplus(b\oplus c) \ \text{(Associative of } \oplus) \\ &= a\oplus c \ \text{(if } b \leq c \text{ then } b\oplus c = c)\end{aligned}$$

Thus $(a\oplus b)\oplus(a\oplus c) = a\oplus c \implies$ *i.e.* $a\oplus b \leq a\oplus c$ (by $a \leq b \iff a\oplus b = a$) □

Theorem 2.10.6 (Distributive Inequality). *Let* $\langle L, \leq \rangle$ *be a lattice and* $a, b, c \in L$ *then*

(i) $a\oplus(b*c) \leq (a\oplus b)*(a\oplus c)$

(ii) $a*(b\oplus c) \geq (a*b)\oplus(a*c)$ [***or*** $(a*b)\oplus(a*c) \leq a*(b\oplus c)$]

Proof. **(1)** From the definition of $\oplus$, $a \leq a\oplus b$ and $a \leq a\oplus c$

$\therefore a$ is lower bound of $\{a\oplus b, a\oplus c\}$
$\therefore a \leq glb\{a\oplus b, a\oplus c\}$
$\therefore a \leq (a\oplus b)*(a*c) - - - - - - - - -(1)$

Now from the definition of $*$ and $\oplus$ we have $b*c \leq b$ and $b \leq a\oplus b$
$\therefore \ b*c \leq a\oplus b - - - - - - - - - - - - - (2)$
also we have $b*c \leq c$ and $c \leq a\oplus c$
$\therefore \ b*c \leq a\oplus c - - - - - - - - - - - - - (3)$
$\implies b*c$ is a lower bound of $\{a\oplus b, a\oplus c\}$
$\therefore \ b*c \ \leq glb\{a\oplus b, a\oplus c\}$
$\therefore \ b*c \ \leq (a\oplus b)*(a\oplus c) - - - - - - -(4)$
From the equation (1) and (4) we have $(a\oplus b)*(a\oplus c)$ is an upper bound of $\{a, b*c\}$
$\therefore \{a, b*c\} \leq (a\oplus b)*(a\oplus c)$
$\boxed{\therefore a\oplus(b*c) \leq (a\oplus b)*(a\oplus c)}$

(2) From the definition of $*$, $a * b \leq a$ and $a * c \leq a$
$\therefore$ a is an upper bound of $\{a * b, a * c\}$
$\therefore$ $lub\{a * b, a * c\} \leq a$
$\therefore$ $(a * b) \oplus (a * c) \leq a - - - - - - - - (1)$
Now from the definition of $*$ and $\oplus$ $a * b \leq b$ and $b \leq b \oplus c$
$\therefore$ $a * b \leq b \oplus c - - - - - - - - - - - - (2)$
also, $a * c \leq c$ and $c \leq b \oplus c$
$a * c \leq b \oplus c \quad - - - - - - - - - (3)$
from the equation (2) and (3) we have $b \oplus c$ is an upper bound of $\{a * b, a * c\}$
$\therefore$ $lub\{a * b, a * c\} \leq (b \oplus c)$
$\therefore$ $(a * b) \oplus (a * c) \leq (b \oplus c) - - - - - - (4)$
from the equation (1) and (4) we have $(a * b) \oplus (a * c)$ is lower bound of $\{a, b \oplus c\}$
$\therefore$ $(a * b) \oplus (a * c) \leq glb\{a, b \oplus c\}$
$\therefore$ $(a * b) \oplus (a * c) \leq a * (b \oplus c)$ □

Theorem 2.10.7 (Modular inequality). *If $\langle L, \leq \rangle$ is a lattice then prove that $a \leq c \iff a \oplus (b * c) \leq (a \oplus b) * c$.*

2.10.8 Example. Let $\langle L, \leq \rangle$ be a lattice and $a, b, c, d \in L$ then prove the following

(i) $(a * b) \oplus (c * d) \leq (a \oplus c) * (b \oplus d)$

(ii) $(a * b) \oplus (b * c) \oplus (c * a) \leq (a \oplus b) * (b \oplus c) * (c \oplus a)$

Solution:
(i) here we know that $(a * b) \leq a,\ a \leq (a \oplus c)$ and $(c * d) \leq c,\ c \leq (a \oplus c)$
$\therefore$ $(a * b) \leq (a \oplus c)$ and $(c * d) \leq (a \oplus c)$
$\therefore$ $(a * b) \oplus (c * d) \leq (a \oplus c) - - - - - - - - - - - (1)$
Now $(a * b) \leq b,\ b \leq (b \oplus d)$ and $(c * d) \leq d,\ d \leq (b \oplus d)$
$\therefore$ $(a * b) \leq (b \oplus d)$ and $(c * d) \leq (b \oplus d)$
$\therefore$ $(a * b) \oplus (c * d) \leq (b \oplus d) - - - - - - - - - - - (2)$
from the eq^n (1) and (2), we can write
$(a * b) \oplus (c * d) \leq (a \oplus c) * (b \oplus d)$

2.11 Lattice as an Algebraic Structure

Suppose L is any non-empty set and $*$ & $\oplus$ are binary operation on L. If algebraic structure $\langle L, *, \oplus \rangle$ is satisfy following property then it is called a Lattice as an algebraic structure.

(i) $*$ and $\oplus$ is commutative.
(i) $a * b = b * a,\ \forall\ a, b \in L$ **(ii)** $a \oplus b = b \oplus a,\ \forall\ a, b \in L$

(ii) $*$ and $\oplus$ is Associative.
(i) $a * (b * c) = (a * b) * c,\ \forall\ a, b, c \in L$ **(ii)** $a \oplus (b \oplus c) = (a \oplus b) \oplus c,\ \forall\ a, b, c \in L$

(iii) $*$ and $\oplus$ is satisfy Absorption.
(i) $a * (a \oplus b) = a,\ \forall\ a, b \in L$

(ii) $a \oplus (a * b) = a,\ \forall\ a, b \in L$

Theorem 2.11.1. *Let $\langle L, \leq \rangle$ be a lattice as a Poset there are two binary operations $*$ and $\oplus$ on L such that $\langle L, *, \oplus \rangle$ is a lattice as an algebraic structure (system).*

Proof. Let $\langle L, \leq \rangle$ be a lattice as a poset and $a, b, c \in L$. Now we define binary operation of $*$ and $\oplus$ on L by
$a * b = glb\{a, b\}$ and $a \oplus b = lub\{a, b\}$
$\therefore\ a * b \in L,\ a \oplus b \in L$ (Because L is a lattice as a poset.)
Now for lattice as algebraic system.

(i) Commutative:
Let $a * b = glb\{a, b\} = glb\{b, a\} = b * a.$ and $a \oplus b = lub\{a, b\} = lub\{b, a\} = b \oplus a$

(ii) Associative:

For Meet: $\Longrightarrow$ let $x = a * (b * c),\ \&\ y = (a * b) * c$
Now $x = a * (b * c)$
$\Rightarrow x = glb\{a, b * c\}$
$\Rightarrow x \leq a,\ x \leq glb\{b, c\}$
$\Rightarrow x \leq a,\ x \leq b,\ x \leq c$
$\Rightarrow x$ is a lower bound of $\{a, b\}$ and c
$\Rightarrow x$ is a lower bound of $\{a * b, c\}$
$\Rightarrow x \leq (a * b) * c$
$\Rightarrow x \leq y$
similarly we get $y \leq x$
hence $x = y,\ i.e\ \ a * (b * c) = (a * b) * c$
let $x = a \oplus (b \oplus c),\ \&\ y = (a \oplus b) \oplus c$
For Join: $\Longrightarrow$ Now $x = a \oplus (b \oplus c)$
$\Rightarrow x = lub\{a, b \oplus c\}$
$\Rightarrow a \leq x,\ lub\{b, c\} \leq x$
$\Rightarrow a \leq x,\ b \leq x,\ c \leq x$
$\Rightarrow x$ is an upper bound of $\{a, b\}$ and c
$\Rightarrow x$ is an upper bound of $\{a \oplus b, c\}$
$\Rightarrow (a \oplus b) \oplus c \leq x$
$\Rightarrow y \leq x$
similarly we get $x \leq y$
hence $x = y,\ i.e\ \ a \oplus (b \oplus c) = (a \oplus b) \oplus c$

(3) Absorption

For Meet: $\Longrightarrow$ let $x = a * (a \oplus b)$

$\Rightarrow x = glb\{a, a \oplus b\}$

$\Rightarrow x \leq a$

$\Rightarrow a * (a \oplus b) \leq a \ ---------- (1)$

Now since $< L, \leq >$ is Lattice. $\Rightarrow \ \leq$ is reflexive

$\Rightarrow a \leq a \ ---------- (2)$

also, $a \leq lub\ \{a, b\}$ for all $b \in L \Rightarrow a \leq a \oplus b \ ----------(3)$

from (2) and (3) a is a lower bound of $\{a, a \oplus b\}$

$\Rightarrow a \ \leq glb\ \{a, a \oplus b\}$

$\Rightarrow a \leq a * (a \oplus b) ----------(4)$

from (1) and (4) $\Rightarrow a = a * (a \oplus b)$

For Join: $\Longrightarrow$ let $x = a \oplus (a * b)$

$\Rightarrow x = lub\{a, a * b\}$

$\Rightarrow a \leq x$

$\Rightarrow a \leq a \oplus (a * b) \ ---------- (1)$

Now since $< L, \leq >$ is Lattice. $\Rightarrow \ \leq$ is reflexive

$\Rightarrow a \leq a \ ---------- (2)$

also, $glb\{a, b\} \leq a\ \{a, b\}$ for all $b \in L \Rightarrow a * b \leq a \ ----------(3)$

from (2) and (3) a is an upper bound of $\{a, a * b\}$

$\Rightarrow lub\ \{a, a * b\} \leq a$

$\Rightarrow a \oplus (a * b) \leq a ----------(4)$

from (1) and (4) $\Rightarrow a = a \oplus (a * b)$

$\therefore \ \langle L, *, \oplus \rangle$ is a lattice as an algebraic system. □

2.11.1 Sub Lattice

Suppose $\langle L, *, \oplus \rangle$ is a lattice and set S is non empty subset of L. If $\forall a, b \in S$ with $a * b \in S$ and $a \oplus b \in S$ then S is Sub Lattice of $\langle L, *, \oplus \rangle$

i.e(1) Here we take lattice $\langle S_{30}, D \rangle$ where $S_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and we take subset of lattice is $S_1 = \{1, 5, 10, 15, 30\}$

$$\begin{aligned} 1*5 &= gcd\{1,5\}=1 \\ 1*10 &= 1 \\ 1*15 &= 1 \\ 1*30 &= 1 \\ 5*10 &= 5 \\ 5*15 &= 5 \\ 5*30 &= 5 \\ 10*15 &= 5 \\ 10*30 &= 10 \\ 15*30 &= 15 \\ \forall a,b \in S_1 &\Longrightarrow a*b \in S_1 \end{aligned} \qquad \begin{aligned} 1\oplus 5 &= lcm\{1,5\}=5 \\ 1\oplus 10 &= 10 \\ 1\oplus 15 &= 15 \\ 1\oplus 30 &= 30 \\ 5\oplus 10 &= 10 \\ 5\oplus 15 &= 15 \\ 5\oplus 30 &= 30 \\ 10\oplus 15 &= 30 \\ 10\oplus 30 &= 30 \\ 15\oplus 30 &= 30 \\ \forall a,b \in S_1 &\Longrightarrow a\oplus b \in S_1 \end{aligned}$$

$\therefore$ $S_1$is a sub lattice of S_{30}

(2) $S_2\{1,10,15,30\}$ is subset of S_{30} and here we have a pair $10,15 \in S_2$ but $10*15=5 \notin S_2$
$\therefore$ S_2 is not sub lattice of S_{30}

2.11.2 Example. show that $\langle \{\phi,\{a\},\{b\},\{a,b\}\},\leq \rangle$ is a sub lattice of $\langle P(A),\leq \rangle$, where $A=\{a,b,c\}$
Solution:
here to show that the set $S=\{\phi,\{a\},\{b\},\{a,b\}\}$ is sub lattice of $\langle P(A),\leq \rangle$, where $A=\{a,b,c\}$, for that we check *glb* and *lub* of given set as follow

$glb\{x,y\}=x\cap y$	ϕ	$\{a\}$	$\{b\}$	$\{a,b\}$
ϕ	ϕ	ϕ	ϕ	ϕ
$\{a\}$	ϕ	$\{a\}$	ϕ	$\{a\}$
$\{b\}$	ϕ	ϕ	$\{b\}$	$\{b\}$
$\{a,b\}$	ϕ	$\{a\}$	$\{b\}$	$\{a,b\}$

$lub\{x,y\}=x\cup y$	ϕ	$\{a\}$	$\{b\}$	$\{a,b\}$
ϕ	ϕ	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a,b\}$	$\{a,b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$

From the table we have
$lub\{x,y\}=x\cup y\in S,\ \ \forall x,y\in S$ and $glb\{x,y\}=x\cap y\in S,\ \ \forall x,y\in S$
$\therefore$ given set S is sub lattice of $\langle P(A),\leq \rangle$.

2.11.3 Example. Show that $\langle \{1,3,6,15\},\leq \rangle$ is not a sub lattice of $\langle S_{30},\leq \rangle$
Solution:
Self

> ***Remark*** . $\langle S_n, D\rangle$ is a sub lattice of $\langle \mathbb{N}, D\rangle$ where $n\in\mathbb{N}$

2.11.2 Complete Lattice

A lattice $\langle L,*,\oplus\rangle$ is called a complete if every non-empty subset S of L has greatest lower bound (*glb*) and least upper bound (*lub*) in L
i.e glb $S\in L$ and *lub* $S\in L$

2.11.3 Bounded Lattice

Suppose $\langle L, *, \oplus \rangle$ is lattice. If *glb* L and *lub* L exist in L then L is said to be bounded lattice.

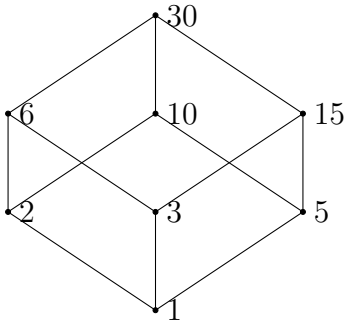
Notation:

(i) If $\langle L, *, \oplus \rangle$ is bounded lattice then *glb* L and *lub* L exist, then *glb* L is denoted by **0** and *lub* L is denoted by **1**.

(ii) *glb* $L = 0$ and *lub* $L = 1$

(iii) Bounded lattice are denoted by $\langle L, *, \oplus, 0, 1 \rangle$

e.g (1) $\langle S_{30}, D \rangle$
$S_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$



$glb(S_{30}) = 1 = 0$ element
$lub(S_{30}) = 30 = 1$ element.

In short 0=1 and 1 = 30 in S_{30}

Remark .

(i) Every finite lattice must be complete.

(ii) Every complete lattice must have a least element and greatest element.

(iii) Every complete lattice is bounded.

Theorem 2.11.4. *If* $\langle L, *, \oplus, 0, 1 \rangle$ *is bounded lattice then* $\forall\ a \in L$

(i) $a * 0 = 0$ *(ii)* $a * 1 = a$ *(iii)* $a \oplus 0 = a$ *(iv)* $a \oplus 1 = 1$

Proof.
Here given that $\langle L, *, \oplus, 0, 1 \rangle$ is bounded lattice then $0 = glb\ L$ and $1 = lub\ L$
$\therefore glb\ L \leq a \leq lub\ L, \quad \forall a \in L$
$\therefore 0 \leq a \leq 1$

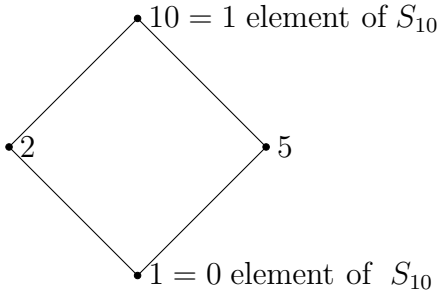
$$\begin{aligned} \text{Now let } 0 \leq a &\implies a * 0 = 0 \ \ (\text{by if } a \leq b \implies a * b = a \ \&\ a \oplus b = b) \\ &\implies a \oplus 0 = a \\ \text{and } a \leq 1 &\implies a * 1 = a \\ &\implies a \oplus 1 = 1 \end{aligned}$$

□

2.11.4 Complement of an element

Let $\langle L, *, \oplus, 0, 1\rangle$ be a bounded lattice and $a \in L$, if there exist an element b such that $a * b = 0$ and $a \oplus b = 1$ then element b is called complement of a. It is denoted by a'

e.g $\implies$ Here we take $\langle S_{10}, D\rangle$
$S_{10} = \{1, 2, 5, 10\}$



For complement of 1

$$1 * 2 = gcd\{1, 2\} = 1 = 0 \text{ element}$$
$$1 * 5 = 1 = 0 \text{ element}$$
$$1 * 10 = 1 = 0 \text{ element of } S_{10}$$
$$\& \; 1 \oplus 2 = lcm\{1, 2\} = 2$$
$$1 \oplus 5 = 5$$
$$1 \oplus 10 = 10 = 1 \text{ element of } S_{10}$$

$\therefore$ 10 is complement of 1 and also 1 is complement of 10.

For complement of 2

$$2 * 5 = gcd\{2, 5\} = 1 = 0 \text{ element}$$
$$\& \; 2 \oplus 5 = lcm\{2, 5\} = 10 = 1 \text{ element of } S_{10}$$

$\therefore$ 5 is complement of 2 and also 2 is complement of 5.

Remark .

(i) If $\langle L, *, \oplus, 0, 1\rangle$ is bounded lattice then always 0-element is complement of 1-element and 1-element is complement of 0-element.

(ii) Any element $a \in L$ may or may not have a complement.

(iii) An element $b \in L$ may have more then one complement.

2.11.5 Complemented Lattice

A Lattice $\langle L, *, \oplus, 0, 1\rangle$ is said to be a complemented lattice if every element of L has at least one complement.
$\implies$ Complemented lattice is denoted by $\langle L, *, \oplus, 0, 1, '\rangle$ or $\langle L, *, \oplus, ', 0, 1\rangle$

2.11.5 Example. Give an example of complete lattice which is an infinite lattice.
Solution:
Let $a, b \in \mathbb{R}$ we take $L = [\ a, b\ ] = \{x \in \mathbb{R} / a \leq x \leq b\}$ is an infinite lattice.
To prove complete lattice we prove that any subset of L has glb and lub in L.
Let $S \subseteq L$, with $S \neq \phi$

$$\text{let } x \in S \implies x \in L$$
$$\implies a \leq x \leq b$$

$\therefore$ S is bounded above by b and S is bounded below by a
since $\mathbb{R}$ has lub and glb property.
$\therefore$ $lub\ S \in \mathbb{R}$ and $glb\ S \in \mathbb{R}$
$\therefore$ $a \leq lub\ S \leq b$ and $a \leq glb\ S \leq b$
$\therefore$ $lub\ S \in L$ and $glb\ S \in L$
$\therefore$ $L = [\ a, b\ ]$ is a complete infinite lattice

2.11.6 Example. Show that $\langle \mathbb{Z}, \leq \rangle$ is not a complete lattice.
Solution:
we know that $\mathbb{N} \subset \mathbb{Z}$ but $\mathbb{N}$ has no upper bound in $\mathbb{Z}$
$\therefore$ $lub\ \mathbb{N}$ does not exist in $\mathbb{Z}$
$\therefore$ $\langle \mathbb{Z}, \leq \rangle$ is not complete lattice.

2.11.7 Example. Show that $\langle S_{30}, D \rangle$ is bounded lattice.
Solution:
Here we have $S_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and division relation D

Now $1\ D\ 1\ D\ 30$
$1\ D\ 2\ D\ 30$
$1\ D\ 3\ D\ 30$
$1\ D\ 5\ D\ 30$
$1\ D\ 6\ D\ 30$
$1\ D\ 10\ D\ 30$
$1\ D\ 15\ D\ 30$
$1\ D\ 30\ D\ 30$

Thus we get $1\ D\ x\ D\ 30,\ \forall x \in S_{30}$
$\therefore$ $glb\ S_{30} = 1 = 0 -$ element of S_{30} and $lub\ S_{30} = 30 = 1 -$ element of S_{30}
$\therefore$ $0\ \&\ 1 \in S_{30}$
$\therefore$ $\langle S_{30}, D \rangle$ is bounded lattice.

2.11.8 Example. Show that $\langle S_{30}, D \rangle$ is complemented lattice.
Solution:
We know that $\langle S_{30}, D \rangle$ is bounded lattice and also $glb\ S_{30} = 1 = 0 -$ element of S_{30} and $lub\ S_{30} = 30 = 1 -$ element of S_{30}
Now we want to prove that $\langle S_{30}, D \rangle$ is complemented lattice for that we find the complement element of every element.
$1 * 30 = 1$ and $1 \oplus 30 = 30$, so complement of 1 is 30 and complement of 30 is 1.
$2 * 15 = 1$ and $2 \oplus 15 = 30$, so complement of 2 is 15 and complement of 15 is 2.
$3 * 10 = 1$ and $3 \oplus 10 = 30$, so complement of 3 is 10 and complement of 10 is 3.
$5 * 6 = 1$ and $5 \oplus 6 = 30$, so complement of 5 is 6 and complement of 6 is 5.
$\therefore$ $\langle S_{30}, D \rangle$ is complemented lattice.

2.11.9 Example. Show that $\langle P(X), \subseteq \rangle$ is a bounded and complemented lattice. where $X = \{a, b, c\}$

Solution:
Here given set $X = \{a, b, c\}$
$\therefore\ P(X) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, X\}$
from the set $P(X)$ we can write $\phi \subseteq A \subseteq X,\ \forall A \in P(X)$
$\therefore\ glb\ P(X) = \phi = 0 -$ element of $P(X)$ and $lub\ P(X) = X = 1 -$ element of $P(X)$.
$\therefore\ 0\ \&\ 1 \in P(X)$.
$\therefore\ \langle P(X), \subseteq \rangle$ is a bounded lattice.
Now we want to prove that $\langle P(X), \subseteq \rangle$ is complemented lattice for that we find the complement element of every element.
$\phi * X = \phi$ and $\phi \oplus X = X = \{a, b, c\}$, so complement of ϕ is $X = \{a, b, c\}$ and complement of $X = \{a, b, c\}$ is ϕ.
$\{a\} * \{b, c\} = \phi$ and $\{a\} \oplus \{b, c\} = \{a, b, c\}$, so complement of $\{a\}$ is $\{b, c\}$ and complement of $\{b, c\}$ is $\{a\}$.
$\{b\} * \{a, c\} = \phi$ and $\{b\} \oplus \{a, c\} = \{a, b, c\}$, so complement of $\{b\}$ is $\{a, c\}$ and complement of $\{a, c\}$ is $\{b\}$.
$\{c\} * \{a, b\} = \phi$ and $\{c\} \oplus \{a, b\} = \{a, b, c\}$, so complement of $\{c\}$ is $\{a, b\}$ and complement of $\{a, b\}$ is $\{c\}$.
$\therefore\ \langle P(X), \subseteq \rangle$ is a complemented lattice.

2.12 Distributive Lattice

A lattice $\langle L, *, \oplus \rangle$ is said to be distributive if lattice satisfy the following properties

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

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

2.13 Direct Product Of Two Lattice

Suppose $\langle L_1, \leq \rangle$ and $\langle L_2, \leq \rangle$ are two lattice. If $\langle L_1 \times L_2, \leq \rangle$ satisfies following axioms then it is called Direct product of Two Lattice.
$\forall\ (a_1, b_1)$ and $(a_2, b_2) \in L_1 \times L_2$ as $(a_1, b_1) \leq (a_2, b_2) \iff a_1 \leq a_2\ \&\ b_1 \leq b_2$

Theorem 2.13.1. *If $\langle L_1, \leq_1 \rangle$ and $\langle L_2, \leq_2 \rangle$ are two lattice then prove that $\langle L_1 \times L_2, \leq \rangle$ also lattice where $(a_1, b_1) \leq (a_2, b_2)$ if $a_1 \leq a_2\ \&\ b_1 \leq b_2,\ \forall\ (a_1, b_1)$ and $(a_2, b_2) \in L_1 \times L_2$*

2.13.2 Example. Show that for $S = \{1, 3, 6\}$ and $L = \{1, 2, 4\}$,$\langle S, D \rangle$ and $\langle L, D \rangle$ is lattice. Also show that $\langle S \times L, D \rangle$ is lattice.where $(a_1, b_1) D (a_2, b_2) \Longrightarrow a_1 D a_2\ \&\ b_1 D b_2$, $\forall (a_1, b_1), (a_2, b_2) \in S \times L$
Solution:
For $S = \{1, 3, 6\}$

(i) Reflexive:
here we have $1D1, 3D3, 6D6$
$\therefore\ aDa\ \forall\ a \in S$
$\therefore\ D$ is reflexive on S

(ii) Anti Symmetric:
here $1D3$ but $3 \not D 1$
$1D6$ but $6 \not D 1$
$3D6$ but $6 \not D 3$
$\therefore\ D$is anti symmetric on S

(iii) Transitive:
here $1D3$ and $3D6 \implies 1D6$
$\therefore$ D is Transitive on S

(iv) For *glb* and *lub*

$glb\{1,3\} = gcd\{1,3\} = 1$ $\quad$ $lub\{1,3\} = lcm\{1,3\} = 3$
$glb\{1,6\} = 1$ $\quad$ $lub\{1,6\} = 6$
$glb\{3,6\} = 3$ $\quad$ $lub\{3,6\} = 6$

$\therefore$ $\forall a, b \in S$ we have $glb\{a,b\} \in S$ and $lub\{a,b\} \in S$
$\therefore$ $\langle S, D \rangle$ is lattice.

For $L = \{1, 2, 4\}$

(i) Reflexive:
here we have $1D1, 2D2, 2D2$
$\therefore$ $aDa \; \forall \; a \in S$
$\therefore$ D is reflexive on L

(ii) Anti Symmetric:
here $1D2$ but $2 \not D 1$
$1D4$ but $4 \not D 1$
$2D4$ but $4 \not D 2$
$\therefore$ $D$is anti symmetric on L

(iii) Transitive:
here $1D2$ and $2D4 \implies 1D4$
$\therefore$ D is Transitive on L

(iv) For *glb* and *lub*

$glb\{1,2\} = gcd\{1,2\} = 1$ $\quad$ $lub\{1,2\} = lcm\{1,2\} = 2$
$glb\{1,4\} = 1$ $\quad$ $lub\{1,4\} = 4$
$glb\{2,4\} = 2$ $\quad$ $lub\{2,4\} = 4$

$\therefore$ $\forall a, b \in L$ we have $glb\{a,b\} \in L$ and $lub\{a,b\} \in L$
$\therefore$ $\langle L, D \rangle$ is lattice.
By above theorem we can say that $\langle S \times L, D \rangle$ is lattice

2.14 Lattice Homomorphism

Let $\langle L_1, *_1, \oplus_1 \rangle$ and $\langle L_2, *_2, \oplus_2 \rangle$ be two lattice and $f : \langle L_1, *_1, \oplus_1 \rangle \longrightarrow \langle L_2, *_2, \oplus_2 \rangle$ be function, if $\forall \; a, b \in L_1$

(i) $f(a *_1 b) = f(a) *_2 f(b)$

(ii) $f(a \oplus_1 b) = f(a) \oplus_2 f(b)$

then f is said to be a lattice homomorphism from $\langle L_1, *_1, \oplus_1 \rangle$ to $\langle L_2, *_2, \oplus_2 \rangle$.

2.15 Lattice Isomorphism

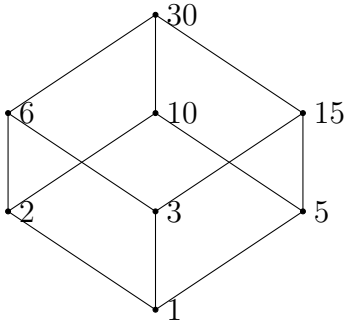
Let $\langle L_1, *_1, \oplus_1 \rangle$ and $\langle L_2, *_2, \oplus_2 \rangle$ be two lattice and $f : \langle L_1, *_1, \oplus_1 \rangle \longrightarrow \langle L_2, *_2, \oplus_2 \rangle$ be function, if $\forall\ a, b \in L_1$

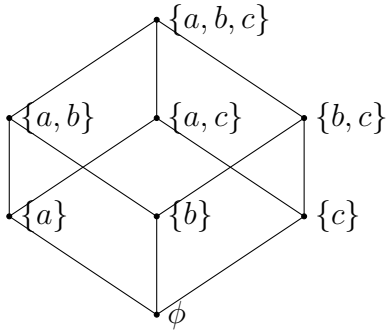
(i) f is one-one and f is onto

(ii) f preserves binary operations Meet and Join

then f is said to be a lattice isomorphism from $\langle L_1, *_1, \oplus_1 \rangle$ to $\langle L_2, *_2, \oplus_2 \rangle$.
In this case we say lattice $\langle L_1, *_1, \oplus_1 \rangle$ is isomorphic to $\langle L_2, *_2, \oplus_2 \rangle$
i.e $\langle L_1, *_1, \oplus_1 \rangle \cong \langle L_2, *_2, \oplus_2 \rangle$

2.15.1 Example. Show that lattice $\langle S_{30}, *_1, \oplus_1 \rangle$ and $\langle P(X), *_2, \oplus_2 \rangle$ are isomorphic lattice for $X = \{a, b, c\}$
Solution:
Here we have $S_{30} = \{1, 2, 3, , 5, 6, 10, 15, 30\}$ and $P(X) = \Big\{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\Big\}$.
Their Hasse Diagrams are





We define function as follow

$f : S_{30} \longrightarrow P(X)$ by

$f(1) = \phi$ $\quad$ $f(6) = \{a, b\}$
$f(2) = \{a\}$ $\quad$ $f(10) = \{a, c\}$
$f(3) = \{b\}$ $\quad$ $f(15) = \{b, c\}$ $\quad$ Then clearly
$f(5) = \{c\}$ $\quad$ $f(30) = \{a, b, c\}$

here define function f is one-one and onto.Now to show that f preserves binary operations Meet and Join. For that we make tables as follow.

$*_1 = gcd$	1	2	3	5	6	10	15	30
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
3	1	1	3	1	3	1	3	3
5	1	1	1	5	1	5	5	5
6	1	2	3	1	6	2	3	6
10	1	2	1	5	2	10	5	10
15	1	1	3	5	3	5	15	15
30	1	2	3	5	6	10	15	30

Table: 1

$*_2 = \cap$	ϕ	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a,b,c\}$
ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ
$\{a\}$	ϕ	$\{a\}$	ϕ	ϕ	$\{a\}$	$\{a\}$	ϕ	$\{a\}$
$\{b\}$	ϕ	ϕ	$\{b\}$	ϕ	$\{b\}$	ϕ	$\{b\}$	$\{b\}$
$\{c\}$	ϕ	ϕ	ϕ	$\{c\}$	ϕ	$\{c\}$	$\{c\}$	$\{c\}$
$\{a,b\}$	ϕ	$\{a\}$	$\{b\}$	ϕ	$\{a,b\}$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a,c\}$	ϕ	$\{a\}$	ϕ	$\{c\}$	$\{a\}$	$\{a,c\}$	$\{c\}$	$\{a,c\}$
$\{b,c\}$	ϕ	ϕ	$\{b\}$	$\{c\}$	$\{b\}$	$\{c\}$	$\{b,c\}$	$\{b,c\}$
$\{a,b,c\}$	ϕ	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a,b,c\}$

Table: 2

From the table: 1 and table:2 we have $f(x *_1 y) = f(x) *_2 f(y), \ \ \forall x, y \in S_{30}$

$\oplus_1 = lcm$	1	2	3	5	6	10	15	30
1	1	2	3	5	6	10	15	30
2	2	2	6	10	6	10	30	30
3	3	6	3	15	6	30	15	30
5	5	10	15	5	30	10	15	30
6	6	6	6	30	6	30	30	30
10	10	10	30	10	30	10	30	30
15	15	30	15	15	30	30	15	30
30	30	30	30	30	30	30	30	30

Table: 3

$\oplus_2 = \cup$	ϕ	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a,b,c\}$
ϕ	ϕ	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a,b,c\}$
$\{a\}$	$\{a\}$	$\{a\}$	$\{a,b\}$	$\{a,c\}$	$\{a,b\}$	$\{a,c\}$	$\{a,b,c\}$	$\{a,b,c\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\{b\}$	$\{b,c\}$	$\{a,b\}$	$\{a,b,c\}$	$\{b,c\}$	$\{a,b,c\}$
$\{c\}$	$\{c\}$	$\{a,c\}$	$\{b,c\}$	$\{a\}$	$\{a,b,c\}$	$\{a,c\}$	$\{b,c\}$	$\{a,b,c\}$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b,c\}$	$\{a,b\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$
$\{a,c\}$	$\{a,c\}$	$\{a,c\}$	$\{a,b,c\}$	$\{a,c\}$	$\{a,b,c\}$	$\{a,c\}$	$\{a,b,c\}$	$\{a,b,c\}$
$\{b,c\}$	$\{b,c\}$	$\{a,b,c\}$	$\{b,c\}$	$\{b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{b,c\}$	$\{a,b,c\}$
$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b,c\}$

Table: 4

From the table: 3 and table:4 we have $f(x \oplus_1 y) = f(x) \oplus_2 f(y), \ \ \forall x, y \in S_{30}$
$\therefore$ f preserves binary operation meet($*$) and join($\oplus$)
$\therefore$ f is an isomorphism $\langle S_{30}, *_1, \oplus_1 \rangle$ to $\langle P(X), *_2, \oplus_2 \rangle$
$\therefore$ $\langle S_{30}, *_1, \oplus_1 \rangle \equiv \langle P(X), *_2, \oplus_2 \rangle$

Chapter 3

Propositional Logic

Intuitively, logic is the discipline that considers the method of reasoning. It provides the rules and techniques for determining whether an argument is valid or not. In everyday life, we use reasoning to prove different points. For example, to prove to our parents that we passed an exam, we might show the test and the score. Or to prove to the utility company that our bill has been paid, we might show the cancelled check. Similarly, in mathematics and computer science, mathematical logic or logic is used to prove results. To be specific, in mathematics we use logic or logical reasoning to prove theorems, and in computer science we use logic or logical reasoning to prove the correctness of programs and also to prove theorems.
In this chapter we take a close look at what constitutes a valid argument and a more conventional proof. When a mathematician wishes to provide a proof for a given situation, he or she must use a system of logic. This is also true when a computer scientist develops the algorithms needed for a program or system of programs. The logic of mathematics is applied to decide whether one statement follows from, or is a logical consequence of, one or more other statements. Some of the rules that govern this process are described in this chapter. We shall use these rules in proofs (provided in the text and required in the exercises) throughout subsequent chapters. However, at no time can we hope to arrive at a point at which we can apply the rules in an automatic fashion.

3.1 Basic Connectives and Truth Table

3.1.1 Statement (Proposition)

A statement (proposition) is a declarative sentence that is either true or false, but not both.

In other words, In the development of any mathematical theory, assertions are made in the form of sentences. Such verbal or written assertions, called statements (propositions), are declarative sentences that are either true or false — but not both. We use the lowercase letters of the alphabet (such as p, q, and r) to represent these statements. for examples, we consider the following sentences.

(i) 4 is an integer. (ii) $\sqrt{6}$ is an integer. (iii) $2+3=5$

Each of these sentences is a declarative sentence. Sentence (i) is true, sentence (ii) is not true, and sentence (iii) is true. Hence, these are examples of statements.
We typically use lowercase letters, with or without subscripts, such as p, q, and r to denote statements. For example, we might write

p : 4 is an integer.
q : $\sqrt{6}$ is an integer.
r : $2+3=5$

Remark: By definition, a statement is a declarative sentence that can be classified as true or false, but not both. Thus, one of the values "*truth*" or "$falsity$" that is assigned to a statement is called its truth value. We abbreviate "truth" to T or 1 and "falsity" to F or 0. If a statement p is true, we say that the (logical) truth value of p is true and write p is T (or p is 1); otherwise, we say the (logical) truth value of p is false and write p is F (or p is 0).
In the above discussion, we assumed intuitively the idea of the words "sentence," "true," and "false," and we defined a "statement" with the help of these words.
New statements can be constructed from existing statements. Next, we describe the different ways of doing so. In the process, we also define various logical operations.

3.1.2 Negation

Let p be a statement. The negation of p, written $\sim p$ (or $\neg p$), is the statement obtained by negating statement p.

Consider the following statements:

p : 2 is positive.
q : It is not the case that 2 is positive.

We see that statement p is true and statement q is false. Statement q is obtained by negating statement p, and the truth values of p and q are opposite. Statement q is the negation of statement p.
It follows that the truth values of p and $\sim p$ are opposite. The symbol $\sim$ is called "not." We read $\sim p$ as "not p." For example, if

p : 3 is positive.
then $\sim p$: It is not the case that 3 is positive.

Some time, $\sim p$ is also written as , $\sim p$: 3 is not positive.
By the definition of the negation of a statement p, the truth value of $\sim p$ is opposite to the truth value of p; i.e., if p is T, then $\sim p$ is F and if p is F, then $\sim p$ is T. We record this in a table, called a truth table, as follows:

p	$\sim p$
T	F
F	T

3.1.3 Conjunction

Let p and q be statements. The conjunction of p and q, written $p \wedge q$, is the statement formed by joining statements p and q using the word "and." The statement $p \wedge q$ is true if both p and q are true; otherwise $p \wedge q$ is false.The symbol $\wedge$ is called "and." Let p and q be statements. For example
Consider the following statements:

$$p : 2 \text{ is an even integer.}$$

$$q : 7 \text{ divides } 14.$$

Now consider the sentence $r : 2$ is an even integer and 7 divides 14.

The truth table of $p \wedge q$ is given by:

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

3.1.1 Example. Let $p : 5$ is an integer and $q : 5$ is not an odd integer. Then find truth value of $p \wedge q$.

Solution: Here given statement are $p : 5$ is an integer and $q : 5$ is not an odd integer. Then $p \wedge q$ is the statement:

$$p \wedge q : \quad 5 \text{ is an integer and } 5 \text{ is not an odd integer.}$$

Now truth value of p is T and q is F, then $p \wedge q$ is F. ■

3.1.4 Disjunction

Let P and q be statements. The disjunction of p and q, written $p \vee q$, is the statement formed by putting statements p and q together using the word "or." The truth value of the statement $p \vee q$ is T if at least one of statements p and q is true. The symbol $\vee$ is called "or." For statements p and q. For example
Consider statement

$$p : 2^2 + 3^3 \text{ is an even integer,}$$

$$q : 2^2 + 3^3 \text{ is an odd integer.}$$

Then

$$p \vee q : 2^2 + 3^3 \text{ is an even integer or } 2^2 + 3^3 \text{ is an odd integer.}$$

Sometimes, for better readability, we write $p \vee q$ as:

$$p \vee q : \quad \text{Either } 2^2 + 3^3 \text{ is an even integer or } 2^2 + 3^3 \text{ is an odd integer}$$

or

$$p \vee q : 2^2 + 3^3 \text{ is an even integer or an odd integer.}$$

The truth table of $p \vee q$ is follow:

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

3.2 Logical Implication

3.2.1 Implication (Conditional Statements)

Let p and q be two statements. Then "if p, then q" is a statement called an implication, or a condition, written $p \to q$. The statement $p \to q$ is also to be read as p implies q. Alternatively, we can also say

(i) If p, then q.

(ii) p is sufficient for q.

(iii) p is a sufficient condition for q.

(iv) q is necessary for p.

(v) q is a necessary condition for p.

(vi) p only if q.

The implication $p \to q$ is considered false when p is true and q is false; otherwise, it is considered true.In the implication $p \to q$, p is called the hypothesis and q is called the conclusion. The truth table of the implication $p \to q$ as follow.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Remark: Let p and q be statements. Then

(i) The statement $q \to p$ is called the **converse** of the implication $p \to q$.

(ii) The statement $\sim p \to \sim q$ is called the **inverse** of the implication $p \to q$.

(iii) The statement $\sim q \to \sim p$ is called the **contrapositive** of the implication $p \to q$.

3.2.1 Example. If the statement is "If today is Sunday, then I will go for a walk", then write converse, inverse and contrapositive implication.

Solution: Here given statement is "If today is Sunday, then I will go for a walk" and we want to write converse, inverse and contrapositive implication, for that
Let p and q be the statement. Then

p : Today is Sunday.

q : I will go for a walk.

Then the given statement can be written as $p \to q$. The converse of this implication is $q \to p$, which is

$q \to p$: If I will go for a walk, then today is Sunday.

The inverse of the above implication is $\sim p \to \sim q$, which is

$\sim p \to \sim q$: If today is not Sunday, then I will not go for a walk.

The contrapositive of the above implication is $\sim q \to \sim p$, which is

$\sim q \to \sim p$: If I will not go for a walk, then today is not Sunday.

■

3.2.2 Biimplication(Biconditional Statements)

Let p and q be two statements, then "p if and only if q," written $p \longleftrightarrow q$, is called the biimplication, or bi-conditional, of statements p and q. For example,

1. 19,302 is divisible by 6 if and only if 19,302 is divisible by 2 and 3.
2. An integer n is divisible by 3 if and only if n is divisible by 9.

The statement $p \longleftrightarrow q$ may also be read as "p is necessary and sufficient for q," or "q is necessary and sufficient for p," or "q if and only if p," or "q when and only when p." We define that the biimplication $p \longleftrightarrow q$ is considered to be true when both p and q have the same truth values and false otherwise. The following table shows the truth values of the biimplication $p \longleftrightarrow q$.

p	q	$p \longleftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Remark:
we have used letters such as p and q to denote statements. From statements p and q we constructed the statements: negation $\sim p$, conjunction $p \wedge q$, disjunction $p \vee q$, implication $p \to q$, and biimplication $p \longleftrightarrow q$.
The symbols $\sim, \wedge, \vee, \to, \longleftrightarrow,$, are called logical connectives. Henceforth, we use the symbols $p, q, r, \cdots$, called statement variables, with or without subscripts to denote statements.

3.2.3 Statement Formula

A statement formula, or formula, is defined as follows.

(i) A statement variable is a statement formula.

(ii) If A and B are statement formulas, then the expressions $(\sim A)$, $(A \vee B)$, $(A \wedge B)$, $(A \longrightarrow B)$, and $(A \leftrightarrow B)$ are statement formulas.

(iii) Those expressions are statement formulas that are constructed only by using (i) and (ii).

Remark: To compute the truth table of statement formula (A) for a given assignment of truth values to the statement variables occurring in statement formula (A), we follow these rules: First compute the truth value of the statement formula within innermost parentheses, then determine the truth value of the statement formula within the next innermost set of parentheses, and continue the process until we determine the truth value for statement formula(A). We show this computation in the following examples.

3.2.2 Example. Construct the truth table for the statement formula A,

$$A: \ (\sim (p \vee q)) \rightarrow (q \wedge p)$$

.

Solution: To construct the truth table for A, we first set up columns labeled p, q, $(p \vee q)$, $\sim (p \vee q)$, $(q \wedge p)$, and A. Write in the p, q columns all possible combinations of the truth values T and F. Then from the truth table of $\vee$ and $\wedge$, we write the truth values in the columns of $(p \vee q)$ and $(q \wedge p)$. Next, with the help of the truth table for $\sim$, we fill in the column of $\sim (p \vee q)$. Finally, using the truth table of $\rightarrow$, we fill in the column of A. Thus, we obtain the truth table for A. The truth table for A is:

p	q	$(p \vee q)$	$(\sim (p \vee q))$	$(q \wedge p)$	$A = (\sim (p \vee q)) \rightarrow (q \wedge p)$
T	T	T	F	T	T
T	F	T	F	F	T
F	T	T	F	F	T
F	F	F	T	F	F

■

3.2.3 Example. Let p, q and r be the statement then construct the truth table for the statement formula A,

$$A: \ (\sim p \wedge q) \rightarrow r$$

.

Solution: Here p, q and r be the statement and we want to construct the truth table for the statement formula A,

$$A: \ (\sim p \wedge q) \rightarrow r$$

Also we know that each variables p, q, and r assigned the value T or F, there are $2^3 = 8$ assignments of formula A. This means that to construct the truth table for $A: \ (\sim p \wedge q) \rightarrow r$, we have to consider all eight assignments and hence there will be eight rows for this table. The following is the truth table for $(\sim p \wedge q) \rightarrow r$.

p	q	r	$\sim p$	$\sim p \wedge q$	$A = (\sim p \wedge q) \rightarrow r$
T	T	T	F	F	T
T	T	F	F	F	T
T	F	T	F	F	T
T	F	F	F	F	T
F	T	T	T	T	T
F	T	F	T	T	F
F	F	T	T	F	T
F	F	F	T	F	T

■

3.2.4 Example. If p and q are any two statement then verify

$$\sim (p \leftrightarrow q) = \sim p \leftrightarrow q = p \leftrightarrow \sim q$$

Solution: Here p and q are statement and we want to verify $\sim (p \leftrightarrow q) = \sim p \leftrightarrow q = p \leftrightarrow \sim q$, for that we construct truth table as follow.

p	q	$p \leftrightarrow q$	$\sim (p \leftrightarrow q)$	$\sim p$	$\sim p \leftrightarrow q$	$\sim q$	$p \leftrightarrow \sim q$
T	T	T	F	F	F	F	F
T	F	F	T	F	T	T	T
F	T	F	T	T	T	F	T
F	F	T	F	T	F	T	F

■

3.2.4 Tautology

A statement formula A is said to be a tautology if the truth value of A is T for any assignment of the truth values T and F to the statement variables occurring in A.

For example, Let A be the statement formula $(\sim p \wedge q) \rightarrow (\sim (q \rightarrow p))$. We construct the truth table for A. This statement formula contains two statement variables, so to construct the truth table of A we have to consider four different assignments of truth values. The following is the truth table of A.

p	$\sim p$	q	$(\sim p \wedge q)$	$q \rightarrow p$	$\sim (q \rightarrow p)$	$A = (\sim p \wedge q) \rightarrow (\sim (q \rightarrow p))$
T	F	T	F	T	F	T
T	F	F	F	T	F	T
F	T	F	F	T	F	T
F	T	T	T	F	T	T

From the truth table it follows that the truth value of A is T for any assignments of truth values T and F to p and q. Hence, A is a tautology.

3.2.5 Contradiction

A statement formula A is said to be a contradiction if the truth value of A is F for any assignment of the truth values T and F to the statement variables occurring in A.

For example, Let A be the statement formula $\sim p \wedge p$. We construct the truth table for A.

p	$\sim p$	$\sim p \wedge p$
T	F	F
F	T	F

From the table, it follows that A is a contradiction.

3.2.6 Logically Imply

A statement formula A is said to logically imply a statement formula B if the statement formula $A \leftrightarrow B$ is a tautology. If A logically implies B, then symbolically we write $A \leftrightarrow B$.

For example, Let A denote the statement formula $p \wedge (p \rightarrow q$ and B be q. We show that A logically implies B. For this, we construct the truth table of $A \rightarrow B$.

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	$A \rightarrow B$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

From the truth table it follows that$A \rightarrow B$ is a tautology and hence A logically implies B.

3.3 Logically Equivalent

A statement formula A is said to be logically equivalent to a statement formula B if the statement formula $A \leftrightarrow B$ is a tautology. If A is logically equivalent to B, then symbolically we write $A \equiv B$ (or $A \Leftrightarrow B$).

In this example, we show that the implication $p \rightarrow q$ is equivalent to $\sim p \vee q$. For this we construct the truth table of $(p \rightarrow q) \leftrightarrow (\sim p \vee q)$.

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

From this table, it follows that $(p \rightarrow q) \leftrightarrow (\sim p \vee q)$ is a tautology and hence $p \rightarrow q$ is equivalent to $\sim p \vee q$; that is,

$$p \rightarrow q \equiv \sim p \vee q.$$

3.3.1 Example. Show that statement formula $A = \sim (p \wedge q)$ and $B = (\sim p) \vee (\sim q)$ is logically equivalent.

Solution: Here we want to show that statement formula $A = \sim (p \wedge q)$ and $B = (\sim p) \vee (\sim q)$ is logically equivalent, for that we construct the truth table as follow.

p	q	$(p \wedge q)$	$\sim (p \wedge q)$	$\sim p$	$\sim q$	$(\sim p) \vee (\sim q)$	$A \leftrightarrow B$
T	T	T	F	F	F	F	T
T	F	F	T	F	T	T	T
F	T	F	T	T	F	T	T
F	F	F	T	T	T	T	T

From the truth table, it follows that $A \leftrightarrow B$ is a tautology and hence A is logically equivalent to B. ■

3.4 Laws of Logic

(i) Commutative laws

Let p and q be statements then commutative law

(i) $p \wedge q \equiv q \wedge p$ and (ii) $p \vee q \equiv q \vee p$

(ii) Associative laws

Let p, q and r be statements then associative law

(i) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ and (ii) $(p \vee q) \vee r \equiv p \vee (q \vee r)$

(iii) Distributive laws

Let p, q and r be statements then distributive law

(i) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge q)$ and (ii) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee q)$

(iv) Absorption laws

Let p, q and r be statements then absorption law

(i) $p \wedge (p \vee q) \equiv p$ and (ii) $p \vee (p \wedge q) \equiv p$

(v) Idempotent laws

Let p be statements then idempotent law

(i) $p \wedge p \equiv p$ and (ii) $p \vee p \equiv p$

(vi) Double negation laws

Let p be statements then double negation law

(i) $\sim\sim p \equiv p$

(vii) DeMorgan's laws

Let p and q be statements then Demorgan's law

(i) $\sim (p \wedge q) \equiv (\sim p) \vee (\sim q)$ and (ii) $\sim (p \vee q) \equiv (\sim p) \wedge (\sim q)$

3.5 Quantifiers

3.5.1 Predicate or Propositional Function

Let x be a variable and D be a set; $P(x)$ is a sentence. Then $P(x)$ is called a predicate or propositional function with respect to the set D if for each value of x in D, $P(x)$ is a statement; i.e., $P(x)$ is true or false. Moreover, D is called the domain of the discourse and x is called the free variable.
For example, Consider the sentence $P(x)$,

$$P(x) : x \text{ is an even integer,}$$

where the domain of the discourse is the set of integers. Then $P(4)$; i.e., 4 is an even integer, is T, and $P(3)$; i.e., 3 is an even integer, is F,
The predicates that we considered until now involved only one variable. We can also have predicates involving two or more variables. For example, consider the following:

$$P(x, y) : \ x = y + 1$$

Consider $P(2, 1)$. Here $x = 2$ and $y = 1$. Because $x = 2 = 1+1 = y+1$, it follows that $P(2, 1)$ is T. Similarly, consider $P(5, 4)$. Here $x = 5$ and $y = 4$. Because $x = 5 = 4 + 1 = y + 1$, it follows that $P(5, 4)$ is T. Now consider $P(6, 4)$. Here $x = 6$ and $y = 4$. Because $x = 6 \neq 4 + 1 = y + 1$, it follows that $P(6, 4)$ is F.

Remark:
The predicate $P(x)$ is also called a propositional function because for each value x in the domain D, $P(x)$ is either true or false. So $P(x)$ acts as a rule that assigns to each value in the domain either the value T or the value F. Although some prefer to use the term propositional function, we prefer the term predicate as it is a commonly used terminology in mathematical logic.

Remark:
Let $P(x)$ be a predicate. Then for each value x in the domain $P(x)$ is a statement. Certain predicates are true for each value of the domain, while others are not. Even though a $P(x)$ is not a statement, it can be turned into a statement through a process called quantification. There are two types of quantifiers, universal and existential. We describe them next.

3.5.2 Universal Quantifier

Let $P(x)$ be a predicate and let D be the domain of the discourse. The universal quantification of $P(x)$ is the statement

$$\text{for all } x,\ P(x)$$
$$\text{or}$$
$$\text{for every } x,\ P(x).$$

The symbol used to denote the adjectives for all (for every) is $\forall$, and it is called the universal quantifier. Thus, in notation, the universal quantification of the predicate $P(x)$ is

$$\forall\, x\ P(x).$$

In fact, the symbol $\forall$ is read as "for all or for every."
for example, Let $P(x)$ be the predicate given by

$$P(x) : x^2 \geq x$$

and let the domain be the set of all integers. Consider the universal quantification of $P(x)$:

$$\forall\, x\ P(x)$$

Because for all integers x, $x^2 \geq x$ is true, it follows that $P(x)$ is true for all integers x. We can now conclude that the value of the universal quantification $\forall\, xP(x)$ is T.

Another example, Let $P(x)$ be the predicate given by $P(x) : \ x \geq 3$ and let the domain of discourse be the set of real numbers. Consider the universal quantification of $P(x) : \ \forall\ x\ P(x)$. If we take $x = 2$, then the statement $P(2)$, i.e., $2 \geq 3$, is false. Because the predicate $P(x)$ is false when x is replaced with 2, it follows that the value of the universal quantification $\forall\, xP(x)$ is F.

Remark:
Remember that for the predicate $P(x)$ the universal quantification $\forall\ x\ P(x)$ is a statement, so it is either true or false. That is, the value of the statement $\forall\, xP(x)$ is either T or F.

3.5.3 Existential Quantifier

Let $P(x)$ be a predicate and let D be the domain of the discourse. The existential quantification of $P(x)$ is the statement

$$\text{there exists } x,\ P(x).$$

The symbol used to denote "there exists" is $\exists$, and it is called the existential quantifier. Thus, in notation, the existential quantification of the predicate $P(x)$ is

$$\exists\, x\ p(x).$$

For example, Let $P(x)$ be the predicate given by

$$P(x) : \ x^2 > x$$

and let the domain of discourse be the set of all real numbers. Consider the existential quantification of $P(x)$:

$$\exists \, x, \ P(x)$$

Let $x = 2$. Now $2^2 = 4 > 2$ is true, so $P(2)$ is true. Because we have found a value in the domain at which the predicate is true, we can conclude that the value of $\exists \, x \ P(x)$ is T. We would like to remark that $P(1)$ is false, so the universal quantification $\forall \, x \ P(x)$ is F.

3.6 Rules of Inference

To verify the validity of a logical consequence in predicate logic, we introduce four more additional rules of inference to the rules of inference already presented in our discussion of propositional logic.

(i) If the statement $\forall \, x \ P(x)$ is assumed to be true, then $P(a)$ is also true, where a is an arbitrary member of the domain of the discourse. This rule is called the universal specification (US).

(ii) If $P(a)$ is true, where a is an arbitrary member of the domain of the discourse, then $\forall \, x \ P(x)$ is true. This rule is called the universal generalization (UG).

(iii) If the statement $\exists \, x \ P(x)$ is true, then $P(a)$ is true, for some member of the domain of the discourse. This rule is called the existential specification (ES).

(iv) If $P(a)$ is true for some member a of the domain of the discourse, then $\exists \, x \ P(x)$ is also true. This rule is called the existential generalization (EG).

3.7 Proof Techniques

In the preceding sections, we presented various ways of using logical arguments and deriving conclusions. As stated earlier, in mathematics and computer science, mathematical logic is used to prove theorems and the correctness of programs. In this section, after formally defining the term theorem, we describe some general techniques that are used in proving theorems. (We already used some of these techniques in earlier sections when we proved some of the theorems.) In the next section, we discuss algorithms and programs, and in later chapters we show how to prove the correctness of an algorithm (program).

Recall that a theorem is a statement that can be shown to be true (under certain conditions). For example, consider the following statement:

If x is an integer and x is odd, then $x$is odd,

or, equivalently, For all integers x, if x is odd, then x^2 is odd. This statement can be shown to be true. We will prove below that it is a true statement.

3.7.1 Direct Proofs

We first discuss the proof of those theorems that can be expressed in the form

$$\forall\, x\ (P(x) \to Q(x)),\ D \text{ is the domain of discourse.}$$

For example, for all integers x, if x is even, then $x+1$ is odd.
To construct a proof of the theorem

$$\forall\, x\ (P(x) \to Q(x)),\ D \text{ is the domain of discourse,}$$

we start by selecting a particular but arbitrarily chosen member a of the domain D. Then we show that the statement $P(a) \to Q(a)$ is true. For this we assume that $P(a)$ is true. We now show that $Q(a)$ is true. If we do this, then by the rule of universal generalization (UG), it follows that

$$\forall\, x\ (P(x) \to Q(x)),\ D \text{ is the domain of discourse,}$$

is true. This procedure is called the proof by direct method, or direct proof.

3.7.1 Example. Using direct proof to prove the theorem, for all integers x, if x is odd, then x^2 is odd.

Solution: Let a be an integer such that a is odd. Then we can write $a = 2n+1$ for some integer n. This implies that $a^2 = (2n+l)^2 = 4n^2+4n+1 = 2(2n^2+2n)+1$. Let $m = 2n^2+2n$. Because n is an integer, $m = 2n^2+2n$ is also an integer. We can therefore write $a^2 = 2m+1$ for some integer m. This implies that a^2 is odd. This completes the proof.

Sometimes such a proof can also be written as: Let a be an odd integer.

$$\begin{aligned}
&\Rightarrow\ a = 2n+1 \ \text{ for some integer } \ n \\
&\Rightarrow\ a^2 = (2n+1)^2 \\
&\Rightarrow\ a^2 = 4n^2+4n+1 \\
&\Rightarrow\ a^2 = 2(2n^2+2n)+1
\end{aligned}$$

■

Chapter 4

Algebraic Structures and Morphism

4.1 Group

A group is one of the fundamental objects of study in the field of mathematics known as abstract algebra. A group consists of a set of elements and an operation that takes any two elements of the set and forms another element of the set in such a way that certain conditions are met. The theory of groups is the subject of intense study within mathematics, and is used in many scientific fields. The branch of algebra that studies groups is called group theory. Group theory has extensive applications in mathematics, science, and engineering. Many algebraic structures such as fields and vector spaces may be defined concisely in terms of groups, and group theory provides an important tool for studying symmetry, since the symmetries of any object form a group. Groups are thus essential abstractions in branches of physics involving symmetry principles, such as relativity, quantum mechanics, and particle physics. Furthermore, their ability to represent geometric transformations finds applications in chemistry, computer graphics, and other fields.
As we noted above, group is an algebraic structure consisting of a set together with an operation that combines any two of its elements to form a third element.To qualify as a group, the set and the operation must satisfy four conditions called the group axioms, namely closure, associativity, identity and invertibility. Many familiar mathematical structures such as number systems obey these axioms: for example, the integers endowed with the addition operation form a group. However, the abstract formalization of the group axioms, detached as it is from the concrete nature of any particular group and its operation, allows entities with highly diverse mathematical origins in abstract algebra and beyond to be handled in a flexible way, while retaining their essential structural aspects. The ubiquity of groups in numerous areas within and outside mathematics makes them a central organizing principle of contemporary mathematics. The concept of a group arose from the study of polynomial equations, starting with 'E variste Galois in the 1830's. After contributions from other fields such as number theory and geometry, the group notion was generalized and firmly established around 1870.
Many structures investigated in mathematics turn out to be groups. These include familiar number systems, such as the integers, the rational numbers, the real numbers, and the complex numbers under addition, as well as the non-zero rationals, reals, and complex numbers under multiplication. Other important examples are groups of non-singular matrices (with specified size and type of entries) under matrix multiplication, and permutation groups,

which consist of invertible functions from a set to itself with composition as group operation. Group theory allows for the properties of such structures to be investigated in a general setting.
In what follows, we will discuss in detail the concept of groups with several illustrating examples. We begin with the definition of binary operations. Recall that a relation between the sets X and Y is any subset $\mathbb{R}$ of $X \times Y$. Also, a function or mapping,ϕ from X to Y is a relation between X and Y such that each $x \in X$ appears as the first member of exactly one ordered pair (x, y) in ϕ. If $\phi : X \to Y$ is a mapping, X is the domain of ϕ, Y is the codomain of ϕ, and the set $\{\phi(x)|x \in X\}$, denoted as $\phi[X]$, is the range of ϕ. A function $\phi : X \to Y$ is one to one if $\phi(x_1) = \phi(x_2)$ only when $x_1 = x_2$. The function ϕ is onto Y if the range of ϕ is Y .

Notations

$\mathbb{Z}^+$, $\mathbb{Q}^+$, and $\mathbb{R}^+$ denotes the sets of positive integers, positive rational numbers, and positive real numbers respectively. Also, $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$ denotes the sets of non zero rational numbers, non zero real numbers, and non zero complex numbers respectively.

4.1.1 Binary Algebraic Structures

If m and n are any given integers, we know that the operations addition and multiplication gives us unique integers $m + n$ and mn respectively. In other words, addition and multiplication are mappings from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$. Such mappings are called binary operations. More precisely, we have the following definition.

Binary Operation

A binary operation $*$ on a set S is a function mapping $S \times S$ into S. Thus, for each $(a, b) \in S \times S$, $*$ assigns a unique element of S, denoted as $a * b$.

We have observed that addition and multiplication are binary operations on $\mathbb{Z}$. It is clear that these operations defines binary operations on the sets $\mathbb{C}, \mathbb{R}, \mathbb{R}^+$, and $\mathbb{Z}^+$. Let $\mathbb{R}^*$ denotes the set of non zero real numbers. Then addition is not a binary operation on $\mathbb{R}^*$ (Why?), where as multiplication defines a binary operation on $\mathbb{R}^*$ (Why?). Is division a binary operation on $\mathbb{Z}$? No, because the quotient of two integers need not be an integer always. Moreover, $\frac{a}{b}$ is not defined if $b = 0$. It may be noted that a binary operation on a set S to be defined for every ordered pair (a, b) of elements of S.

4.2 Groups

Let G be a nonempty set together with a binary operation (usually called multiplication, denoted by $*$). We say G is a group under this operation if the following four properties are satisfied.

(I) Closer

The operation is closer: that is, $a * b \in G$, for all $a, b \in G$

(II) Associativity

The operation is associative; that is, $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.

(III) Identity

There is an element e (called the identity) in G , such that $a * e = e * a = a$, for all $a \in G$.

(IV) Inverses

For each element a in G, there is an element b in G (called an inverse of a) such that $a * b = b * a = e$.

Remark:

1. A set together with an associative binary operation is called a semigroup. Example, $\langle \mathbb{N}, + \rangle$ is semi group.
2. A monoid is a semigroup that has an identity element for the binary operation. Example, $\langle \mathbb{N}, \times \rangle$ is a monoid.
3. Note that a group is both a semigroup and a monoid.
4. Group structure is denoted by $\langle G, * \rangle$.

4.2.1 Example. Show that cube roots of unity from a group under multiplication.

Solution: Here we want to show that cube roots of unity is group under multiplication, for that

$$\begin{aligned} & x^3 = 1 \\ \therefore\ & x^3 - 1 = 0 \\ \therefore\ & (x-1)(x^2 + x + 1) = 0 \\ \therefore\ & x = 1, \frac{-1 \pm \sqrt{3}i}{2} \end{aligned}$$

let $w = \frac{-1+\sqrt{3}i}{2}$ and $w^2 = \frac{-1-\sqrt{3}i}{2}$. Hence $G = \{1, w, w^2\}$, to check the properties of group we prepare composition table as follow

$*$	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

Now we check the properties of group:

(I) Closer

From the composition table closer operations are hold: that is, $a*b \in G$, for all $a, b \in G$

(II) Associativity

From the composition table associative operations are hold: that is, $(a*b)*c = a*(b*c)$ for all $a, b, c \in G$.

(III) Identity

From the composition table the identity element of group G is 1, this identity element hold the operation : $a * 1 = 1 * a = a$, for all $a \in G$.

(IV) Inverses

From the composition table the inverse of each elements are as follow

- Inverse of 1 is 1
- Inverse of w is w^2
- Inverse of w^2 is w

Hence given set $G = \{1, w, w^2\}$ is group under the multiplication. ■

4.2.2 Example. Show that the set of all positive rational number $\mathbb{Q}^+$ form a group under the composition operation define by $a * b = \frac{ab}{2}$

Solution: Here given set $G = \mathbb{Q}^+$= the set of positive rational numbers and $*$ be binary operation of G defined as $a * b = \frac{ab}{2}$ & we want to show that G is group under the given operation, for that we check the properties of group as follow :

(I) Closer

Let $a, b \in G = \mathbb{Q}^+$ then $a * b = \frac{ab}{2} \in G = \mathbb{Q}^+$ because if a & b are positive rational number then $\frac{ab}{2}$ is also positive rational numbers, Hence the closure operation is hold : that is, $a * b \in G$, for all $a, b \in G$

(II) Associativity

let $a, b, c \in G = \mathbb{Q}^+$ and for the associative operation ; $(a * b) * c = a * (b * c)$

$$\begin{aligned} L.H.S &= (a * b) * c \\ &= \left(\frac{ab}{2}\right) * c \\ &= \frac{\left(\frac{ab}{2}\right) c}{2} \\ &= \frac{abc}{4} \quad \ldots\ldots\ldots (i) \end{aligned}$$

$$\begin{aligned} R.H.S &= a * (b * c) \\ &= a * \left(\frac{bc}{2}\right) \\ &= \frac{a\left(\frac{bc}{2}\right)}{2} \\ &= \frac{abc}{4} \quad \ldots\ldots\ldots (ii) \end{aligned}$$

From the equation (i) and (ii) the associative properties hold : that is, $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.

(III) Identity

Let e be the identity of $\mathbb{Q}^+$ under the given operation

$$\begin{aligned}\therefore \text{for any } \ a \in G &\Rightarrow a * e = a \\ &\Rightarrow \frac{ae}{2} = a \\ &\Rightarrow e = 2 \in \mathbb{Q}^+\end{aligned}$$

here we get the identity element $e = 2$ in G , such that $a * e = e * a = a$, for all $a \in G$.

(IV) Inverses

Let b be the inverse of $a \in \mathbb{Q}^+$ under the given operation

$$\begin{aligned}\therefore \text{for any } \ a \in G &\Rightarrow a * b = e \\ &\Rightarrow \frac{ab}{2} = 2 \\ &\Rightarrow b = \frac{4}{a} \in \mathbb{Q}^+\end{aligned}$$

here we get the inverse element of a is $b = \frac{4}{a}$ in G , such that $a * b = b * a = e$.

Hence given set $G = \mathbb{Q}^+$ is group under the composition operation $a * b = \frac{ab}{2}$. ■

4.2.3 Example. Show that fourth roots of unity from a group under multiplication.

Solution: Here we want to show that fourth roots of unity is group under multiplication, for that

$$\begin{aligned}x^4 &= 1 \\ \therefore x^4 - 1 &= 0 \\ \therefore (x^2 - 1)(x^2 + 1) &= 0 \\ \therefore x &= 1, -1, i, -i\end{aligned}$$

Hence $G = \{1, -1, i, -i\}$, to check the properties of group we prepare composition table as follow

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Now we check the properties of group:

(I) Closer

From the composition table closer operations are hold: that is, $a*b \in G$, for all $a, b \in G$

(II) Associativity

From the composition table associative operations are hold: that is, $(a*b)*c = a*(b*c)$ for all $a, b, c \in G$.

(III) Identity

From the composition table the identity element of group G is 1, this identity element hold the operation : $a * 1 = 1 * a = a$, for all $a \in G$.

(IV) Inverses

From the composition table the inverse of each elements are as follow

- Inverse of 1 is 1
- Inverse of -1 is -1
- Inverse of i is $-i$
- Inverse of $-i$ is i

Hence given set $G = \{1, -1, i, -i\}$ is group under the multiplication. ■

4.2.1 Abelian Group

A group $\langle G, * \rangle$ is said to be an abelian group or commutative group if $a * b = b * c$, for all $a, b \in G$. For example, $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{R} - \{0\}, \times \rangle$, $\langle \mathbb{Q} - 0, \times \rangle$ all are abelian group under the given operation.

4.2.4 Example. Show that cube roots of unity from a abelian group under multiplication.

Solution: Here we want to show that cube roots of unity is abelian group under multiplication, for that

$$\begin{aligned} & x^3 = 1 \\ \therefore\ & x^3 - 1 = 0 \\ \therefore\ & (x-1)(x^2 + x + 1) = 0 \\ \therefore\ & x = 1, \frac{-1 \pm \sqrt{3}i}{2} \end{aligned}$$

let $w = \frac{-1+\sqrt{3}i}{2}$ and $w^2 = \frac{-1-\sqrt{3}i}{2}$. Hence $G = \{1, w, w^2\}$, to check the properties of group we prepare composition table as follow

$*$	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

Now we check the properties of group:

(I) Closer

From the composition table closer operations are hold: that is, $a*b \in G$, for all $a, b \in G$

(II) Associativity

From the composition table associative operations are hold: that is, $(a*b)*c = a*(b*c)$ for all $a, b, c \in G$.

(III) Identity

From the composition table the identity element of group G is 1, this identity element hold the operation : $a * 1 = 1 * a = a$, for all $a \in G$.

(IV) Inverses

From the composition table the inverse of each elements are as follow

- Inverse of 1 is 1
- Inverse of w is w^2
- Inverse of w^2 is w

Also from composition table, for any $a, b \in G$ we have $a \times b = b \times a$. Hence given set $G = \{1, w, w^2\}$ is abelian group under the multiplication. ■

4.2.5 Example. Show that fourth roots of unity from a abelian group under multiplication.

Solution: Here we want to show that fourth roots of unity is group under multiplication, for that

$$\begin{aligned} & x^4 = 1 \\ \therefore\ & x^4 - 1 = 0 \\ \therefore\ & (x^2 - 1)(x^2 + 1) = 0 \\ \therefore\ & x = 1, -1, i, -i \end{aligned}$$

Hence $G = \{1, -1, i, -i\}$, to check the properties of group we prepare composition table as follow

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Now we check the properties of group:

(I) Closer

From the composition table closer operations are hold: that is, $a*b \in G$, for all $a, b \in G$

(II) Associativity

From the composition table associative operations are hold: that is, $(a*b)*c = a*(b*c)$ for all $a, b, c \in G$.

(III) Identity

From the composition table the identity element of group G is 1, this identity element hold the operation : $a * 1 = 1 * a = a$, for all $a \in G$.

(IV) Inverses

From the composition table the inverse of each elements are as follow

- Inverse of 1 is 1
- Inverse of -1 is -1
- Inverse of i is $-i$
- Inverse of $-i$ is i

Also from composition table, for any $a, b \in G$ we have $a \times b = b \times a$. Hence given set $G = \{1, -1, i, -i\}$ is group under the multiplication. ■

4.2.6 Example. Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$ show that G is an abelian group under the matrix addition.

Solution: Here given set $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$ and operation is matrix addition and we want to show that G is group under given operation, for that we check the properties of group as follow

Let $A, B, C \in G$, where $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ and $C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$

(I) Closer

$$\text{Let } A + B = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$
$$= \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} \in G$$

Hence we get for all $A, B \in G \Rightarrow\ A + B \in G$.

(II) Associativity We know that matrix addition is always associative under the given operation. Hence associative operations are hold: that is, $(A + B) + C = A + (B + C)$ for all $A, B, C \in G$.

(III) Identity Let $e = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix}$ be the identity of G

$$\text{Now } A + e = A$$
$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$
$$\begin{bmatrix} a_1 + e_1 & b_1 + e_2 \\ c_1 + e_3 & d_1 + e_4 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \ldots\ldots\ldots (i)$$

From the equation (i) we get $a_1 + e_1 = a_1$, $b_1 + e_2 = b_1$, $c_1 + e_3 = c_1$ and $d_1 + e_4 = d_1$, hence we get $e_1 = 0, e_2 = 0, e_3 = 0$ &$e_4 = 0$

$\therefore e = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in G$, hence $e = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ be the identity element of group G.

(IV) Inverses

Let $I = \begin{bmatrix} i_1 & i_2 \\ i_3 & i_4 \end{bmatrix}$ be the identity of G

$$\text{Now } A + I = e$$

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} i_1 & i_2 \\ i_3 & i_4 \end{bmatrix} = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix}$$

$$\begin{bmatrix} a_1 + i_1 & b_1 + i_2 \\ c_1 + i_3 & d_1 + i_4 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \ldots\ldots\ldots (i)$$

From the equation (i) we get $a_1 + i_1 = 0,\ b_1 + i_2 = 0,\ c_1 + i_3 = 0$ and $d_1 + i_4 = 0$, hence we get $i_1 = -a_1, i_2 = -b_1, i_3 = -c_1$ &$i_4 = -d_1$

$\therefore I = \begin{bmatrix} i_1 & i_2 \\ i_3 & i_4 \end{bmatrix} = \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix} \in G$, hence $I = \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix}$ be the inverse element of A in group G.

Also for any two matrices $A, B \in G$ we have $A + B = B + A$, So given set G is abelian group under matrix addition. ■

Exercises

1. Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| ad - bc \neq 0 \text{ and } a, b, c, d \in \mathbb{R} \right\}$ show that G is not an abelian group under the matrix multiplication.
2. Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| ad - bc = 1 \text{ and } a, b, c, d \in \mathbb{R} \right\}$ show that G is not an abelian group under the matrix multiplication.
3. Show that the set of all positive rational number $\mathbb{Q}^+$ form a group under the composition operation define by $a * b = \frac{ab}{5}$
4. Consider the set $\mathbb{R} - 1$ the operation $*$ is define as $a*b = a+b-ab,\ \ \forall a, b \in \mathbb{R} - 1$. Show that the set $\langle \mathbb{R} - 1, * \rangle$ is an abelian group.

4.2.2 Congruence

Let m be a positive integer. Then two integers a, b are said to be congruent modulo m, in symbols

$$a \equiv b (mod\ m),$$

if m divides $a - b$. Thus congruence modulo m is a relation on $\mathbb{Z}$ and an easy check reveals that it is an equivalence relation. Hence the set $\mathbb{Z}$ splits up into equivalence classes, which in this context are called congruence classes modulo m. The unique congruence class to which an integer a belongs is written

$$[a] \text{ or } [a]_m = \{\ a + mq |\ q \in \mathbb{Z}\ \}$$

By the Division Algorithm any integer a can be written in the form $a = mq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < m$. Thus $a \equiv r(mod\ m)$ and $[a] = [r]$. Therefore $[0], [1], \cdots, [m-1]$ are all the congruence classes modulo m.

4.2.3 Addition Modulo (m)

Let a and b be any two integers and m is a fixed positive integer. The addition modulo m of a and b written as $a +_m b$ defined by

$$a +_m b = r, \ \ 0 \leq r < m,$$

where r is the least non-negative remainder when the ordinary sum $a + b$ is divided by m.
$e.g \Longrightarrow 15 +_3 8 = 3, \quad 11 +_4 6 = 1, \ \ 9 +_3 8 = 2, \ \ -20 +_5 6 = 1$

4.2.4 Multiplication Modulo m

Let a and b be any two integers and m is a fixed positive integer. The multiplication modulo m of a and b written as $a \times_m b$ defined by

$$a \times_m b = r, \ \ 0 \leq r < m,$$

where r is the least non-negative remainder when the ordinary product $a \cdot b$ is divided by m.
$e.g \Longrightarrow 7 \times_3 5 = 2$, as $7 \times 5 = 3(11) + 2 = 2, \qquad 15 \times_8 7 = 1$ as $15 \times 7 = 105 = 8(13) + 1$.

Remark The set $\mathbb{Z}_m$ contain elements are $\mathbb{Z}_m = \{0, 1, 2, 3, 4, \cdots, m-1\}$

4.2.7 Example. Prove that the set $G = \{0, 1, 2, 3, 4\}$ is an abelian group under addition modulo 5.

Solution: Here given set is $G = \{0, 1, 2, 3, 4\}$ & operation is addition modulo 5 and we want to prove that G is abelian group under the given operation addition modulo, for that we make composition table to check the properties of group as follow.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(I) Closer

From the composition table closer operations are hold: that is, $a +_5 b \in G$, for all $a, b \in G$

(II) Associativity

From the composition table associative operations are hold: that is, $(a +_5 b) +_5 c = a +_5 (b +_5 c)$ for all $a, b, c \in G$.

(III) Identity

From the composition table the identity element of group G is 0, this identity element hold the operation : $a +_5 0 = 0 +_5 a = a$, for all $a \in G$.

(IV) Inverses

From the composition table the inverse of each elements are as follow

- Inverse of 0 is 0
- Inverse of 1 is 4
- Inverse of 2 is 3
- Inverse of 3 is 2
- Inverse of 4 is 1

Also for any two elements $a, b \in G$ we have $a +_5 b = b +_5 a$, So given set G is abelian group under addition modulo m.

■

4.2.8 Example. Prove that the set $G = \{1, 2, 3, 4\}$ is an abelian group under multiplication modulo 5.

Solution: Here given set is $G = \{1, 2, 3, 4\}$ & operation is multiplication modulo 5 and we want to prove that G is abelian group under the given operation multiplication modulo 5, for that we make composition table to check the properties of group as follow.

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(I) Closer

From the composition table closer operations are hold: that is, $a \times_5 b \in G$, for all $a, b \in G$

(II) Associativity

From the composition table associative operations are hold: that is, $(a \times_5 b) \times_5 c = a \times_5 (b \times_5 c)$ for all $a, b, c \in G$.

(III) Identity

From the composition table the identity element of group G is 1, this identity element hold the operation : $a \times_5 1 = 1 \times_5 a = a$, for all $a \in G$.

(IV) Inverses

From the composition table the inverse of each elements are as follow

- Inverse of 1 is 1
- Inverse of 2 is 3
- Inverse of 3 is 2

- Inverse of 4 is 1

Also for any two elements $a, b \in G$ we have $a \times_5 b = b \times_5 a$, So given set G is abelian group under addition modulo m. ■

Exercises

1. Prove that the set $G = \{0, 1, 2, 3, 4, 5\}$ is an abelian group under addition modulo 6.
2. Show that $\langle\ \mathbb{Z}_5, \times_5\ \rangle$ is not a group.
3. Show that $\langle\ \mathbb{Z}_5 - 0, \times_5\ \rangle$ is an abelian group.

4.2.5 Permutations Group

we introduced the concept of a permutation (or arrangement) of a set of objects. We now return to the subject, but now the focus is different, instead of thinking of a permutation as an arrangement of objects (which it is of course), we think of a permutation as a one-to-one function (bijection) from a set onto itself.
A permutation of a set A is a function from A to A that is both one-to-one and onto. A permutation group of a set A is a set of permutations of A that forms a group under function composition.

For example, a permutation of elements of the set $A = 1, 2, 3, \cdots, n$ is thought of a one-to-one mapping of this set onto itself, which we represent by $f : A \to A$ and define by

$$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$$

Also it is known as f is permutation of degree n.

Remark:

(i) Equality of two permutation
Two permutation f_1 and f_2 of degree n are said to be equal if $f_1(a) = f_2(a),\ \ \forall 1 \leq a \leq n$.

(ii) If P_n be the set of all permutation of degree n, then the set P_n will have $n!$ distinct elements

(iii) The set P_n is called the symmetric set of permutation of degree n.

(iv) The permutation group is also known as symmetric group and it is denoted by S_n.

Remark:

(i) If set $A = \{1, 2\}$ then the set $P_2 = S_2$ of all permutation of degree 3 have 2! distinct element which are $S_2 = \left\{ p_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \; p_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$

(i) If set $A = \{1, 2, 3\}$ then the set $P_3 = S_3$ of all permutation of degree 3 have 2! distinct element which are

$$S_3 = \left\{ p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \; p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \; p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \right.$$
$$\left. p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \; p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \; p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Identity Permutation

If I is a permutation of degree n such that $I(a) = a; \; \forall a \in A$, then I is called the identity permutation of degree n. *e.g.* $\Rightarrow p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ is identity permutation.

Product or Composition of two permutation

Composition of permutations expressed in array notation is carried out from left to right by going from top to bottom, then top to bottom. For example, let

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

and

$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix};$$

then

$$\sigma\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ & \downarrow & & & \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}.$$

4.2.9 Example. Let $A = \{1, 2\}$ and S_2 be the set of permutation on A then show that S_2 be a commutative group.

Solution: Here given set $S_2 = \{p_1, p_2\}$ where $p_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \; p_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ and we want to show that S_2 is commutative group, for that we check the properties of group, so we prepare composition table as follow.

$\cdot$	p_1	p_2
p_1	p_1	p_2
p_2	p_2	p_2

where;
$$p_1 \cdot p_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = p_1$$
$$p_1 \cdot p_2 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = p_2$$
$$p_2 \cdot p_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = p_2$$
$$p_2 \cdot p_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = p_1$$

Now we check the properties of group:

(I) Closer

From the composition table closer operations are hold: that is, $p_i \cdot p_j \in S_2$, for all $p_i, p_j \in S_2,\ 1 \leq i, j \leq 2$

(II) Associativity

From the composition table associative operations are hold: that is, $(p_i \cdot p_j) \cdot p_k = p_i \cdot (p_j \cdot p_k)$ for all $p_i, p_j, p_k \in S_2,\ 1 \leq i, j, k \leq 2$.

(III) Identity

From the composition table the identity element of group S_2 is p_1, this identity element hold the operation : $p_i \cdot p_1 = p_1 \cdot p_j = p_j$, for all $p_j \in S_2,\ 1 \leq j \leq 2$.

(IV) Inverses

From the composition table the inverse of each elements are as follow

- Inverse of p_1 is p_1
- Inverse of p_2 is p_2

Also from composition table, for any two elements $p_i, p_j \in S_2$ we have $p_i \cdot p_j = p_j \cdot p_i;\ \ 1 \leq i, j \leq 2$. Hence given set $S_2 = \{p_1, p_2\}$ is commutative group under the composition. ■

4.2.10 Example. Let $A = \{1, 2, 3\}$ and S_3 be the set of permutation on A then show that S_3 be a non commutative group (non abelian group).

Solution: Here given set $S_2 = \{p_1,\ p_2,\ p_3,\ p_4,\ p_5,\ p_6\}$, where $p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ and we want to show that S_2 is commutative group, for that we check the properties of group, so we prepare composition table as follow.

$\cdot$	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_6	p_5	p_4	p_3
p_3	p_3	p_5	p_1	p_6	p_2	p_4
p_4	p_4	p_6	p_5	p_1	p_3	p_2
p_5	p_5	p_3	p_4	p_2	p_6	p_1
p_6	p_6	p_4	p_2	p_3	p_1	p_5

Now we check the properties of group:

(I) Closer

From the composition table closer operations are hold: that is, $p_i \cdot p_j \in S_2$, for all $p_i, p_j \in S_3,\ 1 \leq i, j \leq 3$

(II) Associativity

From the composition table associative operations are hold: that is,
$(p_i \cdot p_j) \cdot p_k = p_i \cdot (p_j \cdot p_k)$ for all $p_i, p_j, p_k \in S_3,\ 1 \leq i, j, k \leq 3$.

(III) Identity

From the composition table the identity element of group S_3 is p_1, this identity element hold the operation : $p_i \cdot p_1 = p_1 \cdot p_j = p_j$, for all $p_j \in S_3,\ 1 \leq j \leq 3$.

(IV) Inverses

From the composition table the inverse of each elements are as follow

- Inverse of p_1 is p_1
- Inverse of p_2 is p_2
- Inverse of p_3 is p_3
- Inverse of p_4 is p_4
- Inverse of p_5 is p_6
- Inverse of p_6 is p_5

Also from composition table, for any two elements $p_i, p_j \in S_3$ we have $p_3 \cdot p_4 = p_6$ and $p_4 \cdot p_3 = p_5$. Hence $p_3 \cdot p_4 \neq p_4 \cdot p_3$, so given set $S_3 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ is non commutative (non abelian)group under the composition. ■

$*$	0	1
0	0	0
1	0	1

Table:1

$\oplus$	0	1
0	0	1
1	1	1

Table:2

Element	0	1
Complement element	1	0

Table:3

From the above tables we check the properties of boolean algebra as follow.

(I) Lattice Property:

Now from the table (1) and (2) we can say that $\langle B, *, \oplus \rangle$ is a lattice.

(II) Bounded Property:

here $glb\ B = 0 =$ The $0 - element$ of B. and $lub\ B = 1 =$ The $1 - element$ of B

$\therefore B$ is bounded lattice.

$\therefore \langle B,\ *,\ \oplus,\ 0,\ 1, \rangle$ is a bounded lattice.

(III) Complemented Property:

From the table (3), we have every element of B has a unique complement element in B.Here 0 and 1 are complement of each other.

$\therefore \langle B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is bounded complemented lattice.

(IV) Distributive Property:

Here $\langle B, *, \oplus \rangle$ is a lattice with only two element

$\therefore \langle B, *, \oplus \rangle$ is distributive lattice.

Hence from property (I) to (IV). $\langle B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is a Boolean Algebra.

5.1.2 Example. Show that $\langle S_{30},\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is boolean algebra.

Solution:

Here given set is $S_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$. For boolean algebra first we make table of $glb(*)$ and $lub(\oplus)$ as follow.

$* = gcd$	1	2	3	5	6	10	15	30
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
3	1	1	3	1	3	1	3	3
5	1	1	1	5	1	5	5	5
6	1	2	3	1	6	2	3	6
10	1	2	1	5	2	10	5	10
15	1	1	3	5	3	5	15	15
30	1	2	3	5	6	10	15	30

Table:1

$\oplus = lcm$	1	2	3	5	6	10	15	30
1	1	2	3	5	6	10	15	30
2	2	2	6	10	6	10	30	30
3	3	6	3	15	6	30	15	30
5	5	10	15	5	30	10	15	30
6	6	6	6	30	6	30	30	30
10	10	10	30	10	30	10	30	30
15	15	30	15	15	30	30	15	30
30	30	30	30	30	30	30	30	30

Table:2

Element	1	2	3	5	6	10	15	30
Complement element	30	15	10	6	5	3	2	1

Table:3

From the above tables we check the properties of boolean algebra as follow.
(I) Lattice Property:
Now from the table (1) and (2) we can say that $\langle S_{30}, *, \oplus \rangle$ is a lattice.

(II) Bounded Property:
here $glb\ S_{30} = 1 =$ The $0 - element$ of S_{30}. and $lub\ S_{30} = 30 =$ The $1 - element$ of B
$\therefore S_{30}$ is bounded lattice.
$\therefore \langle S_{30},\ *,\ \oplus,\ 0,\ 1, \rangle$ is a bounded lattice.

(III) Complemented Property:
From the table (3), we have every element of S_{30} has a unique complement element in S_{30}.
$\therefore \langle S_{30},\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is bounded complemented lattice.

(IV) Distributive Property:
Here from the table (1) and (2) element of S_{30} is distributive.
$\therefore \langle S_{30}, *, \oplus \rangle$ is distributive lattice.

Hence from property (I) to (IV). $\langle S_{30},\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is a Boolean Algebra.

5.1.3 Example. If $\langle B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is Boolean Algebra then prove that $\langle B \times B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is Boolean Algebra. where $B = \{0, 1\}$ and $\forall\ (a, b), (c, d) \in B \times B$, with $(a, b) * (c, d) = (a * c, b * d)$ & $(a, b) \oplus (c, d) = (a \oplus c, b \oplus d)$
Solution:
Here given set is $\langle B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is Boolean algebra with $B = \{0, 1\}$. Now we want to prove that $\langle B \times B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is boolean algebra. where $B \times B = \{(0,0), (0,1), (1,0), (1,1)\}$ for that we make table of $glb(*)$ and $lub(\oplus)$ as follow.

$*$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,1)$
$(1,0)$	$(0,0)$	$(0,0)$	$(1,0)$	$(1,0)$
$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$

Table:1

$\oplus$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,1)$	$(1,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,0)$	$(1,1)$
$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$

Table:2

Element	(0,0)	(0,1)	(1,0)	(1,1)
Complement element	(1,1)	(1,0)	(0,1)	(0,0)

Table:3

From the above tables we check the properties of boolean algebra as follow.
(I) Lattice Property:
Now from the table (1) and (2) we can say that $\langle B \times B, *, \oplus \rangle$ is a lattice.

(II) Bounded Property:
here $glb\ (B \times B) = (0, 0) =$ The $0 - element$ of $(B \times B)$. and $lub\ (B \times B) = (1, 1) =$ The $1 - element$ of B
$\therefore (B \times B)$ is bounded lattice.

$\therefore \langle B \times B,\ *,\ \oplus,\ 0,\ 1, \rangle$ is a bounded lattice.

(III) Complemented Property:
From the table (3), we have every element of $B \times B$ has a unique complement element in $B \times B$.
$\therefore \langle B \times B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is bounded complemented lattice.

(IV) Distributive Property:
Here from the table (1) and (2) element of $B \times B$ is distributive.
$\therefore \langle B \times B, *, \oplus \rangle$ is distributive lattice.

Hence from property (I) to (IV). $\langle B \times B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is a Boolean Algebra.

5.2 D'Morgan's Low

If $\langle B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is boolean algebra then

(i) $(a * b)' = a' \oplus b'$ (ii) $(a \oplus b)' = a' * b'$

Proof.
(I) $(a * b)' = a' \oplus b'$
let $a, b \in B$ to prove $(a * b)' = a' \oplus b'$ for that we prove that $a' \oplus b'$ is complement of $(a * b)$. For that

$$\begin{aligned}(a * b) * (a' \oplus b') &= [\ (a * b) * a'\ ] \oplus [\ (a * b) * b'\ ] \ (\text{ by distributive law})\\ &= [\ a' * (a * b)\ ] \oplus [\ (a * b) * b'\ ] \ (\text{ by commutative law})\\ &= [\ (a' * a) * b\ ] \oplus [\ a * (b * b')\ ] \ (\text{ by associative law})\\ &= (0 * b) \oplus (a * 0) \ (\ a' \text{and } b' \text{ are complement of } a \text{ and } b \text{ respectively})\\ &= 0 \oplus 0\\ &= 0.\end{aligned}$$

$$\boxed{(a * b) * (a' \oplus b') = 0} \ ---------- (1)$$

Now we shall prove that $(a * b) \oplus (a' \oplus b') = 1$

$$\begin{aligned}(a * b) \oplus (a' \oplus b') &= [\ (a * b) \oplus a'\ ] \oplus [\ (a * b) \oplus b'\ ] \ (\text{ by distributive law})\\ &= [\ (a \oplus a') * (b \oplus a')\ ] \oplus [\ (a \oplus b') * (b \oplus b')\ ] \ (\text{ by distributive law})\\ &= [\ 1 * (b \oplus a')\ ] \oplus [\ (a \oplus b') * 1\ ]\\ &= (b \oplus a') \oplus (a \oplus b')\\ &= [\ b \oplus (a' \oplus (a \oplus b'))\ ] \ (\text{ by associative law})\\ &= [\ b \oplus ((a' \oplus a) \oplus b')\ ] \ (\text{ by associative law})\\ &= [\ b \oplus (1 \oplus b')\ ]\\ &= b \oplus b'\\ &= 1\end{aligned}$$

$\boxed{\therefore a \leq b \Longrightarrow a * b' = 0}$ $-------(1)$

Now we take $a * b' = 0 \Longrightarrow a' \oplus (a * b') = a' \oplus 0$
$\Longrightarrow (a' \oplus a) * (a' \oplus b') = a'$ (by distributive property)
$\Longrightarrow 1 * (a' \oplus b') = a'$
$\Longrightarrow a' \oplus b' = a'$
$\Longrightarrow b' \leq a'$

$\boxed{\therefore a * b' \Longrightarrow b' \leq a'}$ $-------(2)$

Now take $b' \leq a' \Longrightarrow (a' \oplus b') = a'$
$\Longrightarrow (a' \oplus b') \oplus b = a' \oplus b$
$\Longrightarrow a' \oplus (b' \oplus b) = a' \oplus b$ (by associative law)
$\Longrightarrow a' \oplus 1 = a' \oplus b$
$\Longrightarrow 1 = a' \oplus b$

$\boxed{\therefore b' * a' \Longrightarrow a' \oplus b = 1}$ $-------(3)$

Now take $a' \oplus b = 1 \Longrightarrow a * (a' \oplus b) = a * 1$
$\Longrightarrow (a' * a') \oplus (a * b) = a$ (by distributive)
$\Longrightarrow 0 \oplus (a * b) = a$
$\Longrightarrow a * b = a$

$\boxed{\therefore a' \oplus b \Longrightarrow 1 = a \leq b}$ $-------(4)$

From the eq^n (1),(2),(3) and (4). we proved our required result
$a \leq b \implies a * b' = 0 \Longrightarrow b' \leq a' \implies a' \oplus b = 1 \Longrightarrow a \leq b.$ □

5.3 Join Irreducible Element

If $\langle B, *, \oplus \rangle$ is lattice and $a \in B$ is said to be Join-irreducible if it can not be express as a Join (lub) of two distinct element of B.

Remark .

(i) There does not exist $a_1,\ a_2 \in B$ such that $a = a_1 \oplus a_2$, where $a_1 \neq a_2$.

(ii) If there exist such $a_1,\ a_2 \in B,\ a_1 \neq a_2$ such that $a = a_1 \oplus a_2$ then $a = a_1$ or $a = a_2$.

5.3.1 Atoms

Let $\langle B, *, \oplus \rangle$ be a lattice and $a \in B$ then a is said to be Atom if it satisfy the following property

(i) a is join-irreducible

(ii) a is cover of 0.

$\Longrightarrow$ Here 0 means 0-element of B that is *glb* of B.

Remark .

(i) For boolean algebra $\langle B, *, \oplus, 0, 1, ' \rangle$ $a \in B$ is an Atom if $a \neq 0 -$ element $=$ *glb* of B

(ii) a cover 0-element.

(iii)

5.3.2 Meet Irreducible

Let $\langle L, *, \oplus \rangle$ be a lattice and $a \in L$ is said to be meet irreducible if it can not be express as meet of two elements of L.
i.e There does not exist $a_1, a_2 \in B$ such that $a = a_1 * a_2$

5.3.3 Anti-Atom

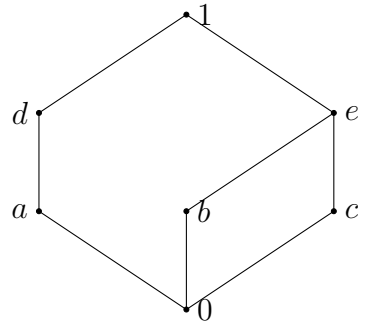
Let $\langle L, *, \oplus \rangle$ be a lattice and $a \in L$ then is said to anti-atoms if it satisfy the following property

(i) a is meet-irreducible

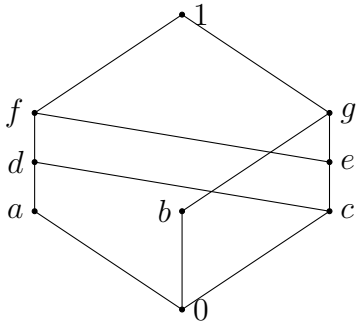
(ii) a is cover of 1.

$\Longrightarrow$ Here 1 means 1-element of B that is *lub* of B.

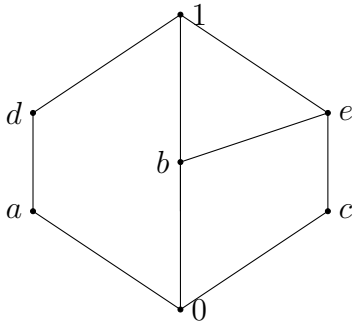
5.3.1 Example. Find the Join-irreducible elements,Meet-irreducible elements,Atom and Anti-atoms of the lattice shown in the following figure.



(A)



(B)

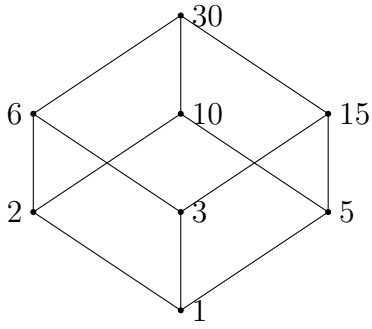


(C)

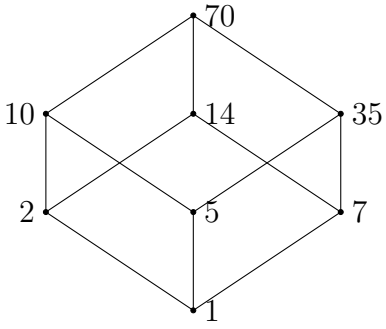
Solution:

	For A	For B	For C
Join-Irreducible element	a, b, c, d	a, b, c, e	a, b, c, d
Atoms	a, b, c	a, b, c	a, b, c
Meet-Irreducible element	a, b, c, d, e	a, b, d, f, g	a, c, d, e
Anti-atoms	d, e	f, g	d, e

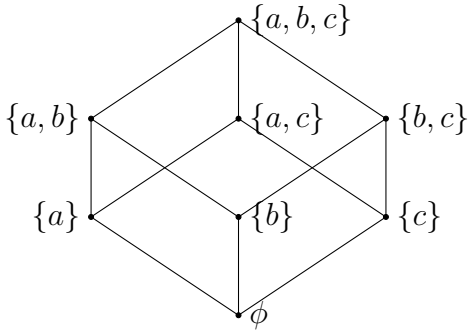
5.3.2 Example. Find the Join-irreducible elements, Meet-irreducible elements, Atom and Anti-atoms for the lattice $\langle S_{30}, D\rangle$, $\langle S_{70}, D\rangle$,and $\langle P(X), \subset \rangle$ where $X = \{a, b, c\}$



$\langle S_{30}, D\rangle$



$\langle S_{70}, D\rangle$



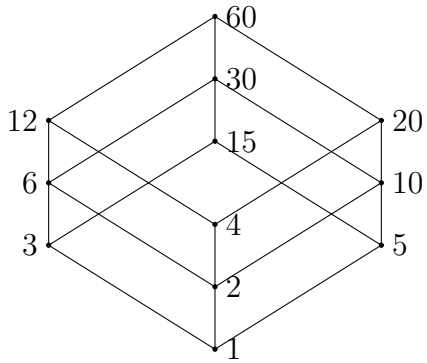
$\langle P(X), \subset \rangle$

Solution:

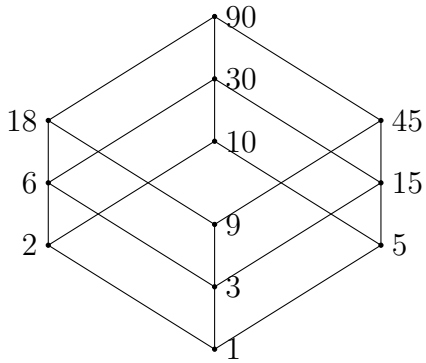
	$\langle S_{30}, D\rangle$	$\langle S_{70}, D\rangle$	$\langle P(X), \subset \rangle$
Join-Irreducible element	2, 3, 5	2, 5, 7	{a}, {b}, {c}
Atoms	2, 3, 5	2, 5, 7	{a}, {b}, {c}
Meet-Irreducible element	6, 10, 15	10, 14, 35	{a,b}, {a,c}, {b,c}
Anti-atoms	6, 10, 15	10, 14, 35	{a,b}, {a,c}, {b,c}

5.3.3 Example. Find the Join-irreducible elements, Meet-irreducible elements, Atom and Anti-atoms for the lattice $\langle S_{60}, D\rangle$, $\langle S_{90}, D\rangle$,and $\langle S_{150}, D\rangle$

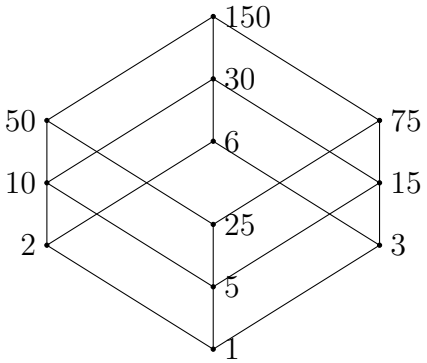
Solution:



$\langle S_{60}, D\rangle$



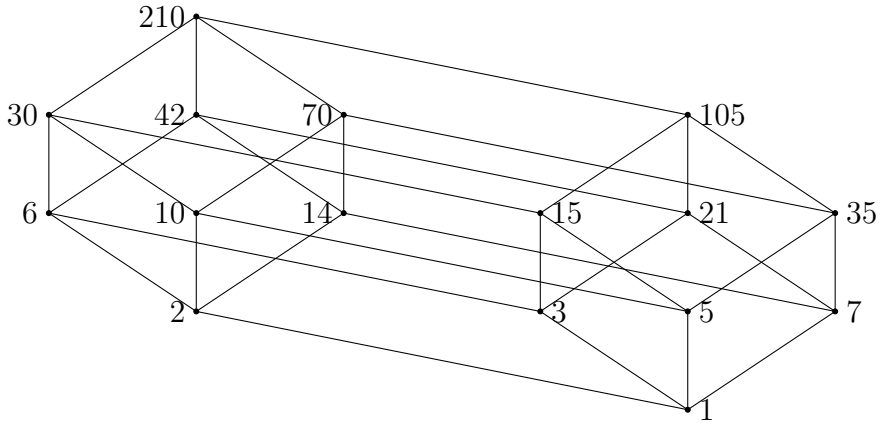
$\langle S_{90}, D\rangle$



$\langle S_{150}, D\rangle$

	$\langle S_{60}, D\rangle$	$\langle S_{90}, D\rangle$	$\langle S_{150}, D\rangle$
Join-Irreducible element	2, 3, 4, 5	2, 3, 5, 9	2, 3, 5, 25
Atoms	2, 3, 5	2, 3, 5	2, 3, 5
Meet-Irreducible element	12, 15, 20, 30	10, 18, 30, 45	6, 30, 50, 75
Anti-atoms	12, 30, 20	18, 30, 45	30, 50, 75

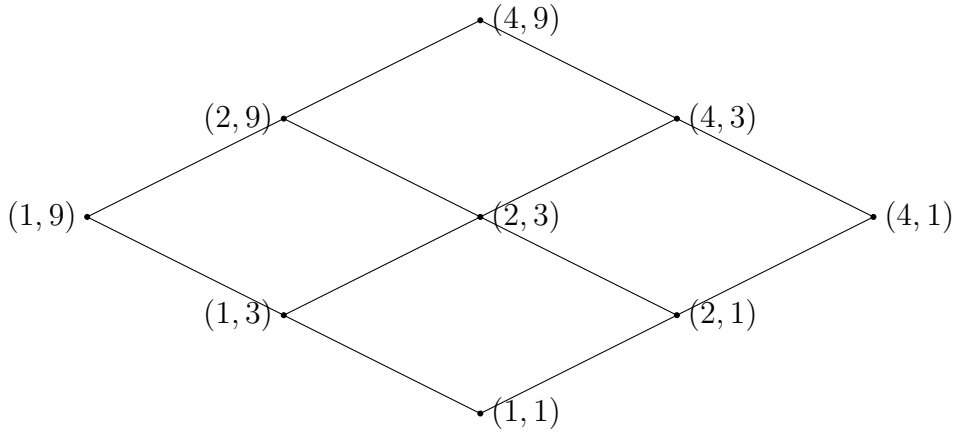
5.3.4 Example. Find the Join-irreducible elements, Meet-irreducible elements, Atom and Anti-atoms for the lattice $\langle S_{210}, D\rangle$.
Solution:



$\langle S_{210}, D\rangle$

	$\langle S_{210}, D\rangle$
Join-Irreducible element	2, 3, 5, 7
Atoms	2, 3, 5, 7
Meet-Irreducible element	30, 42, 70, 105
Anti-atoms	30, 42, 70, 105

5.3.5 Example. Find the Join-irreducible elements, Meet-irreducible elements, Atom and Anti-atoms for the lattice $\langle S_4 \times S_9, D\rangle$.
Solution:



	$\langle S_4 \times S_9, D \rangle$
Join-Irreducible element	(1,3), (1,9), (2,1), (4,1)
Atoms	(1,3), (2,1)
Meet-Irreducible element	(2,9), (4,3), (4,1), (1,9)
Anti-atoms	(2,9), (4,3)

Theorem 5.3.6. *Let* $\langle B, *, \oplus, 0, 1, ' \rangle$ *be Boolean algebra such that* a *is atom with* $a \neq 0$ *if and only if* $a * x = 0$ *or* $a * x = a \; \forall x \in B$.

Theorem 5.3.7. *If* a *and* b *are two distinct atoms of a Boolean algebra then* $a * b = 0$.

Theorem 5.3.8. *If* $\langle B, *, \oplus, 0, 1, ' \rangle$ *is finite Boolean algebra and* x *is a not zero element of* B *then there is an atom* a *of* B *such that* $a \leq x$.

Theorem 5.3.9. *If* $\langle B, *, \oplus, 0, 1, ' \rangle$ *be a Boolean algebra* $a \in B$ *is an anti-atom if and only if* $a \oplus x = 1$ *or* $a \oplus x = a \; \forall x \in B$.

Theorem 5.3.10. *If* a *and* b *are two distinct anti-atoms of a Boolean algebra then* $a \oplus b = 1$.

Theorem 5.3.11. *If* $\langle B, *, \oplus, 0, 1, ' \rangle$ *is finite Boolean algebra and* x *is a not one element of* B *then there is an anti-atom* a *of* B *such that* $x \leq a$.

5.3.4 Set Of Atoms [A(x)]

Let $\langle B, *, \oplus, 0, 1, ' \rangle$ be a Boolean algebra and $x \in B$ then the set of atoms $A(x)$ is define by set of all atoms a such that $a \leq x$.
i.e $A(X) = \{a \in B / a \text{ is an atom and } a \leq x\}$

5.3.12 Example. Consider the Boolean algebra $\langle S_{30}, D \rangle$ then find the following.

(i) $A(3)$ (ii) $A(2)$ (iii) $A(6)$ (iv) $A(10)$ (v) $A(15)$ (vi) $A(30)$

Solution:

Here given Boolean algebra $\langle S_{30}, D \rangle$, where $S_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ whose atoms are $\{2, 3, 5\}$

(i) $A(2) = \{a \in S_{30} / a \text{ is atom and } aD2\} = \{2\}$

(ii) $A(3) = \{a \in S_{30} / a \text{ is atom and } aD3\} = \{3\}$

(iii) $A(6) = \{a \in S_{30} / a \text{ is atom and } aD6\} = \{2, 3\}$

(iv) $A(10) = \{a \in S_{30} / a \text{ is atom and } aD10\} = \{2, 5\}$

(v) $A(15) = \{a \in S_{30} / a \text{ is atom and } aD15\} = \{3, 5\}$

(vi) $A(30) = \{a \in S_{30} / a \text{ is atom and } aD30\} = \{2, 3, 5\}$

5.3.5 Properties of $A(X)$

Let $\langle B, *, \oplus, 0, 1, ' \rangle$ be a Boolean algebra then following properties are holds

(i) $A(0) = \phi$

(ii) $A(1) =$ set of all atoms of B

(iii) $x_1 \leq x_2 \Longrightarrow A(x_1) \subset A(x_2)$

(iv) $A(x_1 * x_2) = A(x_1) \cap A(x_2) \ \forall x_1, x_2 \in B$

(v) $A(x_1 \oplus x_2) = A(x_1) \cup A(x_2) \ \forall x_1, x_2 \in B$

(vi) $A(x') = A(1) - A(x) \ \forall x \in B$ where x' is complement of x.

(vii) $A(x) = A(y) \Longleftrightarrow x = y$.

Remark .

(i) If a is an atom then $A(a) = a$

(ii) Let S_{30} with the atom set $A = \{2, 3, 5\}$.Take $c = \{2, 3, 5\} \subset A$ let $x = 2 \oplus 3 \oplus 5$.

$$\begin{aligned} \text{Now} f(x) &= f(2 \oplus 3 \oplus 5) \\ &= A(2 \oplus 3 \oplus 5) \quad (\text{ if } f(x) = A(x) \text{ is function.}) \\ &= A(2) \cup A(3) \cup A(5) \\ &= \{2\} \cup \{3\} \cup \{5\} \\ &= \{2, 3, 5\} \\ &= c \end{aligned}$$

5.4 Sub Boolean algebra

Let $\langle B, *, \oplus, 0, 1, ' \rangle$ be a Boolean algebra and $S \subset B$. If S contain 0 and 1 elements and for every $x * y \in S$, $x \oplus y \in S$, $x' \in S$ for every $x, y \in S$ then $\langle S, *, \oplus, 0, 1, ' \rangle$ is called sub-boolean algebra of $\langle B, *, \oplus, 0, 1, ' \rangle$.

Remark .

(i) To prove $\langle S, *, \oplus, 0, 1, ' \rangle$ is a sub-boolean algebra of $\langle B, *, \oplus, 0, 1, ' \rangle$ then only prove that it is closed under $*$, $\oplus$, $'$ and $0 \in S$, $1 \in S$.

(ii) let $\langle S, *, \oplus, 0, 1, ' \rangle$ is sub-boolean algebra of $\langle B, *, \oplus, 0, 1, ' \rangle$ if and only if S is closed with respect to meet$(*)$ and complement $(')$.

(iii) let $\langle S, *, \oplus, 0, 1, ' \rangle$ is sub-boolean algebra of $\langle B, *, \oplus, 0, 1, ' \rangle$ if and only if S is closed with respect to join$(\oplus)$ and complement $(')$.

Theorem 5.4.1 (Stones's Representation).
Every finite Boolean algebra is isomorphic to the power set of all atoms of Boolean algebra.

Proof. Let $\langle B, *, \oplus, 0, 1, ' \rangle$ is finite boolean algebra and A is the set of all atoms of B. Obviously $\langle P(A), \cap, \cup, \phi, A, {}^C \rangle$ is also boolean algebra. Now we define mapping as follow
$f : \langle B, *, \oplus, 0, 1, ' \rangle \longrightarrow \langle P(A), \cap, \cup, \phi, A, {}^C \rangle$ by $f(x) = A(x) =$ set of atoms of B.
To prove define function is isomorphic for that we prove

(i) f is one-one

(ii) f is onto

(iii) f preserve the $*$, $\oplus$, $'$

(iv) f preserve both bound 0 and 1

(1) f is one-one

Suppose $f(x) = f(y), \ \forall x, y \in B$

$A(x) = A(y)$

$x = y$ (by property $A(x)$)

$\therefore f$ is one-one.

(2) f is onto

Suppose any set $c \in P(A)$ then $c \subset A$.

(i) If $c = \phi$ then $\phi = A(0) = f(0)$ then onto.

(ii) If $c \neq \phi$ then we take $c = \{x_1, x_2, \cdots, x_k\}$, where each x_i is an atom of B.

Now consider $x = x_1 \oplus x_2 \oplus \cdots \oplus x_k$

$$\begin{aligned}
\therefore \ f(x) &= A(x) \\
&= A(x_1 \oplus x_2 \oplus \cdots \oplus x_k) \\
&= A(x_1) \cup A(x_2) \cup \cdots \cup A(x_k) \quad (\text{ by } A(x \oplus y) = A(x) \cup A(y) \ ) \\
&= \{x_1\} \cup \{x_2\} \cup \cdots \cup \{x_k\} \quad (\text{ by if } x \text{ is atom then } A(x) = x \ ) \\
&= \{x_1, x_2, \cdots, x_k\} \\
&= c
\end{aligned}$$

$\therefore \ f$ is onto.

(3) f preserve the operations $*$, $\oplus$, $'$

(i) For Meet $(*)$

To prove f preserve the meet operation for that we prove $f(x * y) = f(x) \cap f(y)$

$$\begin{aligned}
\text{Let } f(x * y) &= A(x * y) \quad (\text{ by } f(x) = A(x) \ ) \\
&= A(x) \cap A(y) \quad (\text{ by } A(x * y) = A(x) \cap A(y) \ ) \\
&= f(x) \cap f(y) \quad (\text{ by } A(x) = f(x) \ )
\end{aligned}$$

$\therefore f$ follow the $*$ operation

(ii) For Join $(\oplus)$

To prove f preserve the join operation for that we prove $f(x \oplus y) = f(x) \cup f(y)$

$$\begin{aligned}
\text{Let } f(x \oplus y) &= A(x \oplus y) \quad (\text{ by } f(x) = A(x) \ ) \\
&= A(x) \cup A(y) \quad (\text{ by } A(x \oplus y) = A(x) \cup A(y) \ ) \\
&= f(x) \cup f(y) \quad (\text{ by } A(x) = f(x) \ )
\end{aligned}$$

$\therefore f$ follow the $\oplus$ operation

(iii) For complement ($'$)

To prove f preserve the complement operation for that we prove $f(x') = [f(x)]^C$

$$\begin{aligned} \text{Let } f(x') &= A(x') \quad (\text{ by } f(x) = A(x)\ ) \\ &= A - A(x) \quad (\text{ by } A(x') = A - A(x)\ ) \\ &= [A(x)]^C \\ &= [f(x)]^C \end{aligned}$$

$\therefore f$ follow the complementoperation

(4) f preserve the bound 0 and 1

$$\begin{aligned} \text{Let } f(0) &= A(0) \quad (\text{ by } f(x) = A(x)\ ) \\ &= \phi \\ &= 0 - \text{element of } P(A) \\ \text{and } f(1) &= A(1) \\ &= A \\ &= 1 - \text{element of } P(A) \end{aligned}$$

$\therefore$ $f$preserve the both bound 0 and 1.

Hence we proved result that every boolean algebra is isomorphic to power set of all atom of boolean algebra.
$\therefore \langle B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle \cong \langle P(A),\ \cap,\ \cup,\ \phi,\ A,\ ^C \rangle$

□

5.5 Boolean Function

Let $\langle B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ be a boolean algebra. A function $f : B^n \longrightarrow B$ which is associated with a boolean algebra expression (form) in n variable is called a boolean function.

5.5.1 Boolean Expression

A Boolean expression $\alpha(x_1, x_2, x_3, \cdots, x_n)$ in n variable is finite string of symbols formed in the following manner

(i) If $\alpha(x_1, x_2, x_3, \cdots, x_n) = 0$ then 0 is boolean expression.

(ii) If $\alpha(x_1, x_2, x_3, \cdots, x_n) = 1$ then 1 is boolean expression.

(iii) If $\alpha(x_1, x_2, x_3, \cdots, x_n)$ and $\beta(x_1, x_2, x_3, \cdots, x_n)$ are boolean expression then $\alpha(x_1, x_2, x_3, \cdots, x_n) * \beta(x_1, x_2, x_3, \cdots, x_n)$ is also boolean expression.

(iv) If $\alpha(x_1, x_2, x_3, \cdots, x_n)$ and $\beta(x_1, x_2, x_3, \cdots, x_n)$ are boolean expression then $\alpha(x_1, x_2, x_3, \cdots, x_n) \oplus \beta(x_1, x_2, x_3, \cdots, x_n)$ is also boolean expression.

(v) If $\alpha(x_1, x_2, x_3, \cdots, x_n)$ is boolean expression then $[\alpha(x_1, x_2, x_3, \cdots, x_n)]^C$ is also boolean expression.

(vi) $\alpha(x_1, x_2, x_3, \cdots, x_n) = x_i$ where $1 \leq x_i \leq n$ is also boolean expression.

e.g. $\Longrightarrow$ If $\langle B,\ *,\ \oplus,\ 0,\ 1,\ ' \rangle$ is a boolean algebra and x_1, x_2, x_3 are its variable then following all are boolean expression

(i) $\alpha(x_1, x_2, x_3, \cdots, x_n) = 0$

(ii) $\beta(x_1, x_2, x_3, \cdots, x_n) = 1$

(iii) $\gamma(x_1, x_2, x_3, \cdots, x_n) = x_1$

(iv) $\delta(x_1, x_2, x_3, \cdots, x_n) = x'_2$

(v) $\rho(x_1, x_2, x_3, \cdots, x_n) = x_1 * x_2$

(vi) $\psi(x_1, x_2, x_3, \cdots, x_n) = x'_1 * x_2$

(vii) $\mu(x_1, x_2, x_3, \cdots, x_n) = x_1 \oplus x_2$

(viii) $\omega(x_1, x_2, x_3, \cdots, x_n) = x_1 \oplus x'_3$

(ix) $\alpha(x_1, x_2, x_3, \cdots, x_n) = x_1 \oplus x'_3 * x_2$

(x) $\beta(x_1, x_2, x_3, \cdots, x_n) = x_1 \oplus x'_3 * x_2 \oplus x_4$

5.5.2 Equivalent Boolean Expression

Let $\alpha(x_1, x_2, x_3, \cdots, x_n)$ and $\beta(x_1, x_2, x_3, \cdots, x_n)$ be two boolean expression are said to be equivalent if one can be obtained from other by a finite number of application of the identities of a boolean algebra
we write $\alpha(x_1, x_2, x_3, \cdots, x_n) = \beta(x_1, x_2, x_3, \cdots, x_n)$

5.5.1 Example. Show that $x_1 * (x_2 * x_3)'$ and $(x_1 * x_2') \oplus (x_1 * x_3')$ are equivalent boolean expressions.
Solution:
Let $\alpha(x_1, x_2, x_3) = x_1 * (x_2 * x_3)'$ and $\beta(x_1, x_2, x_3) = (x_1 * x_2') \oplus (x_1 * x_3')$

$$\begin{aligned} \text{Now } \alpha(x_1, x_2, x_3) &= x_1 * (x_2 * x_3)' \\ &= x_1 * (x_2' \oplus x_3') \\ &= (x_1 * x_2') \oplus (x_1 * x_3') \\ &= \beta(x_1, x_2, x_3) \end{aligned}$$

$\therefore \alpha(x_1, x_2, x_3)$ and $\beta(x_1, x_2, x_3)$ are equivalent.

5.5.3 Minterm

A boolean expression in n variable $x_1, x_2, x_3, \cdots, x_n$ is called Minterm (complete product or fundamental product) if it of the form ${x_1}^{a_1} * {x_2}^{a_2} * {x_3}^{a_3} * \cdots * {x_n}^{a_n}$ where a_i are either 0 or 1 and define as ${x_i}^{a_i} = \begin{cases} x_i & ;\ \text{if } a_i = 1 \\ x_i' & ;\ \text{if } a_i = 0 \end{cases}$

Remark .

(i) If m_i and m_j are distinct minterms in variable $x_1, x_2, x_3, \cdots x_n$ then $m_i * m_j = 0$ means 0- element.

(ii) The sum (Join) of all minterms in variable $x_1, x_2, x_3, \cdots x_n$ is 1.

(iii) There are exactly 2^n minterm in n boolean variables.

(iv) There are exactly 2^{2^n} non-equivalent boolean expression in n boolean variables.

5.5.2 Example. Find the minterms of boolean algebra with two variables x_1 and x_2.
Solution:
Here x_1 and x_2 are two variable of boolean algebra. Now we find the all possible minterms of two variable. A minterm in two variable is ${x_1}^{a_1} * {x_2}^{a_2}$. Take (a_1, a_2) where $a_1, a_2 \in \{0, 1\}$ so possible pair of $(a_1, a_2) = \{0, 1\} \times \{0, 1\} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$. For possible minterm we make table as follow.

Symbol	Binary Representation	Decimal value	Minterm
(0,0)	00	0	$m_0 = {x_1}' * {x_2}'$
(0,1)	01	1	$m_1 = {x_1}' * x_2$
(1,0)	10	2	$m_2 = x_1 * {x_2}'$
(1,1)	11	3	$m_3 = x_1 * x_2$

$\therefore$ set of minterms is $\{m_0, m_1, m_2, m_3\}$

5.5.3 Example. Find the minterms of boolean algebra with three variables x_1, x_2 and x_3.
Solution:
Here x_1, x_2 and x_3 are three variable of boolean algebra. Now we find the all possible minterms of three variable. A minterm in three variable is ${x_1}^{a_1} * {x_2}^{a_2} * {x_3}^{a_3}$. Take (a_1, a_2, a_3) where $a_1, a_2 \& a_3 \in \{0, 1\}$ so possible pair of $(a_1, a_2, a_3) = \{0, 1\} \times \{0, 1\} = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$. For possible minterm we make table as follow.

Symbol	Binary Representation	Decimal value	Minterm
(0,0,0)	000	0	$m_0 = {x_1}' * {x_2}' * {x_3}'$
(0,0,1)	001	1	$m_1 = {x_1}' * {x_2}' * x_3$
(0,1,0)	010	2	$m_2 = {x_1}' * x_2 * {x_3}'$
(0,1,1)	011	3	$m_3 = {x_1}' * x_2 * x_3$
(1,0,0)	100	4	$m_4 = x_1 * {x_2}' * {x_3}'$
(1,0,1)	101	5	$m_5 = x_1 * {x_2}' * x_3$
(1,1,0)	110	6	$m_6 = x_1 * x_2 * {x_3}'$
(1,1,1)	111	7	$m_7 = x_1 * x_2 * x_3$

$\therefore$ set of minterms is $\{m_0, m_1, m_2, m_3, m_4, m_5, m_6, m_7\}$

Theorem 5.5.4. *Let* $\langle B, *, \oplus, 0, 1, ' \rangle$ *be a boolean algebra then*
(i) For n variable we have 2^n *minterms.*
(ii) Product of two distinct minterm in n variable is zero.

5.5.4 Sum Of Products Canonical Form

Every Boolean expression except 0 can be expressed into an equivalent form consisting of the sums of minterms. Such an equivalent form is called the sum of product (SOP) canonical form in three variable.

5.5.5 Example. Expressed the boolean expression $x_1 * x_2$ in an equivalent sum of products canonical form of three variable.
Solution:
Here we want to boolean expression $x_1 * x_2$ into sum of product for that

$$\begin{aligned}\text{Now } x_1 * x_2 &= (x_1 * x_2) * 1 \\ &= (x_1 * x_2) * (x_3 \oplus {x_3}') \\ &= (x_1 * x_2 * x_3) \oplus (x_1 * x_2 * {x_3}') \\ &= m_7 \oplus m_6 \\ &= \oplus 6, 7\end{aligned}$$

Another Method:

m_j	x_1	x_2	x_3	$x_1 * x_2$
m_0	0	0	0	0
m_1	0	0	1	0
m_2	0	1	0	0
m_3	0	1	1	0
m_4	1	0	0	0
m_5	1	0	1	0
m_6	1	1	0	1
m_7	1	1	1	1

From the table we write as follow

$$\begin{aligned}\text{Now } x_1 * x_2 &= m_7 \oplus m_6 \\ &= \oplus 6, 7 \\ &= (x_1 * x_2 * x_3) \oplus (x_1 * x_2 * {x_3}')\end{aligned}$$

5.5.6 Example. Expressed the boolean expression $x_1 \oplus x_2$ in an equivalent sum of products canonical form.
Solution:
Here we want to boolean expression $x_1 \oplus x_2$ into sum of product for that we make table as follow

m_j	x_1	x_2	x_3	$x_1 \oplus x_2$
m_0	0	0	0	0
m_1	0	0	1	0
m_2	0	1	0	1
m_3	0	1	1	1
m_4	1	0	0	1
m_5	1	0	1	1
m_6	1	1	0	1
m_7	1	1	1	1

From the table we write as follow

$$\begin{aligned}\text{Now } x_1 \oplus x_2 &= m_2 \oplus m_3 \oplus m_4 \oplus m_5 \oplus m_6 \oplus m_7 \\ &= \oplus 2, 3, 4, 5, 6, 7 \\ &= ({x_1}' * x_2 * {x_3}') \oplus ({x_1}' * x_2 * x_3) \oplus (x_1 * {x_2}' * {x_3}') \\ &\quad \oplus (x_1 * {x_2}' * x_3) \oplus (x_1 * x_2 * {x_3}') \oplus (x_1 * x_2 * x_3)\end{aligned}$$

5.5.7 Example. Expressed the boolean expression $(x_1 \oplus x_2)' * x_3$ in an equivalent sum of products canonical form.
Solution:
Here we want to boolean expression $(x_1 \oplus x_2)' * x_3$ into sum of product for that we make

table as follow

m_j	x_1	x_2	x_3	$x_1 \oplus x_2$	$(x_1 \oplus x_2)'$	$(x_1 \oplus x_2)' * x_3$
m_0	0	0	0	0	1	0
m_1	0	0	1	0	1	1
m_2	0	1	0	1	0	0
m_3	0	1	1	1	0	0
m_4	1	0	0	1	0	0
m_5	1	0	1	1	0	0
m_6	1	1	0	1	0	0
m_7	1	1	1	1	0	0

From the table we write as follow

Now $(x_1 \oplus x_2)' * x_3 = m_1$
$= \oplus 1$
$= {x_1}' * {x_2}' * x_3$

5.5.5 Maxterm

A boolean expression in n variable $x_1, x_2, x_3, \cdots, x_n$ is called Maxterm (complete sum or fundamental sum) if it of the form ${x_1}^{a_1} \oplus {x_2}^{a_2} \oplus {x_3}^{a_3} \oplus \cdots \oplus {x_n}^{a_n}$ where a_i are either 0 or 1 and define as ${x_i}^{a_i} = \begin{cases} {x_i}' & ; \text{ if } a_i = 1 \\ x_i & ; \text{ if } a_i = 0 \end{cases}$

5.5.8 Example. Find the maxterms of boolean algebra with two variables x_1 and x_2.
Solution:
Here x_1 and x_2 are two variable of boolean algebra. Now we find the all possible maxterms of two variable. A maxterm in two variable is ${x_1}^{a_1} \oplus {x_2}^{a_2}$. Take (a_1, a_2) where $a_1, a_2 \in \{0, 1\}$ so possible pair of $(a_1, a_2) = \{0, 1\} \times \{0, 1\} = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$. For possible maxterm we make table as follow.

Symbol	Binary Representation	Decimal value	Maxterm
(0,0)	00	0	$M_0 = x_1 \oplus x_2$
(0,1)	01	1	$M_1 = x_1 \oplus {x_2}'$
(1,0)	10	2	$M_2 = {x_1}' \oplus x_2$
(1,1)	11	3	$M_3 = {x_1}' \oplus {x_2}'$

$\therefore$ set of minterms is $\{M_0, M_1, M_2, M_3\}$

5.5.9 Example. Find the maxterms of boolean algebra with three variables x_1, x_2 and x_3.
Solution:
Here x_1, x_2 and x_3 are three variable of boolean algebra. Now we find the all possible maxterms of three variable. A maxterm in three variable is ${x_1}^{a_1} \oplus {x_2}^{a_2} \oplus {x_3}^{a_3}$. Take (a_1, a_2, a_3) where $a_1,\ a_2\ \&\ a_3 \in \{0, 1\}$ so possible pair of $(a_1, a_2, a_3) = \{0, 1\} \times \{0, 1\} = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$. For possible minterm we make table as follow.

Symbol	Binary Representation	Decimal value	Maxterm
(0,0,0)	000	0	$M_0 = x_1 \oplus x_2 \oplus x_3$
(0,0,1)	001	1	$M_1 = x_1 \oplus x_2 \oplus x_3{}'$
(0,1,0)	010	2	$M_2 = x_1 \oplus x_2{}' \oplus x_3$
(0,1,1)	011	3	$M_3 = x_1 \oplus x_2{}' \oplus x_3{}'$
(1,0,0)	100	4	$M_4 = x_1{}' \oplus x_2 \oplus x_3$
(1,0,1)	101	5	$M_5 = x_1{}' \oplus x_2 \oplus x_3{}'$
(1,1,0)	110	6	$M_6 = x_1{}' \oplus x_2{}' \oplus x_3$
(1,1,1)	111	7	$M_7 = x_1{}' \oplus x_2{}' \oplus x_3{}'$

$\therefore$ set of maxterms is $\{M_0, M_1, M_2, M_3, M_4, M_5, M_6, M_7\}$

5.5.6 Products Of Sum Of Canonical Form

Every Boolean expression except 1 can be expressed into an equivalent form consisting of the sums of maxterms. Such an equivalent form is called the product of sum (POS) canonical form in three variable.

5.5.10 Example. Expressed the boolean expression $x_1 * x_2$ in an equivalent product of sum canonical form.
Solution:
Here we want to boolean expression $x_1 * x_2$ into product of sum for that

M_j	x_1	x_2	x_3	$x_1 * x_2$
M_0	0	0	0	0
M_1	0	0	1	0
M_2	0	1	0	0
M_3	0	1	1	0
M_4	1	0	0	0
M_5	1	0	1	0
M_6	1	1	0	1
M_7	1	1	1	1

From the table we write as follow

$$\begin{aligned}\text{Now } x_1 * x_2 &= M_7 * M_6 \\ &= *\,6,7 \\ &= (\ x_1{}' \oplus x_2{}' \oplus x_3) * (\ x_1{}' \oplus x_2{}' \oplus x_3{}'\ )\end{aligned}$$

5.5.11 Example. Expressed the boolean expression $x_1 \oplus x_2$ in an equivalent products of sum canonical form.
Solution:
Here we want to boolean expression $x_1 \oplus x_2$ into product of sum for that we make table as follow

M_j	x_1	x_2	x_3	$x_1 \oplus x_2$
M_0	0	0	0	0
M_1	0	0	1	0
M_2	0	1	0	1
M_3	0	1	1	1
M_4	1	0	0	1
M_5	1	0	1	1
M_6	1	1	0	1
M_7	1	1	1	1

From the table we write as follow

$$\begin{aligned}\text{Now } x_1 \oplus x_2 &= M_2 * M_3 * M_4 * M_5 * M_6 * M_7 \\ &= *\,2,3,4,5,6,7 \\ &= (x_1 \oplus x_2' \oplus x_3) * (\ x_1 \oplus x_2' \oplus x_3{}'\ ) * (\ x_1' \oplus x_2 \oplus x_3{}'\ ) \\ &\quad *(\ x_1' \oplus x_2 \oplus x_3{}'\ ) * (\ x_1' \oplus x_2' \oplus x_3\ ) * (\ x_1' \oplus x_2' \oplus x_3{}'\end{aligned}$$